

Internet Security Appliance

# **Support Notes**

Version 4.02 Dec. 2006



INDEX	
Application Notes	12
Seamless Incorporation into your network	12
Using Transparent (Bridge Mode) Firewall	12
Internet Connection	17
DHCP server/client/relay + flexible port role configuration	19
Using NAT/Multi-NAT	23
Optimize network performance & availability	33
Using Dual WAN / Load Balancing and policy route	33
Using Dual WAN	33
WAN backup (Active/Passive mode)	35
Load Balancing (Active/Active Mode)	45
Using Policy Route	54
Using Bandwidth Management	55
Secure Connections across the Internet and Wireless LAN	69
Site-to-Site VPN (Intranet) Scenario	69
Configure ZyWALLs with Static WAN IP Address	69
Configure ZyWALL with Dynamic WAN IP Address	70
Configure ZyWALL behind NAT Router	72
Mapping multiple Network policy to same gateway policy	74
Using Certificate for Device Authentication	79
Using Self-signed Certificates	80
Online Enroll Certificates	83
Offline Enroll Certificates	92
Using Pre-Shared Key for Device Authentication	125
Using VPN routing between branches	126
Never lost your VPN connection (IPSec High Availability)	136
How to configure the VPN HA	137
Access control and security VPN connection (Security policy	
enforcement IPSec)	139
How to configure access control rule over VPN	140
How to configure Security policy (AV/IDP/AS) over VPN	144
How to configure Web filtering rule over VPN – Content I	Filter146
ZyWALL vs 3rd Party VPN Gateway	147
SonicWALL with ZyWALL VPN Tunneling	147
NetScreen with ZyWALL VPN Tunneling	156
Check Point with ZyWALL VPN Tunneling	170
FortiNet with ZyWALL VPN Tunneling	205

Remote Access VPN Scenario219
Using xAuth for User Authentication
ZyXEL VPN Client to ZyWALL Tunneling
Flexible Wireless Connection and Security231
Deploy the ZyWALL WLAN security policy232
Threat Management236
To protect computer networks against virus intrusions and attacks
from Internet237
To Control IM/P2P Applications Usage to Increase Employee
Productivity243
To filter non-work related and unproductive web surfing to mitigate
spyware and phishing threats248
To eliminate spam mails to block unwanted messages everyday258
Threat Reports
Centralized Management
Using Vantage CNM for Management268
FAQ
A. Product FAQ
A01. What is the ZyWALL Internet Access Sharing Router?273
A02. Will the ZyWALL work with my Internet connection?273
A03. What do I need to use the ZyWALL?273
A04. What is PPPoE?273
A05. Does the ZyWALL support PPPoE?274
A06. How do I know I am using PPPoE?274
A07. Why does my Internet Service Provider use PPPoE?274
A08. How can I configure the ZyWALL?274
A09. What can we do with ZyWALL?274
A10. Does ZyWALL support dynamic IP addressing?274
A11. What is the difference between the internal IP and the real IP
from my ISP?274
A12. How does e-mail work through the ZyWALL?
A13. Is it possible to access a server running behind NAT from the
outside Internet? If possible, how?275
A14. What DHCP capability does the ZyWALL support?275
A15. What are the capability of wireless feature of ZyWALL275
A16. What is the coverage range of Wireless in ZyWALL?275
A17. How do I used the reset button, more over what field of
parameter will be reset by reset button?

A18. What network interface does the new ZyWALL series support?276
A19. How does the ZyWALL support TFTP?276
A20. Can the ZyWALL support TFTP over WAN?
A21. How can I upload data to outside Internet over the one-way
cable?276
A22. My ZyWALL can not get an IP address from the ISP to connect
to the Internet, what can I do?276
A23. What is BOOTP/DHCP?
A24. What is DDNS?277
A25. When do I need DDNS service?278
A26. What DDNS servers does the ZyWALL support?278
A27. What is DDNS wildcard?278
A28. Does the ZyWALL support DDNS wildcard?278
A29. Can the ZyWALL NAT handle IPSec packets sent by the VPN
gateway behind ZyWALL?278
A30. How do I setup my ZyWALL for routing IPSec packets over
NAT?
A31. What is STP (Spanning Tree Protocol) /RSTP (Rapid STP)? 279
A32. What is the flow ZyWALL handles inbound and outgoing
traffic?
A33. What is "UTM"?
A34. What are the differences between ZyWALL UTM models and
previous ZyWALL models?279
A35. What are the key new features of ZyWALL UTM?280
B. Firmware Upgrade FAQ
B01. Which ZyWALL models are eligible to be upgraded to run
ZyNOS v4.01?280
B02. Why it's conditional to upgrade to ZyNOS v4.01 for ZyWALL
70?
B03. What is ZyNOS v3.65 for ZyWALL 70?281
B04. What happens if I wrongfully upgrade firmware of a ZyWALL
70 with only 32MB of RAM to ZyNOS v4.01 directly?281
B05. What happened if I upgrade a ZyWALL 70 running ZyNOS
v3.62/3.63/3.64 to v4.01 directly?282
B06. I am a 32MB ZyWALL 70 owner, how can I upgrade to ZyNOS
v4.01 having AV+IDP and AS features?282
B07. If I were a 32MB ZyWALL 70 owner and a Content Filtering
service subscriber, will my current license status be retained after

joining your ZyWALL 70 trade-in promotion?282
B08. What's the firmware upgrade path for my current ZyWALL 5
and ZyWALL 35?
B09. After a successful firmware upgrade to ZyNOS v4.01, what's the
default setting of AV+IDP, AS and CF?282
B10. What happens to my original system configurations after a
successful firmware upgrade to ZyNOS v4.01?
B11. What's the downgrade procedure of ZyWALL 70 running
ZyNOS v4.01?
B12. Can I downgrade a ZyWALL 5 or ZyWALL 35 running ZyNOS
v4.01 back to ZyNOS v3.64 (or below)?283
C. Turbo Card FAQ
C01. Can I insert the ZyWALL Turbo Card & wireless card
simultaneously into ZyWALL 5, ZyWALL 35 or ZyWALL 70?283
C02. Except ZyWALL Turbo Card is a must when use AV+IDP service,
what exactly I can get benefit from it?
C03. Do I must have a ZyWALL Turbo Card inserted if I upgraded to
ZyNOS v4.01? If not, when must I insert a ZyWALL Turbo Card into
my ZyWALL device?
C04. Can I insert the ZyWALL Turbo Card & 3G wireless card
C04. Can I insert the ZyWALL Turbo Card & 3G wireless card
C04. Can I insert the ZyWALL Turbo Card & 3G wireless card simultaneously into ZyWALL 5, ZyWALL 35 or ZyWALL 70?
C04. Can I insert the ZyWALL Turbo Card & 3G wireless card simultaneously into ZyWALL 5, ZyWALL 35 or ZyWALL 70?
C04. Can I insert the ZyWALL Turbo Card & 3G wireless card simultaneously into ZyWALL 5, ZyWALL 35 or ZyWALL 70?
C04. Can I insert the ZyWALL Turbo Card & 3G wireless card simultaneously into ZyWALL 5, ZyWALL 35 or ZyWALL 70?
C04. Can I insert the ZyWALL Turbo Card & 3G wireless card simultaneously into ZyWALL 5, ZyWALL 35 or ZyWALL 70?
C04. Can I insert the ZyWALL Turbo Card & 3G wireless card simultaneously into ZyWALL 5, ZyWALL 35 or ZyWALL 70?
C04. Can I insert the ZyWALL Turbo Card & 3G wireless card simultaneously into ZyWALL 5, ZyWALL 35 or ZyWALL 70?
C04. Can I insert the ZyWALL Turbo Card & 3G wireless card simultaneously into ZyWALL 5, ZyWALL 35 or ZyWALL 70?
C04. Can I insert the ZyWALL Turbo Card & 3G wireless card simultaneously into ZyWALL 5, ZyWALL 35 or ZyWALL 70?       284         D. Firewall FAQ.       285         D01. What is a network firewall?       285         D02. What makes ZyWALL secure?       285         D03. What are the basic types of firewalls?       285         D04. What kind of firewall is the ZyWALL?       286         D05. Why do you need a firewall when your router has packet       286         D06. What is Denials of Service (DoS)attack?       286
C04. Can I insert the ZyWALL Turbo Card & 3G wireless card simultaneously into ZyWALL 5, ZyWALL 35 or ZyWALL 70?284D. Firewall FAQ.285D01. What is a network firewall?285D02. What makes ZyWALL secure?285D03. What are the basic types of firewalls?285D04. What kind of firewall is the ZyWALL?286D05. Why do you need a firewall when your router has packet286D06. What is Denials of Service (DoS)attack?286D07. What is Ping of Death attack?287
C04. Can I insert the ZyWALL Turbo Card & 3G wireless card simultaneously into ZyWALL 5, ZyWALL 35 or ZyWALL 70?284D. Firewall FAQ.285D01. What is a network firewall?285D02. What makes ZyWALL secure?285D03. What are the basic types of firewalls?285D04. What kind of firewall is the ZyWALL?286D05. Why do you need a firewall when your router has packet286D06. What is Denials of Service (DoS)attack?286D07. What is Ping of Death attack?287D08. What is Teardrop attack?287
Colspan="2">Colspan="2"Cols
C04. Can I insert the ZyWALL Turbo Card & 3G wireless card simultaneously into ZyWALL 5, ZyWALL 35 or ZyWALL 70?284D. Firewall FAQ.285D01. What is a network firewall?285D02. What makes ZyWALL secure?285D03. What are the basic types of firewalls?285D04. What kind of firewall is the ZyWALL?286D05. Why do you need a firewall when your router has packetfiltering and NAT built-in?286D07. What is Denials of Service (DoS)attack?287D08. What is Teardrop attack?287D09. What is SYN Flood attack?287D10. What is LAND attack?
C04. Can I insert the ZyWALL Turbo Card & 3G wireless card simultaneously into ZyWALL 5, ZyWALL 35 or ZyWALL 70?284D. Firewall FAQ.285D01. What is a network firewall?285D02. What makes ZyWALL secure?285D03. What are the basic types of firewalls?285D04. What kind of firewall is the ZyWALL?286D05. Why do you need a firewall when your router has packetfiltering and NAT built-in?286D07. What is Denials of Service (DoS)attack?287D08. What is Teardrop attack?287D10. What is LAND attack?287D11. What is Brute-force attack?
Colspan="2">Colspan="2"Colspan="2">Colspan="2"Colspan="2"Colspan="2">Colspan="2"Colspan="

D16. Why does traffic redirect/static/policy route be blocked by
ZyWALL?
D17. How can I protect against IP spoofing attacks?
E. Security Service licenses FAQ
E01. What is iCard?291
E02. Where can I buy the iCard and how much does it cost?291
E03. How many kinds of iCard does ZyXEL provide?292
E04. Is each type of iCard device specific?
E05. What are the available security service licenses which require
additional purchase and license activation in ZyNOS v4.01?292
E06. What kind of iCard should I buy?292
E07. If I violate the mappings described above, for example, using a
silver iCard for ZyWALL 35 or ZyWALL 70, what will happen?292
E08. Can I try the Content Filtering service for free? How long is the
free trial period of Content Filtering service?
E09. Does ZyXEL provide customers free trial for AV+IDP service?
How long is it?
E10. Does ZyXEL provide customers free trial for Anti-Spam service?
How long is it?
F. Security Service Activation and UpdateFAQ
F. Security Service Activation and UpdateFAQ293
F. Security Service Activation and UpdateFAQ293 F01. Why do I have to register?
<ul> <li>F. Security Service Activation and UpdateFAQ</li></ul>
<ul> <li>F. Security Service Activation and UpdateFAQ</li></ul>
<ul> <li>F. Security Service Activation and UpdateFAQ</li></ul>
<ul> <li>F. Security Service Activation and UpdateFAQ</li></ul>
F. Security Service Activation and UpdateFAQ
F. Security Service Activation and UpdateFAQ
F. Security Service Activation and UpdateFAQ.       293         F01. Why do I have to register?       293         F02. In addition to registration, what can I do with myZyXEL.com? 294       F03. Is there anything changed on myZyXEL.com because of the launch of ZyNOS v4.00? Which ZyWALL models can be registered via myZyXEL.com?       294         F04. What's the difference between new registration flow and previous registration? What's the advantage of new registration flow over the previous registration flow?       295
F. Security Service Activation and UpdateFAQ.293F01. Why do I have to register?293F02. In addition to registration, what can I do with myZyXEL.com? 294F03. Is there anything changed on myZyXEL.com because of thelaunch of ZyNOS v4.00? Which ZyWALL models can be registeredvia myZyXEL.com?294F04. What's the difference between new registration flow andprevious registration? What's the advantage of new registration flowover the previous registration flow?295F05. If I were new to myZyXEL.com, what are the required fields
F. Security Service Activation and UpdateFAQ
F. Security Service Activation and UpdateFAQ.       293         F01. Why do I have to register?       293         F02. In addition to registration, what can I do with myZyXEL.com?       294         F03. Is there anything changed on myZyXEL.com because of the       100         launch of ZyNOS v4.00? Which ZyWALL models can be registered       294         F04. What's the difference between new registration flow and       294         F05. If I were new to myZyXEL.com, what are the required fields       295         F05. If I were new to myZyXEL.com, what are the required fields       295         F06. When using the new registration flow of myZyXEL.com for       295
F. Security Service Activation and UpdateFAQ
F. Security Service Activation and UpdateFAQ.       293         F01. Why do I have to register?       293         F02. In addition to registration, what can I do with myZyXEL.com? 294       F03. Is there anything changed on myZyXEL.com because of the launch of ZyNOS v4.00? Which ZyWALL models can be registered via myZyXEL.com?       294         F04. What's the difference between new registration flow and previous registration? What's the advantage of new registration flow over the previous registration flow?       295         F05. If I were new to myZyXEL.com, what are the required fields when I register my ZyWALL device on myZyXEL.com?       295         F06. When using the new registration flow of myZyXEL.com for ZyNOS v4.0, do I have to create a new account if I were already a registered user on myZyXEL.com?       296
F. Security Service Activation and UpdateFAQ.       293         F01. Why do I have to register?       293         F02. In addition to registration, what can I do with myZyXEL.com? 294       F03. Is there anything changed on myZyXEL.com because of the         launch of ZyNOS v4.00? Which ZyWALL models can be registered       via myZyXEL.com?         via myZyXEL.com?       294         F04. What's the difference between new registration flow and       previous registration? What's the advantage of new registration flow         over the previous registration flow?       295         F05. If I were new to myZyXEL.com, what are the required fields       295         F06. When using the new registration flow of myZyXEL.com for       295         F06. When using the new registration flow of myZyXEL.com for       296         F07. What is mySecurityZone?       296
F. Security Service Activation and UpdateFAQ.       .293         F01. Why do I have to register?       .293         F02. In addition to registration, what can I do with myZyXEL.com? 294       F03. Is there anything changed on myZyXEL.com because of the launch of ZyNOS v4.00? Which ZyWALL models can be registered via myZyXEL.com?       .294         F04. What's the difference between new registration flow and previous registration? What's the advantage of new registration flow over the previous registration flow?       .295         F05. If I were new to myZyXEL.com, what are the required fields when I register my ZyWALL device on myZyXEL.com?       .295         F06. When using the new registration flow of myZyXEL.com for ZyNOS v4.0, do I have to create a new account if I were already a registered user on myZyXEL.com?       .296         F07. What is mySecurityZone?       .296         F08. What is Update Server?       .296

G01. Why should I need a gateway Anti-Virus solution while I already
deployed the Anti-Virus software on each desktop/laptop?297
G02. Why does ZyWALL bundle Anti-Virus and IDP feature
together?
G03. Can I subscribe to the Anti-Virus service alone or IDP service
alone?
G04. What are the hardware requirements to run AV+IDP security
service?
G05. Now I know that the ZyWALL Turbo Card is a must when use
AV+IDP service; but what exactly I can benefit from the ZyWALL
Turbo Card?
G06. How do I keep signatures of AV+IDP service updated?298
G07. How often does ZyXEL release signatures of AV+IDP security
service?
G08. Will the traffic coming in through the VPN tunnel also be
scanned by Anti-Virus, IDP and Anti-Spam feature in ZyWALL
ZyNOS v4.0?
H. IDP FAQ
H01. Why does ZyWALL bundle Anti-Virus and IDP feature
together?
H02. Can I subscribe to the Anti-Virus service alone or IDP service
alone?
H03. What are the hardware requirements to run AV+IDP security
service?
H04. Now I know that the ZyWALL Turbo Card is a must when use
AV+IDP service; but what exactly I can benefit from the ZyWALL
Turbo Card?
H05. Could I duplicate the IDP feature's policy settings from one
ZyWALL device to another?
H06. How do I keep signatures of AV+IDP service updated?
H07. How often does ZyXEL release signatures of AV+IDP security
service?
H08. Will the traffic coming in through the VPN tunnel also be
scanned by Anti-Virus, IDP and Anti-Spam feature in ZyWALL
ZyNOS v4.0?
I. Anti-Spam FAQ
I01. What's the difference between gateway Anti-Spam and
client-based Anti-Spam filter such as Microsoft Outlook's?

J.

	I02. A customer already has her/his own exchange server including the
	Anti-Spam software from other vendors; is there any good reason for
	her/him to use ZyXEL's Anti-Spam service in addition to the current
	solution?
	I03. What happens when an email with large attachment in size, e.g.
	5MB, is downloaded which has virus in it?
	I04. What happens if the virus is in the last part of the email message
	and the email receiver already got a part of the contaminated file in
	her/his laptop or desktop?
	105. Will the traffic coming in through the VPN tunnel also be
	scanned by Anti-Virus, IDP and Anti-Spam feature in ZyWALL
	ZyNOS v4.0?
	I06. In ZyWALL's Anti-Spam feature, what's your recommendation to
	handle identified spam emails?
	I07. What's the specification of Anti-Spam feature in ZyNOS v4.01? 302
	I08. How do I keep signatures of Anti-Spam service update?
С	ontent Filter FAQ
	J01. What's the operation between ZyXEL appliance and BlueCoat
	data center?
	J02. How many entries can the cache of Web Site Auto Categorization
	keep at most?
	J03. Can I specify the time out value of the query response from
	BlueCoat data center?
	J04. Can I decide whether to forward or drop the HTTP response if
	the query to BlueCoat data center is timed out?
	J05. How to register for BlueCoat service?
	J06. Why can't I make registration successfully?
	J07. What services can I get with Trial Registration?
	J08. What types of content filter does ZyWALL provide?
	J09. What are the primary features of ZyXEL Content Filtering?304
	J10. Who needs ZyXEL Content Filtering? Is ZyXEL Content
	Filtering for small companies or for large corporations?
	J11. Can I have different policies in effect for different times of the
	day or week?
	J12. How many policies can I create?
	J13. Can I create my own categories?
	J13. Can I create my own categories?

J15. How many URL keywords does ZyWALL support?305
J16. How do I keep database of Content Filtering service updated?305
J17. What is BlueCoat Filter list?
J18. How many ratings does the BlueCoat database contain?
J19. How often does BlueCoat update the database?
J20. How do I locate sites to block?
J21. Do humans review the ratings?
J22. How can I do if I find a WEB site is mis-categorized?306
J23. How many and what categories do you provide?
J24. How does the ZyXEL content filtering handle dynamically
generated sites?
J25. Does BlueCoat have more than one data center? Is the BlueCoat
Web Filter geographically load balanced?
J26. Who can generate and view reports on BlueCoat WEB site?308
J27. How can I get Content Filtering report?
J28. Can I change the password for BlueCoat service?
J29. Which User Name & Password should I input for Content
Filtering report?
J30. My device can't get connected to Http://myZyXEL.com, so I can't
soon my device can t get connected to mep.//myzyzzzzeni, so i can t
get into Registration page. What should I check?
get into Registration page. What should I check?
get into Registration page. What should I check?
get into Registration page. What should I check?
get into Registration page. What should I check?
get into Registration page. What should I check?
get into Registration page. What should I check?
get into Registration page. What should I check?
get into Registration page. What should I check?309K. IPSec FAQ.310K01. How many VPN tunnels are supported on ZyWALL?310K02. How to count my VPN tunnels on ZyWALL?310K03. What is VPN?311K04. Why do I need VPN?311K05. What are most common VPN protocols?312K06. What is PPTP?312
get into Registration page. What should I check?309K. IPSec FAQ.310K01. How many VPN tunnels are supported on ZyWALL?310K02. How to count my VPN tunnels on ZyWALL?310K03. What is VPN?311K04. Why do I need VPN?311K05. What are most common VPN protocols?312K06. What is PPTP?312K07. What is L2TP?312
get into Registration page. What should I check?309K. IPSec FAQ.310K01. How many VPN tunnels are supported on ZyWALL?310K02. How to count my VPN tunnels on ZyWALL?310K03. What is VPN?311K04. Why do I need VPN?311K05. What are most common VPN protocols?312K06. What is PPTP?312K07. What is L2TP?312K08. What is IPSec?312
get into Registration page. What should I check?309K. IPSec FAQ.310K01. How many VPN tunnels are supported on ZyWALL?310K02. How to count my VPN tunnels on ZyWALL?310K03. What is VPN?311K04. Why do I need VPN?311K05. What are most common VPN protocols?312K06. What is PPTP?312K07. What is L2TP?312K08. What is IPSec?313K09. What is SA?313
get into Registration page. What should I check?309K. IPSec FAQ.310K01. How many VPN tunnels are supported on ZyWALL?310K02. How to count my VPN tunnels on ZyWALL?310K03. What is VPN?311K04. Why do I need VPN?311K05. What are most common VPN protocols?312K06. What is PPTP?312K07. What is L2TP?312K08. What is IPSec?313K10. What is Pre-Shared Key?313
get into Registration page. What should I check?309K. IPSec FAQ.310K01. How many VPN tunnels are supported on ZyWALL?310K02. How to count my VPN tunnels on ZyWALL?310K03. What is VPN?311K04. Why do I need VPN?311K05. What are most common VPN protocols?312K06. What is PPTP?312K07. What is L2TP?312K08. What is IPSec?313K10. What is Pre-Shared Key?313K11. What is Phase 1 ID for?313
get into Registration page. What should I check?309K. IPSec FAQ.310K01. How many VPN tunnels are supported on ZyWALL?310K02. How to count my VPN tunnels on ZyWALL?310K03. What is VPN?311K04. Why do I need VPN?311K05. What are most common VPN protocols?312K06. What is PPTP?312K07. What is L2TP?312K08. What is IPSec?313K10. What is Pre-Shared Key?313K11. What is Phase 1 ID for?314
get into Registration page. What should I check?309K. IPSec FAQ.310K01. How many VPN tunnels are supported on ZyWALL?310K02. How to count my VPN tunnels on ZyWALL?310K03. What is VPN?311K04. Why do I need VPN?311K05. What are most common VPN protocols?312K06. What is PPTP?312K07. What is L2TP?312K08. What is IPSec?313K10. What is Pre-Shared Key?313K11. What is Phase 1 ID for?314K13. Is my ZyWALL ready for IPSec VPN?314
get into Registration page. What should I check?309K. IPSec FAQ.310K01. How many VPN tunnels are supported on ZyWALL?310K02. How to count my VPN tunnels on ZyWALL?310K03. What is VPN?311K04. Why do I need VPN?311K05. What are most common VPN protocols?312K06. What is PPTP?312K07. What is L2TP?312K08. What is IPSec?313K10. What is Pre-Shared Key?313K11. What is Phase 1 ID for?313K12. What are Local ID and Peer ID?314K13. Is my ZyWALL ready for IPSec VPN?315

L.

10

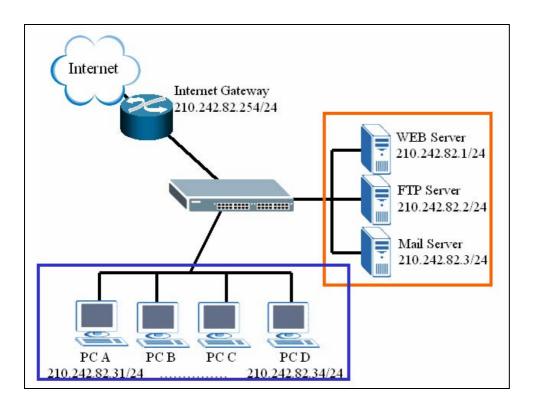
L14. How can I have Self-signed certificate for ZyXEL appliance?324
L15. Can I create self-signed certificates in addition to the default
one?
L16. Will Self-signed certificate be erased if I reset to default
configuration file?
L17. Will certificates stored in ZyXEL appliance be erased if I reset to
default configuration file?
L18. What can I do prior to reset appliance's configuration?
L19. If I export My Certificates from ZyXEL appliance, save them
locally, and then import them back after resetting the configuration
file, can I reuse the imported My Certificates ?
M. Dual WAN Auto Fail-over/Fail-back and Load Balance FAQ325
M01. How do ZyWALLs dispatch outgoing sessions to different WAN
connections?
M02. Can ZyWALL support VPN load balancing?
N. Bandwidth Management FAQ
N01. How many class can I create in ZyWALL Bandwidth
Management class tree? And, what is the max depth of a class?326
O. Wireless FAQ
O01. Which wireless cards does it support in ZyWALL 5/35/70?327
O02. Which wireless security option can I use while using related
wireless cards?

# **Application Notes**

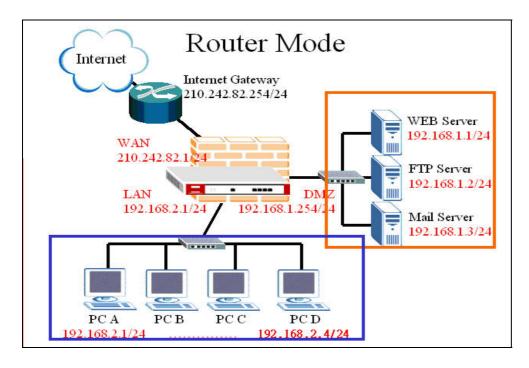
Seamless Incorporation into your network

# Using Transparent (Bridge Mode) Firewall

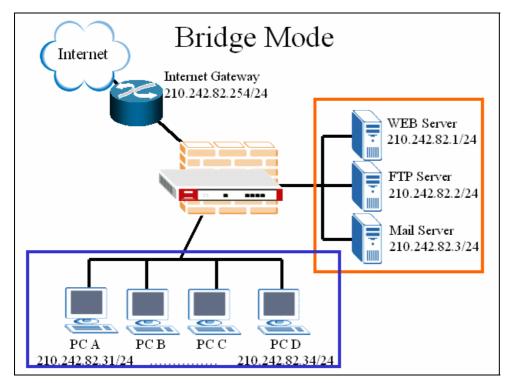
If user wants to insert a firewall into current network, IP setting of hosts and servers may need to change. Following example illustrates an example of current deployment: servers and other hosts sit in the same IP segment.



If a router mode firewall is inserted into existing network, user may need to reassign the IP of all servers and hosts and related setting of applications. However, it may be a huge task to administrators.



Deploying a transparent mode firewall doesn't require any changes of settings on the original network topology. It works as bridge/switch; therefore, all the hosts can communicate with each other as without firewall in between. At the same time, the transparent firewall can check the packets passing through it and block attacks and limit unauthorized access through access control right.



In the following section, we will explain how to configure ZyWALL as bridge firewall. Therefore, all hosts and servers can keep using the same IP as that of current network.

User can configure ZyWALL to act as a router mode firewall or bridge (transparent) firewall. The default is router mode firewall.

Step1. Before changing ZyWALL to bridge mode, if admin wants to make the ZyWALL's LAN PC be able to get DHCP IP address assignment from the DHCP server or the gateway upper than the ZyWALL, there is one firewall rule needs to be activated.

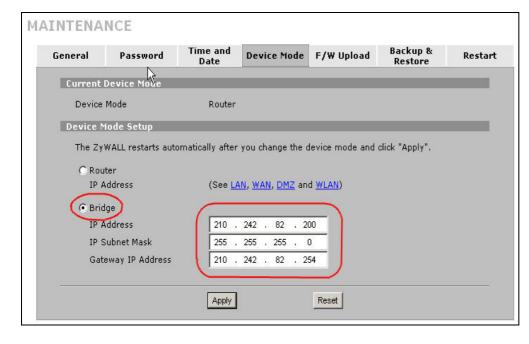
Go to **Firewall** >> **Rule Summary**; choose '**WAN to LAN**' from 'Packet Direction'. You will see a rule to permit the service type, 'BOOTP\_CLIENT(UDP:68)', to pass firewall. It's INACTIVE by default. Admin can activate the rule by clicking the '**N**' as following picture. Then the rule will be activated right away.

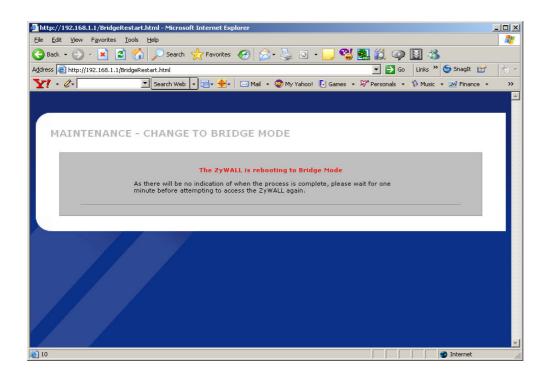
FIREWALL
Default Rule Rule Summary Anti-Probing Threshold Service
Rule Summary
Firewall Rules Storage Space in Use
0% 1% 100%
Packet Direction: WAN to LAN
Default Policy: Drop, Log
# Name Active Source Destination Service Type Action Sch.Log Modify
■ * Name Study Address Address Service Type Action Stillery Houry
2 W2L_Rule_2 N Any ▼ Any ▼ NetBIOS(TCP/UDP:137~139,445) ▼ Permit No No 📝 ①
Move rule 1 to rule 1 (rule number)
Move rule 1 to rule 1 (rule number)
FIREWALL
N
Default Rule Rule Summary Anti-Probing Threshold Service
Default Rule Rule Summary Anti-Probing Threshold Service
Rule Summary Firewall Rules Storage Space in Use
Rule Summary
Rule Summary     Intervision     Service       Firewall Rules Storage Space in Use     1%     100%
Rule Summary     Intervision     Service       Firewall Rules Storage Space in Use     1%     100%
Rule Summary     Firewall Rules Storage Space in Use     1%       0%     1%       Packet Direction:     WAN to LAN       Default Policy: Drop, Log
Rule Summary       Firewall Rules Storage Space in Use       0%       100%         0%       1%       100%         Packet Direction:       WANto LAN       Image: Control of the storage space in Use         Default Policy: Drop, Log       Image: Control of the storage space in Use       Image: Control of the storage space in Use         Image: Wanto LAN       Image: Control of the storage space in Use       Image: Control of the storage space in Use         Image: Control of the storage space in Use       Image: Control of the storage space in Use       Image: Control of the storage space in Use         Image: Control of the storage space in Use       Image: Control of the storage space in Use       Image: Control of the storage space in Use         Image: Control of the storage space in Use       Image: Control of the storage space in Use       Image: Control of the storage space in Use         Image: Control of the storage space space in Use       Image: Control of the storage space
Rule Summary     Firewall Rules Storage Space in Use     1%       0%     1%       Packet Direction:     WAN to LAN       Default Policy: Drop, Log         # Name     Active       Address     Service Type       Action Sch. Log     Modify       1 W2L_Rule_1     Any   BOOTP_CLIENT(UDP:68) Permit No Yes
Rule Summary       Firewall Rules Storage Space in Use       0%       100%         0%       1%       100%         Packet Direction:       WANto LAN       Image: Control of the storage space in Use         Default Policy: Drop, Log       Image: Control of the storage space in Use       Image: Control of the storage space in Use         Image: Wanto LAN       Image: Control of the storage space in Use       Image: Control of the storage space in Use         Image: Wanto Lan       Image: Control of the storage space spac
Rule Summary       Firewall Rules Storage Space in Use       0%       100%         0%       1%       100%         Packet Direction:       WANto LAN       Image: Control of the storage Space in Use         Default Policy: Drop, Log       Image: Control of the storage Space in Use       Image: Control of the storage Space in Use         Image: Ward of the storage Space in Use       Image: Control of the storage Space in Use       Image: Control of the storage Space in Use         Default Policy: Drop, Log       Image: Control of the storage Space in Use       Image: Control of the storage Space in Use         Image: Image: Image: Variation of the storage Space in Use       Image: Control of the storage Space in Use       Image: Control of the storage Space in Use         Image: I
Rule Summary       Firewall Rules Storage Space in Use       0%       1%         0%       1%       100%         Packet Direction:       WAN to LAN       Image: Control of the storage state storage
Pordar Rate       Rate Summary       Firewall Rules Storage Space in Use       0%       1%       100%         0%       1%       100%       100%       100%       100%       100%         Packet Direction:       WANto LAN       V       100%       100%         Default Policy:       Drop, Log       V       Active Address Address Address       Service Type       Action Sch. Log       Modify         1       W2L_Rule_1       Y       Any       BOOTP_CLIENT(UDP:68)       Permit       No       V       V         1       W2L_Rule_2       N       Any       NetBIOS(TCPAUDP:137~139,445)       Permit       No       V       V         Insert       new rule before       rule1       (rule number)       V

Step2. To change the device mode, go to MAINTENANCE >> Device Mode. Select 'Bridge' and

assign a management IP for ZyWALL. The Gateway IP Address is used as next-hop of default route. ZyWALL will restart after applying the change.

(Note: Here we suggest admin to dedicate an IP address to ZyWALL itself at the same subnet as original one (like 210.242.82.X/24 in this example). In this way, admin doesn't need to change his PC's IP address when he wants to access Internet and ZyWALL's web GUI at the same time.)





Step3. After rebooting, login ZyWALL's GUI by accessing ZyWALL's management IP address. (Accessing ZyWALL by the PC with a static IP address configured in the same subnet or with an IP from DHCP server (refer to step1 for the pre-configured firewall rule).

Step4. In this example, since we want to apply a DMZ zone for servers. So for ZyWALL5/35 which the ports of LAN & DMZ can be configured, user can decide the roles of each port.

Go to **Network** >> **Bridge** >> **Port Roles**. By default, 4 ports are assigned to LAN. In this example, we use port 1 & 2 assigned to LAN and Port 3 & 4 assigned to DMZ as following picture.

Bridge	Port Roles				
Port Roles	Setup				
		LAN ©	0 0 0	LAN	
		DMZ 6	Fo 7 Fo 7 Fo 7)	DMZ C	0.157
2YWALL 35		WLAN C	000	WLAN C	(Genner )
					Wireless Card
	ur device must have a w e system will restart if w				
3				4.0	

Step5. Furthermore, to configure firewall rule to control the access of your network, go to **SECURITY** >> **FIREWALL** as you do in router mode firewall. For example, user wants to block the access from a FTP server (210.242.82.2) in DMZ zone to LAN hosts (210.242.82.31~34) (Note that they all sits in the same IP segment 210.242.82.0/24). Edit the firewall rule via **Firewall** >> **Rule Summary** and with packet direction: **DMZ to LAN**.

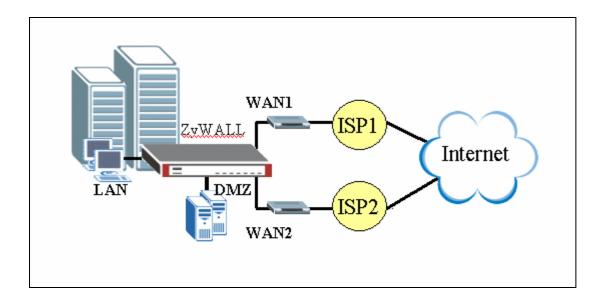
Rule Summary		
Flammell Bulan Sterrore Sugar in I		
Firewall Rules Storage Space in U	Jse	
0%	1%	100%
-		
DMZ IS LAN		
Packet Direction: DMZ to LAN	•	

And enter 210.242.82.2 as the source address and 210.242.82.31~34 as destination address. And then select the service and set the action for 'Matched Packet' to '**BLOCK'**.

FIREWALL - EDIT RUL	E	
Edit Source Address		
Address Editor		Source Address(es)
Address Type	Any Address 💌	210.242.82.2
Start IP Address	0.0.0.0	
End IP Address	0.0.0.0	
Subnet Mask	0.0.0.0	
Add Modify		Delete
Edit Destination Address		
Address Editor		Destination Address(es)
Address Type	Any Address 💌	210.242.82.31 - 210.242.82.34
Start IP Address	0.0.0.0	
End IP Address	0.0.0.0	
Subnet Mask	0.0.0.0	
Add Modify		Delete

#### **Internet Connection**

A typical Internet access application of the ZyWALL is shown below. This section guides you how to configure ZyWALL to gain the Internet access.



Step1. First of all, Select **Home** menu and click **Internet Access** Wizard to configure your WAN1 connection. Click "**Internet Access**" under **Home** >> **Wizards for WAN 1 Quick Setup** 



Wizards for WAN 1 Quick Setup
Internet Access

A pop-up window as below will indicate you to enter ISP Parameters for Internet Access .

the or	'ou can select ethernet, PPPoE or PPTP according to in which the network you f you don't know, please ask your network administrator. The most popular type network is ethernet.
	ncapsulation Ethernet
	AN IP Address Assignment
	P Address Assignment Dynamic 💌
	P Address Assignment Dynamic 💌

There are three kinds of encapsulation which are supported by ZyWALL: **Ethernet**, **PPPoE** & **PPTP**. Select the correct encapsulation type from the drop-down menu. The wizards will requests related information needed. These fields vary depending on what you select in the Encapsulation field. Fill them in with the information exactly as given by the ISP or network administrator.

Following picture is an example while PPPoE is selected.

ISP Parameters for Inter	net Access	
	t, PPPoE or PPTP according to se ask your network administra	in which the network you are. ator. The most popular type of
Encapsulation	PPP over Ethernet	
Service Name		(Optional)
User Name		
Password	******	
Retype to Confirm	*****	
🗖 Nailed-Up		
Idle Timeout	100 (Seconds)	
WAN IP Address Assignm	nent	
IP Address Assignment	Dynamic 💌	
		Finish

Once the required information is correctly configured, click on the "**Finish**" button to apply the setting and then you have finished configuring Internet Access on WAN1 link. To configure the WAN2 link for backup or load balance, go to **Network** >> **WAN** for advanced configuration.

#### DHCP server/client/relay + flexible port role configuration

#### ZyWALL supports

(1) DHCP client on the WAN port

User can choose either a static IP or a dynamic IP address for WAN port. When choosing dynamic IP, ZyWALL will get a DHCP IP address from ISP or upper layer DHCP server.

(2) DHCP server/relay/none on the LAN/DMZ/WLAN ports

Since ZyWALL v4.0, ZyWALL not only supports DHCP server for LAN ports, but also for DMZ and WLAN ports. Besides, since v4.0, ZyWALL also support flexible port role setting. With these 2 features, admin can take advantage and easily connect servers / clients into a ZyWALL-ready environment. Following are the description about two features.

1. Each interface own an independent subnet. For example, LAN is 1.1.1.x/24, DMZ is 2.2.2.x/24, and WLAN is 3.3.3.x/24.

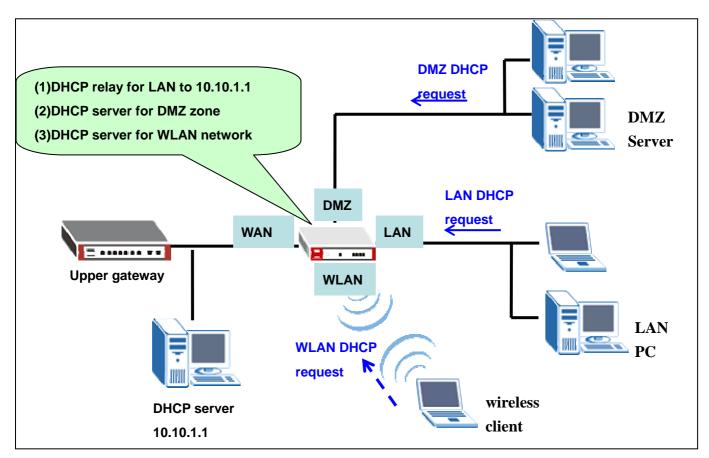
2. When choosing DHCP setting as 'None', the LAN/DMZ/WLAN will NOT assign IP address to the associated hosts. Client PCs need to configure IP address manually.

3. When choosing DHCP setting as a 'Server', the LAN/DMZ/WLAN will automatically assign IP, subnet, gateway and DNS to the associated clients.

4. When choosing DHCP setting as a 'Relay', the LAN/DMZ/WLAN will forward the DHCP request to another DHCP server.

5. There are 4 ports could be flexibly assigned to be LAN or DMZ or WLAN port. To assign a port to WLAN, user needs to insert a proper wireless card (ex. ZyAIR G-100) and enable wireless from **GUI** >> **network** >> **Wireless Card**. After assigning a port to WLAN, the hosts connected to the port will be in the same subnet as other wireless clients which associate to the ZyWALL. Generally speaking, it's especially for troubleshooting or user wants to dedicate a server for wireless network use only.

Following is an example to configure LAN as a DHCP relay, DMZ as a DHCP server, and WLAN as a DHCP server. In this example, since network admin would like to central manage IP address of all LAN hosts. There is a DHCP server (IP: 10.10.1.1) to handle all DHCP request from LAN hosts. So ZyWALL will be configured as a relay role to pass DHCP request from LAN to the DHCP server. For DMZ, and WLAN, network admin would like to configure them as independent subnet.



Interface	DHCP setting	IP Pool Starting Address or DHCP server address
LAN	Relay	10.10.1.1 (DHCP server's IP address)
DMZ	Server	192.168.5.1/24
WLAN	Server	192.168.10.1/24

Step1. Insert a wireless card in ZyWALL's PCMCIA slot before booting the ZyWALL. Since we will enable wireless network to allow wireless clients associate with.

Step2. Configure DHCP setting for LAN. Choose '**Relay**' from DHCP setting and enter the IP address of the DHCP server, '**10.10.1.1**'.

LAN Static DHCF	P IP Alias Port Role	:5	
LAN TCP/IP			
IP Address	192 . 168 . 1 . 1	RIP Direction	Both 💌
IP Subnet Mask	255 , 255 , 255 , 0	RIP Version	RIP-1
Multicast	None 💌		
DHCP Setup			
DHCP	Relay 💌		
IP Pool Starting Address	192 . 168 . 1 . 33	Pool Size	128
DHCP Server Address	10 . 10 . 1 . 1		

Step3. Configure DHCP setting for DMZ. Choose '**Server**' from DHCP setting and enter the IP Pool address starting from '192.168.5.33'.

DMZ	Static DI	ICP	1	IP	Alias	; J.	Port Role	5	
DMZ TCP/II	,								
IP Address		192	. 168		5	1	Ĩ	RIP Direction	Both 💌
IP Subnet I	Mask	255	. 255	163	255	0	F	RIP Version	RIP-1 💌
Multicast		None	-						
DHCP Setup	1	h	5						
DHCP		Serve	r 💌				2		
IP Pool Sta	rting Address	192	. 168	- 20	5	33	F	Pool Size	128
DHCP Serv	er Address	0	, 0		0	0			

Step4. Configure DHCP setting for WLAN. Choose 'Server' from DHCP setting and enter the IP Pool address starting from '192.168.10.33'.

WLAN	Static D	НСР	IP Alias	312	Port Roles	
WLAN TCP/II						
IP Address		192 , 16	68.10.	1	RIP Direction	Both 💌
IP Subnet Ma	<sup>isk</sup> 🖟	255 . 25	55 . 255 .	0	RIP Version	RIP-1 💌
Multicast	~	None	]			
DHCP Setup						
DHCP Setup		Server 💌		_		$\overline{}$

Step5. Configure Port Role from either LAN or DMZ or WLAN >> Port Roles. Configure the roles as following. Then click 'Apply' to save the setting.(1). port 1-2 for LAN

ZyXEL

#### (2). port3 for DMZ

(3). Click '**WLAN**' from the right wireless card. It will make the wireless card be an independent interface and own an independent subnet. After it's done, the WLAN selection for 4 ports will be available. Choose port4 for WLAN. So the server or PC hosts connect to port4 will be in the same subnet with WLAN.

LAN	Static DHCP	IP Alias	Port Roles	
Port Role	s Setup			
ZyWI				
4111001 9429		WLA	NOOOO	WLAN Wireless Card
	Your device must have The system will restart		lled to use the WLAN port ( guration is changed,	role.
Note 2:	The system will restart	if wireless card confi	guration is changed.	

In this way, admin can utilize 4+1 ports flexibly.

#### Using NAT/Multi-NAT

- What is Multi-NAT?
- <u>How NAT works</u>
- NAT Mapping Types
- SUA versus Multi-NAT
- Example
   <u>Step 1. Applying NAT on WAN Interface</u>
   <u>Step 2. Configuring NAT Address Mapping</u>
   <u>Step 3. Using Multiple Global IP addresses for clients and servers (One-to-One, Many-to-One, Server Set mapping types)</u>
- <u>Application -- Non NAT-Friendly Support</u>
- What is Multi-NAT?

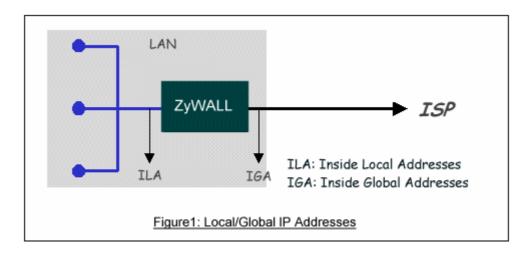
NAT (Network Address Translation-NAT RFC 1631) is the translation of an Internet Protocol address used within one network to a different IP address known within another network. One network is designated the *inside* network and the other is the *outside*. Typically, a company maps its local inside network addresses to one or more global outside IP addresses and "unmaps" the global IP addresses on incoming packets back into local IP addresses. The IP addresses for the NAT can be either fixed or dynamically assigned by the ISP. In addition, you can designate servers, e.g., a web server and a telnet server, on your local network and make them

accessible to the outside world. If you do not define any servers, NAT offers the additional benefit of firewall protection. In such case, all incoming connections to your network will be filtered out by the ZyWALL, thus preventing intruders from probing your network.

The SUA feature that the ZyWALL supports previously operates by mapping the private IP addresses to a global IP address. It is only one subset of the NAT. The ZyWALL supports the most of the features of the NAT based on RFC 1631, and we call this feature as 'Multi-NAT'. For more information on IP address translation, please refer to RFC 1631, *The IP Network Address Translator (NAT)*.

#### • How NAT works

If we define the local IP addresses as the Internal Local Addresses (ILA) and the global IP addresses as the Inside Global Address (IGA), see the following figure. The term 'inside' refers to the set of networks that are subject to translation. NAT operates by mapping the ILA to the IGA required for communication with hosts on other networks. It replaces the original IP source address (and TCP or UDP source port numbers) and then forwards each packet to the Internet ISP, thus making them appear as if they had come from the NAT system itself (e.g., the ZyWALL router). The ZyWALL keeps track of the original addresses and port numbers so incoming reply packets can have their original values restored.



#### • NAT Mapping Types

NAT supports five types of IP/port mapping. They are:

#### 1. One to One

In One-to-One mode, the ZyWALL maps one ILA to one IGA.

#### 2. Many to One

In Many-to-One mode, the ZyWALL maps multiple ILA to one IGA. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature that previous ZyNOS routers supported (the SUA only option in today's routers).

#### 3. Many to Many Overload

In Many-to-Many Overload mode, the ZyWALL maps the multiple ILA to shared IGA.

#### 4. Many One to One

In Many One to One, the ZyWALL maps each ILA to unique IGA.

#### 5. Server

In Server mode, the ZyWALL maps multiple inside servers to one global IP address. This allows us to specify multiple servers of different types behind the NAT for outside access. Note, if you want to map each server to one unique IGA please use the One-to-One mode.

The following table summarizes these types.

<b>NAT Туре</b>	IP Mapping
One-to-One	ILA1<>IGA1
Many-to-One (SUA/PAT)	ILA1<>IGA1 ILA2<>IGA1 
Many-to-Many Overload	ILA1<>IGA1 ILA2<>IGA2 ILA3<>IGA1 ILA4<>IGA2 
Many One-to-One	ILA1<>IGA1 ILA2<>IGA2 ILA3<>IGA3 ILA4<>IGA4 
Server	Server 1 IP<>IGA1 Server 2 IP<>IGA1

#### • SUA Versus Multi-NAT

SUA (Single User Account), if you get only one public IP address from your ISP, then you should use SUA. With SUA, PCs on ZyWALL's LAN side can access Internet without further configuration. If you have internal servers to be accessed by remote users on Internet, you need to go to **ADVANCED -> SUA/NAT -> SUA Server** to setup which service, or port numbers, you would like to forward to which Internal server.

Multi-NAT, if you get multiple public IP addresses from your ISP, then you may use Multi-NAT. With Multi-NAT, you can choose different types of NAT mapping methods to utilize the public IP addresses. You should define each NAT mapping rules clearly in **ADVANCED -> SUA/NAT -> Address Mapping**, so that internal PCs can access Internet and internal servers can be accessed by remote uses on Internet.

#### Step 1. Applying NAT in WAN Interface

You can choose the NAT mapping types to either SUA Only or Full Feature in WAN setup.

## NETWORK -> WAN

General	WAN 1	WAN 2	Traffic Redirect	Dial Backup	
ISP Param	eters for Internet Acce	ess			
Encapsul Service 1		Ethernet	•		
WAN IP Ad	dress Assignment				
💿 Get A	Automatically from ISI	ס			
	ixed IP Address				
-	VAN IP Address VAN IP Subnet Mask				
-	way IP Address				
	-				
Advanced	Setup				
🗹 Enab	le NAT (Network Addr	ess Translation)			
RIP Direc	tion		None 🔻		
RIP Versi	on		RIP-1		
🗌 Enab	le Multicast				
	ast Version		IGMP-v1		
<b>Spoo</b>	f WAN MAC Address				
	the computer's MAC	address - IP Addres	s 192 . 168 . 10	00.33	
			,		

## or ADVANCED -> NAT -> NAT Overview

NAT Overview	Address Mapping	Port Forwarding	Port Triggering			
Global Set	tinge					
Giunai Sei	ungs					
Max. Co	ncurrent Sessions		10000			
	ncurrent Sessions Pe	er Host	· · · · · · · · · · · · · · · · · · ·	cal high since las	t startup: 5)	
WAN Op	eration Mode		Active/Passive F	ail Over		
WAN 1						
Addro	ole NAT ess Mapping Rules SUA					
0	Full Feature	L	2/100			
Port I	Forwarding Rules		0/100		Copy to WAN 2	
Port	Triggering Rules		0/12		Copy to WAN 2	
WAN 2						
Addro	ole NAT ess Mapping Rules SUA					
0	Full Feature	Γ	2/100			
Port I	Forwarding Rules		0/100		Copy to WAN 1	
Port	Triggering Rules		0/12		Copy to WAN 1	

# Key Settings

Field	Options	Description
	Full Feature	Set to <b>'Full Feature'</b> if there are multiple IP addresses given by ISP and can assigned to your clients.
Network Address Translation	Routing	Set to <b>'Routring'</b> if you clients use Internet IP addresses and thus do not need NAT function.
	SUA Only	Set this field to 'SUA Only' if you want all clients share one IP to Internet.

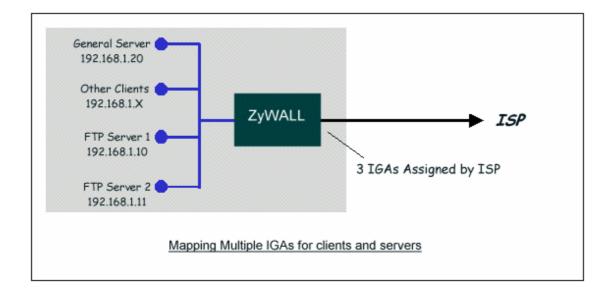
# Step 2. Configuring NAT Address Mapping

To configure NAT, go to ADVANCED -> NAT -> Address Mapping



NAT Overvi	iew Address Ma	apping Port Forv	warding Port Ti	iggering		
SIIA A	Address Mapping I	Julos				
JUA A	wuress mapping i	Aures				
#	Local Start IP	Local End IP	Global Start IP	Global End IP	Туре	
1	0.0.0	255.255.255.255	0.0.0	N/A	M-1	
2	N/A	N/A	0.0.0	N/A	Server	
Full F	eature Address M	apping Rules				
WA	AN Interface WA	N 1 💌				
#	Local Start IP	Local End IP	Global Start IP	Global End IP	Туре	Modify
						B Û
1	0.0.0.0	255.255.255.255	0.0.0.0	N/A	M-1	
2	N/A	N/A	0.0.0	N/A	Server	e î
3					-	e î
4					-	e î
5			•••		-	e î
6					-	ef û
7					-	e î
8					-	e î

Step 3. Using Multiple Global IP addresses for clients and servers (One-to-One, Many-to-One, Server Set mapping types)



In this case we have 3 IGAs (IGA1, IGA2 and IGA3) from the ISP. We have two very busy internal FTP servers and also an internal general server for the web and mail. In this case, we want to assign the 3 IGAs by the following way using 4 NAT rules.

- Rule 1 (One-to-One type) to map the FTP Server 1 with ILA1 (192.168.1.10) to IGA1 (200.1.1.1).
- Rule 2 (One-to-One type) to map the FTP Server 2 with ILA2 (192.168.1.11) to IGA2 (200.1.1.2).

- Rule 3 (Many-to-One type) to map the other clients to IGA3 (200.1.1.3).
- Rule 4 (Server type) to map a web server and mail server with ILA3 (192.168.1.20) to IGA3. Type
   Server allows us to specify multiple servers, of different types, to other machines behind NAT on the LAN.

Rule 1 Setup: Select One-to-One type to map the FTP Server 1 with ILA1 (192.168.1.10) to IGA1 (200.1.1.1).

ZyXEL			HELP (	?
номе	SUA/NAT - Address N	lapping		
NETWORK LAN WIRELESS LAN WAN DMZ SECURITY FIREWALL CONTENT FILTER VPN CERTIFICATES AUTH SERVER	Address Mapping Rule Type Local Start IP Local End IP Global Start IP Global End IP	One-to-One 192 . 168 . 1 . 10 N/A 200 . 1 . 1 . 1 N/A		
ADVANCED SUA/NAT STATIC ROUTE POLICY ROUTE		Apply	Cancel	
BW MGMT REMOTE MGMT				

Rule 2 Setup: Selecting **One-to-One** type to map the FTP Server 2 with ILA2 (192.168.1.11) to IGA2 (200.1.1.2).

ZyXEL		HELP (?)
номе	SUA/NAT - Address Mapping	
NETWORK LAN WRELESS LAN WAN DMZ SECURITY FIREWALL CONTENT FILTER VPN CERTIFICATES AUTH SERVER	Address Mapping Rule         Type       One-to-One       Image: Colspan="2">Image: Colspan="2">Image: Colspan="2">Image: Colspan="2">Image: Colspan="2">Image: Colspan="2">Image: Colspan="2" Image: Colspa="" Image: Colspan="2" Image: Colspan="2" Image: Colspan="2" Imag	
ADVANCED SUA/NAT STATIC ROUTE POLICY ROUTE BW MGMT PEMOTE MGMT	Apply Cancel	

Rule 3 Setup: Select Many-to-One type to map the other clients to IGA3.

ZyXEL			HELP ?
НОМЕ	SUA/NAT - Address Mapp	ping	
NETWORK LAN WIRELESS LAN WAN DMZ SECURITY FREWALL CONTENT FILTER VPN CERTIFICATES	Address Mapping Rule Type Local Start IP Local End IP Global Start IP Global End IP	Many-to-One 192 . 168 . 1 . 50 192 . 168 . 1 . 254 200 . 1 . 1 . 3 N/A	
AUTH SERVER ADVANCED SUANAT STATIC ROUTE POLICY ROUTE BW MGMT REMOTE MGMT		Apply Cancel	

Rule 4 Setup: Select Server type to map our web server and mail server with ILA3 (192.168.1.20) to IGA3.

ZyXEL		HELP 🕐
НОМЕ	SUA/NAT - Address Mapping	
NETWORK LAN WRELESS LAN WAN DMZ SECURITY FIREWALL CONTENT FILTER VPN CERTIFICATES AUTH SERVER	Address Mapping Rule         Type       Server         Local Start IP       N/A         Local End IP       N/A         Global Start IP       200 . 1 . 1 . 3         Global End IP       N/A	
ADVANCED SUANAT STATIC ROUTE POLICY ROUTE BW MGMT	Apply Cancel	

When we have configured all four rules in the rule summary page.

NAT Ove	erview Address M	apping Port Forv	warding Port T	riggering					
SU	SUA Address Mapping Rules								
	# Local Start IP	Local End IP	Global Start IP	Global End IP	Туре				
	1 0.0.0.0	255.255.255.255	0.0.0	N/A	M-1				
	2 N/A	N/A	0.0.0	N/A	Server				
Ful	l Feature Address M	apping Rules							
	WAN Interface WA	N 1 🔻							
	# Local Start IP	Local End IP	Global Start IP	Global End IP	Туре	Modify			
	1 0.0.0.0	255.255.255.255	0.0.0	N/A	M-1	B Û			
	2 N/A	N/A	0.0.0	N/A	Server	BÍ Û			
	3 192.168.1.10	N/A	200.1.1.1	N/A	1-1	e î			
	4 192.168.1.11	N/A	200.1.1.2	N/A	1-1	e î			
	5 192.168.1.50	192.168.1.254	200.1.1.3	N/A	M-1	<b>B</b> Î			
	6				-	<b>F</b> î			

Now we configure all other incoming traffic to go to our web server and mail server in "Port Mapping" page,

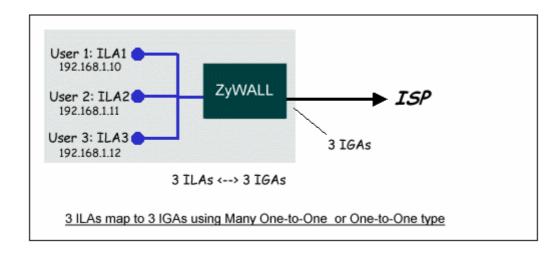
NAT Oven	view	Address Ma	pping	Port Forwarding	Port T	riggering					_	
Port	Forwa	arding Rules										
W/	WAN Interface WAN 1 💌											
De	fault S	Server		0.0.0	. 0		6	io To	Page	1 💌	[	
# /	Active	Name	In	coming Port(s)	Po	rt Translation		S	erver l	P Ad	dres	s
1	◄	web	80	- 80	80	- 80		192	. 168	. 1	•	80
2	◄	mail	25	_ 25	25	_ 25		192	. 168	. 1	•	25
3			0	_ 0	0	. 0		0	. 0	. 0		0
4			0	_ 0	0	. 0		0	. 0	. 0		0
5			0	_ 0	0	_ 0		0	. 0	. 0		0
6			0	_ 0	0	_ 0		0	. 0	. 0	•	0
7			0	_ 0	0	_ 0		0	. 0	. 0		0
8			0	_ 0	D	_ 0		0	. 0	. 0		0
9			0	_ 0	0	_ 0		0	. 0	. 0		0
10			O	_ 0	0	. 0		0	. 0	. 0		0
		'ou may also Port Translatio		create a <u>Firewall</u> tional.	rule.							

Please note that if you turn on ZyWALL's firewall function, then you should add a firewall rule from **WAN to LAN** to forward the incoming connections. If you would like to only allow traffic going to the internal server, you should specify server's private IP address in the field of the destination IP address.

ZyXEL		HELP (?)
номе	FIREWALL	
NETWORK LAN WRELESS LAN WAN DMZ SECURITY FIREWALL CONTENT FILTER VPN CERTIFICATES AUTH SERVER	Default Rule     Rule Summary     Anti-Probing     Threshold       Rule Summary       Firewall Rules Storage Space in Use       0%     1%     100%       Racket Direction: WAN to LAN       Default Policy: Block, Log	l
AUTH SERVER ADVANCED SUANAT STATIC ROUTE POLICY ROUTE BW MGMT REMOTE MGMT UPnP LOGS	Rule Active     Source Address     Destination Address     Scrube Type     Action     Schedule     Log     Alert     Modify       1     Y     Any •     192.168.1.25 •     SMTP(TCP:25) •     Forward     No     Enable     No     If       2     Y     Any •     192.168.1.80 •     HTTP(TCP:80) •     Forward     No     Disable     No     If       3     Y     Any •     192.168.1.10 •     PPTP(TCP:1723) •     Forward     No     Disable     No     If     If	l
MAINTENANCE	Insert new rule before rule 1 (rule number).           Move         rule         1         (rule number).	IJ
	Status: Ready	

#### Application for Non NAT Friendly Support

Some servers providing Internet applications such as some mIRC servers do not allow users to login using the same IP address. In this case it is better to use Many One-to-One or One-to-One NAT mapping types, thus each user login to the server is using a unique global IP address. The following figure illustrates this.



One rule configured for using Many One-to-One mapping type is shown below.

ZyXEL		HELP (?)
номе	SUA/NAT - Address Mapping	
NETWORK LAN WRELESS LAN WAN DMZ SECURITY FIREWALL CONTENT FILTER VPN CERTIFICATES AUTH SERVER	Address Mapping Rule         Type       Many One-to-One       Image: Colspan="2">Image: Colspan="2" Image: Colspan="	
ADVANCED SUA/NAT STATIC ROUTE POLICY ROUTE BW MGMT REMOTE MGMT	Apply Cancel	

The three rules configured for using **One-to-One** mapping type is shown below.

ZyXEL						
номе	SUA/NAT					
NETWORK	SUA Server	Address Mapping	Trigger Port			
LAN WIRELESS LAN WAN	Address	Mapping Setup				
DMZ		# Local Start IP	Local End IP	Global Start IP	Global End IP	Туре
SECURITY	•	1 192.168. 1. 10	N/A	200. 1. 1. 1	N/A	1-1
FIREWALL	•	2 192.168. 1. 11	N/A	200. 1. 1. 2	N/A	1-1
CONTENT FILTER		3 192.168. 1. 13	N/A	200. 1. 1. 3	N/A	1-1
VPN CERTIFICATES		4				-

Optimize network performance & availability

Using Dual WAN / Load Balancing and policy route

# **Using Dual WAN**

WAN backup (Active/Passive mode)

Condition: ZyWALL gets one public IP address

1. WAN Setup (Go to Network >> WAN)

2. LAN Setup (Go to NETWORK >> LAN)

3. DMZ Setup (Go to NETWORK >> DMZ)

4. NAT Setup (Go to ADVANCED >> NAT)

5. Firewall Setup (Go to SECURITY >> FIREWALL)

6. Setup DDNS (Go to ADVANCED >> DNS)

7. Notes about VPN Setup (Go to SECURITY >> VPN)

Load Balancing (Active/Active Mode)

- 1. WAN Setup (Go to Network >> WAN)
- 2. LAN Setup (Go to NETWORK >> LAN)

3. DMZ Setup (Go to NETWORK >> DMZ)

4. NAT Setup (Go to ADVANCED >> NAT)

5. Firewall Setup (Go to SECURITY >> FIREWALL)

6. Setup DDNS (Go to ADVANCED >> DNS)

7. Setup VPN (Go to SECURITY >> VPN)

**Using Dual WAN** 

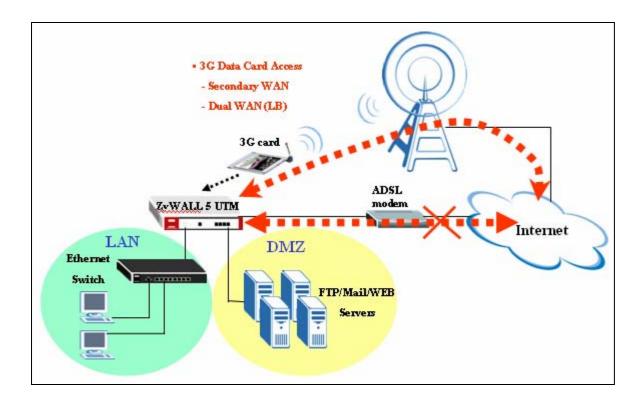
With firmware v4.02, ZyWALL 5 start to support this feature since it can insert a 3G wireless card in the PCMCIA card slot as a secondary WAN interface (WAN2). There are two operation modes for dual WAN. The "Active/Passive" is for fail-over and fall-back. And the "Active/Active" is not only for fail-over and fall-back, but also can perform load balancing to make outgoing traffic will be processed efficiently.

# WAN backup (Active/Passive mode)

With ZyWALL's **Active/Passive** mode, users can achieve backup of Internet connectivity, so when the primary WAN (normally it's lower-cost) is down, the secondary WAN (normally the 3G wireless access is higher-cost) can take over the connectivity job.

This section describes how to use ZyWALL's WAN backup feature to let ZyWALL's Internet connectivity always available including LAN users' Internet access and DMZ servers' availability.

Following is an example of a possible network topology. Company A has two Internet access methods, one is ADSL, the other is 3G wireless access. Since cost for ADSL is lower than 3G wireless access, so the IT staff decides to use ADSL for general Internet Access and 3G wireless access for backup.



LAN Segment	DMZ Segment	WAN1	WAN2
192.168.1.0/24	192.168.2.0/24	ADSL PPPoE	3G wireless access
	FTP: 192.168.2.21	dynamic	dynamic
	Mail: 192.168.2.25	NAT: Enabled(SUA)	NAT: Enabled(SUA)
	WEB: 192.168.2.80		

1. WAN Setup (Go to **Network** >> **WAN**)

**Step1**. Setup operation mode of ZyWALL. Select **Active/Passive** (**Fail Over**) **mode**. So that when WAN1 is down, WAN2 can take over connectivity. If IT staff wants to let ZyWALL fall back to WAN1 when WAN1 is available again, then check the box of "**Fall Back to Primary WAN When Possible**".

**Step2**. Configure Route Priority for WAN1 and WAN2. The metric number works like priority, lower number gets higher priority. In this example, because WAN1 is low-cost, so we set WAN1's metric number to 1, and WAN2 to 2.

**Step3.** Setup connectivity check. Specify a public IP address for WAN1 and WAN2 respectively. This IP address will be a check point for ZyWALL, ZyWALL periodically ping the IP address to check the connectivity of WAN1 and WAN2.

General	WAN 1	WAN 2 T	raffic Redirect	Dial Backup	1
Operation M	ode				-
TO 0000000000	/Passive (Fall Over) N				ר
and the second se	Fall Back to Primary \ /Active Mode	WAN When Possible	ć.		J .
Load Balancing Algorithm		n	None	-	
Route Priori	<u>۷</u>				
WAN 1		Priorit	ty (metric)	1(Highest) - 15(Lovest	
WAN 2			ty (metric) <sup>2</sup>	f(Highest) ~ 15(Lowest	<b>_</b>
Traffic Re			ty (metric) 14	1(Highest) - 15(Lovest	
Dial Back	1p	Priorit	ty (metric) <sup>15</sup>	1(Highest) - 15(Lovest	)
Connectivity	Check				
Check Per	riod		5 5-300	Seconds)	
Check Tin	neout		3 1 = 10 (54		
Check Fai	I Tolerance		3 1 = 10 (Su	ocessive Checks)	
Check	WAN 1 Connectivity				
C Ping Default Gateway			192.168.2.1		
© 1	Ping this Address		168.95.1.1		(Domain Name or IP Addre
Check	WAN 2 Connectivity				
C Ping Default Gateway		r	0.0.0		
Ping this Address			168.95.1.1		(Domain Name or IP Addre

Step4. Setup WAN1. Configure Internet Access parameters for WAN1.

General	WAN 1	WAN 2	Traffic	Redire	ct	Di	ial Backu
ISP Parame	ters for Internet Ac	cess					
Encapsula	ntion	PPP over E	themet 💌				
Service N	ame	Í			_	(0	ptional)
User Nam	e	85111279@	hinet.net				S S
Password		*******					
Retype to	Confirm						
🗆 Nailed	I-Up						
Idle Time	out	0	(Seconds)				
WAN IP Add	lress Assignment						
	utomatically from IS	21					
C Use Fi My W Remo	ixed IP Address (AN IP Address ote IP Subnet Mask ote IP Address		0	. 0		0. 0.	0
C Use Fi My W Remo	xed IP Address AN IP Address ote IP Subnet Mask ote IP Address		0	. 0		Ο.	0
C Use Fi My W Remo Remo Advanced S	xed IP Address AN IP Address ote IP Subnet Mask ote IP Address		0	. 0		Ο.	0
C Use Fi My W Remo Remo Advanced S	xed IP Address (AN IP Address ote IP Subnet Mask ote IP Address etup e NAT (Network Add		0	. 0		Ο.	0
♥ Use Fi My W Remo Remo Advanced S	xed IP Address (AN IP Address ote IP Subnet Mask ote IP Address etup e NAT (Network Add tion		) )	. 0 . 0		Ο.	0
<ul> <li>C Use Fi My W Remo Remo</li> <li>Advanced S</li> <li>☑ Enable</li> <li>RIP Direct</li> <li>RIP Version</li> </ul>	xed IP Address (AN IP Address ote IP Subnet Mask ote IP Address etup e NAT (Network Add tion		) Nor	. 0 . 0		Ο.	0
<ul> <li>C Use Fi My W Remo</li> <li>Remo</li> <li>Re</li></ul>	xed IP Address (AN IP Address ote IP Subnet Mask ote IP Address etup e NAT (Network Add tion		) Nor RIP	. 0 . 0	-	Ο.	0
<ul> <li>C Use Fi My W Remo</li> <li>Remo</li> <li>Remo</li> <li>Remo</li> <li>Remo</li> <li>Remo</li> <li>Remo</li> <li>RiP Direct</li> <li>RIP Direct</li> <li>RIP Versio</li> <li>I Enable</li> <li>Multica</li> </ul>	xed IP Address (AN IP Address ote IP Subnet Mask ote IP Address etup e NAT (Network Add tion on	dress Translation	) Nor RIP	. 0 . 0	-	Ο.	0

**Step5**. Setup WAN2. Switch to GUI menu **Network** > **WAN2** tab. Configure the APN, username, password, PIN code, phone number, the authentication type and other further settings got from your service provider. Click **Apply** button then.



General	WAN 1	WAN 2	Traffic Redirect	Dial Backup	
ISP Parame	ters for Internet /	Access			
3G Wireles	s Card	AC850			
Access Poir	nt Name (APN)				
User Name					
Password					
Retype to (	Confirm				
PIN Code					
Phone Num	iber				
Authenticat	tion Type	CHAP/PAP 💌			
🗐 Nailed-	Up				
Idle Timeo	ut	100 (Sec	:onds)		
WAN IP Add	ress Assignment	_			_
🖲 Get Au	tomatically from ISF	e			
🕤 Use Fix	ed IP Address				
My Wi	AN IP Address		0 7 0 4	0 // 0	
Advanced S	etup	_			_
🔽 Enable	NAT (Network Addr	ess Translation)			
🗖 Enable	Multicast				
Multica	st Version		IGMP-v1		

2. LAN Setup (Go to NETWORK >> LAN)

Leave the setup as default.

LAN	Static DHCP	IP Alias		
LAN TCP/	IP			
IP Addr	ess	192 . 168 . 1 . 1	RIP Direction	Both •
IP Subr	net Mask	255 . 255 . 255 . 0	RIP Version	RIP-1 *
Multica	st	None 💌		_
DHCP Set	սթ			
₽ DHC	CP Server			
IP Pool	Starting Address	192 . 168 . 1 . 33	Pool Size	128
Windows	Networking (NetBI	OS over TCP/IP)		
	w between LAN an	d WAN (You also need to create a firewall rule)	)	
	w between LAN an			
		Apply	Reset	

3. DMZ Setup (Go to NETWORK >> DMZ)

Give ZyWALL's DMZ a private IP address other than LAN segment.

DMZ TCP/IP	
IP Address	192 . 168 . 2 . 1
IP Subnet Mask	255 . 255 . 255 . 0
RIP Direction	Both 💌
RIP Version	RIP-1 ·
Multicast	None 💌
Windows Networking (NetBIO	S over TCP/IP)
C Allow between DMZ and	d LAN (You also need to create a firewall rule!)
F Allow between DMZ and	
Allow between DMZ and	3 WAN

#### 4. NAT Setup (Go to **ADVANCED** >> **NAT**)

**Step1**. Choose Address Mapping rules for WAN1 and WAN2. Turn on the NAT function of WAN2. And the settings are just the same as what you configure on WAN1.



NAT Overview	Address Mapping	Port Forwarding	Port Triggering
Global Settin	igs		
	rent Sessions rent Sessions Per Hos ion Mode	6000 t 4000 (H Active/Passiv	listorical high since last startup: 12) re Fail Over
WAN 1			
🖲 SUA	1apping Rules		
Port Forw-	arding Rules		Copy to WAN 2
Port Trigg	ering Rules		2 Copy to WAN 2
WAN 2			
♥ Enable M Address M ● SUA	1apping Rules		
Port Forw-	arding Rules		Copy to WAN 1
Port Trigg	ering Rules		2 Copy to WAN 1
	Apply		Reset

**Step 2**. Configure Port Forwarding. Setup the port forwarding for HTTP/FTP/MAIL ports based on WAN1 interface.

2		Address M		Port Forwarding	Futth	iggering					
Port	Forw	rarding Rules									
W	AN In	terface		WAN 1 💌							
De	fault	Server		0.0.0	. 0		Go To	Page	1	-	
11	Activ	e Name	Inco	oming Port(s)	Por	t Translation		Server	IP A	ddre	155
1	•	HTTP	80	. 80	80	. 80	192	. 168	).	2.	. 80
2	7	FTP	21	. 21	21	. 21	192	. 168	۱.	2 .	. 21
3	V	MAIL	25	. 25	25	. 25	192	. 168	۱.	2 .	. 2
4	Г		0	. 0	0		0	. 0	S 20	0	. 0
5	Г	-	0	. 0	0	.p	0	. 0	•	ο,	. 0
6	Г		0	. 0	0	.0	0	. 0		0,	. 0
7	Г		0	. 0	0	.0	0	. 0	•	0 .	. 0
8	Г		0	. 0	0	.0	0	. 0		0	. 0
9	Г		0	. 0	0	.0	0	. 0		0,	. 0
10	Г		0	. 0	0	.0	0	. 0		0 .	. 0

5. Firewall Setup (Go to **SECURITY** >> **FIREWALL**)

Step1. Enable Firewall.

**Step2**. Make sure traffic from "**WAN to DMZ**" is '**Forward**'. If you change Default Action to 'Block', then please proceed for Step3. Otherwise, you have finished firewall setting.

NUMBER OF TAXABLE PARTY.	PR Destance			
Default Ru	le Setup			
🖂 Ena	ble Firewall			
			this box is checked, all LAN to LA	N, WAN to WAN an
to D	MZ packets will bypas	s the Firewall che	ск.)	
	Packet Directio	n yapanananananii 1.	Default Action	anal lananas Log ta
	LAN to LAN / ZyWALL		Forward 💌	Г
	LAN to WAN		Forward 💌	Г
	LAN to DMZ		Forward -	<b></b>
	WAN to LAN		Block .	<u>a</u>
:	WAN to WAN / ZyW	ALL	Block	
	WAN to DMZ		Forward 💌	Г
	DMZ to LAN		Block •	2
	DMZ to WAN		Forward •	Г
	DMZ to DMZ / ZyW	ALL	Block 💌	2
			,	

Step3. Setup firewall rule to forward traffic from "WAN to DMZ"

Rule	Summary	1								
Fire	wall Rul	es Storage Spa	ace in Use							
0%				15					10	0%
Rule	Active	Source Address	Destination Address	Service Type	an and a set of the	Schedule	Log	Alert	Mo	life
<b>D</b> 1	Y	Any 💌	192.168.2.80 💌	HTTP(TCP:80)	Forward	No	Disabled	No	3	Ę
<b>D</b> 2	Y	Any 💌	192.168.2.21 💌	FTP(TCP:20,21)	Forward	No	Disabled	No	3	ť
5700		Any 🔻	102 100 2 25	SMTP(TCP:25)	Conward	No	Disabled	No	3	F

### 6. Setup DDNS (Go to **ADVANCED** >> **DNS**)

In this example, since WAN1 and WAN2's IP address are dynamic and WAN2 will take over the

connectivity when WAN1 is down. This means the remote users may need to use dynamic domain name and turn on HA (High Availability) option so that remote users can always find the servers no matter which interface is on.

	C Active Servic Userna Passw	e Provider ame	WWW.D support	ynDNS	.ORG	_		
	My Domain D	Names Iomain Name	DDNS Type	Offline	Wildcard	WAN	IP Address Update Policy	НА
	Turveleurope	rt.dyndns.org	Dynamic 💌	Г	Г	WAN 1 💌	Let DDNS Server Auto Detect	• 17
1	zyxeisuppu					The second second second		_
			Dynamic 💌	Г		WAN 1 -	Use WAN IP Address	
-	1		Dynamic 💌			and the second s	and a second	
2	1		and the second design of the s			WAN 1 💌	Use WAN IP Address	

7. Notes about VPN Setup (Go to **SECURITY** >>**VPN**)

VPN setup example requires a clear scenario for two VPN gateways. Please refer to IPSec application notes for the scenario. Here, we describe notes users should take when setup VPN in multiple WAN environment.

**Note1**. If your ZyWALL has dynamic WAN IP address like this example, or you want the VPN always available no matter VPN go through WAN1 or WAN2, and then you should choose pre-configured DDNS instead.

Gateway Information								
My Address	_							1
IP Address		•	0	•	0	•	0	
💿 My Domain Name	ZyX	elsu	ipro	rt. 1	ynd	ns.a	org 💌	(See <u>DDNS</u> )

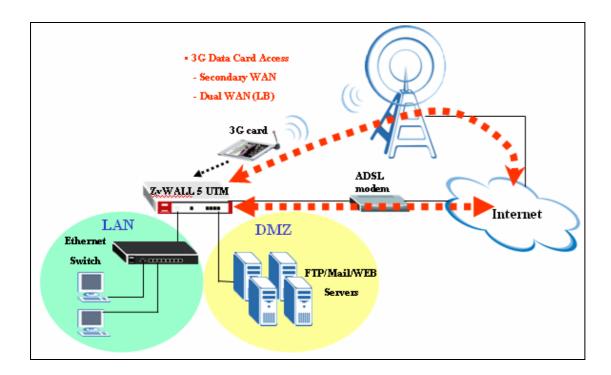
### Load Balancing (Active/Active Mode)

With ZyWALL's load balancing function, users can utilize WAN1 and WAN2 interface at the same time. Every time new outgoing TCP sessions come to ZyWALL's LAN or DMZ, ZyWALL will decide which WAN interface to throw the packet out. The connection is then controlled by a session manager inside ZyWALL to make sure every packet going back and forth of this TCP session will go out through the same interface as the initial one. Similar mechanism is also applied to UDP/ICMP traffic to make sure the returned packets always go through the same interface as the first one. Following we introduce three different methods ZyWALL's WAN1 and WAN2 share Internet loading.

**Least Load First**: ZyWALL measures outbound loading, inbound loading or outbound + inbound loading within a preset time frame.

**Weighted Round Robin**: ZyWALL decides the loading ratio of WAN1 and WAN2. For example if 9:2 is setup, this means the number of TCP sessions going from WAN1 and WAN2 in average is 9 to 2.

**Spill Over**: A threshold is preset for primary WAN, once the loading exceeds the threshold within a measured period of time, the secondary WAN will take over. Once the loading of primary WAN decreases, then the next session will go through the primary WAN.



LAN Segment	DMZ Segment	WAN1	WAN2
192.168.1.0/24	192.168.2.0/24	Ethernet	3G wireless access
	FTP: 192.168.2.21	211.63.1.0/28	Dynamic
	Mail: 192.168.2.25	NAT Type: Full Feature	NAT Type: SUA
	WEB: 192.168.2.80		

8. WAN Setup (Go to **Network** >>**WAN**)

**Step1**. Setup operation mode of ZyWALL. Select **Active/Active Mode**. Choose one of the Load Balancing Algorithm, for example **Weighted Round Robin**. Give a ratio to each interface.

**Step2**. Configure Route Priority for WAN1 and WAN2. The metric number works like priority, lower number gets higher priority. In this example, because WAN1 is low-cost, so we set WAN1's metric number to 1, and WAN2 to 2.

**Step3**. Setup connectivity check. Specify a public IP address for WAN1 and WAN2 respectively. This IP address will be a check point for ZyWALL, ZyWALL periodically ping the IP address to check the connectivity of WAN1 and WAN2.

General	WAN 1	WAN 2	Traffic Redirect	Dial Backup	
Operation N	lode				
C Active	/Passive (Fail Over	Mode			
	Fall Back to Primar		ossible		
	Active Mode		3/100		
223.69	d Balancing Algorit	MGE	Weighted Round	-Robin 📩	
and the second se	terface Rat	io			
	VAN 1 9	(0 ~ 10)			
L V	VAN 2 2	(0 - 10)			
Route Priori	ity				
WAN 1			Priority (metric)	- 1(Highest) ~ 15(Lowest)	
WAN 2			Priority (metric)	- 1(Highest) - 15(Lowest)	na s
Traffic Re	direct		Priority (metric) 14	1(Highest) = 15(Lowest)	-
Dial Back	up		Priority (metric) 15	1(Highest) ~ 15(Lowest)	
Connectivity	/ Check				
Check Pe	riod		5 5 - 300 (5		
Check Tir	neout		3 1 = 10 (Sec		
Check Fa	il Tolerance			cessive Checks)	
Check	WAN 1 Connectivit	w			
Data 934030.00	Ping Default Gatew		192.168.2.1		
۲	Ping this Address	970.	168.95.1.1		(Domain Name or IP )
Check	WAN 2 Connectivi	v			
1000 C	Ping Default Gatew		211.62.22.15		

Step4. Setup WAN1. Configure Internet Access parameters for WAN1.

General	WAN 1	WAN 2	Traffic Redirect	Dial Backu
ISP Parame	ters for Internet Ac	cess		
Encapsula	ition	Ethernet	•	
Service Ty	ype	Standard	-	
WAN IP Add	ress Assignment			
🔿 Get Aı	utomatically from I	SP		
• Use Fi	xed IP Address		22	
My W	AN IP Address		211 . 63 .	1.1
My W	AN IP Subnet Mask	¢	255 . 255 . 2	255 . 240
Gatev	way IP Address		211 . 63 .	1.15
Advanced S	etup			
🔽 Enable	e NAT (Network Ad	dress Translation)		
RIP Direct	tion		None 💌	
<b>RIP Versio</b>	on		RIP-1	
🗖 Enable	e Multicast			
	ast Version		IGMP-v1	
Multica				
	WAN MAC Address	\$		

Step5. Setup WAN2. Configure Internet Access parameters for WAN2.

General	WAN 1	WAN 2	Traffic Redirect	Dial Backup			
ISP Parame	ters for Internet Ac	cess					
Encapsula	ation	PPP over Et					
Service Name							
User Nam	e	85111279@h	85111279@hinet.net				
Password							
Retype to	Confirm	******					
🗖 Naileo	d-Up						
Idle Time	out	0 (;	Seconds)				
WAN IP Add	Iress Assignment						
· Get A	utomatically from I	SP					
🔿 Use Fi	ixed IP Address		2				
My W	AN IP Address		0.0.	0.0			
Remo	ote IP Subnet Mask		0.0.	0.0			
Remo	ote IP Address		0.0.	0.0			
Advanced S	etun						

### 9. LAN Setup (Go to **NETWORK** >>LAN)

Leave the setup as default.

LAN	Static DHCP	IP Alias		
LAN TCP/IP				
IP Address		192 . 168 . 1 . 1	RIP Direction	Both 💌
IP Subnet M	ask	255 . 255 . 255 . 0	RIP Version	RIP-1 ·
Multicast		None 💌		
DHCP Setup				
DHCP Se	over			
	ing Address	192 . 168 . 1 . 33	Pool Size	128
Windows Netw	orking (NetBIO	S over TCP/IP)		
C Allow he	human I AN and	WAN (You also need to create a firewall rule!)		
	tween LAN and			
		Apply	Reset	

10. DMZ Setup (Go to NETWORK >>DMZ)

Give ZyWALL's DMZ a private IP address other than LAN segment.

DMZ TCP/IP	
IP Address	192 . 168 . 2 . 1
IP Subnet Mask	255 . 255 . 255 . 0
RIP Direction	Both
RIP Version	RIP-1 •
Multicast	None 💌
Windows Networking (NetBl	nd LAN (You also need to create a finewall rule!)

11. NAT Setup (Go to ADVANCED >>NAT)

Step1. Setup the NAT (Network Address Translation) for WAN1 and WAN2.

NAT Overview	Address Mapping	Port Forwarding	Port Triggering	
Global Settin	igs			
	rent Sessions rent Sessions Per Hos ion Mode	6000 t 4000 (F Active/Passiv	Historical high since last startup: 12) ve Fail Over	
WAN 1				
C SUA	1apping Rules			
💿 Full	Feature			
Port Forw	arding Rules		0 Copy to WAN 2	
Port Trigg	ering Rules		2 Copy to WAN 2	
WAN 2				
✓ Enable N Address N ● SUA	1apping Rules			
🔘 Full	Feature			
Port Forw	arding Rules		0 Copy to WAN 1	
Port Trigg	ering Rules		2 Copy to WAN 1	
	Apply		Reset	

Step2. Setup Address Mapping and Port Forwarding for WAN1.

AT Overv	iew Address M	lapping Port For	warding Port Ti	riggering		
SUA /	Address Mapping	Rules				
#	Local Start IP	Local End IP	Global Start IP	Global End IP	Туре	
1	0.0.0	255.255.255.255	0.0.00	N/A	M-1	
2	N/A	N/A	0.0.0	N/A	Server	
	eature Address M	apping rates				
WA	N Interface	WAN 1	•		Go To Pa	ge 1 💌
WA			▼ Global Start IP	Global End IP	Go To Pa Type	ige <mark>1 •</mark> Modify
	N Interface	WAN 1		Global End IP N/A	000000000000	Settlemonerie
	N Interface Local Start IP	WAN 1	Global Start IP	CARA CONTRACTOR	Туре	Modify
# 1	N Interface Local Start IP 192.168. 2. 80	WAN 1 Local End IP N/A	Global Start IP 211. 63. 1. 2	N/A	Type 1-1	Modify

Step3. Configure Port Forwarding for FTP/MAIL services.

AT Overview	Address Ma	pping P	ort Forwarding	Port Tri	iggering	_		_	_	_
Port Forw	arding Rules									
WAN In	terface	Γ	WAN 1 💌							
Default	Server	ſ	0.0.0	. 0		Go To	o Pag	e 1	•	
# Active	Name	Inco	ning Port(s)	Por	t Translation		Serve	r IP	Ade	Ires
1 💌	FTP	21	. 21	21	. 21	192	. 18	8.	2	
2 🔽	Mail	25	. 25	25	. 25	192	. 16	8.	2	•
3 🗖		0	+ 0	0		0	. 0		0	
4 🗖		0	- 0	D		0	. 0	1	0	54
5 🔽		0	.0	0		0	. (	).	0	
6 🗖		0	- 0	0		0	. 0	۰. ا	0	
7 🗖		0	.0	0		0	. 0		0	
8		0	.0	0	.0	0	. (	).	0	۰.
9 🔲		0	. 0	0		0	. 0	1 12	0	4
10		0	.0	0	.0	0	. 0	).	0	

### 12. Firewall Setup (Go to **SECURITY** >> **FIREWALL**)

Step1. Enable Firewall.

**Step2**. Make sure traffic from "**WAN to DMZ**" is '**forward**'. If you change Default Action to block, then please proceed for Step3. Otherwise, you have finished firewall.

Default Rule	Rule Summary Anti-Probing	1. Sectored and the sec	
Default Ru	le Setup		
🔽 Ena	ble Firewall		
Allo	w Asymmetrical Route (Warning: Whe	n this box is checked, all LAN to LA	N, WAN to WAN an
to D	MZ packets will bypass the Firewall ch	leck.)	
	Packet Direction	Default Action	Log
	LAN to LAN / ZyWALL	Forward -	F
	LAN to WAN	Forward 💌	Г
	LAN to DMZ	Forward 💌	Г
	WAN to LAN	Block -	1
	WAN to WAN / ZyWALL	Block ·	1
	WAN to DMZ	Forward 💌	Г
	DMZ to LAN	Block 💌	5
	DMZ to WAN	Forward -	Г
	DMZ to DMZ / ZyWALL	Block 💌	2

Step3. Setup firewall rule to forward traffic from "WAN to DMZ"

Rule	Summary	/								
Fi	rewall Rul	es Storage Spa	ace in Use							
0				1%					10	05
Ru	le Active	Address	Address	Service Type		Schedule	Log	Alen	Mo	
D	1 Y	Any 💌	192.168.2.80 💌	HTTP(TCP:80) •	Forward	No	Disabled	No	3	1
	2 <u>Y</u>	Any 💌	192.168.2.21 💌	FTP(TCP:20,21)	Forward	No	Disabled	No	3	Ę
	3 Y	Any 💌	192.168.2.25 .	SMTP(TCP:25) ·	Forward	No	Disabled	No	3	1

13. Setup DDNS (Go to **ADVANCED** >> **DNS**)

Because WAN1 uses two IP addresses for the FTP/HTTP/MAIL servers, users need to update these two IP addresses. To let the servers still accessible, users have to turn on **HA** for both entries.

System	Cache	LAN	DDNS			
Account Set	tup					
Active						
Servic	e Provider		nDNS.ORG			
oserna	Inne	support				
Passw	ord	******				
My Domain	Names			WAN		
My Domain			OfflineWildcard	WAN	IP Address Update Po	olic
My Domain	Names		Offline Wildcard	Interiore	Use User Defined	olic

14. Setup VPN (Go to **SECURITY** >> **VPN**)

**Note1**. If you are sure to make VPN always go through WAN1, then specify WAN1's IP address in My Address field.

Gateway Information								
My Address								
IP Address	211	•	63	•	1	•	1	
🔿 My Domain Name	zyxe	elsi	Jppo	rt1.	dyn	dns	.org	(See <u>DDNS</u> )

**Note 2**. If you want the VPN always available no matter VPN go through WAN1 or WAN2, then you should choose pre-configured DDNS instead.

Gateway Information							
My Address	_						
IP Address	0	•	0	•	0		0
💿 My Domain Name	zyx	elsı	Jbbo	rt1.	dyn	dns	.org 💌 (See <mark>DDNS</mark> )

### **Using Policy Route**

The relationship of ZyWALL handles traffic between policy route and Load Balancing is as following.

(1) <u>Traffic from WAN:</u> -> NAT -> FW -> **Policy Route** -> **Load Balance** -> Static Route -> IDP -> AV -> AS -> CF -> BWM

(2) <u>Traffic to WAN:</u> -> FW -> **Policy Route** -> **Load Balance** -> Static Route -> IDP -> AV -> AS -> CF -> BMW -> NAT

That means, user still can assign which WAN interface to process specific traffic which load balance mechanism is chosen. Following is the example to assign VOIP traffic from LAN will be handled by WAN2.

Criteria	
Active	1
IP Protocol	Predefined 💌 TCP (6) 💌
Type of Service	Any
Precedence	Any 💌
Packet Length	0
Length Comparison	Equal
Source	
Interface	
Starting IP Address	
Ending IP Address	192 , 168 , 1 , 255
Starting Port	5060
Ending Port Destination	5060
Starting IP Address	0.0.0.0
Ending IP Address	0.0.0.0
Starting Port	
Ending Port	
Action Applies to	Matched Packets.
Routing Action	
Gateway	
O User-Defined	0.0.0.0
WAN Interface	WAN 2 💌
	he specified WAN interface is not available.
Converted Type of Service	Don't Change 💌
Converted Precedence	Don't Change 💌
Log	Yes 💌

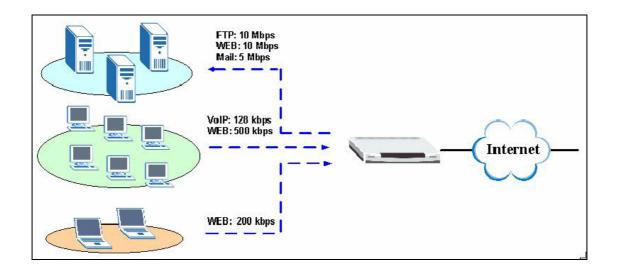
After it's done, the outgoing VOIP traffic with source port 5060 from 192.168.1.x network will be always processed by WAN2 except WAN2 is not available. Since we choose 'Use another interface when the specified WAN interface is not available', when WAN2 is down, the traffic will be handled by WAN1 then.

For other outgoing traffic not defined in policy route will be assigned to either WAN1 or WAN2 when traffic reaches session manager in ZyWALL.

### **Using Bandwidth Management**

### Why Bandwidth Management (BWM)?

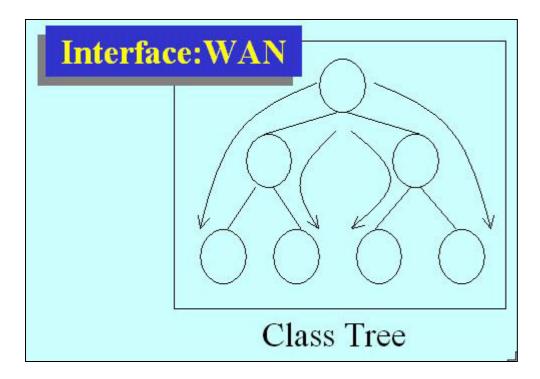
Nowadays, we have many different traffic types for Internet applications. Some traffic may consume high bandwidth, such as FTP (File Transfer Protocol), if you are downloading or uploading files with large size. Some other traffic may not require high bandwidth, but they requires stable supply of bandwidth, such as VoIP traffic. The VoIP quality would not be good, if all of the outgoing bandwidth is occupied via FTP. Additionally, chances are that you would like to grant higher bandwidth for some body special who is using specific IP address in your network. All of these are reasons why we need bandwidth management.



How Bandwidth Management in ZyWALL?

ZyWALL achieves BWM by classifying packets, and control when to send out the classified packets. Bandwidth Management of ZyXEL appliances operates on the IP layer. The major step to configure BWM is defining filter rules by fields of IP header or TCP/UDP port number. Then specify the volume of bandwidth you want to allocate to the filtered traffic. There are two types of BWM in ZyXEL implementations, Full and Lite versions.

**Full version:** Supported in SMB level devices, such as ZyWALL100, ZyWALL 70...etc. Users can define how they want to classify traffic on each interface. In this version, child-class can borrow bandwidth from parent-class if necessary by **Bandwidth Borrowing**. For classes that need more bandwidth even after bandwidth borrowing, users can also apply **Maximize Bandwidth Usage** from the interface.



### Using BWM

Go to ADVANCED->BW MGMT->Summary, activate bandwidth management on the interface you would like to manage. We enable the BWM function on WAN1 interface in this example. Enter the total speed for this interface that you want to allocate using bandwidth management. This appears as the bandwidth budget of the interface's root class.

Select how you want the bandwidth to be allocated. Priority-Based means bandwidth is allocated via priority, so the traffic with highest priority would be served first, then the second priority is served secondly and so on. If Fairness-Based is chosen, then the bandwidth is allocated by ratio. Which means if A class needs 300 kbps, B class needs 600 kbps, then the ratio of A and B's actual bandwidth is 1:2. So if we get 450 kbps in total, then A would get 150 kbps, B would get 300 kbps.

Summary	Class Setup	Monitor		
Bandwidth	Management Setu	ıp		
				specific interface. BW Manager
		ependently for each i		
Class	Active	Speed (kbps)	Scheduler	Maximize Bandwidth Usage
WAN1		1500	Priority-Based 💌	
		100000	Fairness-Based 💌	
WAN2				
WAN2 LAN		100000	Fairness-Based 💌	
		100000	Fairness-Based 💌	
LAN				

## **Key Settings:**

Active	Check the box to enable BWM on the interface. Note that if you would like to manage traffic from <b>WAN to LAN</b> , you should apply BWM on <b>LAN</b> interface. If you would like to management traffic from <b>WAN to DMZ</b> , please apply BWM on <b>DMZ</b> interface.
Speed	Enter the total speed to manage on this interface. This value is the budget of the class tree's root.
Scheduler	Choose the principle to allocate bandwidth on this interface. <b>Priority-Based</b> allocates bandwidth via priority. <b>Fairness-Based</b> allocates bandwidth by ratio.
Maximize Bandwidth Usage	Check this box if you would like to give residuary bandwidth from Interface to the classes who need more bandwidth than configured amount. Do not select this if you want to reserve bandwidth for traffic that does not match a bandwidth class or you want to limit the bandwidth of each class at the configured value. (Please note that to meat the second condition, you should also disable bandwidth borrowing on the class.)

Go to **ADVANCED->BW MGMT->Class Setup**, select the interface on which you would like to setup the Class tree.

Click the radio button besides the Root Class, then press 'Add Sub-Class'

Class Configuration	
Class Name	Арр
Bandwidth Budget	300 (Kbps)
Priority	3 (0-7)
🗖 Borrow bandwidth from parent c	lass
Filter Configuration	
🔽 Enable Bandwidth Filter	
Destination IP Address	211 . 1 . 1 . 1
Destination Subnet Mask	255 . 255 . 255 . 0
Destination Port	2121
Source IP Address	192 . 168 . 1 . 0
Source Subnet Mask	255 . 255 . 255 . 0
Source Port	
Protocol ID	0

### Key Settings:

5 0	
Class Name	Give this class a name, for example, 'App'
Bandwidth Budget	Configure the speed you would like to allocate to this class
Priority	Enter a number between 0 and 7 to set the priority of this class. The higher the number, the higher the priority. The default setting is 3.
Bandwidth Borrowing	Check this box if you would like to let this class to borrow bandwidth from it's parents when the required bandwidth is higher than the configured amount. Do not check this if you want to limit the bandwidth of this class at the configured value.(Please note that you should also disable <b>Maximize Bandwidth Usage</b> on the interface to meat the condition.)
Enable Bandwidth Filter	Check this to specify the traffic types via IP addresses/Port numbers.
Destination IP Address	Enter the IP address of destination that meats this class.
Destination Subnet Mask	Enter the destination subnet mask.
Destination Port	Enter the destination port number of the traffic.

Source IP Address	Enter the IP address of source that meats this class. Note that for traffic from <b>'LAN to WAN'</b> , since BWM is before NAT, you should use the IP address before NAT processing.
Source Subnet Mask	Enter the destination subnet mask.
Source Port	Enter the source port number of the traffic.
Protocol ID	Enter the protocol number for the traffic. 1 for ICMP, 6 for TCP or 17 for UDP

After configuration BWM, you can check current bandwidth of the configured traffic in

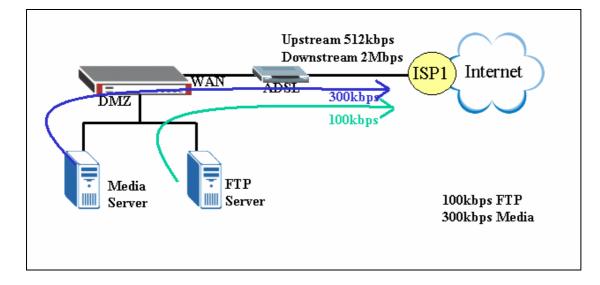
**ADVANCED->BWM MGMT->Monitor.** The values in the column of **Current usage (kbps)** would display the actually number.

s) Current Usage (kbps)				
300 300				

Scenario 1 - Limit (protect) bandwidth usage for ADSL uplink bandwidth

Description

We have a 2M/512kbps ADSL link. At DMZ side, we have one FTP server and one media server, suppose we want to restrict upload FTP traffic at 100kbps, while restrict streaming traffic at 300kbps

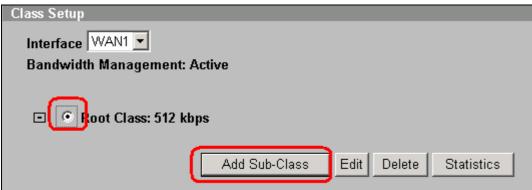


Step1.

Activate Bandwidth Management on the interface on which you want to control. In this example, it is WAN1. Assign the bandwidth of the ADSL upstream because Bandwidth Management only manages traffic that "flow out" the router's interface.

Bandwidt	h Management Setu	In		
	, i i i i i i i i i i i i i i i i i i i			
		bandwidth of traffic f ependently for each i		e specific interface. BW Manager
Class	Active	Speed (kbps)	Scheduler	Maximize Bandwidth Usage
WAN1		512	Fairness-Based V	
WANZ		100000	Fairness-Based -	
	·			
LAN		100000	Fairness-Based 💌	
DMZ		100000	Fairness-Based 🔻	

Step2. Go to "Class Setup". Click on Root Class and then click on "Add Sub-Class" to create and add a new class under root.



We add a service and allocate 100kbps for FTP. Select the Service as FTP from drop-down list. Specify

FTP server's IP address as Source IP address.

Class Configuration	
Class Name	FTP
Bandwidth Budget	100 (Kbps)
Priority	3 (0-7)
🗖 Borrow bandwidth from parent class	
Filter Configuration	
Enable Bandwidth Filter	
Service	FTP 💽
Destination IP Address	0.0.0.0
Destination Subnet Mask	0.0.0.0
Destination Port	0
Source IP Address	192 . 168 . 1 . 21
Source Subnet Mask	255 . 255 . 255 . 255
Source Port	0
Protocol ID	0

Step3. Add another class, Medial. In this case the server IP address is 192.168.1.10 and it uses UDP for streaming. We allocate 300kbps for Media. Select the **Service** as Custom and assign Protocol ID to 17 for UDP.

Class Configuration	
Class Name	Madia
	Media
Bandwidth Budget	300 (Kbps)
Priority	3 (0-7)
🗖 Borrow bandwidth from parent class	
Filter Configuration	
🗹 Enable Bandwidth Filter	
Service	Custom 💌
Destination IP Address	0.0.0.0
Destination Subnet Mask	0.0.0.0
Destination Port	0
Source IP Address	192 . 168 . 1 . 10
Source Subnet Mask	255 . 255 . 255 . 255
Source Port	0
Protocol ID	17

Step 4. Now, two services are added. (FTP & Media)

	p e WAN1 💌 dth Manager	nent: Active	3				
• • 	Root Class: - • FTP: 10 - • Media:	O kbps 300 kbps	Add Sub-Class Edit	Delete St	atistics		
Filter List							
# Fi	ilter Name	Service	Destination IP Address	Destination Port	Source IP Address	Source Port	Protocol ID
1	FTP Media	FTP	0.0.0/0	0	192.168.1.21/32 192.168.1.10/32	0	0
2	meula	n/a	0.0.0/0	U	192.100.1.10/32	U	17

When you go to Monitor, one Default Class is created automatically and its bandwidth is the reset. This class will apply to other kind of traffic like HTTP.

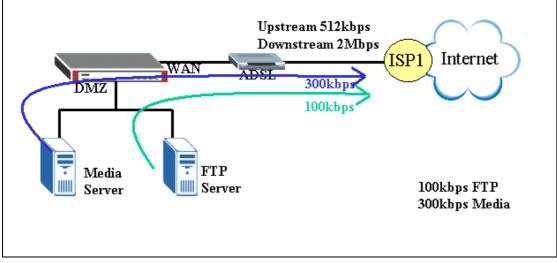


Summary	Class Setup	Monitor	
Monitor			
Interfac	e WAN1 🗸	Budget (kbps)	Current Usage (kbps)
Root Cla		512	0
		100	0
FTP			
FTP Media		300	0

**Scenario 2** - Limit bandwidth usage but hope to use bandwidth as many as possible for specific FTP traffic.

#### Description

Suppose we have the same topology as scenario 1. We want FTP can be transferred in higher rate when there is extra bandwidth.



#### Step1.

Activate Bandwidth Management on the interface on which you want to control. In this example, it is WAN1. Assign the bandwidth of the ADSL upstream because Bandwidth Management only manages traffic that "flow out" the router's interface.

Bandwi	dth Management Setu	p		
				e specific interface. BW Manager
can b	e switched on/off inde	ependently for each	interface.	
Clas	ss Active	Speed (kbps)	Scheduler	Maximize Bandwidth Usage
NAW NAW	11 🔽	512	Fairness-Based 💌	
WA	12 🗆	100000	Fairness-Based 💌	
LAI	٦ ا	100000	Fairness-Based 💌	
DM	Z 🗆	100000	Fairness-Based 💌	

Step2. Go to "Class Setup" and add a new class under root. We add a service and allocate 100kbps for FTP. Select the **Service** as FTP from drop-down list. Specify FTP server's IP address as Source IP address. Enable "**Borrow bandwidth from parent class**"

Class Name	FTP
Bandwidth Budget	100 (Kbps)
Priority	3 (0-7)
Borrow bandwidth from parent class	
Iter Configuration	
Enable Bandwidth Filter	
Service	FTP 👤
Destination IP Address	0.0.0.0
Destination Subnet Mask	0.0.0.0
Destination Port	0
Source IP Address	192 . 168 . 1 . 21
Source Subnet Mask	255 . 255 . 255 . 255
Source Port	

Step3. Add another class, Medial. In this case the server IP address is 192.168.1.10 and it uses UDP for streaming. We allocate 300kbps for Media. Select the **Service** as Custom and assign Protocol ID to 17 for UDP.

Class Configuration	
Class Name	Media
Bandwidth Budget	300 (Kbps)
Priority	3 (0-7)
🗖 Borrow bandwidth from parent class	
Filter Configuration	
Enable Bandwidth Filter	
Service	Custom 💌
Destination IP Address	0.0.0.0
Destination Subnet Mask	0.0.0.0
Destination Port	0
Source IP Address	192 . 168 . 1 . 10
Source Subnet Mask	255 . 255 . 255 . 255
Source Port	D
Protocol ID	17

Step 4. Now, two services are added. (FTP & Media) We expect that when there is not real-time UDP traffic, class 1 can use up to 512kbps for FTP.

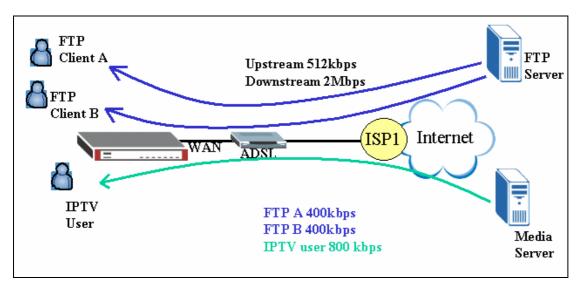
**Scenario 3** - Limit bandwidth usage, but when there is residual bandwidth, we hope it can be shared fairly among several active traffic.

### Description

FTP Client A can get 400kbps FTP traffic and FTP Client B can get 800 kbps FTP traffic and IPTV user can retrieve 800 kbps UDP streaming.

LAN Interface: Fairness-based, Speed = 2048kbps

Class 1: Budget = 400kbps, Dest. IP = FTP Client A's IP, Service = FTP, Priority = 3, enable Borrow Class 2: Budget = 800kbps, Dest. IP = FTP Client B's IP, Service = FTP, Priority = 3, enable Borrow Class 3: Budget = 800kbps, Dest IP = IPTV Client's IP, Protocol = UDP.

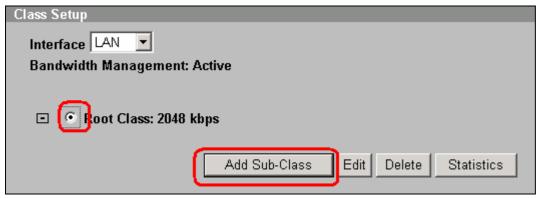


Step1.

Activate Bandwidth Management on the interface on which you want to control. In this example, it is LAN. Assign 2048Kbps to LAN interface.

BW Manage				specific interface. BW Manager
Class	Active	Speed (kbps)	Scheduler	Maximize Bandwidth Usage
WAN1		100000	Fairness-Based 💌	
WAN2		100000	Fairness-Based 💌	
LAN		2048	Fairness-Based 💌	
DMZ		100000	Fairness-Based 💌	

Step2. Go to "Class Setup" and select LAN from the drop-down list of Interface. Click on Root Class and then click on "Add Sub-Class" to create and add a new class under root.



We add a service and allocate 400kbps for FTP and destined to FTP Client A. Select the **Service** as FTP from drop-down list. Input Client A's IP address as Destination IP Address.

Class Configuration	
Class Name	FTP_A
Bandwidth Budget	400 (Kbps)
Priority	3 (0-7)
Borrow bandwidth from parent class	
Filter Configuration	
Enable Bandwidth Filter	
Service	FTP 👤
Destination IP Address	192 . 168 . 1 . 33
Destination Subnet Mask	255 . 255 . 255 . 255
Destination Port	0
Source IP Address	0.0.0.0
Source Subnet Mask	0.0.0.0
Source Port	0
Protocol ID	0

Step3. Add another service and allocate 800kbps for FTP and destined to FTP Client B. Select the **Service** as FTP from drop-down list. Input Client B's IP address as Destination IP Address.

Class Configuration	
<u></u>	
Class Name	FTP_B
Bandwidth Budget	800 (Kbps)
Priority	3 (0-7)
🗖 Borrow bandwidth from parent class	
Filter Configuration	
Enable Bandwidth Filter	
Service	FTP 🕤
Destination IP Address	192 . 168 . 1 . 34
Destination Subnet Mask	255 . 255 . 255 . 255
Destination Port	0
Source IP Address	0.0.0.0
Source Subnet Mask	0.0.0.0
Source Port	0
Protocol ID	0

Step4. Add another service and allocate 800kbps for IPTV user and destined to Media traffic to IPTV user. Select the **Service** as Custom from drop-down list and set Protocol IP as 17 (UDP). Input IPTV user's IP address as Destination IP Address.

Class Configuration	
Class Name	IPTV
Bandwidth Budget	800 (Kbps)
Priority	3 (0-7)
🗖 Borrow bandwidth from parent class	
Filter Configuration	
Enable Bandwidth Filter	
Service	Custom 💌
Destination IP Address	192 . 168 . 1 . 35
Destination Subnet Mask	255 . 255 . 255 . 255
Destination Port	0
Source IP Address	0.0.0.0
Source Subnet Mask	0.0.0.0
Source Port	O
Protocol ID	17

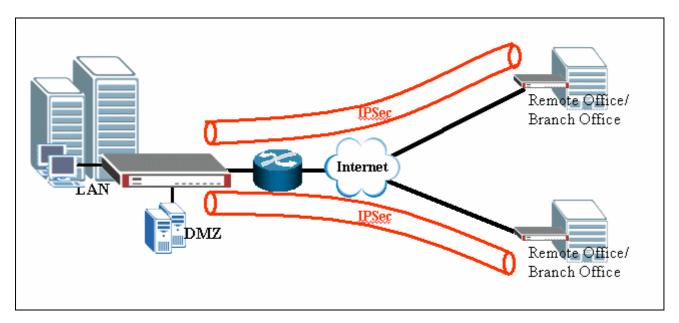
Step 5. Three classes are created for FTP Client A, B & IPTV user as below:

Class Setup
Interface LAN 💌 Bandwidth Management: Active
<ul> <li>Root Class: 2048 kbps</li> <li>FTP_A: 400 kbps</li> <li>FTP_B: 800 kbps</li> <li>O IPTV: 800 kbps</li> </ul>
Add Sub-Class Edit Delete Statistics

# Secure Connections across the Internet and Wireless LAN

## Site-to-Site VPN (Intranet) Scenario

A site-to-site VPN protects the network resources on your protected networks from unauthorized use by users on an unprotected network, such as the public Internet. Site-to-site VPN connects offices in different locations with encryption technology.



Configure ZyWALLs with Static WAN IP Address

This section describes an example configuration ZyWALL with static WAN IP address.

If ZyWALL is used as Internet gateway and public IP address is assigned on ZyWALL's WAN interface. ZyWALL uses this public WAN IP address for terminating the VPN tunnels from remote VPN gateways.

In following example, local VPN gateway (ZyWALL) uses a static public IP address.

	St: DMZ	atic Public IP	Internet	
Local VPN	[ Gateway		1	Peer VPN Gateway
Get Automatically from ISP Die Stood IP Address By WAR IP Address By WAR IP School Mask Gabeersy IP Address	210 - 540 - 140 251 - 251 - 251 210 - 240 - 140	and a second		
Une Sound D'Address      My WAR P Address      Wy WAR P Address      General P Address      General P Address      General P Okry Information	291 . 291 . 291	1.24	2 Gatmany Pallicy Information	
The Secol & Address     My WAR IP Address     My WAR IP Scheel Mask     Growery IP Address      Concessory Product Mask     Growery Product II     Sorter Statement     Sorter Statement     Sorter Statement	200, 200, 200 200, 200, 10 2002427270	1.24	(	D000 D0 D0
Une Stand IF Address      By WAR IF Address      By WAR IF Address      General IF Address      G	201 , 201 , 201 210 , 240 , 10	- 1	Continency Policy Internation	Line anno
<ul> <li>The Societ &amp; Address By WAX IF Scheme By WAX IF Scheme Mach Gammay &amp; Address</li> <li>Extremy Policy Information</li> <li>My 20WALL</li> <li>By Address</li> <li>By Address</li> <li>By UDITIES SCHEME</li> </ul>	210.2427270	. 1 . 24	Continuery Delity Information	00000 (Denor New or 7 Mills 710 240 fc 70
I for Sourd P Address By WAR IP Address By WAR IP Solved Made Gammay P Address Category P Address Category P Address Category P Address Solved P Address	210.2427270	. 1 . 24	Colorery Policy Internation	Line anno

- Configure the static Public IP address to WAN interface through Network-> DMZ-> WAN1 (or 2) -> WAN IP Address Assignment
- 2) Enter the WAN IP address as My Address in Gateway Policy

3) On peer VPN gateway, use the same IP address as **Remote Gateway Address** in Gateway Policy On Local VPN gateway, select **IP** as the **Local IP Type** and enter the public WAN IP address as the **content** of identify. One remote VPN peer, select IP as the Peer ID Type and enter the same IP address as the content of identify.

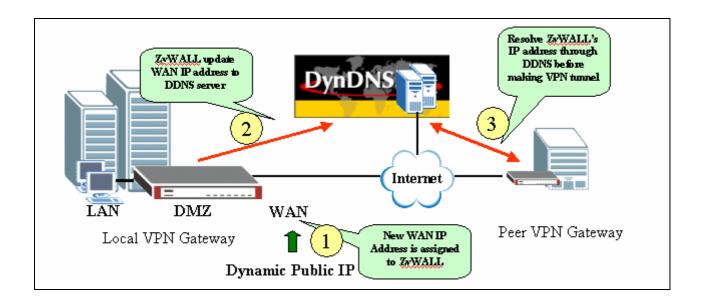
### Configure ZyWALL with Dynamic WAN IP Address

This section describes an example configuration ZyWALL with dynamic WAN IP address.

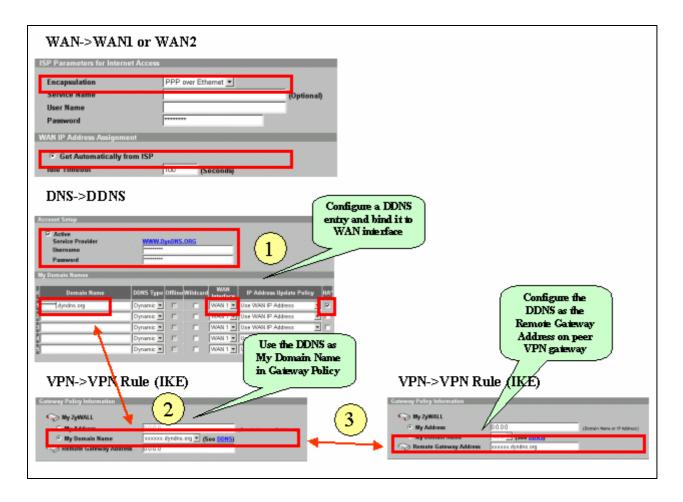
If ZyWALL uses PPPoE or Ethernet/DHCP for its Internet connection, WAN IP address is dynamically assigned by ISP. Since ZyWALL has no idea about its WAN IP address before it is assigned, it is difficult/impossible to use WAN IP Address for My Address in Gateway Policy.

To overcome this problem, Dynamic DNS can be used to resolving the VPN gateway. When new IP

address is assigned to ZyWALL's WAN interface, ZyWALL will updates the related record in DDNS server. Therefore the peer VPN gateway can resolve ZyWALL's IP address to make a VPN tunnel.



In following example, local VPN gateway (ZyWALL) uses a dynamic WAN IP address (PPPoE with dynamic IP assignment).



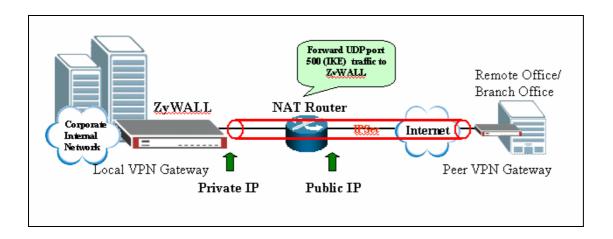
- 4) Configure the DDNS entry under DNS-> DDNS and bind it to a WAN interface (WAN1 or WAN2).
- Under Gateway Policy menu, select the DDNS entry from drop-down list and use it as My Domain Name.
- 6) Configure the DDNS entry in **Remote Gateway Address** on peer VPN gateway.
- 7) Both **DNS** and **E-mail** can be used as the Local ID & Peer ID for authentication.

Note: If Hi-Available (HA) for incoming VPN HA is necessary, enable the **HA** option while configure the DDNS entry under DNS-> DDNS ZyWALL will update its DDNS entry with another WAN interface when the specified WAN interface is not available. Therefore, the next coming VPN connection will go through second WAN interface.

## Configure ZyWALL behind NAT Router

This section describes an example configuration ZyWALL behind NAT Router (Internet Gateway).

NAT routers sit on the border between private and public (Internet) networks, converting private addresses in each IP packet into legally registered public ones. NAT is commonly supported by Internet access routers that sit at the network edge. However, IPSec is NAT-sensitive protocol which means modification on IPSec traffic may cause failure of VPN connection.



By far the easiest way to combine IPSec and NAT is to completely avoid these problems by locating IPSec endpoints in public address space. This can be accomplished in two ways:

- 1) Perform NAT on a device located behind IPSec gateway
- 2) Use an IPSec gateway for both IPSec (VPN) and NAT (Internet Access).

However, in some situation, it is inevitable to locate IPSec gateway in public IP address and it must be placed behind the NAT router. For example, the NAT router has a different interface (e.g. leased line,

ISDN) which are not supported by IPSec gateway. This example gives some guideline for configuring ZyWALL behind NAT router.

Configuration on NAT Router	If firewall is also running on the NAT Router
NAT Forwarding on NAT Router	Firewall Rule to allow IPSec traffic
Part anwarding Plate       With interface     Well       Default Server     0     0     0       Part Part I     Part Translation     Server IP Address       Part I     Part Translation     Server IP Address       Forward UDP port     500 (IKE) traffic to ZvWALL	Edit Service Available Services IPCPAG 0 IPSEC_TRANSPORT/TUNNEL(AH:0) IPSEC_TUNNEL(ESP.0) INCLUEPTOOP 50007 MULTICAST(IGMP Firewall Rule to allow IPSec AH/ESP traffic

- 1) UDP 500 (IKE) must be forwarded to ZyWALL to accept incoming VPN connection from peer VPN gateway or client.
- 2) If Firewall is running on the same NAT router, make sure a firewall rule is configured to allow IKE/IPSec (AH/ESP) traffic to pass-through.

Configuration	n on Local ZyWALL	Configuratio	n on Peer VPN gateway
WAN->WAN1 01	· WAN2		
Get Automatically from ISP Use Fixed IP Address My WAN IP Address My WAN IP Subnet Brass Gateway IP Address	192 . 168 . 1 . 70 295 . 255 . 255 . 0 192 . 168 . 1 . 1		
VPN->VPN Rul Property RAT Traversal Name	e (IKE) on ZyWALL	4	
Cateway Policy Information	e (IKE) on ZyWALL	VPN->VPN Ru Cateway Policy Laforn at an Why ZyWALL Why Description Remote Gateway Address	(Decan Terry on ZyWALL (Decan Terry of Materia) (Decan Terry of Materia)
Authentication Key © Pre-Shared Key © Certificate Local ID Type	12345678 Chiron-self cell (See bly Certificates)	Authentication Key © Pre Shared Key © Certificate Local ID Type	12345678 Chiron-self-cert V (See My Certificates)
Content Peer ID Type Content	210.242.82.70 P X 210.242.82.1	Content Peer ID Type Content	210.242.82.1 IP 210.242.82.70

3) On ZyWALL, enable "**NAT Traversal**" no matter if the front NAT router supports NAT Traversal (IPSec pass-through) or not. With this option enabled, ZyWALL can detect if it is placed behind NAT when peer VPN entity also support NAT Traversal function. If yes, the IPSec traffic will be encapsulated in UDP packet to avoid traversal problem on NAT routers.

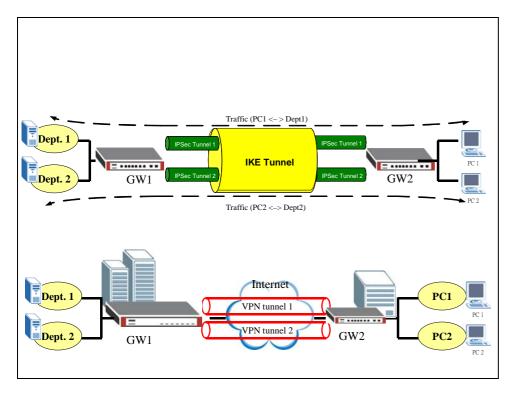
- Under VPN->Gateway Policy-> Gateway Policy Information configure the private IP address as "My Address" on local ZyWALL gateway (behind NAT router).
- 5) On peer VPN gateway, use the public **WAN IP address of NAT Router** as the "**Remote Gateway Address**" of Gateway Policy rule.

The ID must be consistent no matter if IP/DNS/EMAIL is used. So long as if the ID Type and content are consistent on both VP entities.

#### Mapping multiple Network policy to same gateway policy

This section describes an example configuration to map multiple (different) network policies to same gateway policy which is built between two VPN gateways. Different network policies allow user in one network to access multiple destination networks which are not in the continuous range. The other feature of this application is to limit some users to access some specific destination and prevent others from accessing the same network.

In following example, the owner of PC1 belongs to financial department and needs to connect to the financial department (Dept.1) for business sensitive application. PC2 belongs to other group (Dept.2) and need to access Dept.2.



The configuration goal is to achieve following two :

1) Setup VPN rule to allow PC1 to access Dept.1 through the tunnel between GW1 & GW2

2) Setup VPN rule to allow PC2 to access Dept.2 through the tunnel between GW1 & GW2

PC1	PC2	GW2	GW1	Dept.1	Dept.2
102 169 25 101	102 169 25 102	WAN	WAN	102 169 71 0/24	192.168.72.0/24
192.108.33.101	192.168.35.102	210.242.82.35	210.242.82.70	192.100.71.0/24	192.100.72.0724

The following will illustrate how to configure on the GW1:

1) Login ZyWALL and click at "VPN"



3) Click on the icon to add a new "gateway policy" of the VPN tunnel



4) Enable "NAT Traversal" and configure the WAN IP as the "My Address" of My ZyWALL and

Property		
Name	Static Public IP Address	_
🗹 NAT Traversal		
Gateway Policy Information		
Gateway Policy Information		
	210.242.82.70	(Domain Name or IP Address)
Ny ZyWALL	210.242.82.70 None (See DDNS)	Domain Name or IP Address)

 Under Authentication Key, "Pre-Shared Key" or "Certificate" can be used as authentication method. For detailed usage of "Pre-Shared Key" and "Certificate", please refer to XXX. In this example, "Pre-Shared Key" is used and the string "12345678" is used as example.

Authentication Key	
Pre-Shared Key	12345678
C Certificate	auto_generated_self_signed_cert 🔽 (See <u>My Certificates</u> )
Local ID Type	
Content	210.242.82.70
Peer ID Type	
Content	210.242.82.35

6) Extended Authentication (xAuth) can be enabled or not depending on your application. For detailed info, you can refer to XXX.

<b>F</b>	
Extended Authentication	
Enable Extended Authentication	
	/
Server Mode	(Search <u>Local User</u> first then <u>RADIUS</u> )
	·
🔍 Client Mode	
User Name	
User name	
Password	
r dooworu	

7) Under "IKE Proposal", select the Encryption and Authentication Algorithm. Note the configuration must be consist on both ZyWALLs (GW1 & GW2)

(E Proposal		
Negotiation Mode	Main 💌	
Encryption Algorithm	DES 💌	
Authentication Algorithm	MD5 💌	
SA Life Time (Seconds)	28800	
Key Group	DH1 -	
Enable Multiple Proposals		

8) Click on "Apply" to save profile

Apply

9) The IKE rule will be configured as below:

/PN Rules (IKE) VPN I	Rules (Manual) S.	A Monitor Glob	al Setting		
VPN Rules					
Local		Internet		Remote	
Network		VPN Tunnel		Network	
	My ZyWALL		Remote Gateway	~~~	
# VPN Rules				_	<del>ه</del> +
					$\sim$
1 Static Public Address	IP 🕎210.243	2.82.70 🔊	10.242.82.35	<b>B</b> î	- CCC

10) Click on the icon to add a new "Network Policy" over the configured Gateway Policy.



11) Activate the profile and name this policy as "PC1-to-Dept1" in this example. Enable "Nailed-Up" option if you need the functionality that will automatically re-initiate a tunnel to a configured peer in the event of SA Lifetime expires, failure on the link.

Property	
Active	
Name	PC1-to-Dept1
Protocol Nailed-Up Allow NetBIOS Traffic Throw	ugh IPSec Tunnel
🗖 Check IPSec Tunnel Conne	ctivity 🗖 Log
Ping this Address	0.0.0

12) This network policy "PC1-to-Dept1" will be mapped to Gateway Policy, "Static Public IP Address" by default. If you need to change to other pre-defined Gateway Policy, you can select from the drop-down list.

Gateway Policy Information	
🌍 🧇 Gateway Policy	Static Public IP Address

13) Under "Local Network", choose "Subnet" and input "192.168.71.0" and "255.255.255.0" for Dept1 in this example.



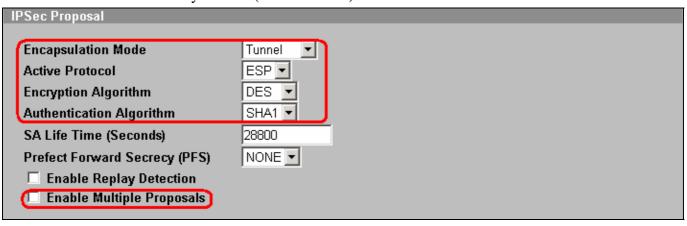
Local Network

💭 Address Type	Subnet Address 💌
Starting IP Address	192 . 168 . 71 . 0
Ending IP Address / Subnet Mask	255 . 255 . 255 . 0
Local Port	Start D End D

14) Under "Remote Network", choose "Single" and input "192.168.1.101" for PC1 in this example.

Remote Network	
🛞 Address Type	Single Address 💌
Starting IP Address	192 . 168 . 35 . 101
Ending IP Address / Subnet Mask	0.0.0.0
Remote Port	Start D End D

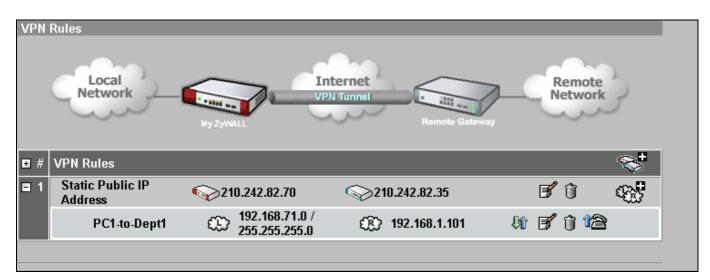
15) Under "IPSec Proposal", select the Encryption and Authentication Algorithm. Note the configuration must be consist on both ZyWALLs (GW1 & GW2)



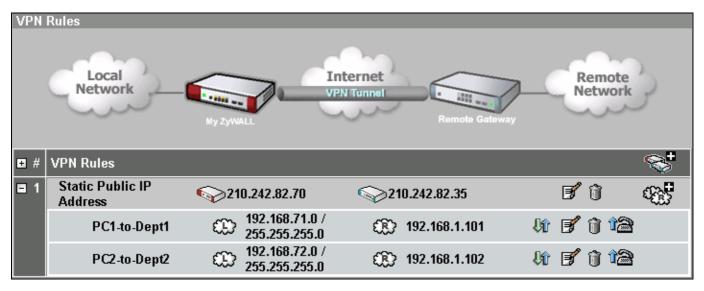
16) Click on "Apply" to save profile



17) The new Network Policy, PC1-to-Dept1 is added to the Gateway Policy.



18) Follow the same procedures as step 10~16 to add 2<sup>nd</sup> Network Policy, PC2-to-Dept2.



Finish

#### **Using Certificate for Device Authentication**

IKE must authenticate the identities of the systems using the Diffie-Hellman algorithm. This process is known as primary authentication. IKE can use two primary authentication methods:

- 1) Digital Signatures
- 2) Pre-shared keys

Digital signature and public-key encryption are both based on asymmetric key encryption and require a mechanism for distributing public keys. This is usually done using security certificates and a Public Key Infrastructure (PKI).

If certificate (Digital Signatures) is used for authentication, there are five available types of identity: IP,

#### DNS, E-mail, Subject Name and Any.

Depending how certificates are generated, it can be classified into three methods:

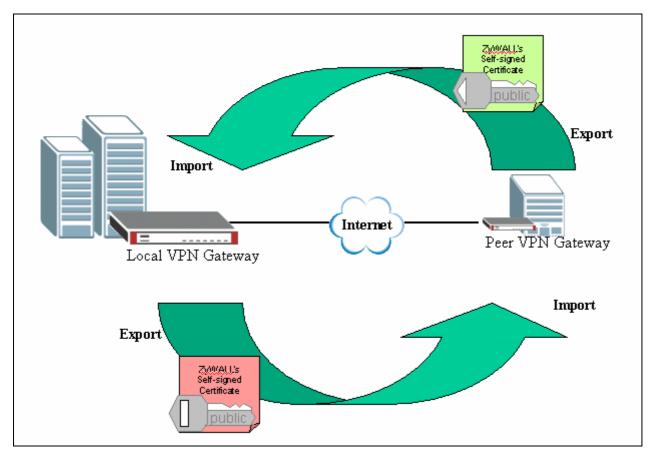
- 1) Using Self-signed Certificates (both entities must be ZyXEL IPSec gateway)
- 2) Online Enroll Certificates
- 3) Offline Enroll Certificates

This example displays how to use PKI feature in VPN function of ZyXEL appliance. Through PKI function, users can achieve party identification when doing VPN/IPSec negotiation.

#### **Using Self-signed Certificates**

For customers who don't have CA service support in their environment but would like to use PKI feature, ZyWALL provides self-signed certificates to achieve this. As the name indicates, a self-signed certificate is a certificate signed by the device (ZyWALL) itself.

ZyWALL has the feature to sign itself a so-called self-signed certificate which can be imported to other ZyWALL for authentication. This feature allows users to use certificate without CA. The certificate must be exchanged and imported into **Trusted Remote Hosts** before making a VPN connection.



The factory default self-signed certificates are the same on all ZyWALL models. It is not secure to use the default self-signed certificate. To make the self-signed certificate unique for this device, you should replace the factory default certificate by pressing the Apply button in the following page at the first time you login to ZyWALL.

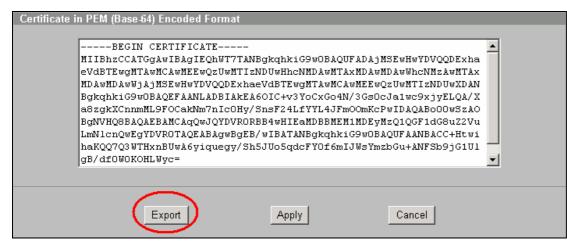


If you reset ZyWALL to default configuration file, the original self-signed certificate is also erased, and a new self-signed certificate should be created at the first boot up time.

To use self-signed certificate, go to ZyWALL **CERTIFICATES->My Certificates** and export ZyWALL's certificate.

My Certificates						
# Name	Туре	Subject	lssuer	Valid From	Valid To	Modify
1 auto_generated_self_signed_cert			CN=ZyWALL 1000 00A0C5012345	2000 Jan 1st, 00:00:00 GMT	2030 Jan 1st, 00:00:00 GMT	ÊÌÌ

1) Press "Export" to save the ZyWALL self-signed certificate to local computer in **Binary X.509** format.



2) Or mark the certificate in **PEM (Base-64) Encoded Format** and then copy to a test editor (e.g.

Notepad) and then save to you local computer in PEM (Base-64) Encoded Format.

BEGIN CERTIFICAT	ГЕ		
MIIBhzCCATGgAwIBAgIE(	2hWT7TANBgkqhkiG9w0BA	QUFADAjMSEwHwYDVQQDExha	
eVdBTEwgMTAwMCAwMEEw(	QzUwMTIzNDUwHhcNMDAwM	TAxMDAwMDAwWhcNMzAwMTAx	
MDAwMDAwWjAjMSEwHwYDV	/QQDExhaeVdBTEwgMTAwM	CAWMEEwQzUwMTIzNDUwXDAN	
BgkqhkiG9w0BAQEFAANL	ADBIAREA60IC+v3YoCxGo	4N/3GsOcJa1wc9xjyELQA/X	
a8zgkXCnnmML9F0CakNm <sup>*</sup>	7nIcOHy/SnsF24LfYYL4J	FmOOmKcPwIDAQABoOOwSzAO	
BGNVHQ8BAQAEBAMCAqQwd	JQYDVRORBB4wHIEaMDBBM	EM1MDEyMzQ1QGF1dG8uZ2Vu	
LmN1cnQwEgYDVROTAQEAI	3AgwBgEB/wIBATANBgkqh	kiG9w0BAQUFAANBACC+Htwi	
haKQQ7Q3WTHxnBUwA <u>6yi</u> c	quegy/Sh5JUo5qdcFYOf6	mIJWsYmzbGu+ANFSb9jG1U1	-
gB/dfOWOKOHLWyc=			•
Export	Apply	Cancel	

Then import the certificate to the other ZyWALL VPN gateway. Go to the other ZyWALL and click

#### "Import" button under CERTIFICATES->Trusted Remote Hosts

Trusted Remote Host Certific	ates			
lssuer (My Default Self-sigr	ed Certificate): CN=ZyV	VALL 1000 00A0C50123	345	
# Name	Subject	Valid From	Valid To	Modify
		Refresh		

Select the certificate from local computer.

Please specify the locati following formats.	on of the certificate file to	be imported. The certificate file must be in one of the	
<ul> <li>Binary X.509</li> <li>PEM (Base-64) enc</li> <li>Binary PKCS#7</li> <li>PEM (Base-64) enc</li> </ul>			
File Path:	Ē	Browse	

Truste	d Remote Host Certifica	tes			
Issue	er (My Default Self-sign	ed Certificate): CN=ZvV	VALL 1000 00A0C50123	45	
10041	, (m) bondant bon orgin	sa contineditoji en 231			
#	Name	Subject	Valid From	Valid To	Modify
1	zw35-self-cert	CN=0.0.0.0	2005 Jan 18th, 03:12:18 GMT	2008 Jan 19th, 03:12:18 GMT	ÊÎ

When you configure VPN rule with certificate, select **Certificate** under **VPN-> Gateway Policy**. Select My Certificate from the drop-down list. When (My) certificate is selected, ZyWALL will show what is the Local ID Type and Content in my certificate. You must configure the same setting on peer ZyWALL and vise versal.

For example, on Local ZyWALL, the Local ID Type is E-mail and content is <u>00A0C5012345@auto.gen.cert</u>. Therefore, configure Peer ID Type and content on peer ZyWALL.

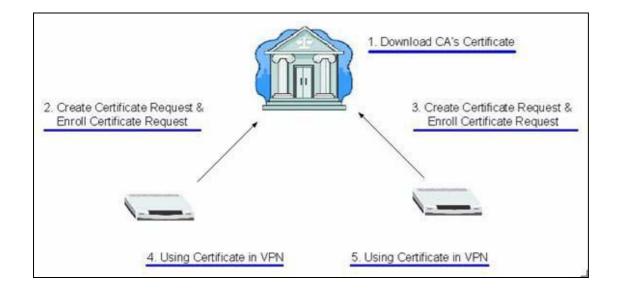
uthentication Key	e (IKE) on Local ZyWALL	Authentication Key	
Pre-Shared Key     Certificate	auto generated self signed cert - (See My Certificates)	C Pre-Shared Key Certificate	12345678 chiron-self-cert <b>• (See My Certificates)</b>
Local ID Type Content	E-mail 00ADC5012345@auto.gen.cert	Local ID Type Content	IP 0.0.0.0
Peer ID Type Content		Peer ID Type Content	E-mail  O04005012345@auto.gen.cert

#### **Online Enroll Certificates**

This example displays how to use PKI feature in VPN function of ZyXEL appliance. Through PKI function, users can achieve party identification when doing VPN/IPSec negotiation. With online enrollment, ZyWALL firstly create certification request locally, then send certification request to trusted CA (Certificate Authority)

servers, and finally get a certificate for further usage. ZyWALL supports both SCEP and CMP protocols as methods of online enrollment. Both SCEP and CMP online enrollment protocols provide secure mechanisms to transmit ZyWALL's certification request securely over Internet. In this example, we adopt SCEP protocol to enroll certificates.

<u>Step 1. Download CA server's Certificate</u> <u>Step 2. Create certificate request and enroll certificate request on ZyWALL A</u> <u>Step 3. Create certificate request and enroll certificate request on ZyWALL B</u> <u>Step 4. Using Certificate in VPN on ZyWALL A</u> Step 5. Using Certificate in VPN on ZyWALL B



LAN 1	ZyWALL A	ZyWALL B	LAN 2
10.1.133.0/24	LAN: 10.1.133.1	LAN: 192.168.2.1	192.168.2.0/24
10.1.155.0/24	WAN: 192.168.1.35	WAN:192.168.1.36	192.100.2.0/24

## Step 1. Download CA server's Certificate

The most critical part for online certification request would be we need to send the certification request over Internet, which is an insecure environment. To prevent certification request from being modified or eavesdropped, we need to download CA server's certificate in the first step. When ZyWALL delivers the certification requests, the public key in CA server's certificate will be used to protect the data.

You may need to access CA server's WEB interface or contact the administrator to get CA's certificate. Then you can go to **SECURITY->CERTIFICATES->Trusted CAs** to import the downloaded certificate.

ly Certificate	s Trus	ted CAs Trus	ted Remote D Hosts	irectory Servers			
PKI St	orage Spac	e in Use					
0%				15			100%
Trusted	CA Setting						
#	Name	Subject	Issuer	Valid From	Valid To	CRL	Modify
,	SSH-CA	1 No Liabilities O-SSH	A CN-SSH Test 5, 1 No Liabiliti 0-SSH ns Communication , Security Cor C=F1	es, 2001 Aug 1st, ons 07:08:32 GMT	2004 Aug 1st, 07:08:32 GMT	No	8 ()

Step 2. Create certificate request and enroll certificate request on ZyWALL A

- 1. Input a name, for this Certificate so you can identify this Certificate later.
- 2. In Subject Information, give this certificate a Common Name by either Host IP Address, Host Domain Name or E-Mail address. Organizational Unit, Organization, Country are optional fields, you are free to either enter them or not.
- 3. Finally, specify the key length.
- 4. Select Create a certification request and enroll for a certificate immediately online.
- 5. Specify the Enrollment Protocol to Simple Certificate Enrollment Protocol (SCEP).
- 6. In the "CA Server's Address" field, input the URL to access CA server, for example, http://1.1.1.18080/scep/
- 7. Choose the previously downloaded CA server's certificate from the drop down list.
- 8. Input user name and password if necessary.
- 9. Then click Apply.

Certificate Name	ZyWALL_A	
Subject Information		
Common Name		
C Host IP Address	0.0.0.	
C Host Domain Name		
🙃 E-Mail	test1@zyxel.com.tw	
Organizational Unit		
Organization		
Country		
Key Length	1024 <u>bits</u>	
Enrollment Options		
C Create a self-signed certifi	icate	
	est and save it locally for later manual enrollment	
	est and enroll for a certificate immediately online	
Enrollment Protocol	Simple Certificate Enrollment Protocol (SCEP) -	
CA Server Address	http://1.1.1.1.8080/scep/	
CA Certificate	SSH-CA - (See Trusted CAs)	

After pressing the **Apply** button, ZyWALL would create the certification request and send it to the CA server for enrollment. It may take one minutes to complete the whole process. After CA server agrees to issue the corresponding certificate, you will find a newly enrolled certificate in **My Certificates**.

ly Certificates	- P 1. II	Ho	sts Directory Serv				
0%	ge Space in Use						100%
My Certifica	tes Setting						
	Name	Туре	Subject	Issuer	Valid From	Valid To	Modify
auto_gene	rated_self_signed_cen	*SELF	CNZyWALL 70 80A0C559B543	CN-ZyWALL 70 00A0C559B543	2000 Jan 1st, 00:08:00 GMT		8 (
2	ZyWALL_A	CERT	CN-test1@zyxel.com.tw	CN-SSH Test CA 1 No Liabilities, 0-SSH Communications Security Corp, C-FI	2003	2004	8 (

Step 3. Create certificate request and enroll certificate request on ZyWALL B

- 1. Input a name, for this Certificate so you can identify this Certificate later.
- 2. In Subject Information, give this certificate a Common Name by either Host IP Address, Host Domain Name or E-Mail address. Organizational Unit, Organization, Country are optional fields, you are free to either enter them or not.
- 3. Finally, specify the key length.
- 4. Select Create a certification request and enroll for a certificate immediately online.
- 5. Specify the Enrollment Protocol to Simple Certificate Enrollment Protocol (SCEP).
- 6. In the "CA Server's Address" field, input the URL to access CA server, for example, http://1.1.1.18080/scep/
- 7. Choose the previously downloaded CA server's certificate from the drop down list.
- 8. Input user name and password if necessary.
- 9. Then click Apply.

Certificate Name	ZyWALL_B
Subject Information	
Common Name	······································
C Host IP Address	0.0.0.0
C Host Domain Name	
E-Mail	test2@zyxel.com.tw
Organizational Unit	
Organization	
Country	
Key Length	1024 💌 bits
Enrollment Options	
C Create a self-signed certif	ficate
Contraction of the World Contraction of the Contrac	uest and save it locally for later manual enrollment
Create a certification required	uest and enroll for a certificate immediately online
Enrollment Protocol	Simple Certificate Enrollment Protocol (SCEP) -
CA Server Address	http://1.1.1.18080/scep/
CA Certificate	SSH-CA (See Trusted CAs)
Request Authentication	

After pressing the **Apply** button, ZyWALL would create the certification request and send it to the CA server for enrollment. After CA server agrees to issue the corresponding certificate, ZyWALL will receive it automatically, and you will find a newly enrolled certificate in **My Certificates**.

PKI Storage Space in Use 0% 3% 3% My Certificates Setting			
My Certificates Setting			100%
But			
e Name Type Subject Issuer		/alid To	Modify
1 auto_generated_self_signed_cert*SELF CN=ZyWALL70 CN=ZyWALL70 00A0C559B533 00A0C559B533 0	Jan 1st, Jan 00:00:00 00:		8 (
CN-SSH Test CA 1 No Liabilities, 2 ZyWALL_B CERT CN-test2@zyxel.com.tw Communications Security Corp, C=Fi	Dec J 23rd, 22 10:06:39 10:	2004 Jan 2nd, :36:39 GMT	6 (

Step 4. Using Certificate in VPN on ZyWALL A

- 1. Activate the rule
- 2. Give this VPN rule a name "toZyWALL\_B"
- 3. Select Key Management to "IKE"
- 4. Select Negotiation Mode to "Main"

5. Edit Local: Address Type="Subnet Address", Starting IP Address="10.1.33.0", End IP Address/Subnet

#### Mask="255.255.255.0"

- 6. Edit Remote: Address Type="Subnet Address", Starting IP Address="192.168.2.0", End IP Address/Subnet Mask="255.255.255.0"
- 7. Authentication Key, Select Certificate, and choose certificate you enrolled for this device from drop down list.
- 8. Fill in My IP address= "192.168.1.35"
- 9. Peer ID type= "ANY"
- 10. Secure Gateway Address= "192.168.1.36"
- 11. Encapsulation Mode="Tunnel"
- 12. Leave other options as default.

Active	
☐ Keep Alive	
NAT Traversal	
Name	to_ZyWALLB
Key Management	IKE 💌
Negotiation Mode	Main 💌
Encapsulation Mode	Tunnel
DNS Server (for IPSec VPN)	0.0.0.0
Extended Authentication	
Enable Extended Authenticatio	n
Server Mode	(Search Local User first then <u>RADIUS</u> )
Client Mode	
User Name	
Password	
Local Policy	
Address Type	Subnet Address 💌
Starting IP Address	101 . 1 . 133 . 0
Ending IP Address / Subnet Mask	255 , 255 , 255 , 0
Remote Policy	
Address Type	Subnet Address Z
Starting IP Address	192.168.2.0
Ending IP Address / Subnet Mask	255 . 255 . 255 . 0
Authentication Method	
Pre-Shared Key	
Certificate	ZyWALL_A (See My Certificates)
Local ID Type	E-mail
Content	00A0C559B546@auto.generated.certificate
Peer ID Type	Any
Content	
Gateway Information	6
My Address	
IP Address	192 . 168 . 1 . 35
My Domain Name	louisezywall dyndns org 🗾 (See DDNS)
Secure Gateway Address	192.168.1.36
PSec Algorithm	
· ESP	C AH
Encryption Algorithm	DES Authentication Algorithm MD5
Authentication Algorithm	MD5 -
	- An and a second s

13. You can check detailed settings by clicking Advanced button.

Negotiation Mode	Main	
Encryption Algorithm	DES 💌	
Authentication Algorithm	MD5 💌	
SA Life Time (Seconds)	28800	
Key Group	DH1 -	
hase 2		
Active Protocol	ESP -	
Encryption Algorithm	DES 💌	
Authentication Algorithm	MD5 💌	
SA Life Time (Seconds)	28800	
Encapsulation	Tunnel	
Perfect Forward Secrecy (PFS)	NONE -	
Enable Replay Detection	NO •	
Protocol	0	
Local Port		
Start	lo l	
End	lo l	
Remote Port		
Start	0	
End	0	

Step 5. Using Certificate in VPN on ZyWALL B

- 1. Activate the rule
- 2. Give this VPN rule a name "toZyWALL\_A"
- 3. Select Key Management to "IKE"
- 4. Select Negotiation Mode to "Main"

5. Edit Local: Address Type="Subnet Address", Starting IP Address="192.168.2.0", End IP Address/Subnet Mask="255.255.255.0"

6. Edit Remote: Address Type="Subnet Address", Starting IP Address="10.1.33.0", End IP Address/Subnet Mask="255.255.255.0"

- 7. Authentication Key, Select Certificate, and choose certificate you enrolled for this device from drop down list.
- 8. Fill in My IP address= "192.168.1.36"
- 9. Peer ID type= "ANY".
- 10. Secure Gateway Address= "192.168.1.35"
- 11. Encapsulation Mode="Tunnel"
- 12. Leave other options as default.

Active	
🗖 Keep Alive	
NAT Traversal	
Name	to_ZyWALLA
Key Management	IKE
Negotiation Mode	Main
Encapsulation Mode	Tunnel
DNS Server (for IPSec VPN)	0.0.0
xtended Authentication	
Enable Extended Authenticatio	
Server Mode	(Search Local User first then RADIUS)
C Client Mode	
User Name	
Password	
ocal Policy	
Address Type	Subnet Address 💌
Starting IP Address	192.168.2.0
Ending IP Address / Subnet Mask	255 . 255 . 255 . 0
temote Policy	
Address Type	Subnet Address
Starting IP Address	10 . 1 . 133 . 0
Ending IP Address / Subnet Mask	255.255.255.0
uthentication Method	
C Pre-Shared Key	
Certificate	ZyWALL_B See My Certificates)
Local ID Type	E-mail
Content	00A0C559B546@auto.generated.certificate
Peer ID Type	Any
Content	
ateway Information	
My Address	
IP Address	192 . 168 . 1 . 36
My Domain Name	louisezywall.dyndns.org 🗾 (See DDNS)
Secure Gateway Address	192.168.1.35
PSec Algorithm	
• ESP	CAH
Encryption Algorithm	DES 💌 Authentication Algorithm MD5 💌
Authentication Algorithm	MD5 V

13. You can check detailed settings by clicking Advanced button.

'hase 1	
Negotiation Mode	Main
Encryption Algorithm	DES 💌
Authentication Algorithm	MD5 💌
SA Life Time (Seconds)	28800
Key Group	DH1 -
hase 2	
Active Protocol	ESP -
Encryption Algorithm	DES 💌
Authentication Algorithm	MD5 💌
SA Life Time (Seconds)	28800
Encapsulation	Tunnel
Perfect Forward Secrecy (PFS)	NONE -
Enable Replay Detection	NO 💌
Protocol	0
Local Port	
Start	0
End	0
Remote Port	
Start	0
End	<u>lo</u>
	Apply Cancel

#### **Offline Enroll Certificates**

In this guide, we describe how ZyWALL devices, both ZyWALL A and ZyWALL B as IPSec/VPN tunnel end points, authenticate each other through PKI. We use CA (Certificate Authority) service provided by Windows 2000 server in this example. The whole procedure includes

Step 1. Create certificate request on ZyWALLA.

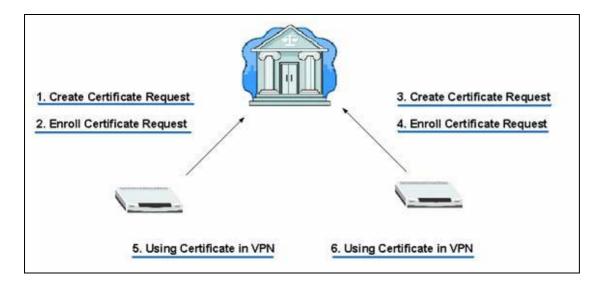
Step 2. Enroll the certificate request to Windows 2000.

Step 3. Create certificate request on ZyWALL B.

Step 4. Enroll the certificate request to Windows 2000.

Step 5. Setup VPN rule on ZyWALL A

Step 6. Setup VPN rule on ZyWALL B.



LAN 1	ZyWALL A	ZyWALL B	LAN 2
10.1.133.0/24	LAN: 10.1.133.1 WAN: 192.168.1.35	LAN: 192.168.2.1 WAN:192.168.1.36	192.168.2.0/24

Step 1. Create Certificate Request on ZyWALL A

1. Go to **VPN->My Certificates ->** Click **Create** button.

My Certificates	Trusted CAs	Trusted Remote Hosts	Directory Servers		
PKI Storag	je Space in Use				
0%			2%		100%
My Certificat	es Setting				
	Name		oject Issuer	Valid From Valid To	Modify
auto_gen	erated_self_signed_	cert*SELF 7	WALL CN=ZyWALL 70 00A0C559B543	2000 Jan 2030 Jan 1st, 00:00:00 1st, 00:00:00 GMT GMT	1 🖻 🛈

2. Input a name, for this Certificate so you can identify this Certificate later. In Subject Information, give this certificate a Common Name by either Host IP Address, Host Domain Name or E-Mail address. Organizational Unit, Organization, Country are optional fields, you are free to either enter them or not. Finally, specify the key length and select **Create a certification request and save it locally for later manual enrollment**.

	ZyWALL_A
Subject Information	
Common Name C Host IP Address C Host Domain Name	0.0.0.0
E-Mail	test1@zyxel.com.tw
Organizational Unit	
Organization	
Country	
Key Length	1024 <u>)</u> bits
Enrollment Options	
C Create a self-signed certil	ficate
Create a certification required	uest and save it locally for later manual enrollment uest and enroll for a certificate immediately online
Create a certification required	uest and save it locally for later manual enrollment
<ul> <li>Create a certification required</li> <li>Create a certification required</li> <li>Enrollment Protocol</li> </ul>	uest and save it locally for later manual enrollment uest and enroll for a certificate immediately online
<ul> <li>Create a certification required</li> <li>Create a certification required</li> <li>Enrollment Protocol</li> <li>CA Server Address</li> <li>CA Certificate</li> </ul>	uest and save it locally for later manual enrollment uest and enroll for a certificate immediately online Simple Certificate Enrollment Protocol (SCEP)

3. Wait for 1-2 minutes until "**Request Generation Successful**" displays. During this period, ZyWALL is working on creation of private, public key pair, and certificate request.

Request Generation in Progress This may take up to one minute. Please wait	
This may take up to one million. Flease work.	

4. After creating certificate request, ZyWALL would return Successful Message.

Request Generation Successful	
Please click on Return to go to the My Certificates screen.	

5. In **My Certificates** tab, you can get a new entry in grey color. This is the **Certificate Request** you just created. Click **Details** to export the request.

ty Certificates	Trusted CAs T	rusted Re Host		Servers				
PKI Stora	ge Space in Use							
0%							10	0%
My Certifica	tes Setting							
-	Name	Type	Subject	Issuer	Valid From	Valid To	Mo	dify
i auto_gen	erated_self_signed_ce	rt*SELF	CN-ZyWALL 00A0C559B5		Jan Ist,	2030 Jan 1st, 00:00:00 GMT	2	0
	ZYWALL A	RED	CN-test1@zyzel.	om.tw N/A	N/A	W/A	e	T

Step 2. Enroll Certificate Request

1. Copy the content of Certificate in PEM Encoded Format, by selecting all of the content, then right click your mouse, and select **Copy**. Keep your copy in clipboard for later paste.

ZyXEL	Name	[ZyWALL_A	
IOME	Contilicate Information Type Serial Number Subject	PKCS#10 Certification Request 0 CN=test1@zyxel.com.tw	
LAN WIRELESS LAN WAN DMZ	Issuer Signature Algorithm Valid From Valid To	N/A rsapkcs1-sha1 N/A N/A	
FREWALL CONTENT FR. TER	Key Algorithm Subject Alternative Name	rsaEncryption (1024 bits) EMAIL=teat1@zyxel.com.tw	
VPN CERTIFICATES AUTH SERVER	Key Usage MD5 Fingerprint SHA1 Fingerprint	DigtalSignature, KeyEncipherment 67.6e 0a 93.71.74.29.12.68.42.6f.34.80.67.d3.4f 45.20.6f.d1.61.87.30.89.02.a5.8e.d6.91.69.0a.63.e1.8d.d2.c3	
	CSQG81b3D b3H3H70CcQ Y1XHXYhaq Y2XH470CcQ YR0RBBTW7 g007J70Pb2 UqRrj00wL2 1pl+TCqCQ8	ONCAQAWHTEDNBKCAIUEAwwSdGVzdBFAen142Wwu729tLnB3NIGENAGG QEBAQUAA+GNADCB1QKBgQCVY91V1xbDgB1e6+AhyRI9EW+LUwoC1B11 WKJotNoRqvXVQ1yBBb1aTjCeLumomebNGQKF+KpFAEUv2DD/pF24 pdyw5z3FwObc5ft USAgvAboDucWr 21DAQABoDUcWr 21DAQABoDUcWr 20D5X5A501Q757Y CG09 D95XXKDDWL+b3T Nx+OgBWOR9A0A D96XXKDDWL+b3T D96XXXDWL+b3T D96XXXDWL+b3T D96XXXDWL+b3T D96XXXDWL+b3T D96XXXDWL+b3T D96XXXDWL+b3T D96XXXDWL+b3T D96XXXDWL+b3T D97XXDWL+b3T D97XXDWLAT D97XXDWL+b3T D97XXDWLAT D9	
logour		Export Apply Cancel	
	ylxHXyhsqp 7WlWq7wCc VPORBSYWF1 gcGyJVWpXg UqFi3ODwL0 lpL+TcgrQS	pdys5187 AODESC + 10000 comp (pCINAPQUE) BDQuE TgCKA+KWMBVEB06 QEDAQABobDwOwT BESd5VadFARAL gbjKSASO1Q757Y gbjKSASO1Q757Y OSKAKDBVL-hb37 CCOV FINE COV FINE COV Select AI Select AI	

In this support note, we utilize certificate enrollment service from **Microsoft Windows 2000 CA server**. The enrollment procedure of your CA server may be different, you may need to check your CA service provider for details.For how to setup Windows 2000 CA server, users may refer to http://www.microsoft.com.

2. Issue the URL to access the CA server, type in User Name/Password/Domain fields.

Edit View Favorites Tool		
880k + ⇒ + 🥥 🖸 🚮 🔍 ess 🕘 192.168.1.33/certsrv	Search 🝙 Favorites 🎯 Media 🎯 🔂 - 🎒 🖼 📓 🔝	
Enter Nel	work Password	
J~	Site: 192.168.1.33	
	Password mean	
	Domain cso.locat      Save this password in your password list      OK Cancel	
	itsrv	Internet

3, Select **Request a Certificate**, then press **Next>** button.

Microsoft Certificate Services CSO-CA       Home         Welcome	Microsoft Certificate Services - Microsoft Internet Explorer	
iddress       Image: http://192.168.1.33/certsrv/         Microsoft Certificate Services CSO-CA       Home         Melcome       Melcome         You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more depending upon the type of certificate you request.         Select a task: <ul> <li>Retrieve the CA certificate or certificate revocation list</li> <li>Request a certificate</li> </ul>	File Edit View Favorites Tools Help	
Microsoft Certificate Services CSO-CA       Home         Welcome	← Back - → - ③ ③ ④ ④ QSearch ● Favorites ③Media ③ 🗟 -	🎒 🖸 • 🗐 🛄
Welcome You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more depending upon the type of certificate you request. Select a task:	Address 🕘 http://192.168.1.33/certsrv/	<b>▼</b> ∂∞
You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more depending upon the type of certificate you request.  Select a task:  C Retrieve the CA certificate or certificate revocation list  Request a certificate	Microsoft Certificate Services CSO-CA	Home
secure program. Once you acquire a certificate, you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more depending upon the type of certificate you request. Select a task: C Retrieve the CA certificate or certificate revocation list Request a certificate	Welcome	
	secure program. Once you acquire a certificate, you will be able other people over the web, sign your e-mail messages, encrypt y more depending upon the type of certificate you request. Select a task: C Retrieve the CA certificate or certificate revocation list	to securely identify yourself to
		Next > C
Next >		
Next >		
Next >	Done	👩 Internet

4. Choose Advanced request, the press Next> button.

	Microsoft Certificate Services - Microsoft Internet Explorer	_ _  ×
Address       Address       http://192.168.1.33/certsrv/certrqus.asp       Image: Construct Certificate Services CSO-CA         Microsoft Certificate Services CSO-CA       Home         Choose Request Type       Please select the type of request you would like to make:         C User certificate request       User Certificate request         Image: Certificate request       Image: Certificate request         C Advanced request       Image: Certificate request	File Edit View Favorites Tools Help	18
Microsoft Certificate Services CSO-CA       Home         Choose Request Type       Please select the type of request you would like to make:            • User certificate request           • User Certificate             • Advanced request           • Advanced request	💠 Back 🔹 🚽 🖉 🕼 🖓 Search 🝙 Favorites 🛞 Media 🎲 🖓 📲 🎲 💽 🔹 🔜	
Choose Request Type Please select the type of request you would like to make:	Address et http://192.168.1.33/certsrv/certrgus.asp	▼ ∂GO
Please select the type of request you would like to make:  C User certificate request  Advanced request	Microsoft Certificate Services CSO-CA	Home
<ul> <li>Certificate request</li> <li><u>User Certificate</u></li> <li>Generate</li> <li>Advanced request</li> </ul>	Choose Request Type	
<ul> <li>User certificate request</li> <li>User Certificate</li> <li>Advanced request</li> </ul>	Please select the type of request you would like to make:	
Next >	<ul> <li>Advanced request</li> </ul>	
	[	Next >
2) Done		

5. Choose "Submit a certificate request using a base64...", then press Next> button.

Microsoft Certificate Services - Microsoft Internet Explorer	
File Edit View Favorites Tools Help	
🕁 Back 🔹 🔿 🕐 🚱 🖓 🔞 Search 💼 Favorites 🛞 Media 🧭 🔂 - 🎒 🚳 - 📄 📓	
Address (a) http://192.168.1.33/certsrv/certrqad.asp	• ଜିକ
Microsoft Certificate Services CSO-CA	Home
Advanced Certificate Requests	
You can request a certificate for yourself, another user, or a computer using one of methods. Note that the policy of the certification authority (CA) will determine the ce hat you can obtain.	
C Submit a certificate request to this CA using a form.	
<ul> <li>Submit a certificate request using a base64 encoded PKCS #10 file or a rener using a base64 encoded PKCS #7 file.</li> </ul>	wal request
<ul> <li>Request a certificate for a smart card on behalf of another user using the Smar Enrollment Station.</li> </ul>	t Card
You must have an enrollment agent certificate to submit a request for another user.	
	Next >
Done	ernet

6. Right click your mouse, then paste the certificate request you get in step 2.1.

the second second second	Favorites Tools Help	
	) 🗿 🕼 🧿 Search 💼 Favorites 🞯 Media 🧭 🖏 🕢 🕢 🗐 🔝	
Iddress 🔊 http://192	2.168.1.33/certsrv/certrgxt.asp	🗾 ଜିଭ
Microsoft Certificat	te Services CSO-CA	Home
Submit A Saved	d Request	
	encoded PKCS #10 certificate request or PKCS #7 renewal reque ion (such as a web server) into the request field to submit the reque	
aven request	BEGIN CERTIFICATE REQUEST	
	MIIBkzCB/QIBADAaMRgwFgYDVQQDDA90ZXNOHUB6	
ertificate Request		
PKCS #10 or #7):	2	
1000 1000 1000 1000	Browse for a file to insert.	
ertificate Templa		
	User	
dditional Attribut	tes:	
and segmentation of	*	
Attributes:	2	
,		
		Submit >N
6		internet

7. Click "Download CA certification path"

🗿 Microsoft Certificate Services - Microsoft Internet Explorer	
File Edit View Favorites Tools Help	111 A
↓ += Back • → • ③ ③ ④ ④ ◎ Search   🗃 Favorites   ③ Media   ④   🔄 • ④   💿 • 📄 💷	
Address a http://192.168.1.33/certsrv/certfnsh.asp	<b>.</b> ∂60
Microsoft Certificate Services CSO-CA	Home
Certificate Issued	
The certificate you requested was issued to you.	
DER encoded or C Base 64 encoded	
Download CA certificate Download CA certification path	
	*
Download CA certification path	🔮 Internet 🏼 🎼

8. A **file download** would pop out, press **Save** button, and choose the local folder you would like to store the certification path.

9. Double click the saved file, Select Certificates, right click the Certificate, choose All Tasks-> Export...

🖼 Certificates				_0×
Action View				
Tree	Issued To /		Issued By	Exp
Certificates - File	CSO-CA		CSO-CA	200
G:\CERT\ZWA-PATH.P7B	E test1	Open	CSO-CA	200
Cercinates	1	All Tasks 🕨	Open	
		Сору	Export	
		Help	10	
		-		
	•			•
Export a certificate	Turner			ſ

10. Certificate Export Wizard would be popped up, then press Next>.



All contents copyright (c) 2006 ZyXEL Communications Corporation.

11. Choose DER encoded binary X.509(.CER), then press Nxet>,

tificate E	Export Wizard	2
	<b>ile Format</b> ficates can be exported in a variety of file formats.	
Selec	t the format you want to use:	
G	DER encoded binary X.509 (.CER)	
0	Base-64 encoded X.509 (.CER)	
0	Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)	
	$\square$ Include all certificates in the certification path if possible	
(	C Personal Information Exchange - PKCS #12 (.PFX)	
	Include all certificates in the certification path if possible	
	Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above)	
	Delete the private key if the export is successful	

12. Specify the path to store your exported Certificate.

Specify the name of the file you (		
<u>File name:</u>		
G:\cert\zywall_a.cer		B <u>r</u> owse )

### 13. Click Finish.

tificate Export Wizard		
	Completing the Certificate E Wizard	
	You have specified the following settings: File Name Export Keys Include all certificates in the certification path File Format	G:\cert No No DER En
	<b>I</b>	Þ
	< Back Finish	Canc

14. Go to ZyWALL WEB GUI -> VPN -> My Certificates -> click **Import** button.

PKI Storage Space in Use 0% 3% 100% My Certificates Setting # Name Type Subject Issuer Valid Valid Modify 1 auto_generated_self_signed_cert *SELF CN=ZyWALL 70 00ADC559B543 00.00.000 00.000.00 (00.00.000 00.000 00.000 00 00.000 00 00	dy Certificates	Trusted CAs Tr	usted R Host	ternote ts	Directory Serve	ns				
My Certificates Setting           #         Name         Type         Subject         Issuer         Valid From         Valid To         Modify           1         auto_generated_self_signed_cert*SELF         CN=ZyWALL 70 00A0C559B543         CN=ZyWALL 70 00A0C559B543         CN=ZyWALL 70 0A0C559B543	PKI Storag	e Space in Use								
#         Name         Type         Subject         Issuer         Valid From         Valid To         Modify           1 auto_generated_self_signed_cert         *SELF         CN=ZyWALL 70 00ADC559B543         CN=ZyWALL 70 00ADC559B543         2000 00ADC559B543         2000 00ADC559B543         2000 00ADC559B543         2000 00ADC559B543         2000 00ADC559B543	0%								10	0%
1 auto_generated_self_signed_cert*SELF CN-ZyWALL 70 00A0C5598543 CN-ZyWALL 70 00A0C5598543 00:00:00 00:00:00 00:00:00 00A0C5598543 00:00:00 00:00:00 00:000 00:00 00:00 00:000	5	Name	Туре		Subject	Issuer			Mo	dify
	1 auto_gene	erated_self_signed_ce		CN-	000600612	70	2000 Jan 1st, 00:00:00	2030 Jan 1st, 00:00:00		
ZyWALL_A REQ CN=test1@zyxel.com.tw N/A N/A N/A 🖻 Ĵ	2	ZyWALL_A	REQ	CN-tost	1@zyxel.com.tw	N/A			Ð	Û

15. Click **Browse...** button to find the location you stored ZyWALL's certificate then press **Apply** button.

Import			
	n of the certificate file to b	e imported. The certifi	cate file must be in one of the
following formats.			
<ul> <li>Binary X.509</li> <li>PEM (Base-64) enco</li> </ul>	dad V 600		
<ul> <li>Binary PKCS#7</li> </ul>			
<ul> <li>PEM (Base-64) enco</li> </ul>	ded PKCS#7		
For my certificate importa			
certificate must already e	cist on ZyWALL. After the i	mportation, the certific	ation request will automatical
be deleted.			
File Path: G:\cert\zywa	l_a cert	Browse.	

16. After a while, if you see the gray entry turns to a black one, then it means the import of ZyWALL's certificate is successful.

ly Certificates	Trusted CAs		Hosts	irectory Servers				
1993-199	ge Space in Use							
0%						100	0%	
My Certifica	ites Setting							٩.
-	Name	Type	Subject	Issuer	Valid From	Valid To	Mod	lify
1 auto_generate	ed_self_signed_cert	*SELF	CNZyWALL 70 00A0C559B543	CN-ZyWALL 70 00A0C559B543	2000 Jan 1st, 00:00:00 GMT	2030 Jan 1st, 00:00:00 GMT	6	0
2 1	wa.cer	CERT	CN-Administrat	CN-ZyIP, OU-PQA, O-ZyXEL, or C-TW, MAILTO-eichen@zyxel.com.tw	2003 Oct 24th,	2004 Oct 23rd,	۲	0

17. Repeat the same procedure from 9 to 13, to export CA's certificate. Note that you may get more than one CA server's certificate, it's not necessary to export all of the CA server's certificates, you can double click ZyWALL's certificate, such as zywall\_a.cert.cert in this example, and select **Certification Path** to view the nearest CA server's name, and then - export that CA server's certificate.

Import the saved CA server's certificate. Click Browse... button, and then select the location.

ly Certificates	Trusted CAs	Trusted Remote Hosts	<sup>8</sup> Directory Servers			
PKI Stora	ge Space in Use					
0%						100%
Trusted CA	Setting					
	Name	Subject Issu	er Valid From	Valid To	CRL Issuer	Modify

After import CA's certificate, you will get this display.

Ay Certificates	Trusted CAs	Trusted Remote Hosts	Directory Se	ervers			
PKI Stora	ge Space in Use						
0%							100%
Trusted CA	Setting						
# Name	e Subject	Issuer		Valid From	Valid To	CRL Issuer	Modify
root.co	er CN-test	CN-ZyIP, OU-PQA, C-TW, MAILTO-elchen@zy	and stands and	2003 Oct 24th, 07:11:19 GMT	2004 Oct 23rd, 07:11:19 GMT		• 1

Step 3. Create Certificate Request on ZyWALL\_B

1. Go to **VPN->My Certificates ->** Click **Create** button.

y Certificates	Trusted CAs	Trusted Remote Hosts	Directory Servers			
PKI Stora	ge Space in Use					
0%						100%
My Certifica	ates Setting					
#	Name	Type Sub	ject Issuer	Valid From	Valid To	Modify
1 auto_ge	nerated_self_signed	I_cert*SELF 7 00A0C5	WALL CN=ZyWALL70 0 598533 00A0C5598533	1st. 00:00:00	2030 Jan 1st, 00:00:00 GMT	
		00A0C5	59B533 00A0C559B533	GMT	GMT	

2. Input a name, for this Certificate so you can identify this Certificate later. In Subject Information, give this certificate a Common Name by either Host IP Address, Host Domain Name or E-Mail address. Organizational Unit, Organization, Country are optional fields, you are free to either enter them or not. Finally, specify the key length and select **Create a certification request and save it locally for later manual enrollment**.

Certificate Name	ZyWALL_B
Subject Information	
Common Name	
O Host IP Address	0.0.0
🔿 Host Domain Name	
E-Mail	test2@zyxel.com.tw
Organizational Unit	
Organization	
Country	
Key Length	1024 <b>bits</b>
Enrollment Options	
~ ~ · · · · · ·	
Create a self-signed certif	ncate uest and save it locally for later manual enrollment
	uest and enroll for a certificate immediately online
Enrollment Protocol	Simple Certificate Enrollment Protocol (SCEP) 🔽
CA Server Address	
CA Server Address CA Certificate	(See <u>Trusted CAs</u> )
CA Certificate	
CA Certificate Request Authentication	
CA Certificate Request Authentication	

3. Wait for 1-2 minutes until "**Request Generation Successful**" displays. During this period, ZyWALL is working on creation of private, public key pair, and certificate request.

Desurent Connection in Desuren	
Request Generation in Progress This may take up to one minute. Please wait	

4. After creating certificate request, ZyWALL would return Successful Message.

ERTIFICATES	S - MY CERTIFICATE - CREATE - STATUS	
	Request Generation Successful Please click on Return to go to the My Certificates screen.	
	r rease circk on return to go to the my certurcates screen.	
	Return	

5. In **My Certificates** tab, you can get a new entry in grey color. This is the **Certificate Request** you just created. Click **Details** to export the request.

/ Certificates	Trusted CAs	Trusted R Hos		Directory Serve	rs				
PKI Stora	ge Space in Use								
0%				2%				10	)%
My Certifica	tes Setting								
#	Name	Туре	9	Subject	lssuer	Valid From	Valid To	Mo	lify
1 auto_gen	erated_self_signed_c	ert*SELF		ZyWALL70 DC559B533	CN=ZWVALL 70 00A0C559B533	2000 Jan 1st,	2030 Jan 1st, 00:00:00 GMT		Û
and the second se	ZyWALL B	REQ	CN=test2	@zyxel.com.tw	N/A	N/A	N/A		Û

# Step 4. Enroll Certificate Request on ZyWALLB

1. Copy the content of Certificate in PEM Encoded Format, by selecting all of the content, then right click your mouse, and select **Copy**. Keep your copy in clipboard for later paste.

Certificate Information	
Туре	PKCS#10 Certification Request
Serial Number	0
Subject	CN=test2@zyxel.com.tw
lssuer	N/A
Signature Algorithm	rsa-pkcs1-sha1
Valid From	N/A
Valid To	N/A
Key Algorithm	rsaEncryption (1024 bits)
Subject Alternative Name	EMAIL=test2@zyxel.com.tw
Key Usage	DigitalSignature, KeyEncipherment
MD5 Fingerprint	04:09:58:e2:a0:78:c1:7c:e9:4a:75:5b:41:50:95:8e
SHA1 Fingerprint	30:5c:e9:d2:75:e3:f9:1c:b1:a5:21:6f:59:31:96:4c:ca:74:0b:56
SHA1 Fingerprint Certificate in PEM (Base	
Certificate in PEM (Base	-64) Encoded Format
Certificate in PEM (Base	-64) Encoded Format QMCAQAwHTEbMBkGA1UEAwwSdGVzdDJAen142WwuY29tLnR3MIGfMAOG
Certificate in PEM (Base MIIBmjCCA( CSqGSIb3D0	-64) Encoded Format QMCAQAwHTEbMBkGA1UEAwwSdGVzdDJAen142WwuY29tLnR3MIGfMAOG QEBAQUAA4GNADCBiQKBgQD8NwPUIwEII1ofnvJ8vPQ+x4+sXKisIgPb
Certificate in PEM (Base MIIBmjCCA (CSqGSIb3D( seyo5JOAE)	-64) Encoded Format QMCAQAwHTEbMBkGA1UEAwwSdGVzdDJAen14ZWwuY29tLnR3MIGfMAOG QEBAQUAA4GNADCBiQKBgQD8NwPUIwEII1ofnvJ8vPQ+x4+sXKisIgPb N2C/50fZaQhTXWrkmjXaZtznqZFtP03BR2ZtjC9taUB8u18ioPcUafb
Certificate in PEM (Base MIIBmjCCA CSqGSIb3D seyo5JOAEN S38oTuyPo3	-64) Encoded Format QMCAQAwHTEbMBkGA1UEAwwSdGVzdDJAen14ZWwuY29tLnR3MIGfMAOG QEBAQUAA4GNADCBiQKBgQD8NwPUIwEII1ofnvJ8vPQ+x4+sXKisIgPb N2C/50f2aQhTXWrkmjXaZtznqZFtP03BR2ZtjC9taUB8u18ioPcUafb 1in/9D0g0s8Li0+v7oVkRZNTe2D8axsV+LM2fgPDQ8ocIHoP48H0g8N
Certificate in PEM (Base MIIBmjCCA CSqGSIb3D seyo5JOAEN 338oTuyPo3 9o5ali0Kju	-64) Encoded Format QMCAQAwHTEbMBkGA1UEAwwSdGVzdDJAen14ZWwuY29tLnR3MIGfMAOG QEBAQUAA4GNADCBiQKBgQD8NwPUIwEII1ofnvJ8vPQ+x4+sXKisIgPb N2C/50fZaQhTXWrkmjXaZtznqZFtP03BR2ZtjC9taUB8u18ioPcUafb 1in/9D0g0s8Li0+v7oVkRZNTeZD8axsV+LM2fgPDQ8ocIHoP48H0g8N wIDAQABoD0w0wYJKoZIhvcNAQkoMS4wLDALBgNVHQ8EBAMCBaAwHQYD
Certificate in PEM (Base MIIEmjCCA CSqCSIB3D seyo5J0AEM S38oTuyPo 9o5ali0Kju VRORBBYwF:	-64) Encoded Format QMCAQAwHTEbMBkGA1UEAwwSdGVzdDJAen14ZWwuY29tLnR3MIGfMAOG QEBAQUAA4GNADCB1QKBgQD8NwPUIwEII1ofnvJ8vPq+x4+sXKisIgPb N2C/50f2aQhTXWrkmjXa2tznqZFtP03BR2ZtjC9taUB8u18ioPcUafb 1in/9D0g038Li0+v7oVkRZNTeZD8axsV+LMZfgPDQ8ocIHoP48H0g8N WIDAQABoD0wOwJJKoZIhvcNAQKOMS4wLDALBgNVHQeEBAMCBaAwHQYD IESdGVzdDJAer Undo NR3MA0GCSqGSIb3DQEBBQUAA4GBAG75
Certificate in PEM (Base MIIEmjCCA CSqCSIb3D seyo5JOAEI S380TuyPo 9058I10Kj VRORBBYwFJ 7Y6/7G8IKj	-64) Encoded Format QMCAQAwHTEbMBkGA1UEAwwSdGVzdDJAen14ZWwuY29tLnR3MIGfMAOG QEBAQUAA4GNADCBiQKBgQD8NwPUIwEIIIofnvJ8vPQ+x4+sXKisIgPb N2C/S0f2aQhTXWrkmjXa2tznq2FtP03BR2tjC9aUB8u18ioPCUafb 1in/9D0g0s8Li0+v7oVkRZNTe2D8axsV+LM2fgPDQ8ocIHoP48H0g8N wIDAQABoD0w0wVXKoZIhvcNAQkOMS4wLDALBgNVHQEEBAMCBaAwHQYD IESdGVzdDJAer Updo nR3MA0GCSqGSIb3DQEBBQUAA4GBAG75 pL7VH7SIDV01c
Certificate in PEM (Base MIIBmjCCA CSqCSIb3D0 seyo5JOAEN S38oTuyPo 9o5aIiOKjt VRORBBYWF) 7Y6/7G8IKj doHVk526ZI	-64) Encoded Format QMCAQAwHTEbMBkGA1UEAwwSdGVzdDJAen14ZWwuY29tLnR3MIGfMAOG QEBAQUAA4GNADCBiQKBgQD8NwPUIwEIIIofnvJ8vPQ+x4+sXKisIgPb N2C/S0f2aQhTXWrkmjXaZtznq2FtP03BR2ZtjC9taUB8u18ioPcUafb 1in/9D0g0s8Li0+v7oVkRZNTeZD8axsV+LMZfgPDQ8ocIHoP48H0g8N wIDAQABoD0w0wYJKoZIhvcNAQkOMS4wLDALBgNVHQ8EBAMCBaAwHQYD IESdGVzdDJAer Undo nR3MA0CCSqG5Ib3DQEBBQUAA4GBAC75 pL7VH7SIDV01c Cut ioYWUF1SdCEy/7uraE2jC3dzVjcVXuyN
Certificate in PEM (Base MIIBmjCCA CSqCSIb30 seyo5JOAEN S380TuyPo 9o5aIi0Kju VRORBBVwF 7Y6/7G8IK doHVk5262I yU07f5JRW	-64) Encoded Format QMCAQAwHTEbMBkGA1UEAwwSdGVzdDJAen14ZWwuY29tLnR3MIGfMAOG QEBAQUAA4GNADCBiQKBgQD8NwPUIwEII1ofnvJ8vPQ+x4+sXKisIgPb N2C/50f2aQhTXWrkmJXa2tznq2FtP03BR2ZtjC9taUB8u18ioPcUafb 1in/9D0g0s8Li0+v7oVkRZNTeZD8axsV+LM2fgPDQ8ocIHoP48H0g8N wIDAQABoD0w0wYJKoZIhvcNAQkOMS4wLDALBgNVHQ8EBAMCBaAwHQYD IESdGVzdDJAer Undo hR3MAOGCSqGSIb3DQEBBQUAA4GBAG75 pL7VH7SIDV01c Cut ioYWUF1SdCEy/7uraE2jC3dzVjcVXuyN
Certificate in PEM (Base MIIBmjCCA CSqCSIb30 seyo5JOAEN S380TuyPo 9o5aIi0Kju VRORBBVwF 7Y6/7G8IK doHVk5262I yU07f5JRW	-64) Encoded Format QMCAQAwHTEbMBkGA1UEAwwSdGVzdDJAen14ZWwuY29tLnR3MIGfMAOG QEBAQUAA4GNADCBiQKBgQD8NwPUIwEII1ofnvJ8vPQ+x4+sXKisIgPb NZC/50fZaQhTXWrkmjXa2tznq2FtP03BR2ZtjC9taUB8u18ioPcUafb 1in/9D0g0s8Li0+v7oVkRZNTeZD8axsV+LM2fgPDQ8ocIHoP48H0g8N wIDAQABoD0w0wYJKo2IhvcNAQkOMS4wLDALBgNVHQ8EBAMCBaAwHQYD IESdGVzdDJAer Undo hR3MA0GCSqGSIb3DQEBBQUAA4GBAG75 pJ7VH7SIDV01c Cut ioYWUF1SdCEy/7uraE2jC3dzVjcVXuyN 615/MqCJbes3t COpy 7nUA4T2
Certificate in PEM (Base MIIBmjCCA CSqCSIb30 seyo5JOAEN S380TuyPo 9o5aIi0Kju VRORBBVwF 7Y6/7G8IK doHVk5262I yU07f5JRW	-64) Encoded Format QMCAQAwHTEbMBkGA1UEAwwSdGVzdDJAen14ZWwuY29tLnR3MIGfMAOG QEBAQUAA4GNADCBiQKBgQD8NwPUIwEII1ofnvJ8vPQ+x4+sXKisIgPb N2C/50f2aQhTXWrkmjXa2tznq2FtP03BR2ZtjC9taUB8u18ioPcUafb 1in/9D0g0s8L0+v70VkRZNTeZD8axsV+LM2fgPDQ8ocIHoP48H0g8N wIDAQABoD0wOwYJKoZIhvcNAQkOMS4wLDALBgNVHQ8EBAMCBaAwHQYD IESdGVzdDJAer Undo nR3MA0GCSqGSIb3DQEBBQUAA4GBAG75 pL7VH7SIDV0IG Cut oVWUF1SdCEy/7uraE2jC3dzVjcVXuyN 615/MqCJbes38 Copy Paste

In this support note, we utilize certificate enrollment service from **Microsoft Windows 2000 CA server**. The enrollment procedure of your CA server may be different, you may need to check your CA service provider for details.For how to setup Windows 2000 CA server, users may refer to http://www.microsoft.com.

2. Issue the URL to access the CA server, type in User Name/Password/Domain fields.

File Edit View Favorites Tools Help	1
↔ Back • → • ② ② ③ ④ 🖓 QSearch 💿 Favorites ③Media ③ 🖏 • ④ 💽 • 🗐 🔯	
Address 🗃 http://192.168.1.33/certsrv	<b>.</b> €
l≩	*
Enter Network Password     Please type your user name and password.   Site:   192:168.1.33   User Name   test2   Password   pomain   cso.loca   Domain   Save this password in your password list     OK   Cancel	
🕙 Opening page http://192.168.1.33/certsrv 🔳 👘 🔮 Inte	ernet //

3, Select **Request a Certificate**, then press **Next>** button.



🚰 Microsoft Certificate Services - Microsoft Internet Explorer	
File Edit View Favorites Tools Help	
] ← Back → → → 🙆 👔 🚮 🔞 Search 👔 Favorites 🛞 Media 🧭 🛃 - 🎒 💽 - 🗐 🔯	
Address 🙆 http://192.168.1.33/certsrv/	• 🗟
<i>Microsoft</i> Certificate Services CSO-CA	<u>Home</u>
Welcome	
You use this web site to request a certificate for your web browser, e-mail client, or othe secure program. Once you acquire a certificate, you will be able to securely identify you other people over the web, sign your e-mail messages, encrypt your e-mail messages, more depending upon the type of certificate you request.	urself to
<ul> <li>Retrieve the CA certificate or certificate revocation list</li> <li>Request a certificate</li> </ul>	
C Check on a pending certificate	
Nex	<u>t &gt; </u>
🗑 Done 🛛 👘 🙆 Internet	

4. Choose Advanced request, the press Next> button.

# **ZyXEL**

🚰 Microsoft Certificate Services - Microsoft Internet Explorer	<u>_</u> _×
File Edit View Favorites Tools Help	
📙 🗘 Back 🔹 🤿 🖉 🚱 🖓 🔞 🐼 Search 👔 Favorites 🎯 Media 🎯 🖏 - 🎒 💽 + 📃 🔯	
Address 🕘 http://192.168.1.33/certsrv/certrqus.asp	▼ 🖓 Go
Microsoft Certificate Services CSO-CA	Home
Choose Request Type	
Please select the type of request you would like to make:	
O User certificate request:	
User Certificate	
Advanced request	
	Next >
🙆 Done	Internet

5. Choose "Submit a certificate request using a base64...", then press Next> button.



🚰 Microsoft Certificate Services - Microsoft Internet Explorer	. D ×
File Edit View Favorites Tools Help	-
] 🕁 Back 🔹 🤿 🖌 🔯 🖄 🔯 Search 👔 Favorites 🐲 Media 🧭 🖏 🖬 🎒 💽 🔹 🗐 🔯	
Address 🙆 http://192.168.1.33/certsrv/certrqad.asp	∂G0
Microsoft Certificate Services CSO-CA Hon	<u>1e</u>
Advanced Certificate Requests	
You can request a certificate for yourself, another user, or a computer using one of the followin methods. Note that the policy of the certification authority (CA) will determine the certificates that you can obtain.	ng
<ul> <li>Submit a certificate request to this CA using a form.</li> </ul>	
Submit a certificate request using a base64 encoded PKCS #10 file or a renewal reques using a base64 encoded PKCS #7 file.	st
<ul> <li>Request a certificate for a smart card on behalf of another user using the Smart Card Enrollment Station.</li> <li>You must have an enrollment agent certificate to submit a request for another user.</li> </ul>	
Next >	T

6. Right click your mouse, then paste the certificate request you get in step 4.1.

Microsoft Certificat	e Services - Microsoft Internet Explorer	_ 🗆 🗵
File Edit View F	Favorites Tools Help	-
] 😓 Back 🔹 🔿 👻 🥝	) 🚱 🚰 🔞 Search 👔 Favorites 🛞 Media 🎯 🖏 - 🎒 🔕 - 🗎 🔯	
Address 餐 http://192	.168.1.33/certsrv/certrqxt.asp	• @60
Microsoft Certificat	te Services CSO-CA	Home 🔺
Submit A Saved	d Request	
	encoded PKCS #10 certificate request or PKCS #7 renewal request generated b ion (such as a web server) into the request field to submit the request to the certific	
Saved Request:		
Base64 Encoded Certificate Request (PKCS #10 or #7):	BEGIN CERTIFICATE REQUEST MIIBkzCB/QIBADAmMrgwFgYDVQQDDA90ZXNOMUB6END CERTIFICATE REQUEST     Browse for a file to insert.	
Certificate Templa		
	User	
Additional Attribut	tes:	
Attributes:		
	Submi	t >]
e	👔 👔 Internet	

# 7. Click "Download CA certification path"

🚰 Microsoft Certificate Services - Microsoft Internet Explorer	-O×
File Edit View Favorites Tools Help	
← Back ← → ∽ 🙆 🗿 🖧   @ Search 🙀 Favorites @ Media 🧭 🗟 ← 🎒 🔯 ∽ 🖃 🔯	
Address 🔞 http://192.168.1.33/certsrv/certfnsh.asp	<b>▼</b> 🖗 Go
Microsoft Certificate Services CSO-CA	Home
The certificate you requested was issued to you.	
DER encoded or C Base 64 encoded	
Download CA certificate Download CA certification path	
Download CA certification path	ternet //

8. A **file download** would pop out, press **Save** button, and choose the local folder you would like to store the certification path.

9. Double click the saved file, Select Certificates, right click the Certificate, choose All Tasks-> Export...

🔤 Certificates				
Action ⊻iew	🖸 🖻 🗟 🔗			
Tree	Issued To 🛛 🗛	Issued	Ву	Expi
🗊 Certificates - File	CSO-CA	CSO-CA	1	200
G:\CERT\ZWB-PATH.P7B	test2	Open		200
		All-Tasks 🔸	Open	
		Сору	Export	
		Help		
		(MC)		
	4			F
I Export a certificate	JEN.		an han dan han dan dan na haini d	

10. Certificate Export Wizard would be popped up, then press Next>.



11. Choose DER encoded binary X.509(.CER), then press Nxet>,

Select the format you want to use:	
DER encoded binary X.509 (.CER)	
Contraction and the second s	
C Base-64 encoded X.509 (.CER)	
C Cryptographic Message Syntax Standard - PKCS	#7 Certificates (.P7B)
$\square$ Include all certificates in the certification path	h if possible
C Personal Information Exchange - PKCS #12 (.PF)	X)
Include all certificates in the certification path	n if possible
Enable strong protection (requires IE 5.0, NT	4.0 SP4 or above)
Delete the private key if the export is succes	sful

12. Specify the path to store your exported Certificate.

to Export		
Specify the name of the file you	want to export	
File name:		
G:\cert\zywall_b.cer		Browse

# 13. Click Finish.

Certificate Export Wizard		×
	Completing the Certificate E Wizard You have successfully completed the Certificate wizard. You have specified the following settings:	
	File Name Export Keys Include all certificates in the certification path File Format	G:\cert No No DER En
	< Back Finish	Cancel

14. Go to ZyWALL WEB GUI -> VPN -> My Certificates -> click **Import** button.

My Certificates	Trusted CAs	rusted F Hos		Directory Serve	rs				
PKI Stora	ge Space in Use								
0%								100	)%
My Certifica	tes Setting								
#	Name	Туре		Subject	lssuer	Valid From	Valid To	Mod	lify
1 auto_gen	erated_self_signed_ce	rt*SELF		=ZyWALL70 A0C559B533	CN=ZWVALL 70 D0A0C559B533	2000	2030 Jan 1st,		Û
2	ZyWALL_B	REQ	CN=test	2@zyxel.com.tw	N/A	N/A	N/A		Û

15. Click Browse... button to find the location you stored ZyWALL's certificate then press Apply button.

Please specify the location of the certificate file to be imported. The certificate file must be in one of the following formats.   Binary X.509  PEM (Base-64) encoded X.509 Binary PKCS#7  PEM (Base-64) encoded PKCS#7  For my certificate importation to be successful, a certification request corresponding to the imported certificate must already exist on ZyWALL. After the importation, the certification request will automatica be deleted.  File Path: G:\cert\zywall_b.cer Browse	mport	
<ul> <li>Binary X.509</li> <li>PEM (Base-64) encoded X.509</li> <li>Binary PKCS#7</li> <li>PEM (Base-64) encoded PKCS#7</li> </ul> For my certificate importation to be successful, a certification request corresponding to the imported certificate must already exist on ZyWALL. After the importation, the certification request will automatica be deleted.		certificate file to be imported. The certificate file must be in one of the
File Path: G:\cert\zywall b.cer Browse	PEM (Base-64) encoded X.50     Binary PKCS#7     PEM (Base-64) encoded PK0 For my certificate importation to b certificate must already exist on Z	CS#7 be successful, a certification request corresponding to the imported

16. After a while, if you see the gray entry turns to a black one, then it means the import of ZyWALL's certificate is successful.

ly Certificates	Trusted CAs	Trusted Remote Hosts	Directory Servers			
PKI Stora	ge Space in Use					
0%						100%
Trusted CA	Setting					_
#	Name	Subject Issue	r Valid From	Valid To	CRL Issuer	Modify

17. Repeat the same procedure from 9 to 13, to export CA's certificate. Note that you may get more than one CA server's certificate, it's not necessary to export all of the CA server's certificates, you can double click ZyWALL's certificate, such as zywall\_a.cert.cert in this example, and select **Certification Path** to view the nearest CA server's name, and then - export that CA server's certificate.

Import the saved CA server's certificate. Click Browse... button, and then select the location.

ly Certificates	Trusted CAs	Trusted Remote Hosts	Directory Servers			
PKI Stora	ge Space in Use					
0%						100%
Trusted CA	Setting					_
#	Name	Subject Issue	r Valid From	Valid To	CRL Issuer	Modify

18. After import CA's certificate, you will get this display.

<u>My Certificates</u>	Trusted CAs	Trusted Remote Hosts	Directory Se	rvers			
PKI Stora	ge Space in Use						
0%							100%
Trusted CA	Setting						
# Nam	e Subject	Issuer		Valid From	Valid To	CRL Issuer	Modify
1 root.c	er CN=test	CN=ZyIP, OU=PQA C=TW, MAILTO=elchen@z	4	2003 Oct 24th, 07:11:19 GMT	2004 Oct 23rd, 07:11:19 GMT	No	ÊÛ

Step 5. Using Certificate in VPN on ZyWALL A

- 1. Activate the rule
- 2. Give this VPN rule a name "toZyWALL\_B"
- 3. Select Key Management to "IKE"
- 4. Select Negotiation Mode to "Main"

5. Edit Local: Address Type="Subnet Address", Starting IP Address="10.1.33.0", End IP Address/Subnet Mask="255.255.255.0"

6. Edit Remote: Address Type="Subnet Address", Starting IP Address="192.168.2.0", End IP Address/Subnet Mask="255.255.255.0"

7. Authentication Key, Select Certificate, and choose certificate you enrolled for this device from drop down list.

8. Fill in My IP address= "192.168.1.35"

- 9. Peer ID type= "ANY".
- 10. Secure Gateway Address= "192.168.1.36"
- 11. Encapsulation Mode="Tunnel"
- 12. Leave other options as default.

Property	
✓ Active	
Keep Alive	
NAT Traversal	
Name	to_ZyWALLB
Key Management	IKE V
Negotiation Mode	Main
Encapsulation Mode	Tunnel
DNS Server (for IPSec VPN)	0.0.0.0
Extended Authentication	
🗖 Englis Estended Authorited	
Enable Extended Authentication Server Mode	on (Search <u>Local User</u> first then <u>RADIUS</u> )
C Client Mode	
User Name	
Password	
Local Policy	
Address Type	Subnet Address -
Starting IP Address	
Ending IP Address / Subnet Mask	255 . 255 . 255 . 0
Linung in Address / Subilet Mask	
Remote Policy	
Address Type	Subnet Address 🔻
Starting IP Address	192.168.2.0
Ending IP Address / Subnet Mask	255 . 255 . 255 . 0
Authentication Method	
O Pre-Shared Key	12345678
Certificate	ZyWALL_A 🔄 (See <u>My Certificates</u> )
Local ID Type	E-mail
Content	00ADC559B546@auto.generated.certificate
Peer ID Type	Any
Content	
Gateway Information	
My Address	
IP Address	192 . 168 . 1 . 35
🔍 My Domain Name	louisezywall.dyndns.org 🗹 (See DDNS)
Secure Gateway Address	192.168.1.36
IPSec Algorithm	
• ESP	○ AH
Encryption Algorithm	DES  Authentication Algorithm MD5
Authentication Algorithm	MD5 V
Advanc	ed Apply Cancel

13. You can check detailed settings by clicking Advanced button.



Negotiation Mode Encryption Algorithm	Main  DES	
Authentication Algorithm	MD5 V	
SA Life Time (Seconds)	28800	
Key Group	DH1 -	
Phase 2		
Active Protocol	ESP -	
Encryption Algorithm	DES	
Authentication Algorithm	MD5 💌	
SA Life Time (Seconds)	28800	
Encapsulation	Tunnel	
Perfect Forward Secrecy (PFS)	NONE -	
Enable Replay Detection	NO 🔽	
Protocol	0	
Local Port		
Start		
End	0	
Remote Port		
Start		
End	<u> 0</u>	

Step 6. Using Certificate in VPNon ZyWALL B

- 1. Activate the rule
- 2. Give this VPN rule a name "toZyWALL\_A"
- 3. Select Key Management to "IKE"
- 4. Select Negotiation Mode to "Main"

5. Edit Local: Address Type="Subnet Address", Starting IP Address="192.168.2.0", End IP Address/Subnet Mask="255.255.255.0"

6. Edit Remote: Address Type="Subnet Address", Starting IP Address="10.1.33.0", End IP Address/Subnet Mask="255.255.255.0"

- 7. Authentication Key, Select Certificate, and choose certificate you enrolled for this device from drop down list.
- 8. Fill in My IP address= "192.168.1.36"
- 9. Peer ID type= "ANY".
- 10. Secure Gateway Address= "192.168.1.35"
- 11. Encapsulation Mode="Tunnel"
- 12. Leave other options as default.

Property	
Active	
Keep Alive	
NAT Traversal	
Name	to_ZyWALLA
Key Management	IKE 🔻
Negotiation Mode	Main
Encapsulation Mode	Tunnel
DNS Server (for IPSec VPN)	0.0.0.0
Extended Authentication	
Enable Extended Authenticatio	
Server Mode Client Mode	(Search <u>Local User</u> first then <u>RADIUS</u> )
User Name	
Password	
Local Policy	
Address Type	Subnet Address 💌
Starting IP Address	192 . 168 . 2 . 0
Ending IP Address / Subnet Mask	255 . 255 . 255 . 0
Remote Policy	-
Remote Foncy	
Address Type	Subnet Address 💌
Starting IP Address	10 . 1 . 133 . 0
Ending IP Address / Subnet Mask	255 . 255 . 255 . 0
Authentication Method	
Pre-Shared Key	12345678
• Certificate	ZyWALL_B (See <u>My Certificates</u> )
Local ID Type	E-mail
Content	00A0C559B546@auto.generated.certificate
Peer ID Type	Any
Content	
Catoway Information	
Gateway Information	
My Address	192.168.1.36
IP Address	
O My Domain Name	louisezywall.dyndns.org 🔽 (See DDNS)
Secure Gateway Address	192.168.1.35
IPSec Algorithm	
• ESP	O AH
Encryption Algorithm	DES 🔽 Authentication Algorithm MD5 🔽
Authentication Algorithm	MD5 🔽
Advanc	cancel Apply

13. You can check detailed settings by clicking Advanced button.

Phase 1		
Negotiation Mode	Main	
Encryption Algorithm	DES	
Authentication Algorithm	MD5 V	
SA Life Time (Seconds)	28800	
Key Group	DH1 -	
<sup>D</sup> hase 2		
Active Protocol	ESP -	
Encryption Algorithm	DES 🗾	
Authentication Algorithm	MD5 💌	
SA Life Time (Seconds)	28800	
Encapsulation	Tunnel	
Perfect Forward Secrecy (PFS)	NONE -	
Enable Replay Detection	NO 🔽	
Protocol		
Local Port		
Start	lo l	
End		
Remote Port		
Start		
End	0	
	Apply Cancel	

## Using Pre-Shared Key for Device Authentication

The IKE protocol also provides primary authentication - verifying the identity of the remote system before negotiating the encryption algorithm and keys. Two kinds of authentication methods are supported on ZyWALL: pre-shared key & certificate.

If pre-shared key is used, a shared, symmetric key must be manually exchanged and configured on the two entities. Three types of identity are available: **IP**, **DNS** and **E-mail**.

Here are some rules to follow in Authentication Key:

- 3) Pre-shared key must be configured identically on both entities
- 4) The Local ID Type & Content of Local ZyWALL must be the same as that of Peer ID Type & Content of peer VPN gateway.
- 5) When IP is selected as ID Type, the **Content** must be in the format of X.X.X.X (e.g. 210.242.82.70)
- 6) When DNS/E-mail are selected as ID Type, the same string must be configured on both entities.

Configuration on Local ZyWALL	Configuration on Peer VPN gateway
Pre-Shared Key must be identical on both entitie	S Authentication Key  C Pre Shared Key  Categories  Control  Contr
Contest Peer ID Type Contest Local ID Type & Content on Local ZyWALL m Peer ID Type & Content on Peer VPN gateway	Content Peer 10 Type Content Content Dia 22 02 70 Dia 22 02 00 Dia 22 02 00 Dia 22 00 Dia 20 00
Authentication Key           P Pe-Shared Key           Context           Clock ID Type           P P           Context           Clock ID Type           Context           Clock ID Type           Context           Context           Context           Context           Context           Context           Context	Authendication Key
Peer ID Type & Content on Local ZyWALL on Local ID Type & Content on Peer VPN gateway	
Certificate usb.governand.etf.supred_cert Certificates) Local D Type P P P P P P P P P P P P P P P P P P P	Continue         Description         Continue         Continue <thcontinue< th="">         Continue         Contin         Continue         Continue</thcontinue<>

Note:

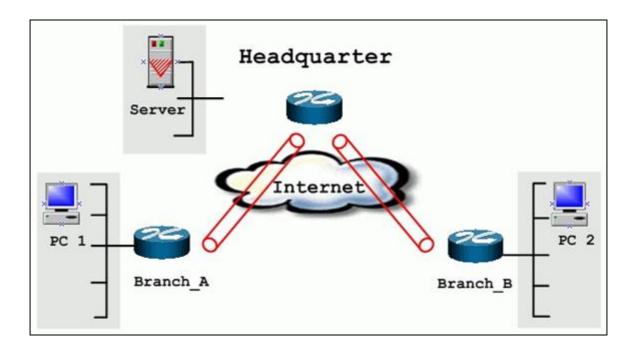
- 1) If "**ID Type**" is mis-configured on Local/Remote IPSec Gateway, the ZyWALL will show [NOTFY:**ERR\_ID\_INFO**] error message in related IKE log.
- 2) If "**Pre-shared Key**" or ID "**Content**" are mis-configured on Local/Remote IPSec Gateway, ZyWALL will show [NOTFY:ERR\_ID\_INFO] error message in related IKE log.

## Using VPN routing between branches

- 1. <u>Setup VPN in Branch Office A</u>
- 2. <u>Setup VPN in Branch Office B</u>
- 3. <u>Setup VPN in Headquarter</u>

This page guides us how to setup VPN routing between branch offices through headquarter. So that whenever branch office A wants to talk to branch office B, headquarter plays as a VPN relay. Users can gain benefit from such application when the scale of branch offices is very large, because no additional VPN tunnels between branch offices are needed. In this support note, we skip the detailed configuration steps for Internet access and presume that you are familiar with basic ZyNOS VPN configuration.

As the figure shown below, each branch office have a VPN tunnel to headquarter, thus PCs in branch offices can access systems in headquarter via the tunnel. Through VPN routing, ZyWALL series now provide you a solution to let PCs in branch offices talk to each other through the existing VPN tunnels concentrated on the headquarter.



The IP addresses we use in this example are as shown below.

Branch_A	Headquarter	Branch_B
WAN:202.3.1.1	WAN:202.1.1.1	WAN:202.2.1.1
LAN:192.168.3.1	LAN:192.168.1.1	LAN:192.168.2.1
LAN of Branch_A	LAN of Headquarter	LAN of Branch_B
192.168.3.0/24	192.168.1.0/24	192.168.2.0/24

# 1. Setup VPN in branch office A

Because VPN routing enables branch offices to talk to each other via tunnels concentrated on headquarter. In this step, we configure an IPSec rule in ZyWALL (Branch\_A) for PCs behind branch office A to access both LAN segments of headquarter and branch office B. Because the LAN segments of headquarter and branch office B are continuous, we merge them into one single rule by including these two segments in **Remote** section. If by any chance, the two segments are not continuous, we strongly recommend you to setup different rules for these segments.

1. Go to SECURITY->VPN->Press Add button

- 2. check **Active** check box and give a name to this policy.
- 3. Give this VPN rule a name, **Branch\_A**.
- 4. Select Key Management to IKE and Negotiation Mode to Main.
- 5. In Local section, select Address Type to Range Address, set IP Address Start to 192.168.3.0, and End to 192.168.3.255. This section covers the LAN segment of branch office A.
- 6. In Remote section, select Address Type to Range Address, set IP Address Start to 192.168.1.0 and End to 192.168.2.255. This section covers the LAN segment of both headquarter and branch office B.
- 7. My IP Addr is the WAN IP of this ZyWALL, 202.3.1.1.
- 8. Set Secure Gateway Addr to the IP address of Headquarter, 202.1.1.1.
- 9. Select Encapsulation Mode to Tunnel.
- 10. Check the **ESP** check box. (AH can not be used in SUA/NAT case)
- 11. Select **Encryption Algorithm** to **DES** and **Authentication Algorithm** to **SHA-1**. These parameters are for IKE phase 2 negotiation. You can set more detailed configuration by pressing **Advanced** button.
- 12. Enter the key string 12345678 in the Pre-shared Key text box, and click Apply.

Property	
Active	
Keep Alive	
NAT Traversal	Private t
Name	Branch_A
Key Management	IKE _
Negotiation Mode	Main
Encapsulation Mode	Tunnel
DNS Server (for IPSec VPN)	0.0.0.0
Extended Authentication	
Enable Extended Authentication	n second s
Server Mode	(Search Local User first then RADIUS)
C Client Mode	
User Name	
Password	
Local Policy	
Address Type	Range Address 💌
Starting IP Address	192.168.3.0
Ending IP Address / Subnet Mask	192 . 168 . 3 . 255
Remote Policy	
	Down Address w
Address Type	Range Address ·
Starting IP Address	192 . 167 . 1 . 0
Ending IP Address / Subnet Mask	192 . 168 . 2 . 255
Authentication Method	
Pre-Shared Key	12345678
C Certificate	auto_generated_self_signed_cert 🔽 (See My Certificates)
Local ID Type	IP 💌
Content	
Peer ID Type	IP •
Content	
Gateway Information	
My Address	
IP Address	202 . 3 . 1 . 1
🔿 My Domain Name	None 🕑 (See DDNS)
Secure Gateway Address	200.1.1.1
PSec Algorithm	
	C AH
Encryption Algorithm	DES  Authentication Algorithm MD5
Authentication Algorithm	MD5 💌
Advanc	ed Apply Cancel

You can setup IKE phase 1 and phase 2 parameters by pressing **Advanced** button. Please make sure that parameters you set in this menu match with all the parameters with the correspondent VPN rule in headquarter.

Negotiation Mode Encryption Algorithm Authentication Algorithm SA Life Time (Seconds) Key Group	Main  DES  MD5  28800 DH1
hase 2	
Active Protocol Encryption Algorithm Authentication Algorithm SA Life Time (Seconds) Encapsulation Perfect Forward Secrecy (PFS) Enable Replay Detection Protocol Local Port Start End Remote Port Start End	ESP - DES - MD5 - 28800 Tunnel - NONE - 0 0 0 0

## 2. Setup VPN in branch office B

Be very careful about the remote IP address in branch office B, because for systems behind branch office B want to systems behind branch office A and headquarter, we have to specify these two segments in **Remote** section. However if we include these two segments in one rule, the LAN segment of branch office B will be also included in this single rule, which means intercommunication inside branch office B will run into VPN tunnel. To avoid such situation, we need two separate rules to cover the LAN segment of branch office A and headquarter.

This rule is for branch office B to access headquarter's LAN and Branch A's LAN.

Property		I)
Active		
🗖 Keep Alive		
NAT Traversal		
Name	Branch_B	
Key Management	IKE 💽	
Negotiation Mode	Main	
Encapsulation Mode	Tunnel	D
DNS Server (for IPSec VPN)	0.0.0.0	
Extended Authentication		
Enable Extended Authenticati		
Server Mode	(Search Local User first then RADIUS)	
C Client Mode		
User Name		
Password		
Local Policy		٩,
Address Type	Range Address 💌	
Starting IP Address	192 . 168 . 2 . 0	
Ending IP Address / Subnet Mask	192 . 168 . 2 . 255	
Remote Policy		i.
Address Type	Range Address 💌	
Starting IP Address	192 . 168 . 1 . 0	
Ending IP Address / Subnet Mask	192 . 168 . 3 . 255	
	102,100,10,120	
Authentication Method		
Pre-Shared Key	12345678	
C Certificate	auto_generated_self_signed_cert 💽 (See My Certificates)	
Local ID Type	IP 🗾	
Content		
Peer ID Type	IP 👱	
Content		
Gateway Information		
My Address		
IP Address	202 . 2 . 1 . 1	
My Domain Name	None (See DDNS)	
Secure Gateway Address	200.1.1.1	
IPSec Algorithm		ľ
	C AH	
Encryption Algorithm	DES 💌 Authentication Algorithm MD5 💌	
Authentication Algorithm	MD5 💌	
Advan	ced Apply Cancel	

Note that since Branch B's LAN is also included in remote policy, please go to ZyWALL's SMT menu 24.8 CI command mode, and issue this command, "ipsec swSkipOverlapIp on", so that local management traffic from Branch B's LAN PC to Branch B's ZyWALL would not go into VPN process.

You can setup IKE phase 1 and phase 2 parameters by pressing **Advanced** button. Please make sure that parameters you set in this menu match with all the parameters with the correspondent VPN rule in headquarter.

Encryption Algorithm Authentication Algorithm SA Life Time (Seconds) Key Group	DES MD5 28800 DH1	R	
hase 2			
Active Protocol Encryption Algorithm Authentication Algorithm SA Life Time (Seconds) Encapsulation Perfect Forward Secrecy (PFS) Enable Replay Detection Protocol Local Port Start End Remote Port Start End	ESP DES MD5 28800 Tunnel NONE 0 0 0 0 0 0 0 0 0		

#### 3. Setup VPN in Headquarter

1. The correspondent rule for Branch\_A in headquarter

Image: Extended Authentication       (Search Local User first then RADIUS)         Image: Client Mode       User Name         User Name       Password         Decal Policy       Image Address Image         Address Type       Range Address Image         Starting IP Address       192 . 168 . 1 . 0         Ending IP Address       192 . 168 . 2 . 255         Address Type       Range Address Image         Starting IP Address       192 . 168 . 3 . 0         Ending IP Address       192 . 168 . 3 . 0         Ending IP Address       192 . 168 . 3 . 0         Ending IP Address       192 . 168 . 3 . 0         Ending IP Address       192 . 168 . 3 . 0         Ending IP Address       192 . 168 . 3 . 0         Ending IP Address       192 . 168 . 3 . 0         Ending IP Address       192 . 168 . 3 . 0         Ending IP Address       192 . 168 . 3 . 0         Ending IP Address       192 . 168 . 3 . 0         Ending IP Address       192 . 168 . 3 . 0         Ending IP Address       192 . 168 . 3 . 0         Ending IP Address       Image Address . 0         Content       Image Address . 0         Decari ID Type       Image Address . 0         Endeway Information       Image Address . 0	Property	
I NAT Traversal   Name   Name <td< th=""><th></th><th></th></td<>		
Name       indEranch_A         Key Management       IVE         Name       IVE         Encapsulation Mode       Tunnel         DNS Server (for IPSec VPN)       0.0.0         Extended Authentication       Server Mode         Server Mode       Search Local User first then RADIUS)         Client Mode       Server Mode         Password       IVE         Address Type       Range Address •         Starting IP Address       192 . 168 . 1 . 0         Ending IP Address / Subnet Mask       192 . 168 . 3 . 0         Ending IP Address       192 . 168 . 3 . 0         Ending IP Address       192 . 168 . 3 . 0         Ending IP Address       192 . 168 . 3 . 0         Ending IP Address       192 . 168 . 3 . 0         Ending IP Address       192 . 168 . 3 . 0         Ending IP Address       192 . 168 . 3 . 0         Ending IP Address       192 . 168 . 3 . 0         Ending IP Address       192 . 168 . 3 . 0         Ending IP Address       192 . 168 . 3 . 0         Encapsulation Method       192 . 168 . 3 . 0         Content       192 . 103 . 3 . 255         Address       192 . 103 . 3 . 255         Address       202 . 1 . 1 . 1         Fore		
Key Management       IKE         Negotiation Mode       Main         Encapsulation Mode       Tunnel         DNS Server (for IPSec VPN)       0.0.0         Extended Authentication       Server Mode         Cheen Mode       Server Mode         User Name       Server Mode         Password       Server Mode         Local Policy       Address         Address Type       Range Address         Starting IP Address       192, 168, 1, 0         Inding IP Address       192, 168, 2, 255         Remote Policy       Address S         Address Type       Range Address S         Starting IP Address       192, 168, 3, 0         Ending IP Address       192, 168, 3, 0         Content       IP = M         Content       IP = M         Content       IP = M         Peer ID Type       IP = M         Content       IP = M         Point Mode       202, 1, 1, 1, 1         My Address       202, 1, 1, 1, 1         My Address       203, 3, 1         <		
Negotiation Mode       Main         Encapsulation Mode       Tunnel         DNS Server (for IPSec VPN)       0.00.0         Extended Authentication       Search Local User first then RADIUS         Cilcuit Mode       (Search Local User first then RADIUS)         Collot Mode       (Search Local User first then RADIUS)         Collot Mode       (Search Local User first then RADIUS)         Collot Mode       (Search Local User first then RADIUS)         Main Paddress       (Search Local User first then RADIUS)         Content       (Search Local User first then RADIUS)         My Address       (Search Local User first then RADIUS)         Secure Content       (Search Local User first then RADIUS)         My A		
Encapsulation Mode DNS Server (for IPSec VPN) D.0.0.0 Extended Authentication © Server Mode © Server Gateway Address © Server Sateway Address © Server Gateway Address © Server G		
DNS Server (for IPSec VPN) 0.0.0 Extended Authentication Server Mode User Name Password Local Policy Address Type Starting IP Address Ending IP Address Subnet Mask 192 . 168 . 1 . 0 Ending IP Address Subnet Mask 192 . 168 . 2 . 255 Remote Policy Address Type Range Address © Starting IP Address Subnet Mask 192 . 168 . 3 . 0 Endi		
Extended Authentication		
Image: Enable Extended Authentication         • Server Mode       (search Local User first then (ADDUS)         • Client Mode         User Name         Password         Local Policy         Address Type       Range Address •         Starting IP Address       192 . 168 . 1 . 0         Ending IP Address       192 . 168 . 2 . 255         Remote Policy       Address •         Address Type       Range Address •         Starting IP Address       192 . 168 . 3 . 0         Ending IP Address       192 . 168 . 3 . 0         Ip 2 . 168 . 3 . 0       192 . 168 . 3 . 0         Ending IP Address       192 . 168 . 3 . 0         Ending IP Address       192 . 168 . 3 . 0         Ending IP Address       192 . 168 . 3 . 0         Ending IP Address       192 . 168 . 3 . 0         Ending IP Address       192 . 168 . 3 . 0         Ending IP Address       192 . 168 . 3 . 0         Content       auto_generated_self_signed_cent       (See My Certificates)	DNS Server (for IPSec VPN)	0.0.0.0
• Server Mode         • Client Mode         User Name         Password           (Search Local User first then RADIUS)             • Client Mode         User Name         Password           Password             Local Policy           Address ▼             Address Type           Range Address ♥             Starting IP Address           192 . 163 . 1 . 0             Ending IP Address           192 . 163 . 2 . 255             Remote Policy           Address ▼             Address Type           Range Address ♥             Starting IP Address           192 . 163 . 3 . 0             Bending IP Address           192 . 163 . 3 . 0             Starting IP Address           192 . 163 . 3 . 0             Bending IP Address           192 . 163 . 3 . 0             Starting IP Address           192 . 163 . 3 . 0             Content           192 . 163 . 3 . 0             Content           IP             Content           Content             My Address	Extended Authentication	
Client Mode User Name Password Local Policy Address Type Range Address ♥ Starting IP Address Subnet Mask 192.168.1.0 Ending IP Address / Subnet Mask 192.168.2.255 Remote Policy Address Type Range Address ♥ Starting IP Address I 192.168.3.0 Ending IP Address / Subnet Mask 192.168.3.		
User Name Password Local Policy Address Type Range Address * Starting IP Address   122.168.1.0 Ending IP Address / Subnet Mask 122.168.2.255 Remote Policy Address Type Range Address * Starting IP Address   192.168.3.0 Ending IP Address   192.168.3.0 Ending IP Address   192.168.3.0 Ending IP Address   1245678 Certificate subnet Mask 122.168.3.255 Authentication Method		(Search Local User first then RADIUS)
Password         Local Policy         Address Type       Range Address ♥         Starting IP Address       192.168.1.0         Ending IP Address / Subnet Mask       192.168.2.255         Remote Policy       Address ♥         Address Type       Range Address ♥         Starting IP Address       192.168.3.0         Ending IP Address       192.168.3.0         Ending IP Address       192.168.3.0         Ending IP Address       192.168.3.0         Ending IP Address       192.168.3.0         Content       192.168.3.0         Pere Shared Key       12345678         Content       IP ♥         Content       IN One ♥ (See DDNS)         Secure Gateway Address       203.1.1         IPSec Algorithm       IN One ♥ (See DDNS)         Secure Gateway Address       203.1.1		
Local Policy Address Type Range Address  Starting IP Address ID2 . 168 . 1 . 0 Ending IP Address / Subnet Mask ID2 . 168 . 2 . 255 Remote Policy Address Type Range Address  Starting IP Address ID2 . 168 . 3 . 0 Ending IP Address ID2 . 168 . 3 . 0 Ending IP Address / Subnet Mask ID2 . 168 . 3 . 255 Authentication Method  Pre Shared Key ID245678 Content ID Type IP  Content Peer ID Type IP  Content Sateway Information My Address P ID Address ID2 . 1 . 1 . 1 My Address P ID Address ID2 . 1 . 1 . 1 My Address P Address ID2 . 1 . 1 . 1 My Address P ID Address ID2 . 1 . 1 . 1 My Address P ID Address ID2 . 1 . 1 . 1 My Address P ID Type ID Content Peer ID Type ID Content Peer ID Type ID Content Peer ID Type ID Content P ID ID Content P ID CONTE		
Address Type Range Address   Starting IP Address 192 . 168 . 1 . 0   Inding IP Address / Subnet Mask 192 . 168 . 2 . 255   Remote Policy Address Type   Address Type Range Address •   Starting IP Address 192 . 168 . 3 . 0   Ending IP Address 192 . 168 . 3 . 0   Ending IP Address 192 . 168 . 3 . 0   Ending IP Address 192 . 168 . 3 . 0   Ending IP Address 192 . 168 . 3 . 0   Ending IP Address 192 . 168 . 3 . 0   Ending IP Address 192 . 168 . 3 . 0   Ending IP Address 192 . 168 . 3 . 0   Ending IP Address 192 . 168 . 3 . 0   Ending IP Address 192 . 168 . 3 . 0   Ending IP Address 192 . 168 . 3 . 0   Certificate 192 . 168 . 3 . 0   Ending IP Address 192 . 168 . 3 . 0   Certificate 192 . 168 . 3 . 0   Encertificate 192 . 168 . 3 . 0   Ical ID Type IP •   Content IP •   Content IP •   Peer ID Type IP •   Content IP •   My Address 202 . 1 . 1 . 1   * IP Address 202 . 1 . 1 . 1   * My Domain Name None (See DDNS)   Secure Gateway Address 200 3 . 1   Peer ID Type IP •   * IP Address 200 3 . 1   * IP Address 200 3 . 1   * IP Address 200 3 . 1	Password	
Starting IP Address       192.168.1.0         Ending IP Address / Subnet Mask       192.168.2.255         Remote Policy       Address *         Address Type       Range Address *         Starting IP Address       192.168.3.0         Ending IP Address       192.168.3.0         Cantent       192.168.3.0         Pre-Shared Key       12345578         Certificate       auto_generated_self_signed_cert *         Local ID Type       IP *         Content       IP *         Peer ID Type       IP *         Content       IP *         Content       IP *         Content       IP *         Peer ID Type       IP *         Content       IP *         Secure Gateway Address       202.1.1.1.1         PSec Algorithm       None * (See DDNS)         Secure Gateway Address       200.3.1.1	Local Policy	
Starting IP Address       192.168.1.0         Ending IP Address / Subnet Mask       192.168.2.255         Remote Policy       Address *         Address Type       Range Address *         Starting IP Address       192.168.3.0         Ending IP Address / Subnet Mask       192.168.3.0         Image Address *       192.168.3.0         Starting IP Address / Subnet Mask       192.168.3.0         Image Address *       192.168.3.0         Starting IP Address / Subnet Mask       192.168.3.0         Image Address *       192.168.3.0         Starting IP Address / Subnet Mask       192.168.3.0         Cantent       192.168.3.255         Local ID Type       IP *         Content       IP *         Peer ID Type       IP *         Content       IP *         Content       IP *         My Address       202.1.1.1.1         * IP Address       202.1.1.1.1         * My Domain Name       None * (See DDNS)         Secure Gateway Address       200.3.1.1         IPSec Adgorithm       IPS *	Address Type	Range Address 💌
Ending IP Address / Subnet Mask 192, 168, 2, 255  Remote Policy  Address Type Range Address  Starting IP Address 192, 168, 3, 0 Ending IP Address Subnet Mask 192, 168, 3, 0 Ending IP Address / Subnet Mask 192, 168, 3, 255  Authentication Method  Pre-Shared Key 12345678 Content auto_generated_self_signed_cert (See My Certificates) Local ID Type IP  Content  Peer ID Type IP  Content   My Address 202, 1, 1, 1 My Address 200, 31, 1  PSec Algorithm  PEES CALGORITHM DES CALGORITHM MD5		( and a second
Remote Policy         Address Type       Range Address ♥         Starting IP Address       192,168,3,0         Ending IP Address / Subnet Mask       192,168,3,255         Authentication Method       192,168,3,255         Certificate       12345578         Local ID Type       IP ♥         Content       IP ♥         Peer ID Type       IP ♥         Content       IP ♥         Seleway Information       202,1,1,1,1         My Address       202,1,1,1,1         © Hy Domain Name       None ♥ (See DDNS)         Secure Gateway Address       200,3,1,1         IPSec Algorithm       DES ♥		
Address Type Range Address ▼   Starting IP Address 192 . 168 . 3 . 0   Ending IP Address / Subnet Mask 192 . 168 . 3 . 0   192 . 168 . 3 . 0 192 . 168 . 3 . 0   192 . 168 . 3 . 0 192 . 168 . 3 . 0   Authentication Method 192 . 168 . 3 . 265   Authentication Method <ul> <li>Pre-Shared Key</li> <li>12345678</li> <li>Certificate</li> <li>auto_generated_self_signed_cert ▼</li> <li>(See My Certificates)</li> <li>Local ID Type</li> <li>IP ▼</li> <li>Content</li> <li>Peer ID Type</li> <li>IP ▼</li> <li>Content</li> <li>IP Address</li> <li>○ 19 Address</li> <li>○ 202 . 1 . 1 . 1</li> <li>○ My Domain Name</li> <li>None ♥ (See DDNS)</li> <li>Secure Gateway Address</li> <li>200.3.1.1</li> </ul> IPSec Algorithm IDES ▼		
Starting IP Address       192.168.3.0         Ending IP Address / Subnet Mask       192.168.3.0         Authentication Method       192.168.3.255         Authentication Method       • Pre-Shared Key         • Pre-Shared Key       12345678         • Certificate       auto_generated_self_signed_cert ♥ (See My Certificates)         Local ID Type       IP ♥         Content       IP ♥         Content       IP ♥         Gateway Information       None ♥ (See DDNS)         Secure Gateway Address       200.3.1.1         PSec Algorithm       IPS ♥	Remote Foncy	
Ending IP Address / Subnet Mask 192 . 168 . 3 . 255 Authentication Method Pre-Shared Key 12345678 Certificate auto_generated_self_signed_cert (See My Certificates) Local ID Type IP . Content . Peer ID Type IP . Content . Gateway Information My Address 202 . 1 . 1 . 1 My Domain Name None (See DDNS) Secure Gateway Address 200.3.1.1 PSec Algorithm IDES Authentication Algorithm MD5 .	Address Type	
Authentication Method   Pre-Shared Key Certificate auto_generated_self_signed_cert Local ID Type Content Peer ID Type Content  Gateway Information  My Address PIP Address Planderss 202.1.1.1  Mone (See DDNS) Secure Gateway Address 200.3.1.1  PSec Algorithm  PES Authentication Algorithm  MD5	Starting IP Address	192.168.3.0
Pre-Shared Key 12345678   Certificate auto_generated_self_signed_cert (See My Certificates)   Local ID Type P   Content P   Peer ID Type P   Content P   Gateway Information   My Address   • IP Address   • IP Address   202 . 1 . 1 . 1   • My Domain Name   Secure Gateway Address   200.31.1   IPSec Algorithm   PESP   Cath   Cath   DES	Ending IP Address / Subnet Mask	192 . 168 . 3 . 255
Certificate auto_generated_self_signed_cert ♥ (See My Certificates) Local ID Type	Authentication Method	
Certificate auto_generated_self_signed_cert ♥ (See My Certificates) Local ID Type	• Pre-Shared Key	12345678
Local ID Type P Content Peer ID Type P Content Content Con		
Content Peer ID Type Content Gateway Information My Address © IP		
Content Gateway Information My Address		
Content Gateway Information My Address	Peer ID Type	
Gateway Information My Address © IP Address Descent for the second se		
My Address       202 . 1 . 1 . 1         IP Address       202 . 1 . 1 . 1         My Domain Name       None (See DDNS)         Secure Gateway Address       200.3.1.1         IPSec Algorithm       C AH         Encryption Algorithm       DES (Authentication Algorithm MD5 (See DDNS))		
IP Address     202 . 1 . 1 . 1       My Domain Name     None (See DDNS)       Secure Gateway Address     200.3.1.1       IPSec Algorithm     C AH       Encryption Algorithm     DES (Authentication Algorithm MD5 (MD5))		
My Domain Name     None (See DDNS)       Secure Gateway Address     200.3.1.1       IPSec Algorithm     C AH       Encryption Algorithm     DES (Authentication Algorithm MD5)	- 0 2 7 8 9 8 9 8 9 8 9 9 9 9 9 9 9 9 9 9 9 9	-
Secure Gateway Address 200.3.1.1		and the second se
IPSec Algorithm  C AH  Encryption Algorithm  DES  Authentication Algorithm  MD5		And a second s
© ESP C AH Encryption Algorithm DES S Authentication Algorithm MD5 S	Secure Gateway Address	200.3.1.1
Encryption Algorithm DES 💌 Authentication Algorithm MD5 🗾	IPSec Algorithm	
		CAH
		DES  Authentication Algorithm MD5
	Authentication Algorithm	

Encryption Algorithm	ESP 💌		
Encryption Algorithm	ESP .		
SA Life Time (Seconds) 2 Encapsulation 2 Perfect Forward Secrecy (PFS)	DES V MD5 V 18800 Tunnel V NONE V NONE V		

2. The correspondent rule for Branch\_B

Property	
Active	
Keep Alive	
NAT Traversal	
Name	toBranch_B
Key Management	IKE _
Negotiation Mode	Main
Encapsulation Mode	Tunnel
DNS Server (for IPSec VPN)	0.0.0.0
Extended Authentication	
Enable Extended Authenticatio	
Server Mode	(Search Local User first then RADIUS)
Client Mode	
User Name	
Password	
Local Policy	
Address Type	Range Address 💌
Starting IP Address	192 . 168 . 1 . 0
Ending IP Address / Subnet Mask	192 . 168 . 3 . 255
Remote Policy	4
Address Type	Range Address 💌
Starting IP Address	192.168.2.0
Ending IP Address / Subnet Mask	192 . 168 . 2 . 255
Authentication Method	
Pre-Shared Key	12345678
C Certificate	auto_generated_self_signed_cert - (See My Certificates)
Local ID Type	IP •
Content	
Peer ID Type	IP •
Content	
Gateway Information	
My Address	200 1 1 1
IP Address     Address	202.1.1.1
C My Domain Name	None (See DDNS)
Secure Gateway Address	200.2.1.1
IPSec Algorithm	
	AH
Encryption Algorithm	DES  Authentication Algorithm MD5
Authentication Algorithm	MD5 💌
	ed Apply Cancel

Negotiation Mode     M       Encryption Algorithm     Did       Authentication Algorithm     M       SA Life Time (Seconds)     28       Key Group     Did
hase 2
Active Protocol       Excryption Algorithm       Display to the second s
Remote Port Start 0

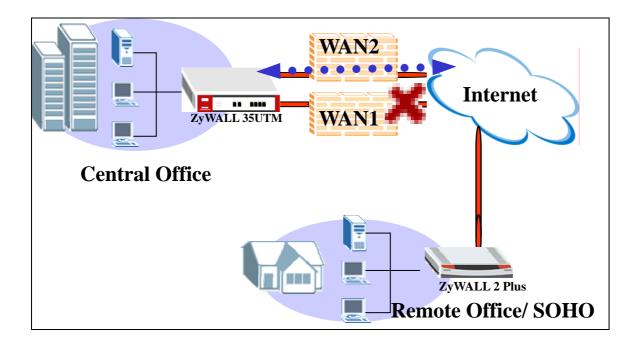
#### Never lost your VPN connection (IPSec High Availability)

#### Setup ZyWALL VPN with high availability

VPN high availability is designed for securing VPN connections. Usually ZyWALL2 Plus is deployed at the branch office or as aSOHO gateway to establish a VPN tunnel to the central office. ZyWALL2 Plus is desgined for IPSec HA as a redundant gateway can be configured.

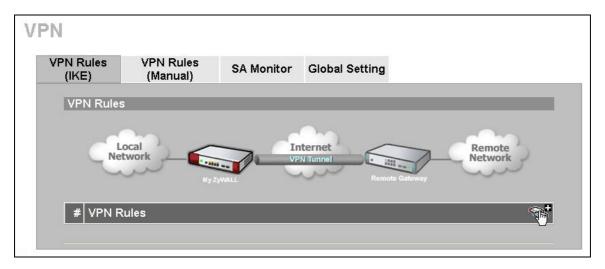
Previously, when Internet connection on the remote gateway is down, the VPN connection automatically disconnects. This is avoided with the dual WAN connection feature on ZyXEL security gateways. When the primary WAN connection is down, ZyXEL's dual WAN connection feature backs up the primary WAN connection and automatically transfers VPN connections to the secondary WAN connection. In addition, DDNS is updated to the secondary WAN connection.

ZyWALL 2 Plus, as a redundant remote gateway, provides always-on Internet and VPN connectivity for network flexibility. You can configure an IP address or domain name depends on the Network deployment.



#### How to configure the VPN HA

- 1. Log into the web configurator on the ZyWALL. In a web browser, enter the IP address (the default is **192.168.1.1**) of your ZyWALL in the Address field. A screen displays, enter the administrative login password (**1234** is the default).
- 2. Click SECURITY > VPN and click Add.

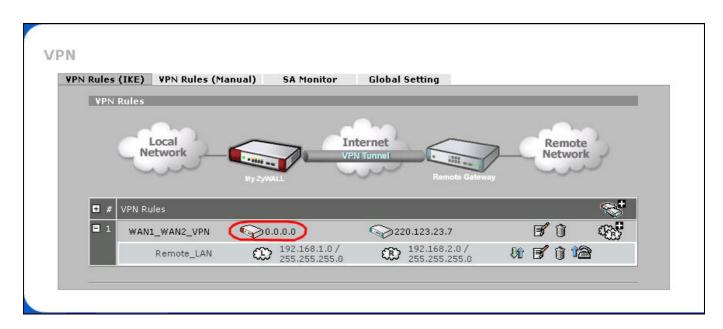


- 3. Enter a descriptive name for the VPN policy. For example, "Dual\_GW\_VPN<sup>..</sup>."
- 4. Enter the WAN IP address (220.123..23.7 in this example) of the ZyWALL in the **My** Address field.
- 5. Enter the WAN address (61.79.95.3 in this example) of the remote VPN gateway in the **Primary Remote Gateway IP Address** field.

- 6. Select **Enable IPSec High Availability** to activate the IPSec HA feature and enter the IP address of WAN2 (61.82.69.2 in this example) in the **Redundant Remote Gateway** field.
- 7. If you want the ZyWALL to route all traffic through the primary WAN connection again, select **Fail back to Primary Remote Gateway when possible**. You must enter the time interval to check the availability of the primary WAN connection. In this example, the check interval is 28800 seconds.
- 8. Set the other fields in the configuration screen depending on your network environment.

Name	Dual_GW_VPN	
🔲 NAT Traversal		
Sateway Policy Information		
My ZyWALL		
My Address	220.123.23.7	(Domain Name or IP Address)
🔍 My Domain Name	None 🗾 (See DDNS)	
🌍 Primary Remote Gateway	61.79.65.3	(Domain Name or IP Address)
🔽 Enable IPSec High Availability		
🥪 Redundant Remote Gateway	61.82.69.2	(Domain Name or IP Address)
🔽 Fail back to Primary Remote Gatew	ay when possible	
Fail Back Check Interval*	28800 (180~86400	seconds)

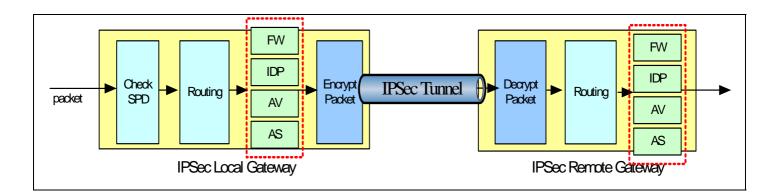
9. After configuring VPN settings on the local ZyWALL 2 Plus, you must also create a VPN tunnel on the remote VPN gateway to connect from the central office to the ZyWALL 2 Plus in the branch office. If you are using ZyWALL 70 or ZyWALL 35 as the remote VPN gateway, you also get the redundant WAN/VPN feature. In this case, enter 0.0.0.0 in the My IP Address field to set the system to automatically detect the IP address of the active WAN interface. Thus if the primary WAN interface is down, the My Address field is the IP address of the secondary WAN interface.



## Access control and security VPN connection (Security policy enforcement IPSec)

<u>Setup ZyWALL VPN with access control - Firewall</u> <u>Setup ZyWALL VPN with security policy enofrcement – AV/IDP/AS</u> <u>Setup ZyWALL VPN with web filtering rule – Content Filter</u>

Normally, the traffic transmitted between VPN tunnel is treated as security connection due on multi authentication and encryption methods. Thus, the security gateway won't inspect the VPN traffic because the traffic sending with cipher text format not in plaintext. The enhanced algorithm we adopted is ZyWALL can inspect the VPN packet before encrypt or after decrypt the packet sending to or receiving from VPN tunnel.



#### How to configure access control rule over VPN

- 1. Log into the web configurator on the ZyWALL. In a web browser, enter the IP address (the default is **192.168.1.1**) of your ZyWALL in the Address field. A screen displays, enter the administrative login password (**1234** is the default).
- 2. Access control in VPN tunnel application can be enforced via Firewall feature. Switch to Security>Firewall menu to configure the traffic from VPN or to VPN access control rule.

Default Rule	Rule Summary	Anti-Probing	Threshold	Service	
Default Rul	e Setup				
Allow	le Firewall Asymmetrical Route ( AN, and VPN to VPN p	Warning: When this b ackets will bypass the	ox is checked, all LAN Firewall check.)	to LAN, WAN to WAN	DMZ to DMZ, WLAN
From	To LAN	WAN	DMZ	WLAN	¥₽N
LAN	Permit 💌 🛄	Permit 💌 🔲	Permit 💌 🔲	Permit 💌 🗌	Permit 💌 🔲
WAN	Drop 💌 🗹	Drop 💌 🗹	Permit 💌 🗖	Drop 💌 🗹	Permit 💌 🗖
DMZ	Drop 💌 🗹	Permit 💌 🗖	Drop 💌 🗹	Drop 💌 🗹	Permit 💌 🗖
WLAN	Drop 💌 🗹	Permit 💌 🔲	Drop 😽 🔽	Drop 💌 🗹	Permit 💌 🗖
¥₽N	Permit 💌 🗌	Permit 💌 🗌	Permit 💌 🔲	Permit 💌 🗌	Permit 💌 🗌
2				* 🔽	Log

3. For example, the remote VPN policy is 192.168.2.0/24 and we want to block the traffic from 192.168.2.33 to access local LAN subnet 192.168.1.0/24. The default VPN to LAN traffic is permit and we have to change the VPN to LAN access control rule in rule summary sub menu.

efault Rule	Rule Summary An	ti-Probing Threshold 9	Service
Rule Sumn	iary		
Firewall R	ules Storage Space in Use		
0%			100%
Insert		<mark>:tination Address   Service Typ</mark> L mber) mber)	e Action Sch. Log Modify

4. Click the Insert button to insert a new rule.

	Rule Summary	Anti-Probing	Threshold	Service	
Rule Sumr	nary				
Firewall R	ules Storage Space in	Use			
0%			1%		100%
Packet D	irection: VPN to LAN	*			
	olicy: Permit, None Log				
# Nan	ne Active Source Ad	ldress Destinatio	n Address   Servic	e Type Action Sch	n. Log Modify
	new rule before rule 1	(rule number)			
Insert	A CONTRACTOR OF	(rule number)			
Sector Se	Fule 1 to rule 1				

5. Edit the source and destination address as 192.168.2.33 and 192.168.1.0/255.255.255.0

Rule Name	VPN_Block	
Edit Source Address	5	
Address Editor		Source Address(es)
Address Type	Any Address	192.168.2.33
Start IP Address	0.0.0.0	
End IP Address	0.0.0.0	
Subnet Mask	0.0.0.0	
Add Modify		Delete
Edit Destination Ad	dress	
Address Editor		Destination Address(es)
Address Type	Any Address 🛛 👻	192.168.1.0 / 255.255.255.0
Start IP Address	0 , 0 , 0 , 0	
End IP Address	0 , 0 , 0 , 0	
Subnet Mask	0.0.0.0	
Add Modify		Delete
Edit Service		

6. The service type is **Any** to block all kind of traffic from 192.168.2.33 to access LAN subnet and **Action for Matched Packets** is **Drop** and then click apply to save and activate the configuration.

Edit Service		
Available Services (See Service)		Selected Service(s)
*ECHO REPLY(ICMP:Type:0/Code:0) *ECHO REQUEST(ICMP:Type:8/Code:0) Any(TCP) Any(UDP) Any(ICMP) AIM/NEVV_ICQ(TCP:5190) AUTH(TCP:113) BGP(TCP:179)		Any(All)
BOOTP_CLIENT(UDP:68) BOOTP_SERVER(UDP:67) CU-SEEME(TCP/UDP:7648,24032) DNS(TCP/UDP:53) FINGER(TCP:79) FTP(TCP:20,21) H.323(TCP:1720)	22	
Edit Schedule		
Day to Apply: ✓ Sun ✓ Mon ✓ Tue ✓ Wed ✓ Thu ✓ Time of Day to Apply: (24-Hour Format) ✓ All day Start: 0 (Hour) 0 (Minute) End: 0		Minute)
Actions When Matched		
✓ Log Packet Information When Matched		
Send Alert Message to Administrator When Action for Matched Packets	Matched	
Apply	Ca	ancel

7. We can see a new rule had been configured and showed in the rule summary page. This will achieve our goal to block all traffic from VPN remote host 192.168.2.33 to access the LAN subnet.

efault Rule	Rule Summary	Anti-Probing	Threshold	Service	_	
Rule Summ	iary					
Firewall R	ules Storage Space in	Use				
0%						100%
Packet Di	rection: VPN to LAN	~				
	olicy: Permit, None Loc	harmen and a				
🛨 # Na	me Active Source	Address Destina	ation Address Se	rvice Type Action		Modify
±1 VPN_	Block <u>Y</u> 192.10	68.2.33 💌 192.168.1.0	) / 255.255.255.0 💌	Any(All) 🚩 Drop	No Yes	<b>F</b> Û
	new rule before rule 1	(rule number)				
Move	rule 1 to rule 1	(rule number)				

## How to configure Security policy (AV/IDP/AS) over VPN

 Please make sure ZyWALL has valid service registration before activate the security policy check (AV/IDP/AS) over VPN. The registration status can be checked in menu Registration>Service. Click the Service License Refresh button to retrieve the service registration status from myzyxel.com.

egistration Service			
Service Management			
Service	Status	Registration Type	Expiration Day
Content Filter Service	Active	Standard	2008-04-03
Anti-Spam Service	Active	Standard	2008-08-30
IDP/Anti-Virus Service	Active	Standard	2008-08-30
License Upgrade			
License Key	Update		

2. The IDP, AV and AS scan direction is configurable in the general setting page. Thus, we can force the ZyWALL scan the traffic from VPN to any destination. VPN to VPN traffic means there are more than one tunnel connected to one ZyWALL and the traffic pass thought one VPN tunnel to another VPN tunnel will apply the VPN to VPN traffic type.



ieneral Signatu	re l	Jpdate	Backup & Re	store		
General Setup						
🗹 Enable Intrusion De	tection and Preve	ntion				
Turbo Card	Installed					
		WAN	DMZ	WLAN	<b>V</b> PN	
From						
WAN						
DMZ						
WLAN						
<b>V</b> PN [						
				* Protected 1	raffic Direction	

3. The configurable scan direction configuration also applies in AntiVirus and ZyWALL can inspect the packet either from VPN or to VPN as well.

General	Signature	Up	date Ba	ckup & Restore	,		
General Set	ир						
🗹 Enable	Anti-Virus						
🗹 Enable	ZIP File Scan						
Turbo C	ard	Installed					
Available Se	rvice						
Service		FTP (TCP 20 HTTP (TCP 8 POP3 (TCP 1 SMTP (TCP 2	80, 8080, 3128) 110)				
🗹 Active	FTP						
	То	LAN	WAN	DMZ	WLAN	<b>V</b> PN	
From							
LAN	· 🗖						
WAW		<b>V</b>	<ul><li>✓</li></ul>		<b>V</b>		
DMZ							
WLA	N 🗖	<b>V</b>	<b>V</b>		<b>V</b>		
		✓	✓				
¥PN					* Protected 1	Traffic Direction	
<b>V</b> PN							

4. The AntiSpam also has the matrix to configure the inspection direction. Thus, we can

configure the mail send from VPN or to VPN and then mail can be inspected by the spam mail server.

eneral E	xternal DB	Li	ists			
General Setup						
🗹 Enable Anti-	-Spam					
	То	LAN	WAN	DMZ	WLAN	¥PN
From						
LAN						
WAN		<b>V</b>			<b>V</b>	
DMZ						
WLAN		<ul><li>✓</li></ul>	<ul><li>✓</li></ul>			
¥PN		<ul><li>✓</li></ul>		<b>V</b>		
					* Protected T	rattic Direction
Action for Spam	Mails					
Phishing Tag	[PHISHING]					
Sparn Tag	[SPAM]					
Forward SM	TP & POP3 ma	il with tag ir	n mail subject.			

5. The above three steps are used to enforce the security policy for VPN traffic and the VPN tunnel can decrease the threat from intrusion, malice attack, virus, worm, Trojan and spam mail flooding.

#### How to configure Web filtering rule over VPN - Content Filter

1. The switch to enable the content filtering over VPN traffic is available in Content Filter general configuration page. The content filtering over VPN can only be enabled after the content filter global switch enabled otherwise the enable content filter for VPN traffic option will be gray out.



TENT FIL	ΓER					
General	Categories	Customization	Cache			
General Se	tup					
	: Content Filter : Content Filter for VPI	V traffic				
Restrict W	eb Features					
Block	🗌 ActiveX	🗌 Java Appl	et 🗌	Cookies	🗌 Web Proxy	
Schedule t	o Block					
Alway	s Block					
O Block		]	то 0 :	0 (24-Hou	r Format)	
Message to	) display when a sit	e is blocked				
Redirect L	cess Message					
Redifectio						
Exempt Co	mputers					

2. The traffic decrypted from VPN tunnel and send to internet can be apply the web filtering rule after enable content filter for VPN traffic.

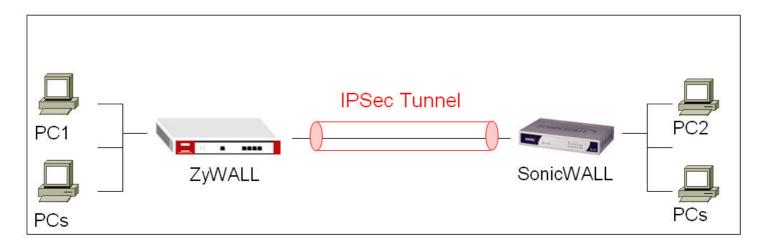
### ZyWALL vs 3rd Party VPN Gateway

#### SonicWALL with ZyWALL VPN Tunneling

- 1. <u>Setup ZyWALL VPN</u>
- 2. <u>Setup SonicWALL VPN</u>

This page guides us to setup a VPN connection between the ZyWALL and SonicWALL router.

As the figure shown below, the tunnel between PC1 and PC2 ensures the packet flows between them are secure. Because the packets go through the IPSec tunnel are encrypted. To setup this VPN tunnel, the required settings for ZyWALL and SonicWALL are explained in the following sections. As the red pipe shown in the following figure, **the tunneling endpoints are ZyWALL router and SonicWALL router**.

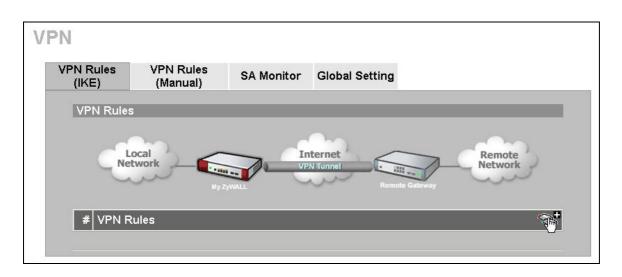


The IP addresses we use in this example are as shown below.

PC 1	ZyWALL	SonicWALL	PC2
192.168.1.33	WAN: 172.22.3.89 LAN: 192.168.1.1	WAN: 172.22.1.251 LAN: 192.168.168.618	192.168.168.6

#### 1. Setup ZyWALL VPN

- Using a web browser, login ZyWALL by giving the LAN IP address of ZyWALL in URL field. Default LAN IP is 192.168.1.1, default password to login web configurator is 1234.
- 2. Go to SECURITY->VPN->Press Add button



3. Give a name for your policy, for example "ToSonicWALL"

- 4. **My IP Addr** is the **WAN IP of ZyWALL**. In this example, you should type 172.22.3.89 IP address on **My ZyWALL** text box.
- 5. Secure Gateway IP Addr is the SonicWALL's WAN IP address. In this example, you should type 172.22.1.251 IP address on **Remote Gateway** text box.

Property		
Name	ToSonicWALL	
NAT Traversal     Gateway Policy Information		_
🖘 My ZyWALL	172.22.3.89	j.
Semote Gateway Address	172.22.1.251	
Address		

6. In Authentication Key, enter the key string 12345678 in the Pre-Shared Key text box.

Authentication Key	
• Pre-Shared Key	12345678
O Certificate	auto_generated_self_signed_cert - (See My Certificates)
Local ID Type	IP 🗸
Content	0.0.0.0
Peer ID Type	IP 💌
Content	0.0.0.0

7. Select Negotiation Mode to Main mode, Encryption Algorithm to DES, Authentication Algorithm to MD5, Key Group to DH1, and then press Apply button on this page.

IKE Proposal	
Negotiation Mode	Main
Encryption Algorithm	DES 🔽
Authentication Algorithm	MD5 💌
SA Life Time (Seconds)	28800
Key Group	DH1 v
🔲 Enable Multiple Proposa	S
Associated Network Policies	
# Name	Local Network Remote Network
App	y Cancel

8. You will see an IKE rule on your VPN page, press L/R button to edit your IPSec rule.

PN Rules (IKE)	VPN Rules (Manual)	SA Monitor	Global Setting
VPN Rules	5		
	ocal twork		nternet Remote PN funnel
	twork		
	twork		PN Tunnel Network

9. Check Active check box and give a name to this policy.

Property		
Active		
Name	ToSonicWALL IPSecRule	
Protocol	0	
Nailed-Up		
Allow NetBIOS Traffic	Through IPSec Tunnel	
🗌 Check IPSec Tunnel C	onnectivity Log	
Ping this Address	0.0.0.0	

10. On Gateway Policy Information, you should choose **ToSonicWALL** IKE policy for your IPSec rule.

Gateway Policy Information		
na kataway Policy 🌍 🖓		
Local Network	Recycle Bin	

11. On Local Network, choose Subnet Address for your Address Type. Starting IP Address and Ending IP Address/Subnet are your local site LAN IP addresses. In this example, you should type 192.168.1.0 on Starting IP Address field and then type 255.255.255.0 on Ending IP Address/Subnet field.

Local Network					
🛞 Address Type	Subr	net Ad	Idres	5 🗸	
Starting IP Address	192.	168	. 1	-13	0
Ending IP Address / Subnet Mask	255 .	255	. 25	5.	0
Local Port	Start	0		E	nd

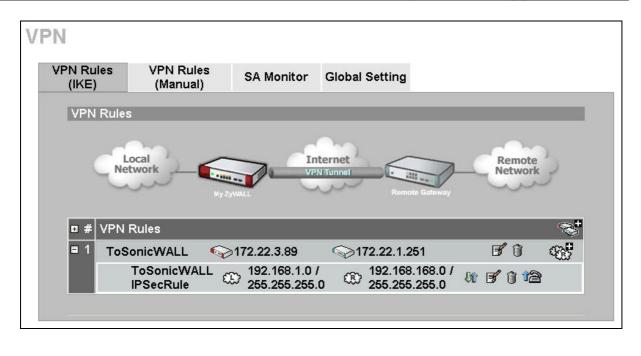
12. On Remote Network, choose Subnet Address for your Address Type. Starting IP Address and Ending IP Address/Subnet are your remote site LAN IP addresses. In this example, you should type 192.168.168.0 on Starting IP Address field and then type 255.255.255.0 on Ending IP Address/Subnet field.

Remote Network	
Address Type	Subnet Address 💌
Starting IP Address	192.168.168.0
Ending IP Address / Subnet Mask	255 . 255 . 255 . 0
Remote Port	Start 0 End 0

13. On IPSec Proposal, select Encapsulation Mode to Tunnel, Active Protocol to ESP, Encryption Algorithm to DES and Authentication Algorithm to SHA1, and then press Apply button on this page.

ncapsulation Mode	Tunnel 🔜	
Active Protocol	ESP 🐱	
Encryption Algorithm	DES 🔽	
Authentication Algorithm	SHA1 🔽	
SA Life Time (Seconds)	28800	
Prefect Forward Secrecy (PFS)	NONE 💌	
Enable Replay Detection		
Enable Multiple Propos	als	

14. When you finished doing your settings, you will see the following page.



2. Setup SonicWALL VPN (We choose SonicWALL TZ150 device in this example.)

1. Using a web browser, login SonicWALL by giving the LAN IP address of SonicWALL in URL field.

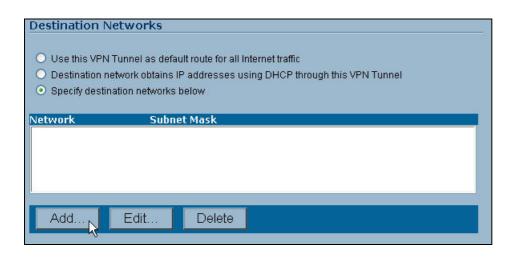
Go to VPN page, check **Enable VPN** check box, and then press **Add** button, it will bring up a page which you could do your VPN settings. (Note: You could use **VPN Policy Wizard** to set up your VPN rules as well.)

VPN > Settings		V	PN Policy Wizarc	Apply	Cancel ?
VPN Global Settings					
Enable VPN					
Unique Firewall Identifier: 0006B1137508	3				
VPN Policies				Items 1 to	01(of1) ᡌ
# Name	Gateway	Destinations	Crypto Suite	Enable	Configure
1 GroupVPN			ESP 3DES HMAC SHA1	(IKE)	8 🕫 🖗
Add					
1 Policies Defined, 0 Policies Enabled, 3 Maxin	num Policies Allo	owed			

 Click General tab, on Security Policy settings, give a name to this policy. In this example, type ToZyWALL on Name text box. IPSec Primary Gateway Name or Address is the ZyWALL's WAN IP Address (remote gateway IP address). In this example, you should type 172.22.3.89 on IPSec Primary Gateway Name or Address text box. Then, enter the key string 12345678 on Shared Secret text box.

General	Proposals	Advanced	
Security Po	olicy		
IPSec Keying N	Aode:		IKE using Preshared Secr 💌
Name:			ToZyWALL
IPSec Primary	Gateway Name (	or Address:	172.22.3.89
IPSec Second	ary Gateway Nam	ne or Address:	
Shared Secret		123456	78

3. On **Destination Networks**, select **Specify destination networks below** option, and then press **Add** button.



4. Network IP Address and Subnet Mask are your remote site LAN IP addresses. In this example, you should type 192.168.1.0 on Network text box and then type 255.255.255.0 on Subnet Mask text box, and then press OK button.



 Click Proposals tab, on IKE(Phase1) proposal settings, select Main mode, DH Group to Group1, Encryption to DES and Authentication to MD5. On IPsec(Phase2) proposal settings, select ESP Protocol, Encryption to DES and Authentication to SHA1. Then, press OK button on this page.

General Proposals	Advanced	
IKE (Phase 1) Proposa	1	
Exchange:	Main Mode	*
DH Group:	Group 1	~
Encryption:	DES	*
Authentication:	MD5	*
Life Time (seconds):	28800	
Ipsec (Phase 2) Propos	sal	
Protocol:	ESP	*
Encryption:	DES	*
Authentication:	SHA1	*
Enable Perfect Forward Sec	recy	
DH Group:	Group 2 🐱	
Life Time (seconds):	28800	
Ready		
	ок р	Cancel Help

6. When you finished doing your settings, you will see the following page.

VP	N Policies				ltems <mark>1</mark>	to 2 (	of 2) 🕅 🤇	
#	Name		Gateway	Destinations	Crypto Suite	Enable	Config	ure
1	GroupVPN				ESP 3DES HMAC SHA1 (IKE)		89 1	
2	ToZyWALL		172.22.3.89	192.168.1.1 - 192.168.1.254	ESP DES HMAC SHA1 (IKE)		8 1	}
	Add	Delete All						
2 F	olicies Defined, 1	Policies Enabled, 3 Ma	aximum Policies	Allowed				

7. When your VPN tunnel is up, you will see the following page.

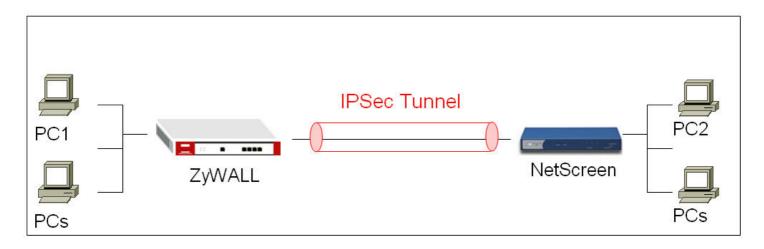
VPN Global Settings					
Enable VPN					
Unique Firewall Identifier: 000	6B1137508				
VPN Policies			Ite	rms 1 to 2 (c	ıf2) [3] <] ▷ [3]
# Name	Gateway	Destinations	Crypto Suite	Enable	Configure
1 GroupVPN			ESP 3DES HMAC SHA	1 (IKE) 🔲	8 🗊 🚳
2 ToZyWALL	172.22.3.89 🧉	192.168.1.1 - 192.16	68.1.254 ESP DES HMAC SHA1	(IKE) 🔽	8 6
Add Delete	All				
2 Policies Defined, 1 Policies En	abled, 3 Maximum Policies A	llowed			
Currently Active VPN T	unnels		Ite	ms <mark>1 to 1 (c</mark>	rf1) [X] <] ▷ [X]
# Name Local		Remote	Gateway		
1 ToZyWALL 192.168.1	68.1 - 192.168.168.255	192.168.1.1 - 192.16	68.1.254 172.22.3.89	Renegotiate	

#### NetScreen with ZyWALL VPN Tunneling

- 1. <u>Setup ZyWALL VPN</u>
- 2. <u>Setup NetScreen VPN</u>

This page guides us to setup a VPN connection between the ZyWALL and NetScreen router.

As the figure shown below, the tunnel between PC1 and PC2 ensures the packet flows between them are secure. Because the packets go through the IPSec tunnel are encrypted. To setup this VPN tunnel, the required settings for ZyWALL and NetScreen are explained in the following sections. As the red pipe shown in the following figure, **the tunneling endpoints are ZyWALL router and NetScreen router**.

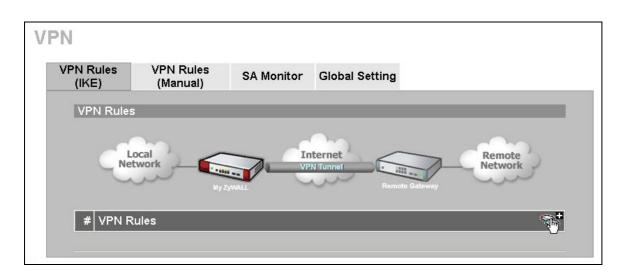


The IP addresses we use in this example are as shown below.

PC 1	ZyWALL	Netscreen	PC2
192.168.2.33	WAN: 172.22.3.89 LAN: 192.168.2.1	WAN: 172.22.1.251 LAN: 192.168.1.1	192.168.1.36

#### 1. Setup ZyWALL VPN

- 15. Using a web browser, login ZyWALL by giving the LAN IP address of ZyWALL in URL field.
- 2. Go to SECURITY->VPN->Press Add button



3. Give a name for your policy, for example "ToNetScreen"

- 4. **My IP Addr** is the **WAN IP of ZyWALL**. In this example, you should type 172.22.3.89 IP address on **My ZyWALL** text box.
- 5. Secure Gateway IP Addr is the NetScreen's WAN IP address. In this example, you should type 172.22.3.130 IP address on Remote Gateway text box.

Property		
Name NAT Traversal	ToNetScreen	
Gateway Policy Information		
My ZyWALL Semote Gateway	172.22.3.89	
Address	172.22.3.130	

6. In Authentication Key, enter the key string 12345678 in the Pre-Shared Key text box.

Authentication Key	
• Pre-Shared Key	12345678
O Certificate	auto_generated_self_signed_cert V (See My Certificates)
Local ID Type	IP 🗸
Content	0.0.0.0
Peer ID Type	IP. 💌
Content	0.0.0.0

7. Select Negotiation Mode to Main mode, Encryption Algorithm to DES, Authentication Algorithm to MD5, Key Group to DH1, and then click Apply button on this page.

IKE Proposal	
Negotiation Mode	Main 🗸
Encryption Algorithm	DES 💌
Authentication Algorithm	MD5 💌
SA Life Time (Seconds)	28800
Key Group	DH1 💌
Enable Multiple Proposa	ls
Associated Network Policies	
# Name	Local Network Remote Network
Ap	Cancel

8. You will see an IKE rule on your VPN page, click L/R button to edit your IPSec rule.

VPN Rules (IKE)	VPN Rules (Manual)	SA Monitor	Global Setting	
VPN Rules				
	ocal twork		ternet	Remote
	twork		NUMBER OF A	
	twork	Martin VP	N Tunnel	

9. Check **Active** check box and give a name to this policy.

roperty		
Active		
Name	ToNetScreen IPSecRule	
Protocol	0	
Nailed-Up		
Allow NetBIOS Traffic	Through IPSec Tunnel	
Check IPSec Tunnel C	onnectivity 🛛 Log	
Ping this Address	0.0.0.0	

10. On Gateway Policy Information, you should choose ToNetScreen IKE policy for your IPSec rule.

Gateway Policy Information		
na cateway Policy 🎧	ToNetScreen	
	ToNetScreen	
Local Network	Recycle Bin	

11. On Local Network, choose Subnet Address for your Address Type. Starting IP Address and Ending IP Address/Subnet are your local site LAN IP addresses. In this example, you should type 192.168.2.0 on Starting IP Address field and then type 255.255.255.0 on Ending IP Address/Subnet field.

Local Network					
💮 Address Type	Subn	et Ado	dress	~	
Starting IP Address	192.	168.	2	. 0	
Ending IP Address / Subnet Mask	255 .	255.	255	. 0	
Local Port	Start	0		End	0

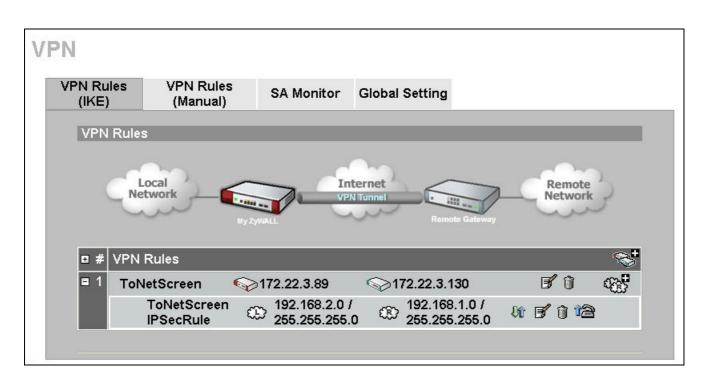
12. On Remote Network, choose Subnet Address for your Address Type. Starting IP Address and Ending IP Address/Subnet are your remote site LAN IP addresses. In this example, you should type 192.168.1.0 on Starting IP Address field and then type 255.255.255.0 on Ending IP Address/Subnet field.

Remote Network					
(R) Address Type	Subr	net A	ddre	SS 1	•
Starting IP Address	192	. 168		1.	0
Ending IP Address / Subnet Mask	255	. 255	. 2	55.	0
Remote Port	Start	0	_		End

13. On IPSec Proposal, select Encapsulation Mode to Tunnel, Active Protocol to ESP, Encryption Algorithm to DES and Authentication Algorithm to SHA1, and then press Apply button on this page.

ncapsulation Mode	Tunnel 🛛 🐱
ctive Protocol	ESP 💌
ncryption Algorithm	DES 🐱
uthentication Algorithm	SHA1 🐱
A Life Time (Seconds)	28800
refect Forward Secrecy PFS)	
Enable Replay Detection	
Enable Multiple Proposa	als

14. When you finished doing your settings, you will see the following page.



2. Setup NetScreen VPN (We choose NetScreen-5GT device in this example.)

- 3. Using a web browser, login NetScreen by giving the LAN IP address of NetScreen in URL field.
- 4. Check your WAN/LAN IP address

Click Network -> Inetrfaces, the trust IP/Netmask used for LAN, the untrust IP/Netmask used for WAN.

NETSCREEN DIREND SECURE	List 20 per List ALL(4)	page Interfaces				N	lew Tunne
NS5GT	Name	IP/Netmask	Zone	Туре	Link	Co	nfigure
ome	serial	0.0.0/0	Null	Unused	down	Edit	
onfiguration	trust	192.168.1.1/24	Trust	Layer3	up	Edit	
<b>twork</b> Binding	untrust	172.22.3.130/16	Untrust	La yer 3	up	Edit	
DNS Zones	vlan1	0.0.0/0	VLAN	Layer3	down	Edit	

Note: About the settings, you could reference to NetScreen user guide to get the detail info.

 If you set a static IP address for your WAN port, your should click Network -> Routing -> Routing Entries to edit your Gateway IP address. In this example, my Gateway IP address is 172.22.0.254.

NETSCREEN DIREND SECURE	Li	st <sup>20</sup> st rou		ll virtual routers 💌					trust-vr 💌	Ne
NS5GT		tr	ust-vr							
ome	^		IP/Netmask	Gateway	Interface	Protocol	Metric	Vsys	Configure	
nfiguration		*	192.168.1.0/24	0.0.0.0	trust	С	0	Root	<u>-</u>	
<b>twork</b> Binding		*	172.22.0.0/16	0.0.0.0	untrust	С	0	Root	-	
DNS		*	0.0.0.0/0	172.22.0.254	untrust	С	1	Root		
Zones Interfaces DHCP PPPoE Routing Routing	*	<sup>k</sup> Active	e route C Conne S Static	cted I Import A Auto-E					F external ty F external ty	

- To edit your IPSec rule, click VPNs -> AutoKey Advanced -> Gateway, and then press New button to edit your IKE rules.
- Give a name for your policy, for example "ToZyWALL". Remote Gateway IP Addr is the ZyWALL'S WAN IP address. In this example, select Static IP Address option and set 172.22.3.89 on the text box. Enter the key string 12345678 on Preshared Key text box, and then press Advanced button to edit the advanced settings.

Gateway Name ToZyWALL	
Security Level O Standard	🔿 Compatible 🔿 Basic 💿 Custom
Remote Gateway Type	
Static IP Address	IP Address/Hostname 172.22.3.89
O Dynamic IP Address	Peer ID
O Dialup User	User None 🗸
O Dialup User Group	Group None 👻
Preshared Key	Use As Seed □
Local ID	(optional)
Outgoing Interface untrust	
ОК	Cancel Advanced

6. On Security Level settings, you could set up phase 1 IKE rules. In this example, select User Defined, and choose pre-g1-des-md5 rule. The pre-g1-des-md5 means Pre-Share Key, group1, **DES** for **Encryption Algorithm** and **MD5** for **Authentication Algorithm**. Select Main (ID Protection) option for Mode (Initiator). Then, press Return button, and press OK button on next page to save your settings.

ned ○ Standard ○ ( ned ⊙ Custom	Com	patible 0	Basic	
Phase 1 Propos	sal			
pre-gl-des-md5	*	None	~	
None	*	None	~	

7. When you finished doing the settings, you will see an IKE rule on the page.

PNs > AutoKey					ns5g1	
ist <sup>20</sup> <mark>v</mark> p	er page	B				Ne
Name	Type	Address/ID/User Group	Local ID	Security Level	Config	ure
	Static	172.22.3.89	-	Custom	Edit	-

- 8. To edit your IPSec rule, click **VPNs** -> **AutoKey IKE**, and then press **New** button to edit your IPSec rules.
- 9. Give a name for your VPN, for example "**ToZyWALL IPSec**". On Remote Gateway, choose Predefined option and select ToZyWALL rule. Then, press **Advanced** button to edit the advanced settings.

VPN Name	ToZyWALL IPSec			
Security Level O	Standard O Compa	tible O Basic	<ul> <li>Custom</li> </ul>	
Remote Gateway⊙ ○	Predefined Create a Simple Gate	1	WALL 🐱	
	Gateway Name			
	Туре	• Static IP	Address/Hostname	
		🔿 Dynamic IP	Peer ID	
		O Dialup User	User	None 💌
		<ul> <li>Dialup Group</li> </ul>	Group	None 🔽
	Local ID		(optional)	
	Preshared Key		Use As S	Seed 🗆
	Security Level	<ul> <li>Standard</li> </ul>	<ul> <li>Compatible</li> </ul>	○ Basic
	Outgoing Interface	untrust 👻		
	ОК Са	ncel Adva	nced 💦	

 On Security Level settings, choose User Defined option, and choose nopfs-esp-des-sha rule on Phase 2 Proposal. The nopfs-esp-des-sha means no PFS, ESP Protocol, Encryption Algorithm to DES and Authentication Algorithm to SHA1.

Security Level Predefined User Defined	<ul> <li>○ Standard ○ Comp</li> <li>○ Custom</li> </ul>	atible 🔿 Basic	
	Phase 2 Proposal		
	nopfs-esp-des-sha 🛛 👻	None	~
	None 🗸	None	*

11. Check **VPN Monitor** check box, thus you can monitor your VPN tunnels. Then, press Return button, and press OK button on next page to save your settings.

VPN Monitor	
Source Interface	default 💌
Destination IP	0.0.0.0
Optimized Rekey	
[	Return Cancel

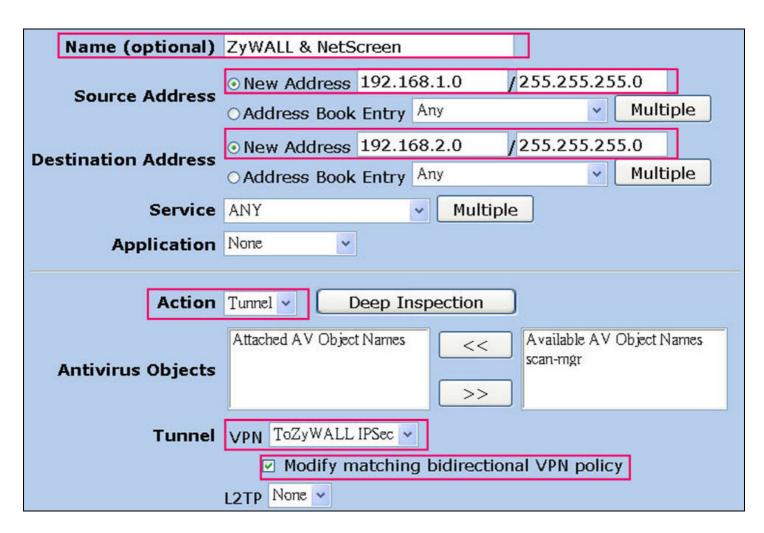
12. When you finished doing the settings, you will see an IPSec rule on the page.

ls > AutoKey IKE				ns5gt
st 20 🍸 per page				
Name	Gateway	Security	Monitor	Configure

13. On your main page, click **Policies** to set up your policy rules. To choose **From** to **Trust**, and **To** to **Untrust** (it means from LAN to WAN), and then press **New** button to edit your policy rules.

	Poli	cies (From A	All zones To All zon	ies)						ns5gt		<b>.</b>
	Lis Fro		er page			To Untrust	~	Go		5	Searc	ch ≷w
NS5GT	Fro	m Trust	To Untrust, to	tal policy	: 1							
Home ^	ID	Source	Destination	Service	Action	Options		Config	jure	Enable	Mo	ve
Network	1	LAN	Any	ANY	0		Edit	Clone	Remove	<b>N</b>	<b>8</b> £	
Screening Policies	Fro	m Untrus	st To Trust, to	tal policy	: 1							
VPNs AutoKey IKE	ID	Source	Destination	Service	Action	Options		Config	gure	Enable	Mo	ve
<ul> <li>AutoKey Advanc</li> <li>Gateway</li> </ul>	2	Any	LAN	ANY	0		Edit	Clone	Remove	ঘ	₿ <b>₽</b>	+

- 14. Give a name for your policy, for example "ZyWALL & NetScreen".
- 15. On Source Address, you should set up Local LAN IP addresses. In this example, select New Address option, and type 192.168.1.0 / 255.255.255.0 on the text box. On Destination Address, you should set up remote IP addresses. In this example, select New Address option, and type 192.168.2.0 / 255.255.255.0 on the text box.
- 16. Select Action to Tunnel, and select ToZyWALLIPSecVPN rule. Check Modify matching bidirectional VPN policy check box, it means that you can create/modify the VPN policy for the opposite direction. Then, press OK button to save your settings.



17. When you finished doing the settings, you will see the policy rules on the page.

Poli	icies (From All zones To All zones)				ns5gt	<b>e</b> (j)
	om All zones 💌	To All zones 💌	Go		Searc	
Fro	m Trust To Untrust, total poli					
ID	Source	Destination	Service	Action	Options	
1	LAN	Any	ANY	0		Edit
3	192.168.1.0/255.255.255.0	192.168.2.0/255.255.255.0	ANY	\$ <b>\$</b> \$		<u>Edit</u>
Fro	m Untrust To Trust, total poli	cy: 2				
ID	Source	Destination	Service	Action	Options	
2	Any	LAN	ANY	0		<u>Edit</u>
4	192.168.2.0/255.255.255.0	192.168.1.0/255.255.255.0	ANY	\$ <b>\$</b> \$		<u>Edit</u>

18. Move your policy rules to top, thus your device will check the rule at first.

Pol	icies (From All zones To All zones)			1	ns5gt	<b>e</b> ()
Lis Fre	st 20 v per page om All zones v	To All zones 🛩	Go		Searc	
Fro	m Trust To Untrust, total poli	су: 2				
ID	Source	Destination	Service	Action	Options	
3	192.168.1.0/255.255.255.0	192.168.2.0/255.255.255.0	ANY	<		Edit
1	LAN	Any	ANY	0		<u>Edit</u>
Fro	m Untrust To Trust, total poli	cy: 2				
ID	Source	Destination	Service	Action	Options	
4	192.168.2.0/255.255.255.0	192.168.1.0/255.255.255.0	ANY	 		Edit
2	Any	LAN	ANY	0		<u>Edit</u>

19. Click VPNs -> Monitor Status, this page displays a table that lists all the VPN groups configured on the NetScreen device. You could check the link states to know your VPN tunnel is up or down.

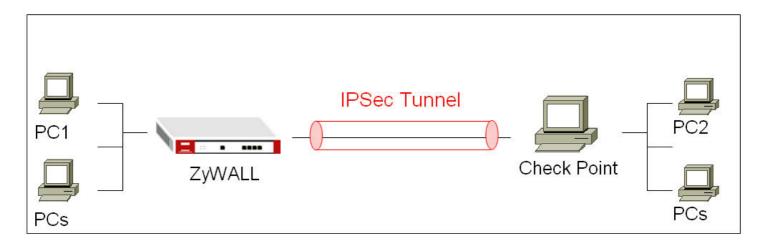
	VPNs > Monitor Status					ns5g	t
NETSCREEN	List 20 yer pag	e			(	Show All	Filt
NS5GT	VPN Name	SA ID	Policy ID	Peer Gateway IP	Туре	SA Status	Link
Home	ToZyWALL IPSec	00000002	4/3	172.22.3.89	AutoIKE	Active	Up
Network Screening Policies VPNs AutoKey IKE AutoKey Advanced Manual Key L 2TP Montor Statuch Objects							

### Check Point with ZyWALL VPN Tunneling

- 1. <u>Setup ZyWALL VPN</u>
- 2. Setup Check Point VPN

This page guides us to setup a VPN connection between the ZyWALL and a PC which uses Check Point software.

As the figure shown below, the tunnel between PC1 and PC2 ensures the packet flows between them are secure. Because the packets go through the IPSec tunnel are encrypted. To setup this VPN tunnel, the required settings for ZyWALL and SonicWALL are explained in the following sections. As the red pipe shown in the following figure, **the tunneling endpoints are ZyWALL router and a PC which uses Check Point software.** 

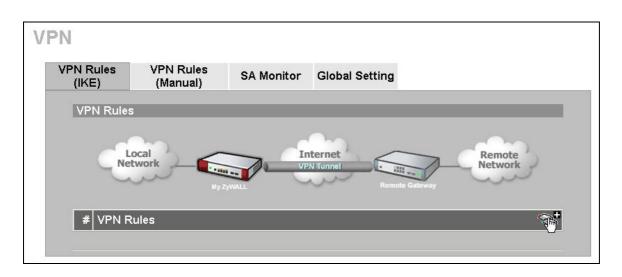


The IP addresses we use in this example are as shown below.

ZyWALL	Check Point
WAN: 172.22.1.236	WAN: 172.22.2.58
LAN: 192.168.1.0/24	LAN: 192.168.2.0/24

#### 1. Setup ZyWALL VPN

- Using a web browser, login ZyWALL by giving the LAN IP address of ZyWALL in URL field. Default LAN IP is **192.168.1.1**, default password to login web configurator is **1234**.
- 2. Go to SECURITY->VPN->Press Add button



3. Give a name for your policy, for example "ToCheckPoint"

- 4. **My IP Addr** is the **WAN IP of ZyWALL**. In this example, you should type 172.22.1.236 IP address on **My ZyWALL** text box.
- 5. Secure Gateway IP Addr is the remote PC's IP address. In this example, you should type 172.22.2.58 IP address on Remote Gateway text box.

Property		
Name	ToCheckPoint	1
NAT Traversal		27
Gateway Policy Informatior	n	
	470.00.4.000	1
Ny ZyWALL	172.22.1.236	

6. In Authentication Key, enter the key string 12345678 in the Pre-Shared Key text box.

Authentication Key	
• Pre-Shared Key	12345678
O Certificate	auto_generated_self_signed_cert
Local ID Type	IP 🗸
Content	0.0.0.0
Peer ID Type	IP 🗸
Content	0.0.0.0

7. Select Negotiation Mode to Main mode, Encryption Algorithm to DES, Authentication Algorithm to MD5, Key Group to DH1, and then press Apply button on this page.

IKE Proposal	
Negotiation Mode	Main
Encryption Algorithm	DES 💌
Authentication Algorithm	MD5 🗸
SA Life Time (Seconds)	28800
Key Group	DH1 🐱
🗌 Enable Multiple Proposa	is
Associated Network Policies	
# Name	Local Network Remote Network
App	y Cancel

8. After you press the **Apply** button, you will see an IKE rule on this page, press L/R button to edit your

• #	VPN Rules				≪*
■ 1	ToCheckPoint	<b>\$</b> 172.22.1.236	\$\$172.22.2.58	<b>f</b> î	975 S

9. Check Active check box and give a name to this policy.

Property	
✓ Active	
Name	ToCheckPoint IPSecRule
Protocol	0
Nailed-Up	
Allow NetBIOS Traffic	Through IPSec Tunnel
🗌 🗌 Check IPSec Tunnel C	Connectivity Log
	0.0.0.0

10. On Gateway Policy Information, you should choose **ToCheckPoint** IKE policy for your IPSec rule.



11. On Local Network, choose Subnet Address for your Address Type. Starting IP Address and Ending IP Address/Subnet are your local site LAN IP addresses. In this example, you should type 192.168.1.0 on Starting IP Address field and then type 255.255.255.0 on Ending IP Address/Subnet field.

Local Network	
🛞 Address Type	Subnet Address 💌
Starting IP Address	192.168.1.0
Ending IP Address / Subnet Mask	255.255.255.0
Local Port	Start 0 End 0

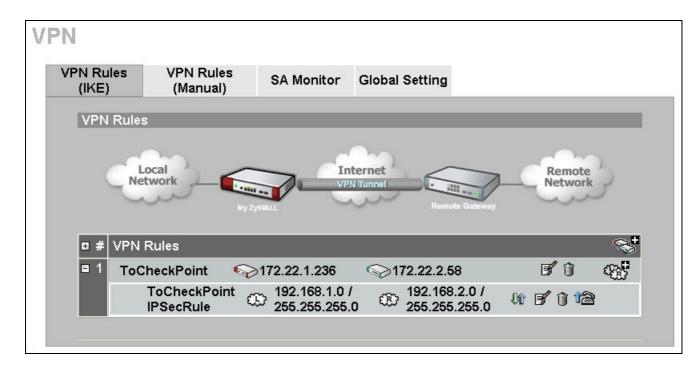
12. On Remote Network, choose Subnet Address for your Address Type. Starting IP Address and Ending IP Address/Subnet are your remote site LAN IP addresses. In this example, you should type 192.168.2.0 on Starting IP Address field and then type 255.255.255.0 on Ending IP Address/Subnet field.

Remote Network	
Address Type	Subnet Address 🐱
Starting IP Address	192.168.2.0
Ending IP Address / Subne Mask	t 255.255.255.0
Remote Port	Start <sup>0</sup> End <sup>0</sup>

13. On IPSec Proposal, select Encapsulation Mode to Tunnel, Active Protocol to ESP, Encryption Algorithm to DES and Authentication Algorithm to SHA1, and then press Apply button on this page.

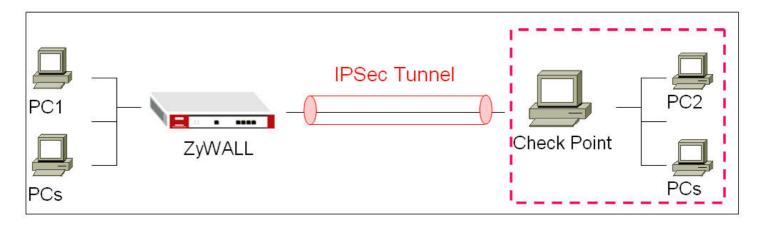
A Life Time (Seconds)	ncapsulation Mode	Tunnel 🔽	
Authentication Algorithm SHA1  SA Life Time (Seconds) 28800 Prefect Forward Secrecy PFS) I Enable Replay Detection	Active Protocol	ESP 🗸	
SA Life Time (Seconds) 28800 Prefect Forward Secrecy NONE  (PFS)  Enable Replay Detection	Encryption Algorithm	DES 🔽	
Prefect Forward Secrecy (PFS) Enable Replay Detection	Authentication Algorithm	SHA1 🐱	
(PFS) NONE	SA Life Time (Seconds)	28800	
Enable Replay Detection		NONE 🗸	

14. After you press the **Apply** button, you will see the following page.



#### 2. Setup CheckPoint VPN

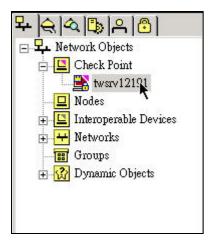
#### I. Setup Network Objects



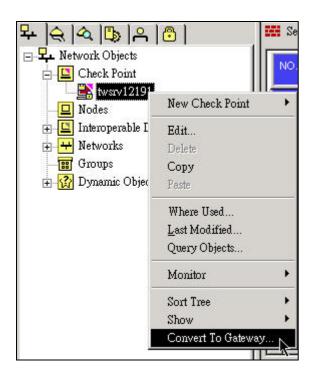
1. on your PC, clicking Start->Programmer->Check Point SmartConsole R60 -> SmartDashboard

2. Enter your user name and password, then press OK button to use your Check Point.

3. On Network Objects, you must see a default check point object here. For this example, my default check point object is **twsrv12191**, double click the object to check its settings.



- 4. Before you did the settings, you should make sure that your object is a **Check Point Gateway**.(not a Check Point Host)
- 5. If your check point object is a Check Point Host, select your object and click the right button on your mouse, then choose **Convert To Gateway** to change its settings.



6. On General Properties, the IP Addrrss field is the WAN IP of your PC. In this example, you should type **172.22.2.58** IP address on the text box. On Check Point Products settings, check VPN check box here.

## ZyXEL

opology IAT VPN	Name: [twsrv12191]				
lemote Access	IP Address: 172.22.2.58	<u>G</u> et address			
ogs and Masters	Qomment:				
Capacity Optimization	Color:	-			
	Secure Internal Communication	7			
	Communication DN: cn=cp_	mgmt,o=twsrv12191a7rstf			
	Version: NGH R60	Get Version			
	OS: Windows	▼ Get OS			
	111111111				
	Type: Check Point Enterprise/Pro				
	Check Point Products				
	Firewall	-			
	QoS	-			
	SecureClient Policy Server				
	SVN Foundation				
	Additional Products:				
	Configure Servers				

7. On **Topology** settings, you should see two interfaces of IP settings here if your PC has two network cards.

Topology NAT + VPN	Topology Get						
	Name	IP Address	Network Mask	IP Addresses behin			
<ul> <li></li></ul>	b57w2k6 rtl81390	172.22.2.58 192.168.2.0	255.255.0.0 255.255.255.0	External External			
	•						

8. Selecting **172.22.2.58 interface**, and press **Edit** button to check its settings. Clicking **Topology** screen, choose **External (leads out to the internet)** for the interface. Then, press OK button to save the settings.

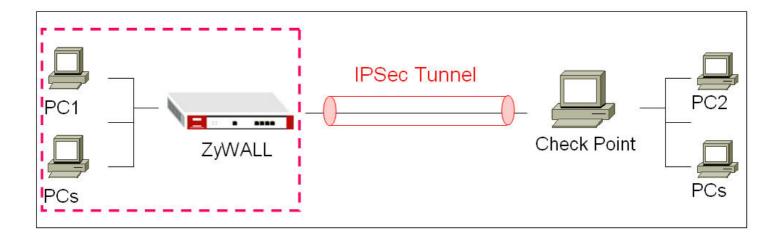
rface Properties	
eneral Topology   Multicast Restricti	ions
Topology	
• External (leads out to the internet)	
C Internal (leads to the local network)	)
IP Addresses behind this interface:	
C Not Defined	
${f C}$ Network defined by the inter	face IP and Net Mask
C Specific:	▼ <u>N</u> ew
Anti-Spoofing	
Perform Anti-Spoofing based on in	iterface topology
🗖 Don't check packets from: 📘	▼ New
Spoof Tracking: C None C L	

Selecting 192.168.2.0 interface, and press Edit button to check its settings. Clicking Topology screen, choose Internal (leads to the local network) and Network defined by the interface IP and Net Mask for the interface, then press OK button to save the settings.

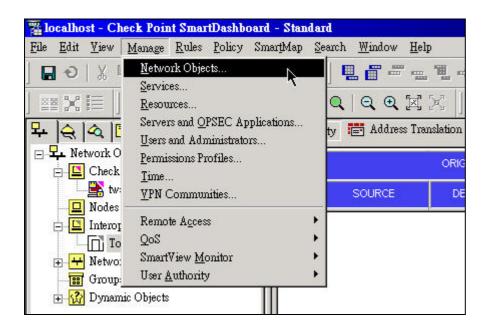
# ZyXEL

Interface Properties		>
General Topology		
Topology		
Internal (leads to the local network)		
IP Addresses behind this interface:		
C Not Defined		
• Network defined by the interface IP and Net Mask		
O Specific:		New
Anti-Spoofing		
🔽 Perform Anti-Spoofing based on interface topology		
🗖 Don't check packets from:	w	New
Spoof Tracking: C None C Log C Alert		

#### **II. Setup Interoperable Device**



10. On the main menu, click **Manage** -> **Network Objects**.



11. You will see the network objects window, press new button and select Interoperable Device.

Network objects: -		
Show: All		▼ More >>
🛟 AuxiliaryNet		
🛟 CPDShield		
<î} DMZNet		-
🛟 InternalNet		
🛟 LocalMachine		-
New	<u>R</u> emove	<u>E</u> dit
<u>C</u> heck Point	<u>R</u> emove	
<u>C</u> heck Point Nod <u>e</u>		<u>E</u> dit <u>H</u> elp
<u>C</u> heck Point Nod <u>e</u> Interoperable I		
<u>C</u> heck Point Nod <u>e</u>		
<u>C</u> heck Point Nod <u>e</u> <u>Interoperable I</u> <u>N</u> etwork		
<u>C</u> heck Point Nod <u>e</u> <u>Interoperable I</u> <u>N</u> etwork <u>D</u> omain		
<u>Check Point</u> Nod <u>e</u> <u>Interoperable I</u> <u>N</u> etwork <u>D</u> omain <u>O</u> SE Device	Device	
<u>Check Point</u> Nod <u>e</u> <u>Interoperable I</u> <u>N</u> etwork <u>D</u> omain <u>O</u> SE Device <u>G</u> roup	Device	
<u>Check Point</u> Nod <u>e</u> <u>Interoperable I</u> <u>N</u> etwork <u>D</u> omain <u>O</u> SE Device <u>G</u> roup <u>L</u> ogical Server	Device	

12. On **General Properties** settings, give a name and an IP address for the Interoperable Device. In this example, the IP address is ZyWALL's WAN IP address.

General Properties	Interoperable	Device - General Pro	operties
- Topology J- VPN	<u>N</u> ame:	ToZyWALL	
	IP <u>A</u> ddress:	172.22.1.236	Get address 🗖 Dynamic Addres
	<u>C</u> omment:	<u></u>	
	Color:		-

13. On **Topology** settings, pressing **Add** button to add a new interface.

Topology VPN	<u>G</u> et	ĺ		
	Name	IP Address	Network Mask	IP Addresses behir.
	<u>A</u> dd	<u>E</u> dit	<u>R</u> emove Sh	ow
	VPN Domain			
	📀 All IP Addi		based on Topology inf	

## **ZyXEL**

14. Giving a name for the interface, and assign the IP address/ subnet mask for the interface. In this example, you should assign ZyWALL's WAN port settings.

Vame:	ToZyWALL_WAN	
P Address:	172.22.1.236	
let Mask:	255.255.0.0	

15. Clicking **Topology** screen, and choose **External** (**leads out to the internet**) for the interface. Then, press OK button to save the settings.

terface	Properties	
General	Topology	
Topolo	ep	
• Ex	ternal (leads out to the internet)	
C Int	emal (leads to the local network)	
IP.	Addresses behind this interface:	
(	🏹 Not De <u>f</u> ined	
(	🖱 Network defined by the interface IP and Net Mask	
(	Specific:	New
Anti-Sj	poofing	
<b>₽</b> Per	form Anti-Spoofing based on interface topology	
Г	Don't check packets from:	New
Spo	oof Tracking: C None C Log C Alert	

16. Pressing Add button to add another interface.

General Properties Topology E VPN	<u>G</u> et			
	Name	IP Address	Network Mask	IP Addresses behin
	ToZyWALL_W	172.22.1.236	255.255.0.0	External
		Edit	Remove Sh	
			<u></u>	
	VPN Domain -			

17. Giving a name for the interface, and assign the IP address/ subnet mask for the interface. In this example, you should assign ZyWALL's LAN port settings.

Name:	ToZyWALL-subnet
P Address:	192.168.1.0
let Mask:	255.255.255.0

18. Clicking **Topology** screen, choose **Internal (leads to the local network)** and **Network defined by the interface IP and Net Mask** for the interface, then press **OK** button to save the settings.

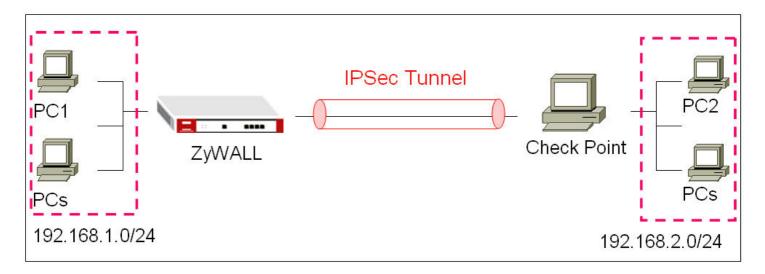
# **ZyXEL**

General Topology					
General Topology					
Topology					
C External (leads out	t to the inter	met)			
📀 Internal (leads to t	he local net	work)			
IP Addresses behir	nd this inter	face:			
C Not Defined					
Network def	ined by the	interface i	IP and Net M	fask	
C Specific:				<b>*</b>	New
Anti-Spoofing —					
🔽 Perform Anti-Spoo	ofing based	on interfa	ce topology		
📕 Don't <u>c</u> heck pa	ckets from			w	New
Spoof Tracking: C	None	C Log	C Alert		

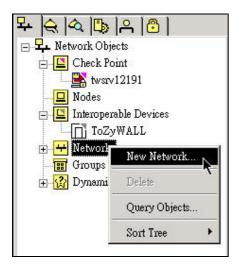
19. Pressing OK button to save the settings.

VPN	<u>G</u> et	TD A 11	[N. 1. 1. 1	[m.41] 11:
	Name ToZyWALL_W ToZyWALL-sub.	IP Address . 172.22.1.236 192.168.1.0	Network Mask 255.255.0.0 255.255.255.0	IP Addresses behir: External This Network
	•			
	<u>A</u> dd	<u>E</u> dit	Remove S	10W
	VPN Domain			
	ⓒ All IP Addresse ○ <u>M</u> anually defin	ed .	ased on Topology inf	formation.
	All IP Addresse	ed .	ased on Topology inf	
	ⓒ All IP Addresse ○ <u>M</u> anually defin	ed .	aæd on Topology inf	

## **III. Setup Networks**



20. Selecting Networks object and click the right button of your mouse, and choose New Network.



21. Give a name for your network policy, and set the network IP address to **192.168.1.0/24**. Then, press **OK** button to save the settings.

eneral NAT ]	
<u>N</u> ame:	Net_192.168.1.0
Network <u>A</u> ddress:	192.168.1.0
Net <u>M</u> ask:	255.255.255.0
<u>C</u> omment:	[
Color:	
– Broadcast addres	s:
Included	C Not included

22. To add another network policy, and set the network IP address **192.168.2.0/24**. Then, press **OK** button to save the settings.

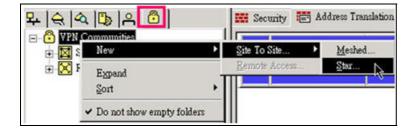
eneral NAT	
<u>N</u> ame:	Net_192.168.2.0
Network <u>A</u> ddress:	192.168.2.0
Net <u>M</u> ask:	255.255.255.0
<u>C</u> omment:	<b>I</b>
Color:	<b></b>
– Broadcast addres	s:
Included	C Not included

## **IV. Setup VPN Communities**

23. Click VPN communities tab to do the settings.



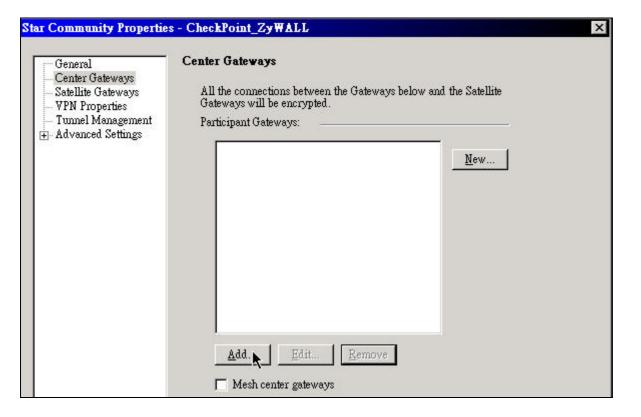
24. On VPN communities, click New -> Site To Site -> Star



25. On General settings, giving a name for your VPN communities. For example, **CheckPoint\_ZyWALL**.

General	
<u>N</u> ame:	CheckPoint_ZyWALL
<u>C</u> omment:	
Co <u>l</u> or:	
Community	Traffic Security
<u> ∏</u> ccept	all encrypted traffic Advanced
Note: 1	he rule applies for all Internally Managed community
L <u>og</u> Tr	affic as defined in Global Properties, Logging

26. On Center Gateways settings, press Add button to add a center gateway.



27. If you have already done the previous settings, you should see a central gateway here. Select the gateway, and then press **OK** button.

Add Cent	ter Gateway	8		×
	🖹 twsrv1	2191		
		be defined as:		
2. Vers	installed. ion NG FP1 a , Gateway, Ga	nd above (Only fo deway Cluster or I	or Internally mans nteroperable Dev	iged). ice
	OK	Cancel	<u>H</u> elp	

28. On Satellite Gateways settings, press Add button to add a remote gateway.

General Center Gateways	Satellite Gateways
Satellite Gateways VPN Properties	All the connections between the Gateways below and the Center Gateways will be encrypted.
Tunnel Management Advanced Settings	Participant Gateways:
	<u>N</u> ew

29. If you have already done the previous settings, you should see a remote gateway here. Select the gateway, and then press **OK** button.

Add Sa	tellite Gatewa	ys	×
	ToZyw	ALL	
The	candidates must	be defined as:	
2. Ve	PN installed. ersion NG FP1 a ost, Gateway, Ga	nd above (Only for teway Cluster or In	Internally managed). teroperable Device
]	OK 📐	Cancel	Help

**ZyXEL** 

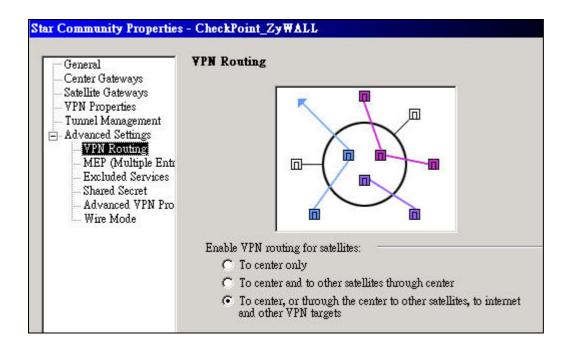
30. On VPN Properties settings, select Encryption Algorithm to DES, Authentication Algorithm to MD5 on phase 1, and also select Encryption Algorithm to DES, Authentication Algorithm to SHA1 on phase 2.

- General - Center Gateways	<b>VPN Properties</b>		
Satellite Gateways	IKE (Phase 1) Properties		
Tunnel Management → Advanced Settings	Perform key exchange encryption with:	DES	•
	Perform <u>d</u> ata integrity with:	MD5	•
	IPsec (Phase 2) Properties		
	Perform IPsec data encryption with:	DES	•
	Perform data integrity with:	SHA1	•

31. On Tunnel Management, leave the settings to default settings.

General	Tunnel Management	
Center Gateways Satellite Gateways VPN Properties	Permanent Tunnels	
Tunnel Management	🔽 Set Permanent Tunnels:	
- Advanced Settings	On all tunnels in the community	
	C On all tunnels of specific Gateways	S <u>e</u> lect Gateways
	$oldsymbol{C}$ On specific tunnels in the community	Select Permanent Tunnels
	📕 Enable <u>R</u> oute Injection Mechanism (RI	M) Settings
	Tunnel <u>d</u> own track:	Log
	Tunnel up track:	Log
	VPN Tunnel Sharing	
	Control the number of VPN tunnels opened bet	ween peer Gateways
	C One VPN tunnel per each pair of <u>h</u> osts	
	One VPN tunnel per subnet pair	
	🔿 One VPN tunnel per Gateway pair	

32. On VPN routing settings, choose **To center**, or through the center to other satellites, to internet and other **VPN targets** option.



33. On Shared Secret settings, choose ToZyWALL option, and press Edit button

General Center Gateways Satellite Gateways VPN Properties Tunnel Management Advanced Settings WPN Routing MEP (Multiple Entr Excluded Services Stared Secret Advanced VPN Pro Wire Mode	Each External membe	cret for all External members or will have the following members in this community.
	Peer Name ToZyWALL	Shared Secret
	<u></u> dit	<u>R</u> emove

34. Enter the secret key in the text box, and then press **OK** button.

Insert Secret			×
Enter secret:	12345678		
OK	<b>N</b>	Cancel	

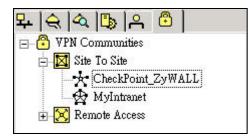
35. On Advanced VPN Properties settings, choose Group 1 for Diffie-Hellman settings.

General Center Gateways	Advanced VPN Properties	
<ul> <li>Satellite Gateways</li> <li>VPN Properties</li> <li>Tunnel Management</li> <li>Advanced Settings</li> <li>VPN Routing</li> <li>MEP (Multiple Entr Excluded Services</li> <li>Shared Secret</li> <li>Advanced VPN Pro</li> </ul>	IKE (Phase 1) Use Diffie-Hellman <u>R</u> enegotiate IKE security associations every Use aggressive <u>m</u> ode	Group 1 (768 bit) Group 1 (768 bit) Group 14 (2048 bit) Group 2 (1024 bit) Group 2 (1024 bit) Hinnues
Wire Mode	IPsec (Phase 2)	Group 2 (1024 bit) 💌
	<u>R</u> enegotiate IPsec security associations every Support IP compression	3600 seconds
	NAT Disable NAT inside the VPN community	Advanced

36. Press **OK** button to save your settings.

Star Community Properties	- CheckPoint_ZyWALL	×
General Center Gateways Satellite Gateways VPN Properties Tunnel Management Advanced Settings MEP (Multiple Entr Excluded Services Shared Secret Advanced VPN Pro Wire Mode	Bypass the Firewall         Image: Allow uninspected encrypted traffic between Wire mode interfaces of this Community's members         Image: Wire mode routing - Allow members to route uninspected encrypted traffic in VPN routing configurations	
	OK Cancel Help	

37. After you press OK button, you should see a new object here.



## **IV. Setup Security**

38. Click **Security** tab on the right side to do the security settings.



Sec	Security 📰 Address Translation   🖶 SmartDefense   🔛 Web Intelligence   🙆 VPN Manager   🏭 QoS   🛅 Desktop Security								
NO.	NAME	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON	TIME

#### 39. Press Add button to add a rule.

ules <u>P</u> o	licy Smar <u>t</u> Map <u>S</u> e:	arch <u>W</u> indow <u>H</u> elp							
# <u></u>	? ▲ ] 🗉		℡ ∞ 🗍 🛡 🛔 🛛						
111			he Bottom						
IN S	ecurity 📑 Address	s Translation 🛛 📕 Sm	uartDefense   🏦 Web In	telligence   🙆 VPN I	vlanager 🛛 🙀 QoS	📔 🛅 Desktoj	p Security		
NO	NAME	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON	TIME
					l				

40. On the default rule, select the source field, and click right button of your mouse, and then choose **Add...** option to add your network objects.

NO.	NAME	SOUF	RCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON	TIME
1		* Any	Add Add Users	Access	Any Traffic	* Any	i drop	- None	* Policy Target:	🗙 Any
			<u>E</u> dit <u>D</u> elete <u>W</u> here Use <u>M</u> anage De	201023						
			<u>N</u> egate Cel Select All	I						
			Cu <u>t</u> <u>C</u> opy <u>P</u> aste							
			Query Col Clear Quer							

41. Choosing Net\_192.168.1.0 network object, and press OK button to save your settings.

Show: All	nine_All_Interface	<mark>. More &gt;&gt;</mark> s ▲
₩ ₩ Net_192.1		
+++ Net_192.1		
ToZyWAL		
kwsrv121	91	<u> </u>
	<u>R</u> emove	Edit

42. To use the same way to add another network object (Net\_192.168.2.0) on the source field.

Show: All	nine_All_Interface	More >>
tif Localivacr		s <u> </u>
+ Net_192.1		
🖺 twsrv1219	91	-

43. On the destination field, please use the same way to add your network objects: **Net\_192.168.1.0** and **Net\_192.168.2.0**.

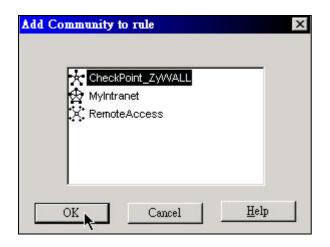
44. On the VPN field, click right button of your mouse, and choose **Edit Cell...** option to add your VPN communities.

A	/PN	SERVIC
* Any T	Edit Cell Edit Delete Where Used	R
	Select All	
	C <u>u</u> t Copy <u>P</u> aste	
	Query Colum <u>C</u> lear Query	n

45. On VPN Match Conditions, choose **Only connections encrypted in specific VPN Communities** option, and press **Add** button to add community to your rule.

	conditions Any connections, whether Clear or Encrypted
	<u>Only connections encrypted in any Site-to-Site VPN Community</u>
G	Only connections encrypted in specific VPN Communities
	A <u>d</u> d <b>Remove</b>
	Add Remove

46. Choosing CheckPoint\_ZyWALL object for your rule, and press OK button.



47. Clicking **OK** button to save your settings.

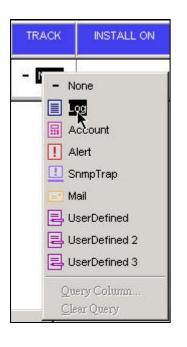
¢	Any connections, whether Clear or Encrypted
¢	Only connections encrypted in any Site-to-Site VPN Community
¢	Only connections encrypted in specific VPN Communities
	Remove

48. On action field, click right button of your mouse, and choose **accept** option for your rule.

# **ZyXEL**



49. On the track field, click right button of your mouse, and choose Log option for your rule.



50. If you finished the settings, you should see a rule as below.

201	Sect	nity 📴 Addre	🕫 Iranslation   💾 Sm	artDefenze   😂 Web I	ntelligence 🛛 🙆 VPN Mane	agar 🚺 Qol	S 📴 Desistor	p Security			
	ND.	NAME	SOURCE	DESTINATION	VPN.	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
Γ	1		부 Net_192.168.1.0 부 Net_192.168.2.0	부 Net_192.168.1.0 부 Net_192.168.2.0	* CheckPoint_ZyWALL	* Any	😗 accept	📕 Log	* Policy Targets	\star Any	

51. Pressing add button to add another rule which could drop packets if it doesn't match your VPN rule.

Sec	curity 📑 Addre	ess Translation 🛛 📕 Sm	artDefense   🙀 Web I	ntelligence   🙆 VPN Mans	ager 🛛 🙀 Qo	S 🛛 🛅 Deskto	p Security			
NO.	NAME	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
1		₩ Net_192.168.1.0 ₩ Net_192.168.2.0	₩ Net_192.168.1.0           ₩ Net_192.168.2.0	CheckPoint_ZyWALL	🗙 Any	🕜 accept	Log	* Policy Target:	🗙 Any	
2		* Any	* Any	* Any Traffic	🗙 Any	🖲 drop	🔳 Log	* Policy Target:	🗙 Any	

### **V. Install Policy**

52. On your main menu, click Policy -> Install.. option to Install your policy.



53. Selecting your policy rule, and press **OK** button to install the policy.

Install Policy					2
Installation Tar	gets Adv:	unced Secu	urity		
twsrv1219					
Installation Mode Install on gat			승규가 아파 특히 다니	 <b>]lear All</b>	Select Targets
C Install on all					
Revision Contro		,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,		 	
Create datab					
		5 00 20 1	4-20-06		
<u>N</u> ame :	Standard 200		4.29.00		
Co <u>m</u> ment :	Created by 'te	st'			
			<u>0</u>	Cancel	<u>H</u> elp

54. Waiting few seconds for the installation.

nstallation Targets	Version	Advanced Security	
stwsrv12191	NGX R60	🤣 Verifying	
			Legend
<b>ogress</b> Verifyi	ma		 
1 CILLYI		<u>A</u> bort	
Show Errors			

55. If you install the policy successfully, your VPN tunnel should work normally with your ZyWALL.

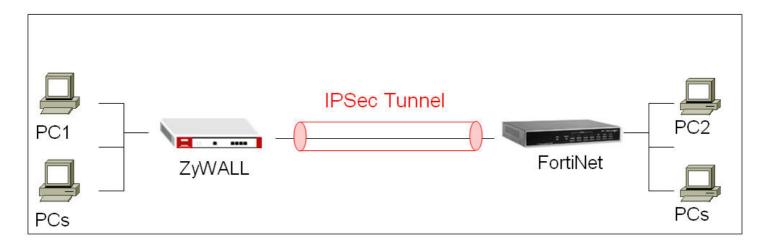
nstallation Targets twsrv12191	Version NGX R60	Advanced Security	
			Legend
ogress			
•	nleted successfu	ווא	
nogress	pleted successfu	Шу	

## FortiNet with ZyWALL VPN Tunneling

- 1. Setup ZyWALL VPN
- 2. <u>Setup FortiNet VPN</u>

This page guides us to setup a VPN connection between the ZyWALL and FortiNet router.

As the figure shown below, the tunnel between PC1 and PC2 ensures the packet flows between them are secure. Because the packets go through the IPSec tunnel are encrypted. To setup this VPN tunnel, the required settings for ZyWALL and FortiNet are explained in the following sections. As the red pipe shown in the following figure, **the tunneling endpoints are ZyWALL router and FortiNet router**.

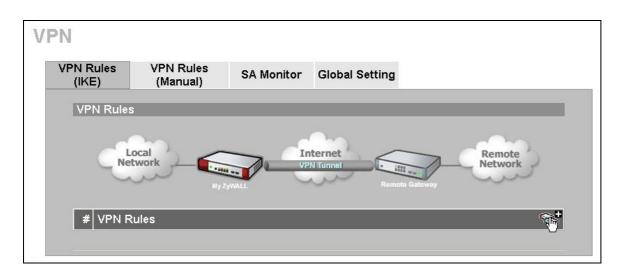


The IP addresses we use in this example are as shown below.

ZyWALL	FortiNet
WAN: 172.22.1.147	WAN: 172.22.2.138
LAN: 192.168.2.0/24	LAN: 192.168.1.0/24

## 1. Setup ZyWALL VPN

- 1. Using a web browser, login ZyWALL by giving the LAN IP address of ZyWALL in URL field.
- 2. Go to SECURITY->VPN->Press Add button



- 3. Give a name for your policy, for example "ToFortiNet"
- 4. **My IP Addr** is the **WAN IP of ZyWALL**. In this example, you should type 172.22.1.147 IP address on **My ZyWALL** text box.

5. Secure Gateway IP Addr is the FortiNet's WAN IP address. In this example, you should type 172.22.2.138 IP address on Remote Gateway text box.

Property		
Name	ToFortiNet	
NAT Traversal		
Gateway Policy Information		
Ny ZyWALL		
<ul> <li>My Address</li> </ul>	172.22.1.147	(Domain Name or IP Address)
🔘 My Domain Name	None 💙 (See <u>DDNS</u> )	
Remote Gateway Address	172.22.2.138	

6. In Authentication Key, enter the key string 12345678 in the Pre-Shared Key text box.

Authentication Key	
• Pre-Shared Key	12345678
O Certificate	auto_generated_self_signed_cert V (See My Certificates)
Local ID Type	IP 🗸
Content	0.0.0.0
Peer ID Type	IP 🗸
Content	0.0.0.0

7. Select Negotiation Mode to Main mode, Encryption Algorithm to DES, Authentication Algorithm to MD5, Key Group to DH1, and then click Apply button on this page.

IKE Proposal	
Negotiation Mode	Main
Encryption Algorithm	DES 💽
Authentication Algorithm	MD5 💌
SA Life Time (Seconds)	28800
Key Group	DH1 💌
🔲 Enable Multiple Proposal	5
Associated Network Policies	
# Name	Local Network Remote Network
Appl	Cancel

8. After you press the **Apply** button, you will see an IKE rule on this page, click L/R button to edit your IPSec rule.

VPN	Rules			
	-		-	
	Local Network		Internet VPN funnel	Remote Network
	un	My ZyWALL	Remote Gatewa	, we
				- 7
#	VPN Rules			S.
1	ToFortiNet	\$\$172.22.1.147	\$\$172.22.2.138	🗗 🛈 🖓 🖓

9. Check Active check box and give a name to this policy.

roperty	
Name	ToFortiNet IPSecRule
Protocol	0
Nailed-Up	
Allow NetBIOS Traffic Through IPS	Sec Tunnel
Check IPSec Tunnel Connectivity Ping this Address	Log

10. On Gateway Policy Information, you should choose ToFortiNEt IKE policy for your IPSec rule.

Gateway Policy Information	
😡 🥪 Gateway Policy	ToFortiNet
	ToFortiNet
	Recycle Bin
Local Network	

11. On Local Network, choose Subnet Address for your Address Type. Starting IP Address and Ending IP Address/Subnet are your local site LAN IP addresses. In this example, you should type 192.168.2.0 on Starting IP Address field and then type 255.255.255.0 on Ending IP Address/Subnet field.

Local Network	
💮 Address Type	Subnet Address 🗸
Starting IP Address	192.168.2.0
Ending IP Address / Subnet Mask	255.255.255.0
Local Port	Start 0 End 0

12. On Remote Network, choose Subnet Address for your Address Type. Starting IP Address and Ending IP Address/Subnet are your remote site LAN IP addresses. In this example, you should type 192.168.1.0 on Starting IP Address field and then type 255.255.255.0 on Ending IP Address/Subnet field.

Remote Network					
(R) Address Type	Subr	net A	ddre	SS 1	•
Starting IP Address	192	. 168		1.	0
Ending IP Address / Subnet Mask	255	. 255	. 2	55.	0
Remote Port	Start	0	_		End

13. On IPSec Proposal, select Encapsulation Mode to Tunnel, Active Protocol to ESP, Encryption Algorithm to DES and Authentication Algorithm to SHA1, and then press Apply button on this page.

ncapsulation Mode	Tunnel 💌
ctive Protocol	ESP 💌
Encryption Algorithm	DES 💌
uthentication Algorithm	SHA1 🐱
A Life Time (Seconds)	28800
Prefect Forward Secrecy PFS)	NONE V
Enable Replay Detectio	
Enable Multiple Propos	als

14. After you press the **Apply** button, you will see the following page.

	(IKE) VPN Rules (	Manual) SA Monitor	Global Setting		
<b>VP</b> N	Rules				
	Local		ternet	Remote	2
	Network	- VP	I Tunnel	Network	5
	un	My ZyWALL	Remote Gatew	ay	
	un	My ZyWALL	Remote Gatew	ay	~
<b>•</b> #	VPN Rules	My ZyWALL	Remote Gatew		<b>*</b>
• # • 1	VPN Rules ToFortiNet	My ZyWALL	Remote Gatew	ay F îj	\$* \$*
ALC: NO.				-	ی بی ایک

- 2. Setup FortiNet VPN (We choose FortiGate-60 device in this example.)
  - 1. Using a web browser, login FortiNet by giving the LAN IP address of FortiNet in URL field.
  - To edit your IPSec rule, click VPN -> IPSec -> Phase 1, and then press Create New button to edit your IKE rules.

lase 1 Phase 3	2 Manu	al Key	Concentrator	Ping Generator	Monitor	
Create New						
NE	e	Gateway IP	Mode		tion Algorithm	

Give a name for your policy, for example "ToZyWALL". Remote Gateway IP Addr is the ZyWALL's WAN IP address. In this example, select Static IP Address option and set 172.22.1.147 on the text box. Choosing Main mode, and also enter the key string 12345678 on Preshared Key text box. Then, press Advanced button to edit the advanced settings.

# ZyXEL

	New VPN Gateway
Gateway Name	ToZyWALL
Remote Gateway	Static IP Address 💌
IP Address	172.22.1.147
Mode	O Aggressive 💿 Main (ID protection)
Authentication Method	Preshared Key 💙
Pre-shared Key	•••••
Peer Options	
	<ul> <li>Accept any peer ID</li> </ul>
Advanced	(XAUTH, Nat Traversal, DPD)
O	Cancel

4. On P1 proposal settings, select **Encryption** to **DES**, **Authentication** to **MD5**, **and DH Group** to **Group1**. Then, press "-" button to delete the second P1 proposal rules.

P1 Proposal		
	1 - Encryption DES 💉 Authentication MD5 💌	
	2 - Encryption 3DES 💉 Authentication MD5 💌 🖽	J.
DH Group	1 🗹 2 🗌 5 🗌	U

5. To uncheck the **Nat-traversal** check box. And then press **OK** button to save the settings.

P1 Proposal	
	1 - Encryption DES 💌 Authentication MD5 💌 🖽
DH Group	1 🗹 2 🗌 5 🗌
Keylife	28800 (120-172800 seconds)
Local ID	(optional)
XAuth	⊙ Disable ○ Enable as Client ○ Enable as Server
Nat-traversal	Enable
Keepalive Frequency	5 (0-900 seconds)
Dead Peer Detection	🗹 Enable
	OK Cancel

6. After you press the **OK** button, you will see a Phase 1 rule on this page.

ise 1 Phase 2	Manual Key Conce	entrator Ping	g Generator	Monitor	
Create New					
Gateway Name	Gateway IP	Mode	Encryption	Algorithm	
	172.22.1.147	Main	DES-N	ADE	💼 🌽

 To edit your IPSec rule(phase 2), click VPN -> IPSec -> Phase 2, and then press Create New button to edit your IPSec rules.

nase 1 <u>Pha</u>	<u>ase 2</u> Mar	nual Key	Concentrator	Ping Generator	Monitor	
Create New <sub>N</sub>						

8. Give a name for your VPN, for example "**ToZyWALL IPSec**", and choose **ToZyWALL** policy rule for your Remote Gateway. Then, press **Advanced** button to edit the advanced settings.

New VPN Tunnel	
ToZyWALL IPSec	
ToZyWALL 🔽 🖸	
×	

9. On **P2 Proposal** settings, select **Encryption** to **DES**, and **Authentication** to **SHA1**, and also press "-" button to delete the second P2 proposal rules.

P2 Proposal	1-Encryption:	DES	~	Authentication:	SHA1	~			
	2-Encryption:	3DES	~	Authentication:	MD5	*	Đ	F.	
	🗹 Enable rep	lay dete	ectio	n				U	

10. To uncheck the **Enable perfect forward secrecy**(**PFS**) check box. And then, press **OK** button to save the settings.

	New VPN Tunnel
Funnel Name	ToZyWALL IPSec
Remote Gateway	ToZyWALL 💽 🖸
Concentrator	
Advanced	
P2 Proposal	1-Encryption: DES 🛛 👻 Authentication: SHA1 😒 🖸
	Enable replay detection
	Enable perfect forward secrecy(PFS).
	DH Group 1 🖲 2 🔘 5 🔘
Keylife:	Seconds 💌 1800 (Seconds) 4608000 (KBytes)
Autokey Keep Alive	Enable
Internet browsing	None 💌
Quick Mode Identities	<ul> <li>Use selectors from policy</li> </ul>
	O Use wildcard selectors
	O Specify a selector
(	OK Cancel

11. After you press the OK button, you will see your IPSec rule(Phase2) on this page.

Phase 1 Phase	ie 2 Manual Key	Concentrator	Ping Generator	Monitor	
Create New	)				
		The second se	1212403000000000000000000000000000000000	A2000 00000000000	
Tunnel Name	Remote Gateway	Lifetime(sec/kb)	Status	Timeout	

12. On the main page, click **Firewall -> Address**, and then press **Create New** button to edit your address rules.

Address Group		
Name	Address	

13. To define the IP source address of the Network behind FortiNet. Giving a name for your address rule, for example "Fortinet network", and enter the IP Range/Subnet in the text box. In this example, you should enter 192.168.1.0/24 IP Range/Subnet for the FortiNet network. Then, press OK button to save your settings.

Address Name	Fortinet network
P Range/Subnet	192.168.1.0/24

14. Press Create New button to edit another address rules.

dress Group		
Create New		
Name	Address	
all	0.0.0/0.0.0.0	2
Fortinet network	192.168.1.0/255.255.255.0	m 🌽

14. 15. To define the IP source address of the Network behind ZyWALL. Giving a name for your address rule, for example "ZyWALL network", and enter the IP Range/Subnet in the text box. In this example, you should enter 192.168.2.0/24 IP Range/Subnet for the ZyWALL network. Then, press OK button to save your settings.

	New Address
Address Name	ZyWALL network
IP Range/Subnet	192.168.2.0/24

16. After you finished the settings, you should see two address rules on this page.

# ZyXEL

Create New		
Name	Address	
all	0.0.0/0.0.0.0	
Fortinet network	192.168.1.0/255.255.255.0	🗌 💼 🎴
ZyWALL network	192.168.2.0/255.255.255.0	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1

17. On the main page, click **Firewall -> Policy**, and then press **Create New** button to edit your policy rules.

Create New       Create New         ID       Source       Dest       Schedule       Service       Action       Enable         internal -> wan1 (1)       Internal -> want (1)       Internal -> want (1)       Internal -> want (1)       Internal -> want (1)	

- 18. On **Interface/Zone** settings, select the interface to internal (private) network, and select the interface to external (public) network. In this example, choose **internal** option for your source Interface/zone, and choose **wan1** option for your destination Interface/Zone.
- 19. On Address Name settings, choose Fortinet network rule for your source address rules, and choose ZyWALL network rule for your destination address rules.
- 20. On Action settings, choose ENCRYPT option, and choose ToZyWALL IPSec rule for your VPN Tunnel. Then, press OK button to save your settings.

	New Polic	У		
	Source		Destination	
Interface/Zone	internal		wan1	~
Address Name	Fortinet network		ZyWALL network	~
Schedule	always			
Service	ANY			
Action	ENCRYPT	~		
☑ Allow inbound     □ Inbound NAT       ☑ Allow outbound     □ Outbound NAT				
Protection Prof	ile strict		2	
Log Traffic	_			
Advanced	<ul> <li>(Traffic Shaping,</li> </ul>	Diffe	erentiated Services	5)
$\subset$	OK C	Ca	incel	

21. After you press the **OK** button, you will the policy rule on this page.

C	reate New								
ID I	Source	Dest	Schedule	Service	Action	Enable			
r int	ternal -> wan1 (2)						-		
1	all	all	always	ANY	ACCEPT	<b></b>	1	2	-
2	Fortinet network	ZyWALL network	always	ANY	ENCRYPT	<b>v</b>	1	2	-

22. Click **VPN** -> **IPSec** -> **Monitor**, this page displays a table that lists all the VPN rules configured on the FortiNet device. You could check the link states here to know your VPN tunnel is up or down.

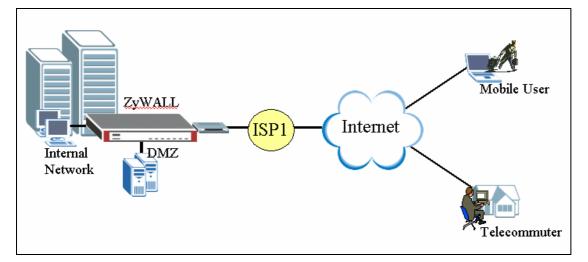


hase 1 Phase 2	2 Manual Key	Concentra	tor Ping Genera	tor <u>Monitor</u>	
dialup tunnels.					
tatic IP and dynam	nic DNS:				<b>(</b>
tatic IP and dynam	nic DNS: Remote gateway	Timeout	Proxy ID Source	Proxy ID Destination	

## Remote Access VPN Scenario

The remote access VPN scenario is to provide a remote users secure connections to access corporate network over a public networking infrastructure.

VPN has become the logical solution for remote access connectivity. The remote access VPN scenario is to provide a remote users secure connections to access corporate network over a public networking infrastructure. Deploying a remote access VPN enables corporations to reduce communications expenses by leveraging the infrastructures of Internet service providers. At the same time, VPN allows remote to take advantage of broadband connectivity. Remote users (e.g. mobile users, telecommuters) may use dial-up, ISDN, digital subscriber line (DSL) or cable technologies to gain Internet access



Because IP address is dynamically assigned by service providers, the **Remote Gateway Address** of gateway way policy must be configured with **0.0.0.0** or **domain name**. If "**0.0.0.0**" is used as **Remote Gateway Address**, ZyWALL accepts all attempts from any IP address and authenticate the remote VPN device with pre-shared key or certificate. If the remote entity passes authentication, ZyWALL and remote

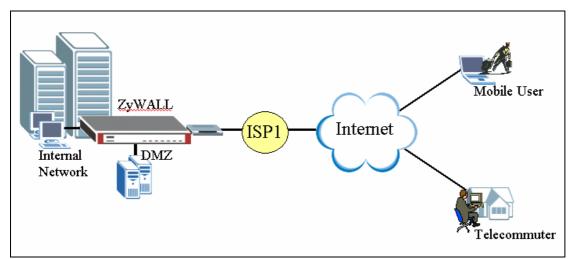
entity will then generate dynamic shared keys for the IKE SAs and IPSec/QM SAs.

## Using xAuth for User Authentication

IKE Extended Authentication (Xauth) is a draft RFC developed by the Internet Engineering Task Force (IETF) based on the Internet Key Exchange (IKE) protocol. The Xauth feature is an enhance to the existing Internet Key Exchange (IKE) Protocol feature. Xauth allows authentication methods to perform user authentication in a separate phase after the IKE authentication phase 1 exchange. The Xauth feature is an extension to the IKE feature, and does not replace IKE authentication.

Before Xauth, IKE only supported authentication of the device, not authentication of the user using the device. With Xauth, IKE can now authenticate the user using the device after the device has been authenticated during normal IKE authentication.

Since remote users may use the same pre-shared key for device authentication, it may have some problem once the key is compromised. Otherwise, an extra authentication would be more.



/PN				
VPN Rules	(IKE) VPN Rules (Ma	nual) 👘 SA Monito	r Global Setting	
VPN	Rules			_
	Local Network	My ZyWALL	Internet VPN Tunnel Remote G	
<b>±</b> #	VPN Rules			<b>≈</b> +
□ 1	Dyn_Remote_Access	Q 172.22.1.9	<b>Solution</b> Dynamic	BÍ Û 🖓
	ZW_P1	255.255.255		k <b>f î la</b>

To Use "xAuth" for authentication, enable "Extended Authentication" while configuring "VPN Gateway Policy". Select "Server Mode" on the VPN concentrator. There are two kinds of user\_identification (username/password) database can be used for authentication: Local\_User & RADIUS. (Note that Local\_User first then RADIUS if both exist).

Extended Authentication	
Enable Extended Authenticati	on (Searc <mark>u <u>Local User</u> first theu <u>RADIUS</u>)</mark>
User Name	
Password	

## Local User

INTUA	UTHENTICATION SERVER					
	l Usei ibase		us			
U	ser Da	atabase				
	#	Active	User Name	Password		
	1		test	*****		
	2					
	3					
	4					
	5					

RADIUS

	CICATION SERV	ER
Local U Databa		
Auth	nentication Server	
Ø	Active	
	Server IP Address	192.168.100.50
	Port Number	1812
	Key	12345678
Acco	ounting Server	
	Active	
	Server IP Address	0.0.0.0
	Port Number	1813
	Кеу	
		Apply

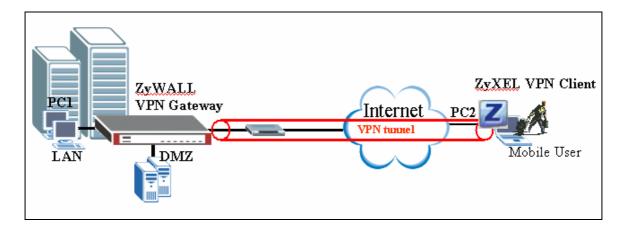
When external "RADIUS" is selected, please input the Service IP address of the external RADIUS server and the shared Key which must be configured on the RADIUS. The default (UDP) port number for RADIUS is 1812. If RADIUS server uses a different port number, please configure it correctly.

## **ZyXEL VPN Client to ZyWALL Tunneling**

- 1. Setup ZyWALL VPN Client
- 2. Setup ZyWALL

This page guides us to setup a VPN connection between the VPN software and ZyWALL router. There will be several devices we need to setup for this case. They are VPN software and ZyWALL router.

As the figure shown below, the tunnel between PC 2 and ZyWALL ensures the packets flow between them is secure. Because the packets go through the IPSec tunnel are encrypted. To setup this VPN tunnel, the required settings for the software and ZyWALL are explained in the following sections.



The IP addresses we use in this example are as shown below.

PC 1	ZyWALL	PC2
202.132.171.33	LAN: 202.132.171.1 WAN: 202.132.170.1	202.132.155.33

## 1. Setup ZyWALL VPN Client

- 1. Open ZyWALL VPN Client Security Policy Editor
- 2. Add a new connection named 'ZyWALL' as shown below.
- 3. Select Connection Security to Secure

Security Policy Editor - ZyWALL VPN Client <u>File Edit Options H</u> elp	
etwork Security Policy	ZS
Durer Connections	Connection Security Secure Non-secure Block
Add a New Connection	Remote Party Identity and Addressing ID Type Any IP Address Any ID 0.0.0
	Connect using Secure Gateway Tunnel
	Click here to find out about program add-ons.

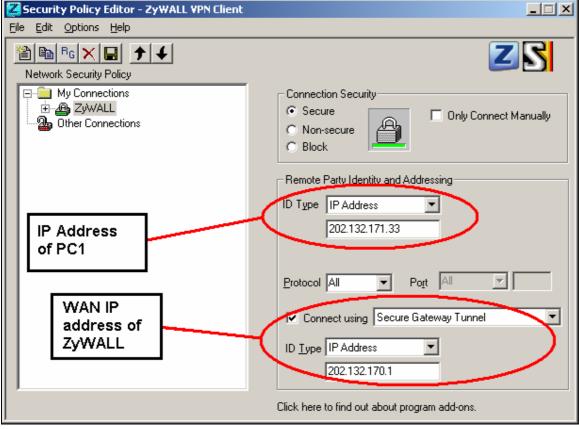
## Remote Party Identity and Addressing settings:

4. In **ID Type** option, please choose **IP Address** option, and enter the IP address of the remote PC (PC 2 in this case).

5. Check **Connect using Secure Gateway Tunnel**, please also select **IP Address** as ID Type, and enter ZyWALL's WAN

IPaddress in the following field.

The detailed configuration is shown in the following figure. Z Security Policy Editor - ZyWALL VPN Client File Edit Options Help



## Pre-Share Key Settings:

6. Extend ZyWALL icon, you may see My Identity.

7. Click My Identity; click the Pre-Shared Key icon in the right side of the window.

8. Enter a key you that later you will also need to configure in ZyWALL in the pop out windows. In this example, we enter

12345678. See below.



Security Policy Editor - ZyWALL VPN Client	
Security Policy Editor - 2yWALL VPN Client         File       Edit         Options       Help         Network       Security Policy         Network       Security Policy         Yes       My Identity         Yes       Security Policy         Other Connections       Other Connections	My Identity Select Certificate None ID Type Port
12345678	nter Pre-Shared Key (at least 8 characters) his key is used during Authentication Phase if the uthentication Method Proposal is "Pre-Shared key".

Security Policy Settings:

9. Click Security Policy option to choose Main Mode as Phase 1 Negotiation

	Security Policy Editor - ZyWALL VPN Client Eile Edit Options Help	
Network Security Policy   My Connections   My Ldentity   My Ldentity   Security Policy   Authentication (Phase 1)   Key Exchange (Phase 2)   Other Connections     Image: Connections     Image: Connections     Security Policy   Image: Connections         Security Policy   Image: Connections <th>Network Security Policy  My Connections  SyWALL  My Identity  Security Policy  Authentication (Phase 1)  Key Exchange (Phase 2)</th> <th>Select Phase 1 Negotiation Mode Main Mode Aggressive Mode Use Manual Keys Enable Perfect Forward Secrecy (PFS) PFS Key Group Diffie-Hellman Group 2</th>	Network Security Policy  My Connections  SyWALL  My Identity  Security Policy  Authentication (Phase 1)  Key Exchange (Phase 2)	Select Phase 1 Negotiation Mode Main Mode Aggressive Mode Use Manual Keys Enable Perfect Forward Secrecy (PFS) PFS Key Group Diffie-Hellman Group 2

10. Extend Security Policy icon, you will see two icons, Authentication (Phase 1) and Key Exchange (Phase 2). 11. The settings shown in the following two figures for both Phases are our examples. You can choose any, but they should match whatever you enter in ZyWALL.

Security Policy Editor - ZyWALL VPN Client	
<u>File E</u> dit <u>O</u> ptions <u>H</u> elp	
Image: Big     ★     ★     ↓       Network Security Policy       □-□-     My Connections	Authentication Method and Algorithms
⊡@ ZyWALL	Authentication Method Pre-Shared Key
E - 🏀 Key Exchange (Phase 2)	Encryption and Data Integrity Algorithms Encrypt Alg DES Hash Alg MD5
	Seconds SA Life Seconds ▼ 3600
	Key Group Diffie-Hellman Group 1

## 2. Setup ZyWALL VPN

- 1. Using a web browser, login ZyWALL by giving the LAN IP address of ZyWALL in URL field. Default LAN IP is **192.168.1.1**, default password to login web configurator is **1234**.
- 2. Go to SECURITY->VPN->Press Add button
- 3. check **Active** check box and give a name to this policy.
- 4. Select **IPSec Keying Mode** to **IKE** and **Negotiation Mode** to **Main**, as we configured in ZyWALL VPN Client.
- 5. Source IP Address Start and Source IP Address End are PC 2 IP in this example. (the secure host behind ZyWALL)
- 6. **Destination IP Address Start** and **Destination IP Address End** are **PC 1** in this example. (the secure remote host) Note: You may assign a range of Source/Destination IP addresses for multiple VPN sessions.
- 7. My IP Addr is the WAN IP of ZyWALL.
- 8. Secure Gateway IP Addr is the remote secure gateway IP, which is PC 1 in this example.
- 9. Select Encapsulation Mode to Tunnel.
- 10. Check the ESP check box. (AH can not be used in SUA/NAT case)
- 11. Select **Encryption Algorithm** to **DES** and **Authentication Algorithm** to **SHA1**, as we configured in ZyWALL VPN Client.
- 12. Enter the key string 12345678 in the Pre-shared Key text box, and click Apply.

## See the VPN rule screen shot

Property	
Active	
🗖 Keep Alive	
NAT Traversal	
Name	VPN
Key Management	
Negotiation Mode	Main
Encapsulation Mode	
DNS Server (for IPSec VPN)	0.0.0.0
Extended Authentication	
🗖 Enable Extended Authenticatio	n
Server Mode	(Search <u>Local User</u> first then <u>RADIUS</u> )
Client Mode	
User Name	
Password	
Local Policy	
Address Type	Single Address 💌
Starting IP Address	<pc 1=""></pc>
Ending IP Address / Subnet Mask	0.0.0.0
Remote Policy	
Address Type	Single Address 🔽
Starting IP Address	<pc 2=""></pc>
Ending IP Address / Subnet Mask	0.0.0.
Authentication Method	
Pre-Shared Key	12345678
C Certificate	auto_generated_self_signed_cert 🔽 (See My Certificates)
Local ID Type	
Content	
Peer ID Type	IP -
Content	
Gateway Information	
My Address	
• IP Address	<zywall wan=""></zywall>
C My Domain Name	None (See DDNS)
Secure Gateway Address	<pre></pre> <pre></pre> <pre></pre> <pre></pre>
-	
IPSec Algorithm	
• ESP	C AH
Encryption Algorithm	DES Authentication Algorithm MD5
Authentication Algorithm	SHA1
Advanc	ed Apply Cancel

You can further adjust IKE Phase 1/Phase 2 parameters by pressing Advanced button.



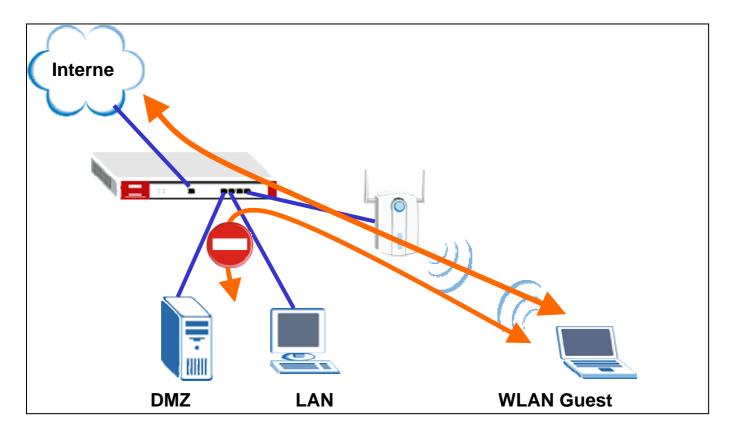
Negotiation Mode Encryption Algorithm	Main 🔽 DES 🔽
Authentication Algorithm	MD5 🔽
SA Life Time (Seconds)	28800
Key Group	DH1 💌
Phase 2	
Active Protocol	ESP 💌
Encryption Algorithm	DES 🔽
Authentication Algorithm	MD5
SA Life Time (Seconds)	28800
Encapsulation	Tunnel
Perfect Forward Secrecy (PFS)	NONE -
Enable Replay Detection	NO 💌
Protocol	0
Local Port	
Start	
End	0
Remote Port Start	lo la
End	

## Flexible Wireless Connection and Security

With the Wireless connection enhanced firmware, ZyWALL comes with a built-in WLAN interface for wireless connectivity.

The purpose for the new independent interface WLAN is to enforce the different security policy like Firewall ACL, AV, IDP or AS to the wireless access user. The wireless traffic is hard to control the access privilege and intruder may access the internal resource by passing the security checking. The other application like administrator may allow the guest using wireless to access the internet but suspend their traffic to internal resource like LAN or DMZ. Thus, the WLAN interface can be applied separate security policy to fulfill the security requirement.

We used the ZyWALL 5 UTM as an example to show how to control the wireless user traffic.



## Deploy the ZyWALL WLAN security policy

Setup WLAN Port Role

Setup WLAN security checking rule

How to define the ZyWALL WLAN Port?

 Switch to NETWORK > WLAN and setup the WLAN interface IP address and configure it as a DHCP server. Thus the PC associated with the AP will be dispatched an IP address from ZyWALL. Click Apply to save the setting.

ZyXEL				
номе	WLAN			
REGISTRATION	WLAN Static DHCP	IP Alias Po	ort Roles	
N <b>ETWORK 🖂</b> LAN	WLAN TCP/IP			
WAN	IP Address	192 . 168 . 3 . 1	RIP Direction	None 🔽
DMZ	IP Subnet Mask	255 . 255 . 255 . 0	RIP Version	RIP-1 💌
WLAN	Multicast	IGMP-v2 🔽		
WIRELESS CARD	DHCP Setup			
SECURITY 💌	DHCP	Server 💌		
ADVANCED 🛛	IP Pool Starting Address	192 . 168 . 3 . 33	Pool Size	64
REPORTS 💌	DHCP Server Address	0.0.0.0		
logs	DHCP WINS Server 1	0.0.0.0		
AINTENANCE	DHCP WINS Server 2	0.0.0.0		
	Windows Networking (NetBI	OS over TCP/IP)		
.0GOUT	Allow between WLAN and	LAN		
	Allow between WLAN and			
	Allow between WLAN and	DMZ		
	Note: You also need to create	a Firewall rule.		
		Apply	Reset	

2. Switch to **Port Roles** setting page, we will change the port 4 role from LAN to WLAN because the wireless AP connected to the ZyWALL port 4. Click the Apply to save the modification and later on the host associated with the AP to connect with the ZyWALL will treat with the WLAN traffic.

WLAN	Static DHCP	IP Alias	Port Roles	
Port Role	s Setup			
		-	LAN	
	ZyWALL S arthur accert an Jacs			

 Switch to ADVANCED > DNS > DHCP configuration page to setup the DNS server for WLAN DHCP. Select the WLAN as selected interface and correctly configure the DNS server IP address. The WLAN host can't resolve the domain name to IP address if the DNS server miss-configure in this page.

ZyXEL							
номе	DNS						
REGISTRATION	System	Cache	DH	CP	DDNS		
NETWORK 🛛	DNS Servers	Assigned by DHC	P Server				
SECURITY 💌			_				
ADVANCED 🖂	Selected Int	DNS	WLAN 🔽	_		IP	
NAT STATIC ROUTE	1 First DNS		From ISP	~	WAN 1st DNS:	172.23.5.2 💌	
SW MGMT	2 Second D	NS Server	From ISP	~	WAN 2nd DNS:	172.23.5.1 💌	
DNS	3 Third DNS	Server	From ISP	~	WAN 1st DNS:	172.23.5.2 💌	
REMOTE MGMT							
UPnP ALG			A	pply	Res	et	
REPORTS 💌							
LOGS							

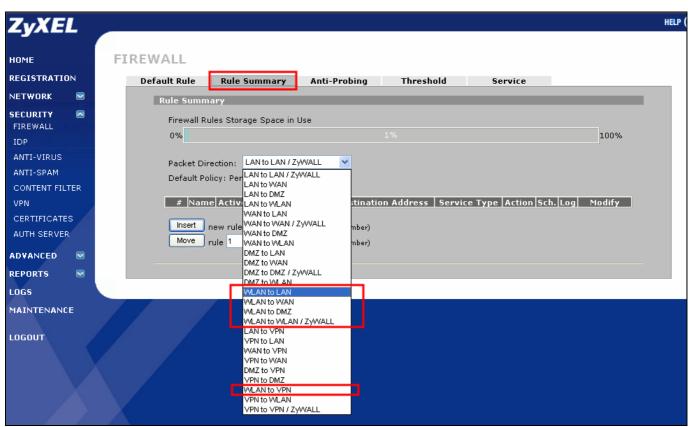
How to apply the security police over ZyWALL WLAN traffic?

 Switch to SECURITY > FIREWALL > Default Rule configuration page. Remember to turn on the firewall global switch otherwise all firewall ACL won't actually take effect on inspecting the packet. We want to control the traffic from WLAN and only allow the WLAN traffic go to internet (WAN). Thus, we **Permit** the traffic from WALN to WAN interface and **Drop** his traffic to LAN, DMZ, WLAN and VPN interface.

ZyXEL						
номе	FIREWALL					
REGISTRATION	Default Rule	Rule Summary	Anti-Probing	Threshold	Service	
NETWORK 🖂	Default Rule S	Setup				
SECURITY A	✓ Enable I ✓ Allow A: to WLAP	Firewall symmetrical Route (Wa I, and VPN to VPN pack	arning: When this box kets will bypass the F	is checked, all LAN t irewall check.)	o LAN, WAN to WAN,	, DMZ to DMZ, WLAN
ANTI-VIRUS						
ANTI-SPAM CONTENT FILTER	From		WAN	DMZ	WLAN	¥PN
VPN	LAN	Permit 💌 🔲	Permit 🔽 🗌	Permit 💌 🗌	Permit 💌 🔲	Permit 🔽 🗌
CERTIFICATES	WAN	Drop 🔽 🗹	Drop 🔽 🗹	Permit 💌 🗔	Drop 🔽 🔽	Permit 🔽 🗔
AUTH SERVER	DMZ	Drop 🔽 🔽	Permit 🔽 🗌	Drop 🔽 🔽	Permit 💌 🗖	Permit 🔽 🗌
ADVANCED 🕅	WLAN	Drop 💌 🔽	Permit 🔽 🗌	Drop 🔽 🔽	Drop 🖌 🗹	Drop 🔽 🗹
	<b>V</b> PN	Permit 💌 🗌	Permit 🔽 🗌	Permit 🔽 🗌	Permit 💌 🔲	Permit 🔽 🗌
					* 🔽	Log
LOGS						
MAINTENANCE			Apply	Reset		
LOGOUT						

2. ZyWALL also can granularity setup the access control rule according to different WLAN host (IP address) or packet services type (protocol types and ports). Switch to **Rule Summary** page and

select the packet direction from WLAN to other interface then insert a dedicate rule to control separate host or services types.



3. ZyWALL also can inspect packet/mails from or to WLAN by IDP/AV and AS features. The configuration is similar to the firewall rule setting. There is a traffic direction matrix available in IDP/AV and AS General configuration page. Used the check box to decide if the traffic from WLAN or to WLAN needs to be inspected by scan engine.

ZyXEL									
OME	TNTRUS	STON DE	TECTION		REVENTI	ON			
EGISTRATION									
	Gen	eral	Signature		Update	Backup & Re	store		
TWORK 💟	G	ieneral Setuj	p						
ECURITY 🔼		🔽 Enable Ir	ntrusion Detectio	on and Prev	ention				
IREWALL		Turbo Ca		Installe					
DP								1	
NTI-VIRUS			То	LAN	WAN	DMZ	WLAN	¥PN	
NTI-SPAM		From					~		
CONTENT FILTER		LAN							
/PN									
CERTIFICATES		WAN							
UTH SERVER		DMZ			Image: A state of the state		Image: A state of the state		
VANCED 🗵	L	WLAN		<b>V</b>			<b>V</b>		
PORTS 🖂		¥PN							
ogs							Protected	raffic Direction	
AINTENANCE					Apply	Rese	1		
IGOUT									

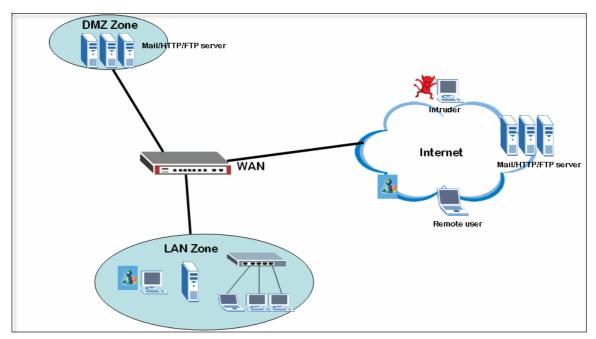
4. The wireless traffic can be applied to separate security checking rule by this WLAN interface enhancement.

# **Threat Management**

There is an emerging demand for an effective and proactive mechanism against Internet threats. These threats cause exhaust of IT resource, reduced productivity, data theft, business disruption and even financial lost in a Small and Medium Business networking environment.

ZyWALL 5/35/70 UTM is engineered to deliver comprehensive protection against internet threats in an effortless manner.

This support note demonstrates the best practice for SMB to minimize the impact of Internet threats using ZyWALL 5 UTM as example.



Proactive protection: hands-on best practice for threat management using ZyWALL 5 UTM

# Scenario

A typical SMB network, as illustrated in the above figure, may be segmented into Intranet (trusted network), DMZ for Internet-facing servers and Internet (distrusted networks).

In Intranet, there are tens of company employees having to access the Internet resources. They need to do web browsing, send/receive emails via company mail server, using hotmail or Google Gmail, doing file download upload and even having IM application to increase productivity.

In the DMZ, they will host couple Internet-facing servers, including DNS, web, email and ftp servers to provide services to their customers/partners.

From Internet, public users may need to access the servers in DMZ.

In addition to basic access control lists deployed on ZyWALL 5 UTM, IT staff must have additional application layer of protection. It should inspect traffics from/to these network segments to ensure malicious activities will not take place.

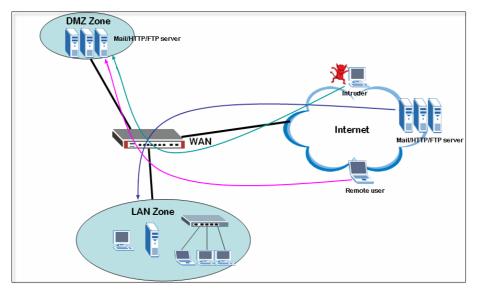
## To protect computer networks against virus intrusions and attacks from Internet

## 1. For Mixed Environment

Following example will demonstrate how to use ZyWALL 5 UTM to prevent virus and worms from entering the intranet and DMZ networks behind ZyWALL.

Since most virus and worms are coming from the internet, thus all incoming traffic from internet (WAN) to intranet (LAN and DMZ) should be inspected. Configure your ZyWALL 5 UTM based on this example will

prevent virus/worms from penetrate your networks.



#### 1.1 Activate AV/IDP license using the iCard

#### 1.1.1 ZyNOS 4 + Turbo Card

ZyWALL 5 UTM started to support AV/IDP service with latest firmware 4.01(WZ.0). In order to take full advantage of the AV/IDP service in ZyWALL 5 UTM, it is mandatory to have a ZyWALL Turbo Card inserted in the Expansion Card Slot at the back of your ZyWALL 5 UTM. This Turbo Card will guarantee your ZyWALL 5 UTM can deliver its best performance.

#### 1.1.2 IDP/AV License Activation

In **Registration** page, if you already have an account exist in myZyXEL.com, then all you have to do is, first select "**Existing myZyXEL.com account**" and enter your username password, and select IDP/AV 3 months trial version to activate

legistration	Service			
Device Regist	ration			
Existing r	nyZyXEL.com a	ccount		
User Name		jacky1234		
Password			(Type username and p characters.)	assword from 6 to 20
Service Activ	ation			
JEIVILE ALLIV	1.1011			
🗌 Content f	iltering 1-mont	n Trial		
🔽 Anti Spar	n 3-month Trial	(Service has been activated	i.)	
🗹 IDP/AV 3	-month Trial (S	ervice has been activated.)		
Note: For mo	re device servic	es management, please go	to <u>mγZγXEL.com</u>	

The ZyWALL 5 UTM has IDP (Intrusion Detection Prevention) service, which will inspect all traffic going through ZyWALL 5 UTM to effectively stop/drop most Worms, Trojans, DoS and DDoS attacks. **TIPS: Although IDP can effectively stop Worms, Trojans, and prevent DoS and DDoS attack, but IDP is not** 

#### capable to stop virus from penetrate ZyWALL 5 UTM.

In addition, the ZyWALL 5 UTM has a stream based AV scan engine that will scan all traffics as them pass through ZyWALL. This stream based AV scan engine can precisely detect virus/worms and then destroy these infected files before they reach intranet hosts.

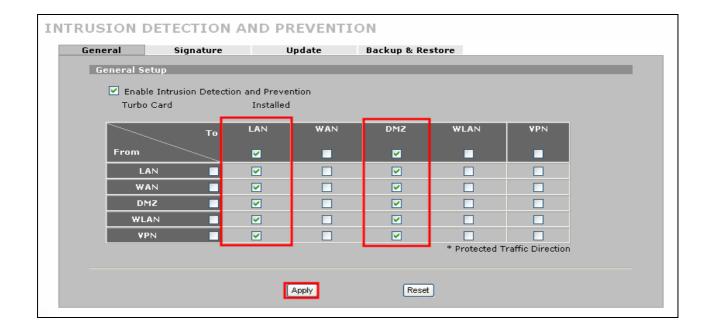
TIPS: Anti-Virus service in ZyWALL 5 UTM can detect and destroy files that are infected with virus/worms, but it cannot stop network DoS and DDoS attack.

#### **1.2 IDP + AV is a perfect combination**

ZyWALL 5 UTM IDP + AV service is ultimate tool to guard your network from most types of attacks coming from any networks. Not only will ZyWALL 5 UTM stop network attacks using IDP service, it will also scan, detect and destroy files that are infected with virus/worms using AV service. Result in your network stability and virus/worms free. Following is an example on how to configure IDP/AV service on your ZyWALL 5 UTM to fulfill this purpose.

#### **1.2.1 Setup the IDP service to prevent the attacks:**

- 1. In **IDP->General**, check the Enable Intrusion Detection and Prevention check box to enable IDP function.
- 2. In the traffic direction matrix, check all the send to LAN and DMZ's check boxes to have the inbound traffic to LAN and DMZ interfaces be protected.
- 3. Click on the **Apply** button to save the above settings.



#### **1.2.2 Setup the ANTI-VIRUS service to inspect if the receiving file infected:**

1. In ANTI-VIRUS->General, check the Enable Anti-Virus to enable the AV function and enable Zip

File Scan to force the AV engine to scan the Zip file. ZyWALL can't inspect the Zip file when it protected by password.

- 2. For **FTP** service, check **all** check boxes that traffic sending to **LAN** and **DMZ** interfaces to be protected accordingly, so that the FTP file upload/download traffic can be protected from the virus infection. And the system can give a warning to IT staff if a virus is found.
- 3. For **HTTP** service, check **all** check boxes that traffic sending to **LAN** and **DMZ** interfaces to be protected accordingly, so that the Web surfing traffic can be protected from virus infection. And the "**Log**" can give a warning to IT staff if virus is found.
- 4. For **POP3** service, check **all** check boxes that traffic sending to **LAN** and **DMZ** interfaces to be protected, so that the LAN users receive POP3 mails traffic can be protected from virus infection. And the system can give a warning to IT staff if a virus is found.
- 5. For **SMTP** service, check **all** check boxes that traffic sending to **LAN** and **DMZ** interfaces to be protected so that the remote users send SMTP mails traffic can be protected from virus infection. And the system can give a warning to IT staff if a virus is found.
- 6. Click on the **Apply** button to save the settings.

General Signatu	ire Up	date Bad	kup & Restor	e	
General Setup					
🗹 Enable Anti-Virus					
🗹 Enable ZIP File Sca	n				
Turbo Card	Installed				
Available Service					
Service	FTP (TCP 20 HTTP (TCP 8 POP3 (TCP SMTP (TCP	30, 8080, 3128) 110)			
		WAN	DMZ	WLAN	<b>V</b> PN
From					
LAN					
WAN					
DMZ					
WLAN					
<b>V</b> PN					
				* Protected 1	Traffic Direction

TIPS: Remember to make sure the AV signatures are most updated thereby the ZyWALL 5 UTM AV engine can stay in the best status. (The "update" can be done manually or automatically).

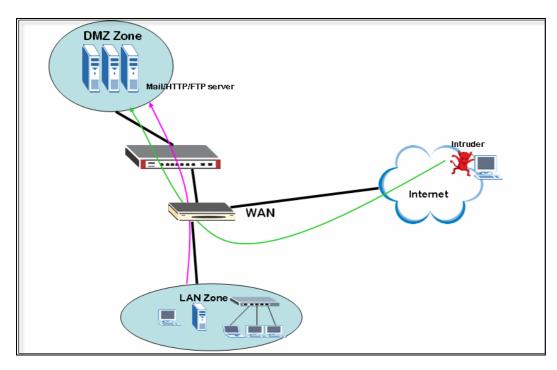
General	Signature	Update	Backup & Restore
Signature	Information		
Current P	attern Version: v1.224		
Release D	ate: 2006-06-28 00:5:	1:24	
Last Upda	te: 2006-06-29 02:24:	20	
Current A	nti-Virus Signatures: 8	00	
Signature	Update		
Service S	tatus: License Active		
Expiration	Date: 2008-08-30		
Synchron	ize the IDP and Anti-Vi	rus Signature to tl	ne latest version with the online update server.
Update Se	erver: myupdate.zywall.z	yxel.com	Update Now
🗹 Auto	Update		
О н	ourly		
💿 D	aily 🛛 🔁 (0	)'clock)	
0 w	eekly Sunday	0 🔨 (Oʻc	lock)

The AV signature update page

## 2. For Server Protection with IDP

In order to protect servers (WEB/Mail/FTP/etc) located on the DMZ of ZyWALL 5 UTM, user can enable the IDP service on ZyWALL 5 UTM to inspect inbound traffic to these servers. A ZyWALL 5 UTM with IDP service enabled can effectively stop hackers from intruding these servers and also stop DoS & DDoS attacks from paralyze the network.

Following procedure demonstrate how to configure your ZyWALL 5 UTM to protect your servers in DMZ zone.



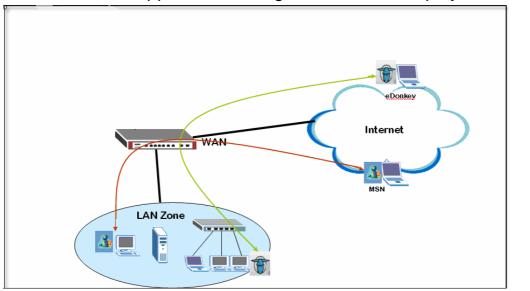
#### 2.1 Setup the IDP service to prevent the intruder's attack:

- 1. In **IDP->General**, check **Enable Intrusion Detection and Prevention** check box to enable IDP function.
- 2. In **Active** option, check all traffic sends to **DMZ**'s check box. Any traffic going from WAN or LAN interface to ZyWALL's DMZ segment can be protected by IDP engine.
- 3. Click on the **Apply** button to save the above settings.

General     Signature     Update     Backup & Restore       General Setup <ul> <li>Enable Intrusion Detection and Prevention</li> <li>Turbo Card</li> <li>Installed</li> </ul> To     LAN     VAN     VILAN     VPN     Image: Constraint of the set o	NTRUSION DE	TECTION AND P	REVENTIO	N			
Image: Construction and Prevention Turbo Card       Installed         Image: Construction and Prevention Turbo Card       Image: Construction and Prevention Turbo Card         Image: Construction and Prevention Turbo Card       Image: Construction Turbo Card         Image: Construction and Prevention Turbo Card       Image: Construction Turbo Card         Image: Construction Turbo Card       Image: Construction Turbo Ca	General	Signature	Update	Backup & Res	store		
Turbo Card     Installed       To     LAN     WAN     DMZ     WLAN     VPN       From     Image: Comparison of the state of the	General Setu	p					
To LAN WAN DMZ WLAN VPN   From Image: Constraint of the second sec	🗹 Enable II	ntrusion Detection and Preve	ention				
From   LAN   WAN   Image: Constraint of the second secon	Turbo Ca	rd Installe	1		_		
LAN		To LAN	WAN	DMZ	WLAN	<b>¥</b> PN	
WAN       Image: Constraint of the second seco	From						
DMZ       Image: Constraint of the second seco	LAN			<b>v</b>			
WLAN     Image: Constraint of the second secon	WAN						
VPN	DMZ						
* Protected Traffic Direction	WLAN						
	¥₽N						
Apply					* Protected T	raffic Direction	
Apply							
		Г	Apply	Report	1 I		
		L	CINANO	Reser	J		

TIPS: IDP/AV scan/detection engine will bypass IPSec VPN traffic, because IPSec VPN traffic are protected in a secure tunnel. IDP/AV services would not be able to scan/detect any files or packets that are protected by either password or secure tunnels.

## To Control IM/P2P Applications Usage to Increase Employee Productivity



IM (Instant Message)/P2P (Peer to Peer) applications are popular nowadays. For example people may use MSN messenger (an IM application from Microsoft) to chat, send/receive files and use eDonkey (a P2P application) to do file-sharing ...such applications are popular medium for spreading viruses, backdoor programs, or Trojans. The computers in the LAN zone might be infected silently when these IM/P2P applications are running in these computers. The ZyWALL 5 UTM IDP security service provides an effective extension to manage (allow or block) these IM/P2P applications.

# 1. The P2P/IM traffic management

Following are examples on how to use the IDP service in ZyWALL 35 UTM to manage MSN messenger usage to stop virus/Trojans from spreading and lead to more productivity.

 $2^{nd}$  portion of the example will show to stop employees from using company's bandwidth to do file sharing at anytime.

# **1.1 Setup IDP service**

## 1.1.1 ZyNOS 4.01 + Turbo Card

ZyWALL 5 UTM started to support AV/IDP service with latest firmware 4.01(WZ.0). In order to take full advantage of the AV/IDP service in ZyWALL 5 UTM, it is mandatory to have a ZyWALL Turbo Card inserted in the Expansion Card Slot at the back of your ZyWALL 5 UTM. This Turbo Card will guarantee your ZyWALL 5 UTM can deliver its best performance.

## 1.1.2 IDP/AV License Activation

Please refer to step 1.1 in the page 4 on how to activate IDP/AV services for your ZyWALL 35 UTM

## **1.2 IDP Common Setting**

1. In **IDP->General**, check the **Enable Intrusion Detection and Prevention** check box to enable IDP

function.

- 2. In **Active** option, check all the traffic to **LAN**, **DMZ** and **WAN** check boxes to have the IM/P2P traffic between LAN zone users and the remote users under controlled.
- 3. Click on the Apply button to save the above settings.

RUSION	DETECTION	AND PF	REVENTIO	D N		
General	Signature	L	Jpdate	Backup & Res	store	
General S	etup					
🗹 Enat	ole Intrusion Detectio	on and Preve	ntion			
Turb	o Card	Installed				
	то	LAN	WAN	DMZ	WLAN	VPN
From						
L	AN	<b>V</b>	<ul><li>✓</li></ul>	<b>V</b>		
w	AN 🗌	<b>V</b>				
D	MZ 🔲	✓				
WL	AN	<ul><li>✓</li></ul>	✓			
v	PN 🗖					
					* Protected T	raffic Direction
		(	Apply	Reset	]	

## 1.2.1 Control IM (Instant Message)

1. In **IDP->Signature**, click on **Switch to query view** to search the specified signature and set them up optionally.

ZyXEL						
номе	INTRUSION	DETECTION A	ND PREVENTI	ON		
REGISTRATION	General	Signature	Update	Backup & Restore		
NETWORK 🛛	Signatu	re Groups			(Q	
SECURITY 🛛 SECURITY	Attack		•		<u>Switch</u>	<u>n to query view</u>
IDP	Na	me 🙏 ID Seve	erity Platfor	m Active	Log Alert	Action
ANTI-VIRUS ANTI-SPAM			· -	-	· ·	-
CONTENT FILTER			Apply	Reset		
CERTIFICATES						
AUTH SERVER						
ADVANCED 💌						
LOGS						
MAINTENANCE						
LOGOUT						

2. To setup policies for the IM applications, say MSN, we use "**Signature search**" "**By Name**" with "**MSN**" keyword to query all signatures about MSN and will get a searched result list.

YXEL +	NIKUSION L	LILCIIONA		VENTI	ION					
	General	Signature	Upd	ate	Backu	ip & Restore				
DME	Query Sign	atures							Back to	group view
GISTRATION	- 0.	ature Search By Nam	e 🔽 MSN							
TWORK 🖾										
		ature Search by Attrib I 'Ctrl' to make multipl		n itoma in I	the lister					
REWALL										
P	Sev	erity Type	Pla Any	atform	Activ	e Log Any	Any	lert	Actio	on 🔥
TI-VIRUS	Severe	DDOS	Windo		Active	Log	Ale	t	No Action	
TI-SPAM	High Medium	Buffer Overflov Access Control		Jnix rk device	Inactive	e No Log	No .	Alert	Drop Packe Drop Sess	
ONTENT FILTER	Low	Scan	×	TR GEVICE			1975		Reset Sen	
PN				-						
PN ERTIFICATES				3	Search					
	Configure 9	Signatures		3	Search					
ERTIFICATES UTH SERVER	Configure S	Signatures			Search					
ERTIFICATES JTH SERVER	Configure s	Signatures	_	5	Search					_
ERTIFICATES JTH SERVER	Configure s		10 5			Platform	Active	Log #	lert Ar	tion
RTIFICATES ITH SERVER VANCED 💌	Configure (	Signatures Name <b>A</b>	ID S		Search Type	Platform	Active	Log #	slert Ac ⊗	tion
RTIFICATES TH SERVER VANCED S INTENANCE			ID 5			Platform <sup>d</sup>	Active	Log #	Ac	
RTIFICATES TH SERVER VANCED S		Name	1051895	everity Low	Туре ІМ	Platform	Active	<ul> <li>✓</li> <li>✓</li> </ul>	A c	ו 💌
RTIFICATES TH SERVER VANCED S INTENANCE	CHAT MSN CHAT MSN attempt	Name <b>A</b> Llogin via proxy Llox vedio request	1051895 1051830	everity	Type IM IM		Active	<ul> <li></li> <li><td>No Action</td><td>1 🗸</td></li></ul>	No Action	1 🗸
RTIFICATES TH SERVER YANCED S S	CHAT MSN CHAT MSN attempt	Name I login via proxy I 6.x vedio request	1051895	everity Low	Туре ІМ	Platform	Active	<ul> <li>✓</li> <li>✓</li> </ul>	A c	1 💙
TTIFICATES TH SERVER ANCED S S NTENANCE	CHAT MSN CHAT MSN attempt CHAT MSN attempt 2	Name Llogin via proxy Lox vedio request Lox audio request Lox audio request	1051895 1051830	everity Low Low	Type IM IM		Active	<ul> <li></li> <li><td>No Action</td><td>1 <b>V</b> 1 <b>V</b></td></li></ul>	No Action	1 <b>V</b> 1 <b>V</b>

## 1.2.1.1 Block MSN (Chat, File transfer)

Select **Drop Packet** in the **Action** field of all the MSN related signatures.

yXEL	Name	ID	Severity	/ Туре	Platform	Active	Log	Aler	t Action	
	Number S			.,,			<b>S</b>	$\otimes$		
IOME	CHAT MSN login via proxy	1051895	Low	бим	<u>∛ta</u> ™ <u>ta</u> ⊗				Drop Packet	
REGISTRATION	CHAT MSN 6.x vedio request	1051830	Low	IM					Drop Packet	
NETWORK 💌	attempt CHAT MSN 6.x audio request		LUW		A A Y				Drop Packet	
SECURITY 🖂	attempt -2	1051829	Low	IM	Main an				Drop Packet	~
FIREWALL	CHAT MSN 6.x audio request attempt -1	1051828	Low	IM					Drop Packet	~
IDP	Worm.KELVIR.A (malicious HTTP link in MSN message)	1051804	High	VirusWorm					Drop Packet	~
ANTI-VIRUS	CHAT MSN online game -2	1051803	Low	IM	2				Drop Packet	~
ANTI-SPAM CONTENT FILTER	CHAT MSN online game -1	1051802	Low	IM	- <u>A</u>				Drop Packet	~
VPN	Worm.Bropia (MSN file transfer via HTTP)	1051789	High	Other	-				Drop Packet	~
CERTIFICATES	<u>Worm.Bropia (MSN file transfer)</u>	1051788	High	Other	a de la companya de l				Drop Packet	~
AUTH SERVER	<u>∠</u> <u>Worm.Bropia (MSN file transfer)</u>			Other	1				Drop Packet	~
ADVANCED 🗵	± <u>CHAT MSN 7.x login attempt &lt;</u> 1024	1051770		IM	<i>≹</i> _™ <u>`</u> _				Drop Packet	~
LOGS	CHAT MSN 6.x (7.x) file transfer	1051746	Low	IM					Drop Packet	~
MAINTENANCE	<u>CHAT MSN 6.x (7.x) file transfer</u>	1051720	Low	IM	- Aug				Drop Packet	~
LOGOUT	<u>request - send</u> CHAT MSN 7.x -> 7.x message	1051719	Low	IM	1 <u>1</u>				Drop Packet	~
	Worm.MSN.funny		Medium	VirusWorm					Drop Packet	~
	CHAT Web MSN login attempt -3	1051696	Low	IM	<u>*</u> ∎				Drop Packet	
	CHAT Web MSN login attempt -2	1051695	Low	IM					Drop Packet	
					▓₩₩		_			
	CHAT Web MSN login attempt -1	1051694	Low	IM	~ <u>~</u> <u>~</u> ~	$\overline{\mathbf{v}}$			Drop Packet	y

## 1.2.1.2 Block MSN (Chat only, no File transfer)

Select **Drop Packet** in the **Action** field of the MSN file transfer related signatures and keep other signatures **No Action**.

ZyXEL	Configure Signatures									
IOME		000000	N 530	2014		Active	e Loa	Alert	10, 1000	
REGISTRATION	Name	ID	Severity	Туре	Platform				Action	
NETWORK 🖾	CHAT MSN login via proxy	1051895	5 Low	IM					No Action	~
ECURITY 🗷	CHAT MSN 6.x vedio request attempt	1051830	) Low	IM					No Action	~
IDP	CHAT MSN 6.x audio request attempt -2	1051829	) Low	IM					No Action	~
ANTI-VIRUS	CHAT MSN 6.x audio request attempt -1	1051828	B Low	IM					No Action	~
ANTI-SPAM	Worm.KELVIR.A (malicious HTTP link in MSN message)	1051804	ł High	VirusWorm	, <sup>2</sup> 🦓				No Action	~
CONTENT FILTER	CHAT MSN online game -2	1051803	B Low	IM	1				No Action	~
CERTIFICATES	CHAT MSN online game -1	1051802	2 Low	IM	a de la companya de l				No Action	*
AUTH SERVER	Worm.Bropia (MSN file transfer via HTTP)	1051789	) High	Other					No Action	~
DVANCED 🖾	Worm.Bropia (MSN file transfer)	1051788	- B High	Other					No Action	~
ogs	≚ Worm.Bropia (MSN file transfer) - 1			Other					No Action	~
AINTENANCE		1051770		IM					No Action	~
	<u>1024</u> CHAT MSN 6.x (7.x) file transfer	1051746		IM					Drop Packet	~
IGOUT	request - receive CHAT MSN 6.x (7.x) file transfer	1051720				···			Drop Packet	~
	request - send	1051720	) Low	IM	-	1000			Drop Packet	_
	CHAT MSN 7.x -> 7.x message	1051719	D Low	IM					No Action	*
	Worm.MSN.funny	1051704	A Medium	VirusWorm	n 🦓	<b></b>			No Action	~
	CHAT Web MSN login attempt -3	1051696	5 Low	IM					No Action	~
	CHAT Web MSN login attempt -2	1051605	5 Low	IM					No Action	~

## 1.2.2 Control P2P (Peer-to-Peer file transfer)

1. In **IDP->Signature**, click on **Switch to query view** to search the specified signature and set them up optionally.

ZyXEL						
номе	INTRUSION DE	TECTION A	ND PREVENTI	ON		
	INTROSION DI		ND FREVENIS			
REGISTRATION	General	Signature	Update	Backup & Restore		
NETWORK 🛛 🖾	Signature Gr	01105			(Q	
SECURITY 🛛 🖂	orginatare ar	oabs			* <u>Switch</u>	to query view
FIREWALL	Attack Type	Select a Type 💊	•			
IDP						
ANTI-VIRUS	Name /	ID Seve		m Active	Log Alert	Action -
ANTI-SPAM						
CONTENT FILTER						
VPN			Apply	Reset		
CERTIFICATES						
AUTH SERVER						
ADVANCED 🖂						
LOGS						
MAINTENANCE						
LOGOUT						

2. To setup policies for the P2P applications, say eDonkey, use the "**eDonkey**" keyword to query all signatures about eDonkey and will get a searched result list.

General	Signature	Update	Backup &	Restore				
Query Si	ignatures						Back to grou	p vie
N	ignature Search By Name	e 🗸 eDonkey						
	ignature Search by Attribu told 'Ctrl' to make multiple		he lists:					
		Platform	Active			ert	Action	
Any		Any	Active	Log	Any	ert	Any	~
Sev Higt	/ere DDOS	Windows Linux/Unix	Active Inactive	Log No Log	Aler No A		No Action Drop Packet	
Med	lium Access Control	Network device	Inactive	NO LOG	NO A	Nert	Drop Session	
ER Lov	v 👱 Scan						Reset Sender	~
		S	earch					
Configur	re Signatures							
						- •		
	🔺			al a tria maa A	ictive I			
	Name	ID S	everityTypel	Platform A	ctive I	.og Aler	t Action	
	NameA	ID 5-	everityTypel Low P2P	Platform A	8	og Aler $\sim$ $\otimes$ $\sim$ $\sim$	t Action	~
P2P eD P2P eD	onkey GET server list onkey Server status requ	1051159	_	<i>8</i> <u>1</u>		🧭 😢		~
P2P eD P2P eD P2P eD	onkey GET server list onkey Server status requ 4665/UDP	1051159 ests and 1051151	Low P2P Low P2P				No Action	~
P2P eD P2P eD	onkey GET server list onkey Server status requ 4665/UDP onkey UDP Server status	1051159 ests and 1051151 request 1051141	Low P2P Low P2P Low P2P				No Action No Action No Action	*
P2P eD P2P eD P2P eD	onkey GET server list onkey Server status requ 4665/UDP	1051159 ests and 1051151	Low P2P Low P2P				No Action	~
P2P eD P2P eD reports P2P eD P2P eD P2P eD	onkey GET server list onkey Server status requ 4665/UDP onkey UDP Server status	ests and request 1051151 1051141 1050423	Low P2P Low P2P Low P2P				No Action No Action No Action	*

3. The IT staff can log all eDonkey traffic by checking the **Log** check box and blocking the eDonkey packet by selecting **Drop Packet** in the **Action** field. And remember to check the **Active** check box to activate the signatures.

ZyXEL	General	Signature	Update	Backu	p & Restore				
—	Query Si	natures						Back to gro	un vieu
IOME									
EGISTRATION	<ul> <li>Si</li> </ul>	gnature Search By N	lame 💌 eDonkey		_				
		gnature Search by Att							
	H	old 'Ctrl' to make mul	tiple selection on item	s in the lists:					
FIREWALL	S	everity Type	Platform				ert	Action	
IDP	Any		Any Windows	Any Active	Any Log	Any		Any No Action	
ANTI-VIRUS	High			Inactive		No A	lert	Drop Packet	
ANTI-SPAM	Medi		trol 🗸 Network devic	e l				Drop Session Reset Sender	~
CONTENT FILTER									
/PN				Search					
CERTIFICATES	Configure	e Signatures							
CERTIFICATES AUTH SERVER	Configure	e Signatures							
AUTH SERVER	Configure			_	_				
UTH SERVER	Configure	e Signatures NameA	ID	SeverityTy	vpePlatform	Active L	og Aleri	Action	,
UTH SERVER DVANCED S			ID 10511	_			og Aleri	Action Drop Packet	1
NUTH SERVER DVANCED 💌 DGS	P2P eDc P2P eDc	Name Name Inkey GET server list	10511	.59 Low P	2P 嶺			Drop Packet	
AUTH SERVER DVANCED 💌 DGS AINTENANCE	P2P eDc P2P eDc reports	Name onkey GET server list onkey Server status re 4665/UDP	10511 equests and 10511	59 Low P 51 Low P	2P 🚑 2P 🍋			Drop Packet Drop Packet	~
AUTH SERVER	P2P eDc P2P eDc reports	Name Name Inkey GET server list	10511 equests and 10511	59 Low P 51 Low P	2P 🝋 2P 🙇 2P			Drop Packet	~
AUTH SERVER DVANCED 💌 DGS AINTENANCE	P2P eDc P2P eDc reports P2P eDc	Name onkey GET server list onkey Server status re 4665/UDP	10511 equests and 10511	59 Low P 51 Low P 41 Low P	2P 🚑 2P 🍋			Drop Packet Drop Packet	~
AUTH SERVER DVANCED 💌 DGS AINTENANCE	P2P eDc P2P eDc P2P eDc P2P eDc	Name Mankey GET server list onkey Server status re 4665/UDP onkey UDP Server stat	10511 equests and 10511 tus request 10511 10504	59 Low P 51 Low P 41 Low P 23 Low P	2P 2P 2P 2 2P 2 2P 2			Drop Packet Drop Packet Drop Packet	<ul><li></li><li></li><li></li><li></li><!--</td--></ul>
AUTH SERVER DVANCED 💌 DGS AINTENANCE	P2P eDc P2P eDc P2P eDc P2P eDc P2P eDc P2P eDc	Name Name Nev GET server list onkey Server status re 4665/UDP onkey UDP Server stat onkey connection	10511 equests and 10511 tus request 10511 10504 4665/TCP 10504	59 Low P 51 Low P 41 Low P 23 Low P 11 Low P	2P 4			Drop Packet Drop Packet Drop Packet Drop Packet	

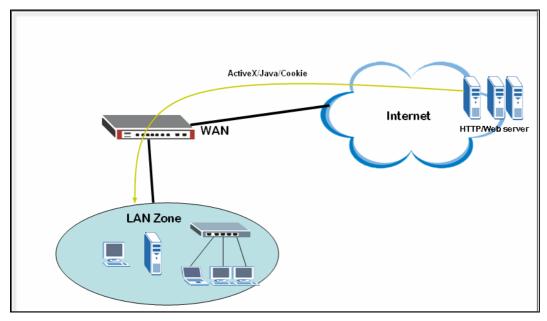
#### 1.2.2.1 **IDP signature update**

To keep the ZyWALL 5 UTM IDP engine stay in the best status, make sure the IDP signature are most updated (The "update" can be done manually or automatically)

IOME I	NTRUSION DETECT	TION AND PREVE	NTION	
REGISTRATION	General Sign	ature Update	Backup & Restore	
ETWORK 🖾	Signature Informati	on		_
ECURITY 🖂 FIREWALL	Current Pattern Vers			
IDP	Release Date: 2005-	)		
ANTI-VIRUS	Last Update: 2005-0			
ANTI-SPAM	Current IDP Signatu	res: 1760		
CONTENT FILTER	Signature Update			
VPN				
CERTIFICATES	Service Status: Trial			
AUTH SERVER	Expiration Date: 200	5-09-25		
	Synchronize the IDP	and Anti-Virus Signature to t	ne latest version with the online update server.	
	Update Server: myu	odate.zywall.zyxel.com	Update Now	
OGS	🗹 Auto Update			
AINTENANCE	<ul> <li>Hourly</li> </ul>			
	O Daily	0 💌 (O'clock)		
.0GOUT	O Weekly	Sunday V 0 V (O'	clock)	
A State				

To filter non-work related and unproductive web surfing to mitigate spyware and phishing threats

Web browsing is one of the most common activity people do on daily bases. However there are lots of threats and traps that are available on the WWW too. Web browsing should be sanctioned as the figure listed below so that the impact of hazardous web content (malicious java and ActiveX), spyware, and phishing attack can be minimized. These attacks are known to be found in websites that provides pirate software, pornography, and other illegitimate websites. Also, the non-business web surfing such as the sports, financial and gambling web sites should be prevented to increase company productivity. With ZyWALL 35 UTM Content Filter service, network administrator can effectively allow/prevent network users from viewing different categories of web sites.



## 1. Minimize Spyware Attack

As mentioned earlier, pornography websites are known to contain Spyware and Trojans, thus it is recommended to use ZyWALL 5 UTM to prevent users from access these types of websites. Below is an example to illustrate how to configure ZyWALL to fulfill this purpose

#### 1.1 <u>CF License Activation</u>

In **Registration** page, if you already have an account exist in myZyXEL.com, then all you have to do is, first select "**Existing myZyXEL.com account**" and enter your username password, and select Content Filter 1 month trial version to activate

egistration	Service		
Device Regi	stration		
💿 Existing	g myZyXEL.com a	ccount	
User Name	е	jacky1234	
Password		characti	username and password from 6 to 20 ars.)
Service Act	ivation		
🗌 Conten	t Filtering 1-mont	n Trial	
🔽 Anti Sp	am 3-month Trial	(Service has been activated.)	
🔽 IDP/AV	/ 3-month Trial (S	ervice has been activated.)	
Note: For n	nore device servic	es management, please go to <u>myZyXEL.com</u>	

#### 1.2 Using external database content filtering to achieve best result

Enable external database content filtering in the **CONTENT FILTER -> Categories**, with selecting the "Adult/Mature Content", "Sex Education", "Pornography", "Nudity", "Hacking/Proxy Avoidance", "Violence/Hate/Racism", "Gay/Lesbian", "Gambling", "Illegal/Questionable", "Illegal Drugs", and "Cult/Occult" categories(*most spyware comes from such kind of websites*) to be filtered while accessing a website which contains these specified categories of contents.



eral Categories	Customization Cache	
uto Category Setup		
🔽 Enable External Database C	ontent Filtering	
🔽 Block 🔽 Log	Matched Web Pages	
🗖 Block 🔲 Log	Unrated Web Pages	
🔽 Block 🔲 Log	When Content Filter Server Is l	Jnavailable
	Content Filter Server Unavailab	le Timeout 10 (1~30 seconds)
elect Categories		
🥅 Select All Categories	🗖 Clear All Categories	
Adult/Mature Content	Pornography	Sex Education
🔲 Intimate Apparel/Swimsuit	🔽 Nudity	🔲 Alcohol/Tobacco
🔽 Illegal/Questionable	🔽 Gambling	🔽 Violence/Hate/Racism
🔲 Weapons	Abortion	🦳 Arts/Entertainment
Business/Economy	🔽 Cult/Occult	🔽 Illegal Drugs
🗖 Education	🔲 Cultural Institutions	🦳 Financial Services
Brokerage/Trading	🗖 Games	🔲 Government/Legal
🥅 Military	Political/Activist Groups	🗖 Health
🗖 Computers/Internet	🔽 Hacking/Proxy Avoidance	🥅 Search Engines/Portals
🔲 Web Communications	🔲 Job Search/Careers	🔲 News/Media
Personals/Dating	Reference	🥅 Chat/Instant Messaging
🗖 Email	Newsgroups	🗖 Religion
🗔 Shopping	Auctions	🗖 Real Estate
🗖 Society/Lifestyle	🔽 Gay/Lesbian	Restaurants/Dining/Food
Sports/Recreation/Hobbies	Travel	🗖 Vehicles
🗖 Humor/Jokes	🗖 Streaming Media/MP3	🔲 Software Downloads
🔲 Pay to Surf	🗖 For Kids	🔲 Web Advertisements
🔲 Web Hosting		
		Basic<<

#### **1.3 Demonstrate Content Filtering by an example:**

Using a browser to browse the nudity website, for example, *www.nudistweb.net*, it will be blocked and redirected to *www.zyxel.com* with "(Website Blocking)" message displayed at the moment.



## 2. Proactively Prevent Phishing

Phishing – The act of sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. With the combination of CF and AS services in ZyWALL 5 UTM, network administrator can dramatically lower the chance of company network users from receiving possible phishing emails and also prevent users from accessing known phishing websites.

# 2.1 Setting up the ZyWALL 5 UTM CF+AS service to prevent phishing CF+AS License Activation

In **Registration** page, if you already have an account exist in myZyXEL.com, then all you have to do is, first select "**Existing myZyXEL.com account**" and enter your username password, and select Content Filter 1 month and AS 3 months trial version to activate

egistration	Service	
Device Regis	tration	
Existing	myZyXEL.com	account
User Name		jacky1234
Password		(Type username and password from 6 to 20 characters.)
Service Activ	vation	
Content	Filtering 1-mon	th Trial
🔽 Anti Spa	ım 3-month Tria	al (Service has been activated.)
🔽 IDP/AV	3-month Trial (S	Service has been activated.)
	ore device servi	ices management, please go to <u>myZyXEL.com</u>
Note: For mo		

# 2.2 $\square$ Setup the ZyWALL 5 UTM CF service to block the known phishing web sites

#### 2.2.1 The General settings:

- 1. In **CONTETN FILTER ->General**, check the **Enable Content Filter** check box to enable CF function.
- 2. In Schedule to Block, select the Always Block to let CF engine to do blocking the web sites.
- 3. In **Message to display when a site is blocked**, you can input the text, say "(**Website Blocking**)", to remind the users that the website he is trying to access is blocked. And you can input the URL in the **Redirect URL** field, for example, "<u>www.zyxel.com</u>" to redirect the original URL to this redirect-URL.
- 4. In **Exempt Computers** item, we can select **Exclude specified address ranges from the content filter enforcement** to NOT apply content filter policies to the specified IP address ranges, for example, if the CEO's computer which is assigned an IP address: 192.168.10.200 needed NOT to be applied by CF engine, the IT staff can add this IP address 192.168.10.200 to the list to meet this exclusion requirement.

5. Click on the Apply button to save the settings.

ZvXEL	General Categories Customization Cache
	General Setup
номе	1
REGISTRATION	Restrict Web Features
NETWORK 🗵	Block ActiveX Java Applet Cookies Web Proxy
SECURITY 🖂	Schedule to Block
IDP	2 OAlways Block
ANTI-VIRUS	O Block From 0 : 0 To 0 : 0 (24-Hour Format)
ANTI-SPAM	Message to display when a site is blocked
CONTENT FILTER	Message to display when a site is blocked
VPN	3 Denied Access Message (Website Blocking)
CERTIFICATES	Redirect URL www.zyxel.com
AUTH SERVER	Exempt Computers
ADVANCED 💌	O Enforce content filter policies for all computers.
LOGS	Include specified address ranges in the content filter enforcement.
MAINTENANCE	4 OExclude specified address ranges from the content filter enforcement.
	Add Address Ranges Address List
LOGOUT	192.168.10.200 - 192.168.10.200
	Add Range Delete Range
	5 Apply Reset

#### 2.2.2 Customize the Forbidden web sites which are known phishing web sites

In addition to use external content filter server to do filtering policies, we can customize the filter policies as our own. Just as the settings in the **CONTETN FILTER->Customization**: Check **Enable Web site customization** check box. Enter the distrusted web site in the **Forbidden Web Site** list. (The forbidden list is similar to the black list.)

ZyXEL	CONTENT FUTED
НОМЕ	General Categories Customization Cache
REGISTRATION	Web Site List Customization
NETWORK 🛛	Enable Web site customization.
SECURITY 🖂	Disable all Web traffic except for trusted Web sites.
FIREWALL	Don't block Java/ActiveX/Cookies/Web proxy to trusted Web sites.
IDP	Trusted Web Sites
ANTI-VIRUS	
ANTI-SPAM	Add Trusted Web Site Trusted Web Sites
CONTENT FILTER	
VPN	
CERTIFICATES	Add
AUTH SERVER	
	Forbidden Web Site List
ADVANCED 🖂	Add Forbidden Web Site Forbidden Web Sites
LOGS	www.phishbank.com
MAINTENANCE	www.phishbank.com
LOGOUT	Add

## 2.2.3 Demonstrate "*Customization*" Content filtering by an example:

Using a browser to browse "www.phishbank.com", the attempt will be blocked (because "www.

*phishbank<u>.com</u>*" is added in the forbidden list) and will be redirected to "<u>www.zyxel.com</u>" with "(**Website Blocking**)" message displayed at the moment.



#### 2.3 Setup the ANTI-SPAM service to filter the phishing mail:

- 1. In **ANTI-SPAM -> General**, check the **Enable Anti-Spam** check box to enable AS function and select all mail send to **LAN** and **DMZ** had to be rated.
- Input 1~16 characters for the phishing tag text which will be used to tagged on the subject of the phishing e-mail, here we input "[PHISHING]". Then select Discard SMTP mail. Forward POP3 mail with tag in mail subject to forward the POP3 spam-mails but discard the SMTP ones.
- In Action taken when mail sessions threshold reached, select Forward to bypass AS inspection while the concurrent mail sessions is over 15 sessions.
   TIPS: the AS engine support maximum 15 mail sessions concurrently.
- 4. Click on the **Apply** button to save the settings.

1. 🗹 Enable Anti-Spam						
	Fo LAN	WAN	DMZ	WLAN	¥PN	
From			<b>Z</b>			
LAN			<b>V</b>			
WAN						
DMZ						
WLAN						
¥PN			<b>V</b>			
				* Protected T	raffic Direction	
Action for Spam Mails						
2. Phishing Tag	SHING]					
Spam Tag [SP	AM]					
O Forward SMTP & P	DP3 mail with tag in	n mail subject.				
Oiscard SMTP mail	Forward POP3 ma	iil with tag in ma	ail subject.			
Action taken when ma	il sessions thres	hold is reache	d			
3. O Forward						
O Block						

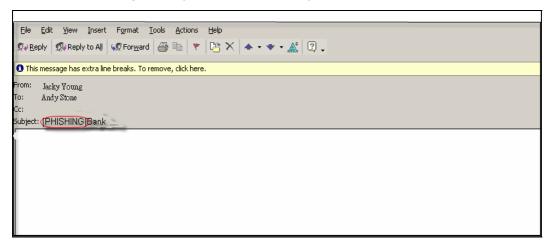
In **ANTI-SPAM -> External DB**, check **Enable External Database** with adjusting the threshold scroll bar which let external database help IT staff to adjudge whether the POP3/SMTP mails are phishing mails or not.

TI-SPAM	
General	External DB Lists
External D	atabase
	e External Database eshold (Mail with a score greater than or equal to the threshold is treated as spam.)
opun m	sindia (nan wara sobre greater anan or equar to ano amosindia is dreated as spanny
Threshold	90 🖪 💶 👘 🖧 📐
Action for	No Spam Score
	Spam Score
-	rd SMTP & POP3 mail with tag in mail subject.
🔘 Disca	rd SMTP mail. Forward POP3 mail with tag in mail subject.
External D	atabase Service Status
Eutone al C	Patabase Service: License Active
	Date: 2008-08-30
Expiration	
	Apply Reset

TIPS: To activate the "External DB" option, the ANTI-SPAM service must be registered at first.

#### 2.3.1 D How a PHISHING mail looked like as it was received?

According to the above settings, if the user behind the ZyWALL 5 UTM LAN zone that received a POP3 mail which is treated as phishing, the mail will be tagged "[PHISHING]" in the original mail subject ("Bank" is the original subject) and the new subject will looks like "[PHISHING]Bank" as listed below:



TIPS: An end user can apply the Junk Mail rule to the received phishing mail which are already tagged by the ZyWALL 5 UTM AS engine.

\*To apply the Junk Mail rule, please refer to the user guide of which mail client software you use.

#### 2. Prevent non-business web surfing

Below is an example that demonstrates how to configure the ZyWALL 5 UTM CF service to prevent employee from surfing websites that are not related to work.

Setting up the ZyWALL 5 UTM CF service to block the non-business web surfing.

#### 2.1 The General settings:

- 1. In **CONTETN FILTER ->General**, check the **Enable Content Filter** check box to enable CF function.
- 2. In **Schedule to Block**, select the **Always Block** to let CF engine to do blocking the websites all the time.
- 3. In Message to display when a site is blocked, you can input the text, say "(Website Blocking)", to remind the users that the website he is trying to access is blocked. And you can input the URL in the Redirect URL field, for example, "<u>www.zyxel.com</u>" to redirect the original URL to this redirect-URL.
- 4. In Exempt Computers, we can select Exclude specified address ranges from the content filter enforcement to NOT apply content filter policies to the specified IP address ranges, for example, if the CEO's computer which is assigned an IP address: 192.168.10.200 needed NOT to be applied by CF engine, the IT staff can add this IP address 192.168.10.200 to the list to meet this exclusion

requirement.

5. Click on the **Apply** button to save the settings.

ZvXEL	General	Categories	Customization	Cache	
	General Set	tup			
номе	1 💌 Enable	Content Filter			
REGISTRATION	Restrict We	b Features			
	Block				
SECURITY 🔤		ActiveX	🗌 Java Apple	t 🗌 Cookies	Web Proxy
FIREWALL	Schedule to	Block			
IDP	2 💿 Always	s Block			
ANTI-VIRUS	O Block I			To 0 : 0 (24-H	iour Format)
ANTI-SPAM	Mossage to	display when a si	to is blockod		
CONTENT FILTER	nessaye to	uispiay witen a si			
VPN	3 Denied Acc	cess Message	(Website Blocking)		
CERTIFICATES	Redirect U	RL	www.zyxel.com		
AUTH SERVER	Exempt Cor	nputers			
	O Enform	e content filter polici	es for all computers.		
LOGS			anges in the content filte	r enforcement.	
MAINTENANCE			ranges from the content f		
MAINTENANCE	Add Addre	cc Danges		Address List	
LOGOUT	_	-		192.168.10.200 - 192.168	10.200
	From				
	To		_		
	Add Rang	e		Delete Range	
			5 Apply	Reset	

#### 2.2 Using external database content filtering

If you have registered the CF service, you can enable external database content filtering in the **CONTENT FILTER -> Categories** page, with selecting the categories check boxes to specify the types of contents to be filtered while accessing a website which contains these specified categories of contents. As the figure listed below, "**Sports/Recreation/Hobbies**" and "**Financial Services**" are selected.

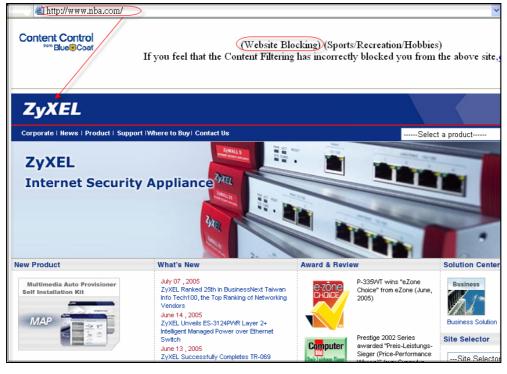
## ZyXEL

ZvXEL	General Categories	Customization Cache	
	Auto Category Setup		
номе	Enable External Database Co	•	
REGISTRATION	Block V Log	Matched Web Pages	
	Block Log	Unrated Web Pages	
NETWORK 🗹	🔽 Block 📃 Log	When Content Filter Server Is Una	
SECURITY 🛛 🖂		Content Filter Server Unavailable	Timeout 10 (1~30 seconds)
FIREWALL	Select Categories		
IDP			
ANTI-VIRUS	Select All Categories	Clear All Categories	
ANTI-SPAM	Adult/Mature Content	Pornography	Sex Education
CONTENT FILTER	Intimate Apparel/Swimsuit	Nudity	
VPN	Illegal/Questionable	Gambling	Violence/Hate/Racism
CERTIFICATES	Weapons	Abortion	Arts/Entertainment
AUTH SERVER	Business/Economy	Cult/Occult	Illegal Drugs
	Education	Cultural Institutions	Financial Services
ADVANCED 🖂	Brokerage/Trading	Games	Government/Legal
LOGS	Military	Political/Activist Groups	Health
MAINTENANCE	Computers/Internet	Hacking/Proxy Avoidance	Search Engines/Portals
	Web Communications	Job Search/Careers	News/Media
LOGOUT	Personals/Dating	Reference	Chat/Instant Messaging
	Email	Newsgroups	Religion
	Shopping	Auctions	🗌 Real Estate
	Society/Lifestyle	Gay/Lesbian	 Restaurants/Dining/Food
	Sports/Recreation/Hobbies	Travel	Vehicles
	Humor/Jokes	Streaming Media/MP3	Software Downloads
	Pay to Surf	For Kids	Web Advertisements

## 2.3 Demonstrate Content Filtering by an example:

Using a browser to browse the sports website, for example, www.nba.com, it will be blocked and redirected

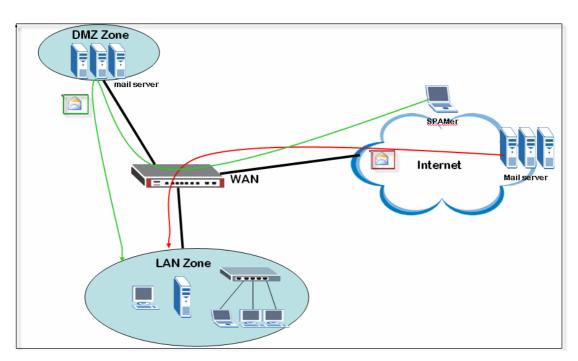
to <u>www.zyxel.com</u> with "(Website Blocking)" message displayed at the moment.



## To eliminate spam mails to block unwanted messages everyday

An employee has to spend the working time to distinguish which mail is spam and which is not, and this will increase his overhead and reduce his performance. Thus for productivity, spam emails should be managed. Activate the ZyWALL 5 UTM AS service can filter the spam e-mail.

TIPS: the AS engine do not support IMAP4, only SMTP (tcp port 25) and POP3 (tcp port 110) are supported.



Red line: POP3 Green line: SMTP

## 1. No Self-hosted Mail servers (POP3)

#### 1.1 Anti-Spam License Activation

In **Registration** page, if you already have an account exist in myZyXEL.com, then all you have to do is, first select "**Existing myZyXEL.com account**" and enter your username password, and select AS 3 months trial version to activate

egistration	Service			
Device Regist	tration			
Existing	myZyXEL.com	account		
-				
User Name		jacky1234		
Password			(Type username and password fr characters.)	om 6 to 20
			charactersij	
Service Activ	ation			
🗖 Content	Filtering 1-mor	th Trial		
🔽 Anti Spa	m 3-month Tria	al (Service has been activat	ted.)	
🖂 IDP/AV :	3-month Trial (	Service has been activated	.)	
Note: For mo	re device serv	ices management, please g	jo to <u>myZyXEL.com</u>	

#### **1.2 Setup the ANTI-SPAM service**

- 1. In ANTI-SPAM -> General, check the Enable Anti-Spam check box to enable AS function.
- Input 1~16 characters for the spam tag text, here we input "!!!SPAM!!!" Select Discard SMTP mail.
   Forward POP3 mail with tag in mail subject to forward the POP3 spam-mails but discard the SMTP ones.
- 3. In Action taken when mail sessions threshold reached, select Forward to bypass AS inspection while the concurrent mail sessions is over 15 sessions.

TIPS: the AS engine support maximum 15 mail sessions concurrently.

 Click on the Apply to save the settings.
 TIPS: For SMTP protocol, the AS engine support "Discard" or "Forward" it with the specified tag text, but for POP3 protocol, "Forward" is supported only.

General 9								
🗹 Enal	1.1.1.0							
100 M	1. Enable Anti-Spam							
	То	LAN	WAN	DMZ	WLAN	¥₽N		
From								
	AN 🔲							
W	AN 🔳	<b>V</b>	<ul><li>✓</li></ul>	<b>V</b>				
D	MZ 🔲							
W	AN 🔲	<ul><li>✓</li></ul>	<ul> <li>Image: A set of the set of the</li></ul>	<b>V</b>	<ul><li>✓</li></ul>			
Y	PN	<ul><li>✓</li></ul>	<ul> <li>Image: A set of the set of the</li></ul>	<b>V</b>	<ul><li>✓</li></ul>			
					* Protected T	raffic Direction		
Action fo	· Spam Mails							
Phishing	Tag (PHISHIN	G]						
Spam Ta	ig [SPAM]							
<ul> <li>Forv</li> </ul>	ard SMTP & POP3	mail with tag ir	n mail subject.					
🔘 Disc	ard SMTP mail. For	ward POP3 ma	il with tag in ma	ail subject.				
Action ta	ken when mail se	ssions thres	hold is reache	d				
. 💿 Forv	and							
O Bloc								

In **ANTI-SPAM -> External DB**, check **Enable External Database** with adjusting the threshold scroll bar which let external database help IT staff to adjudge whether the POP3/SMTP mails are spam mails or not.

ANTI-SPAM
General External DB Lists
External Database
Enable External Database Spam Threshold (Mail with a score greater than or equal to the threshold is treated as spam.)
Threshold:
Action for No Spam Score
Tag for No Spam Score
○ Forward SMTP & POP3 mail with tag in mail subject.
O Discard SMTP mail. Forward POP3 mail with tag in mail subject.
External Database Service Status
External Database Service: License Active
Expiration Date: 2008-08-30
Apply Reset

TIPS: To activate the "External DB" option, the ANTI-SPAM service license must be activated.

## 2. Protect Self-hosted Mail Servers (SMTP)

#### 2.1 Anti-Spam License Activation

In **Registration** page, if you already have an account exist in myZyXEL.com, then all you have to do is, first select "**Existing myZyXEL.com account**" and enter your username password, and select AS 3 month's trial version to activate.

egistration	Service				
Device Regist	tration				
Existing	myZyXEL.com a	account			
User Name		jacky1234			
Password		•••••	(Type use characters	rname and password from 6 to 20	
Service Activ	ation				
🗌 Content	Filtering 1-mon	th Trial			
🔽 Anti Spa	m 3-month Tria	l (Service has been activat	ed.)		
🔽 IDP/AV 🤅	3-month Trial (S	Service has been activated.	.)		
Note: For mo	re device servi	ces management, please g	o to <u>myZyXEL.com</u>		

#### 2.2 Setup the ANTI-SPAM service:

- 1. In ANTI-SPAM -> General, check the Enable Anti-Spam check box to enable AS function.
- 2. Input 1~16 characters for the spam tag text, here we input

"**!!!SPAM!!!**". Select **Discard SMTP mail. Forward POP3 mail with tag in mail subject** to forward the POP3 spam-mails but discard the SMTP ones.

**3.** In **Action taken when mail sessions threshold reached**, select **Forward** to bypass AS inspection while the concurrent mail sessions is over 15 sessions.

TIPS: the AS engine support maximum 15 mail sessions concurrently.

4. Click on the **Apply** to save the settings.

TIPS: For SMTP protocol, the AS engine support "Discard" or "Forward" it with the specified tag text, but for POP3 protocol, "Forward" is supported only.

Enable Anti-Spam							
	То	LAN	WAN	DMZ	WLAN	¥PN	
From							
LAN							
WAN			<ul><li>✓</li></ul>	<ul><li>✓</li></ul>			
DMZ							
WLAN							
¥PN						raffic Direction	
Action for S Phishing Ta		1					
Spam Tag	[SPAM]						
	d SMTP & POP3 m	-	-				
	I SMTP mail. Forw						
Action taker	n when mail ses	sions thres	hold is reache	d			
. 💿 Forwar	£						

Customize the Anti-Spam policies as our own by using black list to let policies be applied and using white list to bypass the policies. The lists are added as in the **ANTI-SPAM -> List**, after finished adding the specified lists, click on the **Apply** button to save the settings.

Resource Usage				
	ist Storage Space ir			
0%				100%
Whitelist				
🗹 Use Whitelist				
# Active	Туре	Content	Modify	1
				-
1 <u>Y</u>	E-Mail	Andy@net.com	Vî 🗗 Î	
Insert new	w record before r	ecord 1 (record number)		
Blacklist	4			
🗹 Use Blacklist				
				8
	Туре	Content	Modify	-
# Active	E-Mail	Sharno@net.com	Vî 🕑 ()	
		1 4		
1 <u>Y</u>	v record hefore r	ecord litecord pumber!		
1 <u>Y</u>	w record before r	ecord 1 (record number)		

## 

According to the above situations, if the user behind the ZyWALL 5 UTM LAN zone that received a POP3 mail which is a spam, the mail will be tagged "**!!!SPAM!!!**" in the original mail subject ("**Hello**" is the original subject) and the new subject will looks like "**!!!SPAM!!!Hello**" as listed below:

🗹 IIISPAN	1!!!Hello - Message (Plain Text)
<u>Eile E</u>	dit <u>V</u> iew Insert F <u>o</u> rmat Iools <u>A</u> ctions <u>H</u> elp
Ø <b>∂</b> <u>R</u> eply	🛛 🕵 Reply to All 🔩 🖗 🖝 🔻 🔛 🖈 🖈 🔹 🛧 🔹 🛠 🖓 🗸
O This m	essage has extra line breaks. To remove, click here.
From: J	acky Young
	ndy Stone
Cc:	
Subject: (	
Long t	ime no see!

## **Threat Reports**

In order to make the ZyWALL more user-friendly and cost-effective, ZyNOS v4.01 comes with the Threat report feature.

## ZyXEL

Threat report displays attack, intrusion and spam statistics of your network.

To display the Threat Report screen, switch to Reports > Threat Reports. Threat reports are categorized into IDP, Anti-Virus and Anti-Spam sections.

ZyXEL		HELP (
номе	THREAT REPORTS	
REGISTRATION	IDP Anti-Virus Anti-Spam	
NETWORK 🖂	Setup	
SECURITY 🛛 🖂	Collect Statistics	
ADVANCED 🛛		
REPORTS 🛛 🗖	Apply	
SYSTEM REPORTS	Summary	
THREAT REPORTS	Total Session Scanned 0	
LOGS	Total Session Dropped 0	
	Total Session Reset 0	
	Total Packet Dropped 0	
LOGOUT	Statistics	
	Top Entry By Signature Name 💌	
X	# Signature Name Type Severity Occurrences	
	· · · · · ·	
	Total: 0	
	Refresh	
St	tatus: Ready	

The IDP report types will be categorized by different **Top** entry; they are Signature name, Source and Destination. These reports can help administrator to manage and control the most dangerous source and most damage victim in the real time.

ZyXEL		HELP (?)
НОМЕ	THREAT REPORTS	
REGISTRATION	IDP Anti-Virus Anti-Spam	_
NETWORK 🖂	Setup	
SECURITY 🖂	Collect Statistics since 2006-06-02 21:01:56	
ADVANCED 🛛		
REPORTS 🛛 🗖 SYSTEM REPORTS	Apply Reset Summary	
THREAT REPORTS	Total Sessions Scanned 59537	
LOGS	Total Sessions Dropped 0	
MAINTENANCE	Total Sessions Reset 0 Total Packets Dropped 0	
LOGOUT	Statistics	
	Top Entry By Signature Name V Signature Name	
	# Signature Name Typ Source :y Occurrences	
	1 <u>IIS msade access</u> AccessControl Medium 5587	
	2 FRONTPAGE / vti bin/ Other Medium 81	
	3 SHELLCODE x86 NOOP - 2 BufferOverflow Medium 54	
	4         SHELLCODE x86 NOOP - 1         BufferOverflow         Medium         34	
	5 SHELLCODE x86 inc ebx NOOP BufferOverflow Medium 32	
	Status: Ready	

The Anti-Virus report types will be categorized by different **Top** entry; they are Virus name, Source and Destination. These reports can help administrator to manage and control the most dangerous source and most damage victim in the real time.

ZyXEL		HELP (?)
НОМЕ	THREAT REPORTS	
REGISTRATION		
	IDP Anti-Virus Anti-Spam	
NETWORK 🖾	Setup	
SECURITY 🗹	Collect Statistics since 2006-06-02 21:02:09	
ADVANCED 🛛		
REPORTS 🛛 🗖 SYSTEM REPORTS	Apply Reset Summary	
THREAT REPORTS		
	Total Files Scanned 2821 Infected Files Detected 1	
LOGS		
MAINTENANCE	Statistics	
LOGOUT	Top Entry By Virus name V Virus name	
	# Virus name Source Occurrences	
	1 EICAR-Test-File 1	
	Total: 1	
	Refresh Flush	
	Status: Ready	

The Anti-Spam report types will be categorized by different **Top** entry; they are Sender mail address and Source. These reports can help administrator to manage and control the most dangerous source and they may report it to Spam analysis organization or block the source by firewall rule straight away.

ZyXEL		HELP (?)
номе	THREAT REPORTS	
REGISTRATION	IDP Anti-Virus Anti-Spam	
NETWORK 🖾	Setup	
SECURITY 💌	Collect Statistics since 2006-04-25 07:18:35	
ADVANCED 🛛		
REPORTS 🛛 🗖	Apply Reset	
THREAT REPORTS		
1000	Total Mail Scanned 13 Spam Mail Detected 12	
LOGS	Phishing Mail Detected 0	
MAINTENANCE	No Score Mail Detected 0	
	Mail Session Forwarded 0 (When mail accelerations intershold in teached.)	
LOGOUT	Mail Session Blocked 0 (When mail sessions Unleshold is leached.)	
	Statistics       Image: Top Entry By       Sender Mail Address       Sender Mail Address	
	Score Distribution Sender Mail Address Source	
	# Sender Mail Address Occurrences	
	1 martin.gu@zyxel.cn 10	
	2 Joe.Zhou@zyxel.cn 2	
	Total:12	
	Status: Ready	

The Anti-Spam report also has a Score Distribution map and this can help administrator to setup a valuable Spam Threshold to make the spam tag more suitable to the local environment.

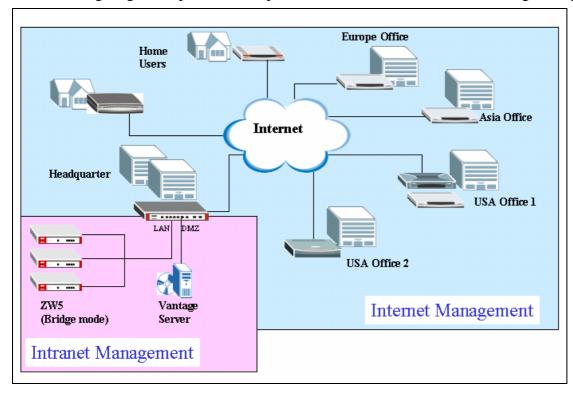
	apari Mari Detectoa - 676	
ZyXEL	Phishing Mail Detected 0	
	No Score Mail Detected 7	
	Mail Session Forwarded 0 (When mail sessions threshold is reached.)	
HOME	Mail Session Blocked 0 (When mail sessions threshold is reached.)	
REGISTRATION	Statistics	
NETWORK 🗹	O Top Entry By Sender Mail Address ∨	
SECURITY 🛛 🖾	• Score Distribution	
ADVANCED 🛛 😒		
REPORTS SYSTEM REPORTS	Spam Threshold: 75	
LOGS		
	1000	
MAINTENANCE		
LOGOUT	Mail 500 0 10 20 30 40 50 60 70 80 90 100 Threshold Score Refresh Flush	
	Status: <mark>Ready</mark>	

## **Centralized Management**

## Using Vantage CNM for Management

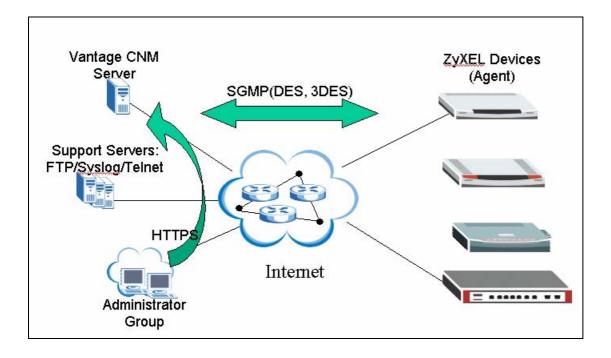
Vantage CNM is a centralized network management solution that allows users to easily configure, manage and monitor ZyWALL devices from any location.

Vantage CNM provides some key features like Centralized Firewall Management, Firmware Upgrade and Management, Intuitive Device and Account Monitoring, Logs and Alarms, One-click VPN and Multiple Administrator, Multiple Domain Management.



The following diagram depicts an example of the network environment for using Vantage CNM.

To manage your ZyWALLs through Vantage CNM, user needs to prepare Vantage CNM server and 3rd party FTP/Syslog/Telnet servers. For the detailed installation & registration process (to myZyXEL.com), please refer to **Vantage CNM Support Note**.



In the following section, we will explain how to add your ZyWALL to Vantage CNM server manually. Note that ZyWALL must be registered on Vantage CNM before it can be managed via Vantage CNM. In the following section, we will explain how to register device manually. Devices can be also added (imported) to Vantage CNM through XML files. For detailed operation, please refer to **Vantage CNM Support Note**. Please check **CNM Reference Guide for XML description files.pdf** for detailed description.

Add device manually

Step 1. Left click on the folder (e.g. AAA) and go to **Device**>>**Registration**.

🚰 https://127.0.0.1 - Van	tage CNM 2.1 - Mic
ZyXEL	
Search	۷

DEVICE	CONF
Status	
Registration	)
Synchronize	
Firmware M	gmt
Firmware U	pgrade
Configuratio	n File

Step 2. Select **Manual Add**, and press **Next**. Select No, for not to associate the device to the device owner now, then press Next.

Devi	ce >> Registration	2
	Welcome to the Device Registration Wizard	
How	do you want to register these new devices?	
6	Manually Add	
o	Import from a XML batch registration file	
	Back	)

You can register (add) as many devices as you wish at one time via importing XML file to Vantage. In the XML file, you need to define

- 1. device type
- 2. device name
- 3. device's LAN MAC address

The XML file can be used for mass deployment.

User can assign a device owner or leave it to the owner of folder AAA.

Device >> Registration		?
Welc	ome to the Device Registration Wizard	
Would you like to associate a device	e owner with these new devices now?	
O Yes	No	
		Next

Step 3. Input the MAC address of LAN interface of the device. Give this device a name. Select the corresponding Device Type, press **Finish**.

Device >> Re	gistration ?
	Welcome to the Device Registration Wizard
Manual	
Please enter	the following device information.
LAN MAC (Hex)	00a0c56fe109 *
Name	Z/WALL70
Device Type	ZWVALL70
O Set Vanta	ge CNM configuration to device. 💽 Get configuration from the device.
Encryption Methods	None 🔽
Encryption Key	
	Back

Note that if the ZyWALL has been deployed (configured) and you want to retrieve the configuration from device. You can select the option "Get configuration from the device". Otherwise, you can use "Set Vantage CNM configuration to device" to overwrite existing configuration on device as soon as it registers to Vantage CNM.

After finishing the configuration on Vantage CNM, click on "Finish" to finish the registration of device on CNM and following screen will show up and ZyWALL is added to CNM under folder AAA.

intersty/ activities a rankage as a rank						
ZyXEL	DEVICE	CONFIGURATION	BUILDING BLOCK	SYSTEM MONITOR	REPORT	
	Vroot\AAA	•				
Search						
root						
Zywall70		Device >> Registra	ation			?
			De	wice Registration Finished	I	
		Device Name	Device Type	WAN IP Address	LAN MAC Address	Register Status
	-	ZWVALL70	ZyWALL70	0.0.0.0	00a0c56fe109	Success!

Step 4. On the device, go to **ADVANCED->REMOTE MGMT->CNM**, enable Vantage CNM and configure Vantage CNM Server Address in the filed. If Encryption Algorithm is enabled, you must select the same algorithm and secret key on both device and Vantage CNM. In the following case, the Encryption Algorithm is disabled.

<b>VIOTE MAN</b>						
www	SSH	TELNET	FTP	SNMP	DNS	CNM
Registration	Information					
Registratio	on Status	No	t Registered			
Last Regis	tration Time	000	0 - 00 - 00, 00 :	00 : 00		
_						
			Refresh			
Vantage CN	M Sotun					_
vantage chi	a setup					
🔽 Enable	•					
Vantag	e CNM Server Add	Iress	0.59.1	. 252		
Encryp	tion Algorithm	IN	ONE 🔻			
	J	1				
		Apply		Reset		

Step 5. After configuring CNM remote management on device, ZyWALL will start to register itself to configured Vantage CNM server. After exchanging the configuration between ZyWALL and Vantage CNM, the Registration Status will change to "Registered". At this moment, the configuration is synchronized on both device and Vantage CNM.

MOTE MAN	AGEMENT					
www	SSH	TELNET	FTP	SNMP	DNS	CNM
Registratio	n Information					
Registrat	tion Status	Re	gistered			
5	istration Time		)5 - 03 - 16, 10 : :	30 : 22		
			Refresh			
Vantage C	NM Setup					
🔽 Enab	le					
Vanta	age CNM Server Ad	dress 1	0.59.1	. 252		
Encry	ption Algorithm	N	ONE 🗾			
		Apply		Reset		

On Vantage CNM, the device icon will turn green and the device status will change to "On" and the WAN IP of the device will be shown on the content screen.

ZyXEL	DEVICE	CONFIGUR	ATION BU	JILDING BLOCK	SYSTEM	MONITOR	REPORT		
Search	© WrootVAA/	AVZYWALL70	_		_	_			
	De	wice >> Statu	\$					2	
	Device Status								
	D	evice Name	Туре	MAC	IP	Status	Firmware Version	Last Edit	
		ZWVALL70	ZyWALL70	00a0c57d1635	10.59.1.25	On	3.63(VVM.2)	2005-3-16 18:31:02	

## FAQ

## A. Product FAQ

## A01. What is the ZyWALL Internet Access Sharing Router?

The ZyWALL series fulfills a range of application environments, from small and medium businesses, SOHO, or Telecommuters, to home user or education applications. The ZyWALL series provides a robust Firewall to protect your network, and the IPSec VPN function allows you to create a secure connection for e-business. ZyWALL's design helps users to save expenses, minimize maintenance, and simultaneously provide a high quality networking environment.

The ZyWALL series is a robust solution complete with everything needed for providing Internet access to multiple workstations through your cable or ADSL modem. It is the most simple and affordable solution for multiple and instant broadband Internet access router with 802.11 wireless support.

## A02. Will the ZyWALL work with my Internet connection?

The ZyWALL is designed to be compatible with most network environment (cable or xDSL modems). Most external Cable and xDSL modems use an Ethernet port to connect to your computer so the ZyWALL can be place between the computer and the External modem. As long as your Internet Access device has an Ethernet port, you can use the ZyWALL. Besides, if your ISP supports PPPoE you can also use the ZyWALL, because PPPoE had been supported in the ZyWALL.

## A03. What do I need to use the ZyWALL?

You need an xDSL modem or cable modem with an Ethernet port to use the ZyWALL. The ZyWALL has two Ethernet ports: LAN port and WAN port. You should connect the computer to the LAN port and connect the external modem to the WAN port. If the ISP uses PPPoE Authentication you need the user account to enter in the ZyWALL.

## A04. What is PPPoE?

PPPoE stands for **P**oint-to-**P**oint **P**rotocol **o**ver **E**thernet that is an IETF draft standard specifying how a computer interacts with a broadband modem (i.e. xDSL, cable, wireless, etc.) to achieve access to the high-speed data networks via a familiar PPP dialer such as 'Dial-Up Networking' user interface. PPPoE supports a broad range of existing applications and service including authentication, accounting, secure access and configuration management.

## A05. Does the ZyWALL support PPPoE?

Yes. The ZyWALL supports PPPoE since ZyNOS 2.50.

## A06. How do I know I am using PPPoE?

PPPoE requires a user account to login to the provider's server. If you need to configure a user name and password on your computer to connect to the ISP you are probably using PPPoE. If you are simply connected to the Internet when you turn on your computer, you probably are not. You can also check your ISP or the information sheet given by the ISP. Please choose PPPoE as the encapsulation type in the ZyWALL if you are using PPPoE service provided by your ISP.

## A07. Why does my Internet Service Provider use PPPoE?

PPPoE emulates a familiar Dial-Up connection. It allows your ISP to provide services using their existing network configuration over the broadband connections. Besides, PPPoE supports a broad range of existing applications and service including authentication, accounting, secure access and configuration management.

## A08. How can I configure the ZyWALL?

- Telnet remote management- CLI command line
- Web browser- web server embedded for easy configurations

## A09. What can we do with ZyWALL?

Browse the World Wide Web (WWW), send and receive individual e-mail, and up/download data on the internet. These are just a few of many benefits you can enjoy when you put the whole office on-line with the ZyWALL Internet Access Sharing Router.

## A10. Does ZyWALL support dynamic IP addressing?

The ZyWALL supports both static and dynamic IP address from ISP.

## A11. What is the difference between the internal IP and the real IP from my ISP?

Internal IPs is sometimes referred to as virtual IPs. They are a group of up to 255 IPs that are used and recognized internally on the local area network. They are not intended to be recognized on the Internet. The real IP from ISP, instead, can be recognized or pinged by another real IP on the internet. The ZyWALL Internet Access Sharing Router works like an intelligent router that route between the virtual IP and the real IP.

## A12. How does e-mail work through the ZyWALL?

It depends on what kind of IP you have: Static or Dynamic. If your company has a domain name, it means that you have a static IP address. Suppose your company's e-mail address is xxx@mycompany.com. Joe and Debbie will be able to send e-mail through ZyWALL Internet Access Sharing Router using jane@mycompany.com and debbie@mycompany.com respectively as their e-mail addresses. They will be able to retrieve their individual private and secure e-mail, if they have been assigned the proper access right.

If your company does not have a domain name, it means that your ISP provides you with a dynamic IP address. Suppose your company's e-mail address is mycompany@ispname.com. Jane and John will be able to send e-mail through ZyWALL Internet Access Sharing Router using

"jane"<mycompany@ispname.com> and "john"<mycompany@ispname.com> respectively as their e-mail addresses. Again, they will be able to retrieve their individual private and secured e-mail, if they have been assigned the proper access right.

## A13. Is it possible to access a server running behind NAT from the outside Internet? If possible, how?

Yes, it is possible because ZyWALL delivers the packet to the local server by looking up to a NAT server table. Therefore, to make a local server accessible to the outsider, the port number and the internal IP address of the server must be configured in NAT menu.

## A14. What DHCP capability does the ZyWALL support?

The ZyWALL supports DHCP client on the WAN port and DHCP server on the LAN port. The ZyWALL's DHCP client allows it to get the Internet IP address from ISP automatically. The ZyWALL's DHCP server allows it to automatically assign IP and DNS addresses to the clients on the local LAN.

## A15. What are the capability of wireless feature of ZyWALL

Wireless in ZyWALL series support embedded 802.1x MD5/CHAP authentication of 32 clients.

## A16. What is the coverage range of Wireless in ZyWALL?

The coverage range typically is 50m~80m indoor, 150m~300m outdoor. The actual range may very depend on environment, as to obstacles and walls, RF interference, in the environment.

## A17. How do I used the reset button, more over what field of parameter will be reset by

## reset button?

You can used a sharp pointed object insert it into the little reset hole beside the power connector. Press down the reset button and hold down for approx 10 second, the unit will be reset. When the reset button is pressed the device's all parameter will be reset back to factory default. The default IP address is 192.168.1.1, Password 1234, ESSID Wireless.

## A18. What network interface does the new ZyWALL series support?

The new ZyWALL series support auto MDX/MDIX 10/100M Ethernet LAN/WAN port to connect to the computer on LAN and 10/100M Ethernet to connect to the external cable or xDSL modem on WAN.

## A19. How does the ZyWALL support TFTP?

In addition to the direct console port connection, the ZyWALL supports the uploading/download of the firmware and configuration file using TFTP (Trivial File Transfer Protocol) over LAN.

## A20. Can the ZyWALL support TFTP over WAN?

Although TFTP should work over WAN as well, it is not recommended because of the potential data corruption problems.

## A21. How can I upload data to outside Internet over the one-way cable?

A workaround is to use an alternate path for your upstream path, such as a dial-up connection to an Internet service provider. So, if you can find another way to get your upstream packets to the Internet you will still be able to receive downstream packets via ZyWALL.

## A22. My ZyWALL can not get an IP address from the ISP to connect to the Internet, what can I do?

Currently, there are various ways that ISPs control their users. That is, the WAN IP is provided only when the user is checked as an authorized user. The ISPs currently use three ways:

- 1. Check if the 'MAC address' is valid
- 2. Check if the 'Host Name' is valid, e.g., @home

If you are not able to get the Internet IP from the ISP, check which authentication method your ISP uses and troubleshoot the problem as described below.

## 1. Your ISP checks the 'MAC address'

Some ISPs only provide an IP address to the user with an authorized MAC address. This authorized MAC can be the PC's MAC which is used by the ISP for the authentication. So, if a new network card is used or the ZyWALL is attached to the cable modem directly, the ISP will reject the DHCP discovery from this MAC, thus no IP is assigned by the ISP.

The ZyWALL supports to clone the MAC from the first PC the ISP installed to be its WAN MAC. To clone the MAC from the PC you need to enter that PC's IP in WAN menu of the ZyWALL web configurator.

## 2. Your ISP checks the 'Host Name'

Some ISPs take advantage of the 'host name' message in a DHCP packet such as @home to do the authentication. When first installing, the ISP's tech people configure the host name as the 'Computer Name' of the PC in the 'Networking' settings. When the ZyWALL is attached to the cable modem to connect to the ISP, we should configure this host name in the ZyWALL's system (menu 1).

## A23. What is BOOTP/DHCP?

BOOTP stands for Bootstrap Protocol. DHCP stands for Dynamic Host Configuration Protocol. Both are mechanisms to dynamically assign an IP address for a TCP/IP client by the server. In this case, the ZyWALL Internet Access Sharing Router is a BOOTP/DHCP server. WinXP/2000 and WinNT clients use DHCP to request an internal IP address, while WFW and WinSock clients use BOOTP. TCP/IP clients may specify their own IP or utilize BOOTP/DHCP to request an IP address.

## A24. What is DDNS?

The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname, allowing your computer to be more easily accessed from various locations on the Internet. To use the service, you must first apply an account from several free Web servers such as <u>WWW.DYNDNS.ORG</u>.

Without DDNS, we always tell the users to use the WAN IP of the ZyWALL to reach our internal server. It is inconvenient for the users if this IP is dynamic. With DDNS supported by the ZyWALL, you apply a DNS name (e.g., www.zyxel.com.tw) for your server (e.g., Web server) from a DDNS server. The outside users can always access the web server using the www.zyxel.com.tw regardless of the WAN IP of the ZyWALL.

When the ISP assigns the ZyWALL a new IP, the ZyWALL updates this IP to DDNS server so that the server can update its IP-to-DNS entry. Once the IP-to-DNS table in the DDNS server is updated, the DNS

name for your web server (i.e., www.zyxel.com.tw) is still usable.

## A25. When do I need DDNS service?

When you want your internal server to be accessed by using DNS name rather than using the dynamic IP address we can use the DDNS service. The DDNS server allows to alias a dynamic IP address to a static hostname. Whenever the ISP assigns you a new IP, the ZyWALL sends this IP to the DDNS server for its updates.

## A26. What DDNS servers does the ZyWALL support?

The DDNS servers the ZyWALL supports currently is <u>WWW.DYNDNS.ORG</u> where you apply the DNS from and update the WAN IP to.

## A27. What is DDNS wildcard?

Some DDNS servers support the wildcard feature which allows the hostname, \*.yourhost.dyndns.org, to be aliased to the same IP address as yourhost.dyndns.org. This feature is useful when there are multiple servers inside and you want users to be able to use things such as www.yourhost.dyndns.org and still reach your hostname.

## A28. Does the ZyWALL support DDNS wildcard?

Yes, the ZyWALL supports DDNS wildcard that <u>WWW.DynDNS.ORG</u> supports. When using wildcard, you simply enter yourhost.dyndns.org in the **Host** field in Network/WAN/DDNS menu.

## A29. Can the ZyWALL NAT handle IPSec packets sent by the VPN gateway behind ZyWALL?

Yes, the ZyWALL's NAT can handle IPSec ESP Tunneling mode. We know when packets go through NAT, NAT will change the source IP address and source port for the host. To pass IPSec packets, NAT must understand the ESP packet with protocol number 50, replace the source IP address of the IPSec gateway to the router's WAN IP address. However, NAT should not change the source port of the UDP packets which are used for key managements. Because the remote gateway checks this source port during connections, the port thus is not allowed to be changed.

## A30. How do I setup my ZyWALL for routing IPSec packets over NAT?

For outgoing IPSec tunnels, no extra setting is required. For forwarding the inbound IPSec ESP tunnel, A 'Default' server set in menu 15 is required. It is because NAT makes your LAN appear as a single machine to

## ZyXEL

the outside world. LAN users are invisible to outside users. So, to make an internal server for outside access, we must specify the service port and the LAN IP of this server in Menu 15. Thus NAT is able to forward the incoming packets to the requested service behind NAT and the outside users access the server using the ZyWALL's WAN IP address. So, we have to configure the internal IPSec as a default server (unspecified service port) in menu 15 when it acts a server gateway.

## A31. What is STP (Spanning Tree Protocol) /RSTP (Rapid STP)?

When the ZyWALL is set to bridge mode, (R)STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a bridge to interact with other (R)STP-compliant bridges in your network to ensure that only one path exists between any two stations on the network. The configuration is especially for the advanced user who knows the protocol well.

## A32. What is the flow ZyWALL handles inbound and outgoing traffic?

(1) For a ZyWALL with **router** mode, following are the inspection flow for inbound and outgoing traffic.

<u>Traffic from WAN</u>: -> NAT -> Firewall-> Policy Route -> Load Balance -> Static Route -> IDP -> AV -> AS -> CF -> BWM

<u>Traffic to WAN</u>: -> Firewall -> Policy Route -> Load Balance -> Static Route -> IDP -> AV -> AS -> CF -> BMW -> NAT

(2) For a ZyWALL with **bridge** mode, the inspection flow is as following.

<u>Traffic will be handled</u>: -> Firewall-> IDP -> AV -> AS -> CF -> BWM

## A33. What is "UTM"?

UTM stands for Unified Threat Management and is a term describing a firewall appliance that integrates multiple security features, including Anti-Virus, IDP, Anti-Spam and VPN features, into a single box. Armed with the UTM appliance, the IT staff can manage the emerging threats from Internet, having lower TCO and reduced management overhead.

## A34. What are the differences between ZyWALL UTM models and previous ZyWALL

## ZyXEL

## models?

The major differences between ZyWALL UTM models (ZyWALL 5 UTM, ZyWALL 35 UTM and ZyWALL 70 UTM) and ZyWALL models (ZyWALL 5, ZyWALL 35 and ZyWALL 70) are:

- 1. Pre-loaded firmware version is ZyNOS v4.00
- 2. A ZyWALL Turbo Card is inside the package.
- 3. 3-month free trial of Anti-Virus, IDP and Anti-Spam security services.

## A35. What are the key new features of ZyWALL UTM?

Key features of ZyWALL UTM include:

1. World-First Anti-Virus & IDP High Performance with ZyWALL Turbo Card

Equipped with ZyWALL Turbo Card, ZyWALL is your worry-free choice to meet your both security and performance needs, and your best investment-protection choice to the coming 20M+ WAN/Internet era.

2. Integrated Gateway Anti-Virus feature

Integrated with top-rate detection and updates from Kaspersky Anti-Virus, ZyWALL can detect the latest threats to protect your network.

## 3. Most Complete 8-in-1 UTM

Based on the new ZyNOS v4.01, ZyWALL UTM is now your application layer firewall best choice to integrate full-featured Firewall, secure VPN connection, Bandwidth Management, Load Balance, Content Filtering, Anti-Virus, IDP (Intrusion Detection and Prevention) and Anti-Spam into a single box.

4. Non-stop Protection with Auto-Update

ZyWALL can automatically and constantly download the latest virus and attack signatures from ZyXEL Security Distribution Network to deliver the highest protection possible against an ever-changing threat landscape.

## B. Firmware Upgrade FAQ

## B01. Which ZyWALL models are eligible to be upgraded to run ZyNOS v4.01?

1. ZyWALL 5, ZyWALL 35 and ZyWALL 70 can be upgraded to run ZyNOS v4.01.

2. However, for ZyWALL 70, upgrade to v4.00 and above is conditional. Details are available in the next few questions.

3. Except ZyWALL 5/35/70, other ZyWALL models can not be upgraded to run ZyNOS v4.01.

## B02. Why it's conditional to upgrade to ZyNOS v4.01 for ZyWALL 70?

Because there are two versions of ZyWALL 70 in the field: the 32MB-RAM and the 64 MB-RAM versions. Only ZyWALL 70 equipped with 64MB RAM can be upgraded to run ZyNOS v4.00 and above. You can identify these two by checking the memory sizes. To check the memory of ZyWALL 70, issue the following command in CLI: "**sys atsh**"

As a result, for ZyWALL 70 with 64MB RAM, the upgrade path is supposed to be like this: ZyNOS v3.62/v3.63/v3.64  $\rightarrow$  ZyNOS v3.65  $\rightarrow$  ZyNOS v4.00 $\rightarrow$  ZyNOS v4.01. Please note, you can NOT upgrade to ZyNOS v4.00 directly. You must go through ZyNOS v3.65.

For ZyWALL 70 with 32MB RAM, the upgrade path is:

ZyNOS v3.62/v3.63/v3.64  $\rightarrow$  ZyNOS v3.65.

Please note, ZyWALL 70 with 32MB RAM can NOT be upgraded to run ZyNOS v4.00 and above.

To summarize, we have created the following table for your reference:

· · · · · · · · · · · · · · · · · · ·									
Firmware	ZW70 (32MB)	ZW70 (64MB)	ZW35	ZW5					
v3.62/3.63/3.64	Х	Х	Х	v3.62/3.64					
v3.65	Х	Х	N/A	N/A					
v4.00	N/A	Х	Х	Х					

Firmware-Model Mappings

## B03. What is ZyNOS v3.65 for ZyWALL 70?

ZyNOS v3.65 is designed solely for ZyWALL 70. It is a "gating" firmware version for upgrading ZyNOS to v4.00 and above.

Firmware v3.65 will verify ZW70's memory size to see if user can upgrade to 4.00 or not. If end user wanted to upgrade to v4.00, she/he needs to upgrade to v3.65 first and this is a MANDATORY process. The ZyNOS v3.65 does NOT support the following features: Anti-Virus + IDP security service and Anti-Spam security service.

ZyXEL will keep maintaining both ZyNOS v3.65, v4.00 and above for all ZyWALL 70 in the field.

## B04. What happens if I wrongfully upgrade firmware of a ZyWALL 70 with only 32MB of RAM to ZyNOS v4.01 directly?

Because of the built-in protection mechanism, the upgrade will fail and you will receive an error message saying the device is not supported.

## B05. What happened if I upgrade a ZyWALL 70 running ZyNOS v3.62/3.63/3.64 to v4.01 directly?

Because of the built-in protection mechanism, the upgrade will fail even the ZyWALL 70 equipped with 64MB RAM. Moreover, you will receive an error message saying the device is not supported.

## B06. I am a 32MB ZyWALL 70 owner, how can I upgrade to ZyNOS v4.01 having AV+IDP and AS features?

For those 32MB ZyWALL 70 owners who wanted to upgrade to ZyNOS v4.00 and above, we have a ZyWALL 70 (small memory) Trade-in Promotion program for you. In this program, ZyXEL offers a package at a very attractive price for those customers. The package includes: A ZyWALL 70 UTM and the 2-year AV+IDP Gold iCard

After joining this program, customers will have a ZyWALL 70 UTM (including a ZyWALL Turbo Card) running ZyNOS v4.01 and enjoy the AV+IDP feature for 30 months!

For detailed information, please contact your local reseller.

# B07. If I were a 32MB ZyWALL 70 owner and a Content Filtering service subscriber, will my current license status be retained after joining your ZyWALL 70 trade-in promotion?

Yes, the current license status will be retained and remain unchanged.

You can keep using the Content Filtering feature on your new ZyWALL 70 UTM until the end of your current CF license period.

## B08. What's the firmware upgrade path for my current ZyWALL 5 and ZyWALL 35?

For ZyWALL 5 running ZyNOS v3.62/v3.64 and ZyWALL 35 running ZyNOS v3.62/v3.63/v3.64, you can upgrade the firmware to ZyNOS v4.00 and above directly.

The system configurations will be automatically converted and reserved.

However, we strongly recommend you to backup your system configurations file (ROM file) prior to the upgrade taking place.

## B09. After a successful firmware upgrade to ZyNOS v4.01, what's the default setting of AV+IDP, AS and CF?

1. Default setting of AV+IDP feature

## ZyXEL

If the device is up and running with a ZyWALL Turbo Card inserted, the default setting is turned off. You can manually enable the AV+IDP feature if you want.

However, if the ZyWALL Turbo Card is not present on the device, the check box is grayed and you will not be able to enable the AV+IDP feature.

2. Default setting of Anti-Spam feature

The default setting of AS feature in ZyNOS v4.01 is disabled. You can manually enable the AS feature if you want.

3. Default setting of Content Filtering feature

The default setting of CF feature in ZyNOS v4.01 is disabled. You can manually enable the CF feature if you want.

## B10. What happens to my original system configurations after a successful firmware upgrade to ZyNOS v4.01?

The original system configurations, including systems settings, firewall policies and VPN rules, will be fully reserved after the upgrade. However, we strongly recommend you to backup your ROM file prior to upgrade.

## B11. What's the downgrade procedure of ZyWALL 70 running ZyNOS v4.01?

You can directly downgrade the firmware of ZyWALL 70 from v4.01 to any of the following versions: v4.00/v3.65/v3.64/v3.63/v3.62.

However, we don't guarantee all the system configurations can be fully converted and reserved after a downgrade because some feature settings may not be available on older firmware versions. Always backup your current ROM file prior to any firmware operation.

## B12. Can I downgrade a ZyWALL 5 or ZyWALL 35 running ZyNOS v4.01 back to ZyNOS v3.64 (or below)?

Yes, downgrade is supported.

However, we don't guarantee all the system configurations can be fully converted and reserved since some feature settings may not be available on older firmware versions.

## C. Turbo Card FAQ

## C01. Can I insert the ZyWALL Turbo Card & wireless card simultaneously into ZyWALL 5,

## ZyWALL 35 or ZyWALL 70?

No, you can NOT insert both ZyWALL Turbo Card and wireless card into ZyWALL device since there is only one expansion slot available on the ZyWALL 5, ZyWALL 35 or ZyWALL 70.

## C02. Except ZyWALL Turbo Card is a must when use AV+IDP service, what exactly I can get benefit from it?

With ZyWALL Turbo Card inserted, customers can enjoy ZyXEL's unique SecuASIC technology which boosts up the performance of AV+IDP inspection while maintaining unmatched protection against network security threats.

## C03. Do I must have a ZyWALL Turbo Card inserted if I upgraded to ZyNOS v4.01? If not, when must I insert a ZyWALL Turbo Card into my ZyWALL device?

No, the ZyWALL Turbo Card is not a must after you upgrade your ZyWALL to run ZyNOS v4.00 and above.

A ZyWALL Turbo Card is required ONLY when you want to activate the AV+IDP security service in ZyNOS v4.00 and above.

For the other two subscription services, which are the Anti-Spam and Content Filtering service, it's NOT required to have a ZyWALL Turbo Card inserted.

## C04. Can I insert the ZyWALL Turbo Card & 3G wireless card simultaneously into ZyWALL 5, ZyWALL 35 or ZyWALL 70?

For ZyWALL 35 and ZyWALL 70, they don't support 3G wireless card feature. Only ZyWALL 5 supports this feature.

However, you can NOT insert both ZyWALL Turbo Card and 3G wireless card into ZyWALL device since there is only one expansion slot available on the ZyWALL 5.

## D. Firewall FAQ

## D01. What is a network firewall?

A firewall is a system or group of systems that enforces an access-control policy between two networks. It may also be defined as a mechanism used to protect a trusted network from an un-trusted network. The firewall can be thought of two mechanisms. One to block the traffic, and the other to permit traffic.

## D02. What makes ZyWALL secure?

The ZyWALL is pre-configured to automatically detect and thwart Denial of Service (DoS) attacks such as Ping of Death, SYN Flood, LAND attack, IP Spoofing, etc. It also uses stateful packet inspection to determine if an inbound connection is allowed through the firewall to the private LAN. The ZyWALL supports Network Address Translation (NAT), which translates the private local addresses to one or multiple public addresses. This adds a level of security since the clients on the private LAN are invisible to the Internet.

## D03. What are the basic types of firewalls?

Conceptually, there are three types of firewalls:

- 1. Packet Filtering Firewall
- 2. Application-level Firewall
- 3. Stateful Inspection Firewall

Packet Filtering Firewalls generally make their decisions based on the header information in individual packets. This header information includes the source, destination addresses and ports of the packets.

Application-level Firewalls generally are hosts running proxy servers, which permit no traffic directly between networks, and which perform logging and auditing of traffic passing through them. A proxy server is an application gateway or circuit-level gateway that runs on top of general operating system such as UNIX or Windows NT. It hides valuable data by requiring users to communicate with secure systems by mean of a proxy. A key drawback of this device is performance.

Stateful Inspection Firewalls restrict access by screening data packets against defined access rules. They make access control decisions based on IP address and protocol. They also 'inspect' the session data to assure the integrity of the connection and to adapt to dynamic protocols. The flexible nature of Stateful Inspection firewalls generally provides the best speed and transparency, however, they may lack the granular application level access control or caching that some proxies support.

## D04. What kind of firewall is the ZyWALL?

- 1. The ZyWALL's firewall inspects packets contents and IP headers. It is applicable to all protocols, that understands data in the packet is intended for other layers, from network layer up to the application layer.
- 2. The ZyWALL's firewall performs stateful inspection. It takes into account the state of connections it handles so that, for example, a legitimate incoming packet can be matched with the outbound request for that packet and allowed in. Conversely, an incoming packet masquerading as a response to a nonexistent outbound request can be blocked.
- 3. The ZyWALL's firewall uses session filtering, i.e., smart rules, that enhance the filtering process and control the network session rather than control individual packets in a session.
- 4. The ZyWALL's firewall is fast. It uses a hashing function to search the matched session cache instead of going through every individual rule for a packet.
- 5. The ZyWALL's firewall provides email service to notify you for routine reports and when alerts occur.

## D05. Why do you need a firewall when your router has packet filtering and NAT built-in?

With the spectacular growth of the Internet and online access, companies that do business on the Internet face greater security threats. Although packet filter and NAT restrict access to particular computers and networks, however, for the other companies this security may be insufficient, because packets filters typically cannot maintain session state. Thus, for greater security, a firewall is considered.

## D06. What is Denials of Service (DoS)attack?

Denial of Service (DoS) attacks are aimed at devices and networks with a connection to the Internet. Their goal is not to steal information, but to disable a device or network so users no longer have access to network resources.

There are four types of DoS attacks:

- 1. Those that exploits bugs in a TCP/IP implementation such as Ping of Death and Teardrop.
- 2. Those that exploits weaknesses in the TCP/IP specification such as SYN Flood and LAND Attacks.
- 3. Brute-force attacks that flood a network with useless data such as Smurf attack.
- 4. IP Spoofing

## D07. What is Ping of Death attack?

Ping of Death uses a 'PING' utility to create an IP packet that exceeds the maximum 65535 bytes of data allowed by the IP specification. The oversize packet is then sent to an unsuspecting system. Systems may crash, hang, or reboot.

## D08. What is Teardrop attack?

Teardrop attack exploits weakness in the reassemble of the IP packet fragments. As data is transmitted through a network, IP packets are often broken up into smaller chunks. Each fragment looks like the original packet except that it contains an offset field. The Teardrop program creates a series of IP fragments with overlapping offset fields. When these fragments are reassembled at the destination, some systems will crash, hang, or reboot.

## D09. What is SYN Flood attack?

SYN attack floods a targeted system with a series of SYN packets. Each packet causes the targeted system to issue a SYN-ACK response, while the targeted system waits for the ACK that follows the SYN-ACK; it queues up all outstanding SYN-ACK responses on what is known as a backlog queue. SYN-ACKs are moved off the queue only when an ACK comes back or when an internal timer (which is set a relatively long intervals) terminates the TCP three-way handshake. Once the queue is full , the system will ignore all incoming SYN requests, making the system unavailable for legitimate users.

## D10. What is LAND attack?

In a LAN attack, hackers flood SYN packets to the network with a spoofed source IP address of the targeted system. This makes it appear as if the host computer sent the packets to itself, making the system unavailable while the target system tries to respond to itself.

## D11. What is Brute-force attack?

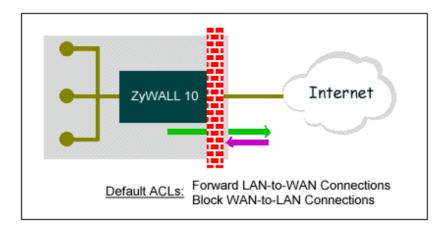
A Brute-force attack, such as 'Smurf' attack, targets a feature in the IP specification known as directed or subnet broadcasting, to quickly flood the target network with useless data. A Smurf hacker flood a destination IP address of each packet is the broadcast address of the network; the router will broadcast the ICMP echo request packet to all hosts on the network. If there are numerous hosts, this will create a large amount of ICMP echo request packet, the resulting ICMP traffic will not only clog up the 'intermediary' network, but will also congest the network of the spoofed source IP address, known as the 'victim' network. This flood of broadcast traffic consumes all available bandwidth, making communications impossible.

## D12. What is IP Spoofing attack?

Many DoS attacks also use IP Spoofing as part of their attack. IP Spoofing may be used to break into systems, to hide the hacker's identity, or to magnify the effect of the DoS attack. IP Spoofing is a technique used to gain unauthorized access to computers by tricking a router or firewall into thinking that the communications are coming from within the trusted network. To engage in IP Spoofing, a hacker must modify the packet headers so that it appears that the packets originate from a trusted host and should be allowed through the router or firewall.

## D13. What are the default ACL firewall rules in ZyWALL?

There are two default ACLs pre-configured in the ZyWALL, one allows all connections from LAN to WAN and the other blocks all connections from WAN to LAN except of the DHCP packets.



## D14. In ZyWALL, is DMZ behind NAT or not?

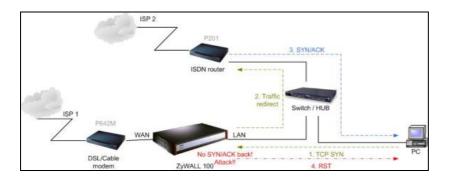
Basically DMZ is behind NAT. But there is one exception. If you use Full Feature as NAT type, and there is no NAT mapping for systems on DMZ. Then NAT will not take effect in this case.

## D15. Can I use both public and private IP addresses on DMZ?

- Yes, you can. To achieve this, you have to use IP alias to separate the DMZ interface into 2 logical segments, one for private IP, and the other for public IP.
- Then you have to use Full Feature as NAT type in Menu 4.
- Set NAT mapping for private IP addresses in Menu 15.1.
- Note that in this case, NAT will not take care of IP addresses without NAT mapping. So private IP address could be sent out by ZyWALL due to users' incaution.

#### D16. Why does traffic redirect/static/policy route be blocked by ZyWALL?

ZyWALL is an ideal secure gateway for all data passing between the Internet and the LAN/DMZ. For some reasons (load balance or backup line), users may want traffic to be re-routed to another Internet access devices while still be protected by ZyWALL. In such case, the network topology is the most important issue. Here is a common example that people mis-deploy the LAN traffic redirect and static route.



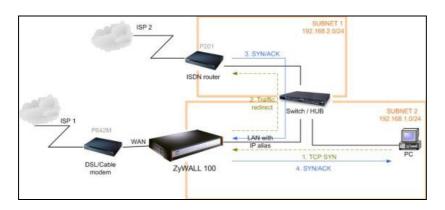
The above figure indicates the "**triangle route**" topology. It works fine if you turn off firewall function on ZyWALL box. However, if you turn on firewall, your connection will be blocked by firewall because of the following reason.

- Step 1. Being the default gateway of PC, ZyWALL will receive all "outgoing" traffic from PC.
- Step 2. And because of **Static route/Traffic Redirect/Policy Routing**, ZyWALL forwards the traffic to another gateway (ISDN/Router) which is in **the same segment** as ZyWALL's LAN.
- Step 3. However the return traffic won't go back to ZyWALL, in stead, the "another gateway (ISDN/Router)" will send back the traffic to PC directly. Because the gateway (say, P201) and the PC are in the same segment.

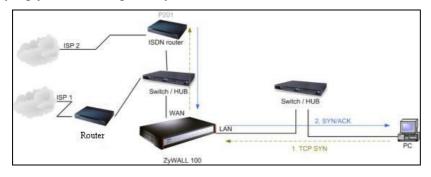
When firewall is turned on, ZyWALL will check the outgoing traffic by ACL and create dynamic sessions to allow return traffic to go back. To achieve Anti-DoS, ZyWALL will send RST packets to the PC and the peer since it never receives the TCP SYN/ACK packet. Thus the connection will always be reset by ZyWALL.

#### [Solutions]

(A) Deploying your second gateway in IP alias segment is a better solution. In this way, your connection can be always under control of firewall. And thus there won't be Triangle Route problem.



(B) Deploying your second gateway on WAN side.



(C) To resolve this conflict, we add an option for users to allow/disallow such **Triangle Route** topology in both CI command and Web configurator. You can issue this command, "**sys firewall ignore triangle all on**", to allow firewall bypass triangle route checking. In Web GUI, you can find this option in firewall setup page.

But we would like to notify that if you allow Triangle Route, any traffic will be easily injected into the protected network through the unprotected gateway. In fact, it's a security hole in your protected network.

#### D17. How can I protect against IP spoofing attacks?

The ZyWALL's firewall will automatically detect the IP spoofing and drop it if the firewall is turned on. If the firewall is not turned on we can configure a filter set to block the IP spoofing attacks. The basic scheme is as follows:

For the input data filter:

- Deny packets from the outside that claim to be from the inside
- Allow everything that is not spoofing us

Filter rule setup:

### ZyXEL

- Filter type =TCP/IP Filter Rule
- Active =Yes
- Source IP Addr =a.b.c.d
- Source IP Mask =w.x.y.z
- Action Matched =Drop
- Action Not Matched =Forward

Where a.b.c.d is an IP address on your local network and w.x.y.z is your netmask:

For the output data filters:

- Deny bounce back packet
- Allow packets that originate from us

Filter rule setup:

- Filter Type =TCP/IP Filter Rule
- Active =Yes
- Destination IP Addr =a.b.c.d
- Destination IP Mask =w.x.y.z
- Action Matched =Drop
- Action No Matched =Forward

Where a.b.c.d is an IP address on your local network and w.x.y.z is your net mask.

### E. Security Service licenses FAQ

#### E01. What is iCard?

iCard is used for delivering security service license of ZyXEL products, including ZyWALL product family. ZyWALL security service is enabled by purchasing an iCard to obtain a user license.

#### E02. Where can I buy the iCard and how much does it cost?

You can buy the iCard from the local dealer or distributor, please contact them for the price. Please check <u>http://www.zyxel.com</u> for ZyXEL global contact information.

#### E03. How many kinds of iCard does ZyXEL provide?

Choices are ranging from **Platinum**, **Silver** and **Gold**, depending on the model of the device. For the models supported by each type, please check the print on the cards.

#### E04. Is each type of iCard device specific?

Yes. Different model of ZyXEL product may uses different type of iCard for registration. Users need to check the supported model names before purchasing.

### E05. What are the available security service licenses which require additional purchase and license activation in ZyNOS v4.01?

V4.01 is a major new release of ZyNOS and it includes the following security services which require license purchase and activation:

- 1. Anti-Virus + IDP security service
- 2. Anti-Spam security service
- 3. Content Filtering security service

#### E06. What kind of iCard should I buy?

It depends on the ZyWALL model you have, the security service you desire and the license period you need. See the following table for those mappings. (Here we highlight ZyWALL 5/35/70 since they especially provide AV+IDP, AS features.

	AV+IDP		A	S	CF	
	1 Year	2 Year	1 Year	2 Year	1 Year	2 Year
ZyWALL 2	N/A	N/A	N/A	N/A	1-year, Silver	N/A
ZyWALL 2WE	N/A	N/A	N/A	N/A	1-year, Silver	N/A
ZyWALL 5	1-year, Silver	2-year, Silver	1-year, Silver	2-year, Silver	1-year, Silver	N/A
ZyWALL 10W	N/A	N/A	N/A	N/A	1-year, Silver	N/A
ZyWALL 35	1-year, Gold	2-year, Gold	1-year, Gold	2-year, Gold	1-year, Gold	N/A
ZyWALL 50	N/A	N/A	N/A	N/A	1-year, Gold	N/A
ZyWALL 70	1-year, Gold	2-year, Gold	1-year, Gold	2-year, Gold	1-year, Gold	N/A
ZyWALL 100	N/A	N/A	N/A	N/A	1-year, Platinum	N/A

# E07. If I violate the mappings described above, for example, using a silver iCard for ZyWALL 35 or ZyWALL 70, what will happen?

The activation will fail.

# E08. Can I try the Content Filtering service for free? How long is the free trial period of Content Filtering service?

Yes, you can try the Content Filtering service for free.

The free trial period is 30 days and is available to ZyWALL 2, ZyWALL 5, ZyWALL 35, ZyWALL 70, ZyWALL 5 UTM, ZyWALL 35 UTM and ZyWALL 70 UTM owners.

**E09.** Does ZyXEL provide customers free trial for AV+IDP service? How long is it? Yes, the free trial period of the AV + IDP security service is 3 months.

Always remember the 2 prerequisites to activate the AV+IDP service: <u>device must be running ZyNOS</u> v4.00 and above with a ZyWALL Turbo Card inserted.

Moreover, if you make the purchase of 1-year (or 2-year) AV+IDP security service within the free trail period (counting form the date of activation of the free trial), you are entitled to get an additional 3-month extension of the AV+IDP security service.

#### E10. Does ZyXEL provide customers free trial for Anti-Spam service? How long is it?

Yes. The free trial period of AS security service is 3 months. Any ZyWALL device with ZyNOS v4.00 and above could activate the AS service and a ZyWALL Turbo Card is NOT required for the activation of AS security service.

Moreover, if you make the purchase of 1-year (or 2-year) Anti-Spam security service within the free trail period (counting form the date of activation of the free trial), you are entitled to get an additional 3-month extension of the Anti-Spam security service.

### F. Security Service Activation and UpdateFAQ

#### F01. Why do I have to register?

1. If you wanted to use the free trial service of ZyWALL, your have to activate it from within myZyXEL.com.

2. If you purchased iCard for a security service, you must activate the security service from within myZyXEL.com. The security services in ZyNOS v4.01 includes: AV+IDP, Anti-Spam and Content Filtering service.

#### F02. In addition to registration, what can I do with myZyXEL.com?

- 1. Access firmware and security service updates.
- 2. Get ZyWALL alerts on services, firmware, and products.
- 3. Manage (activate, change or delete) your ZyWALL security services online.

In summary, myZyXEL.com delivers a convenient, centralized way to register all your ZyWALL security appliances and security services. It eliminates the hassle of registering individual ZyWALL appliances and upgrades to streamline the management of all your ZyWALL security services. Instead of registering each ZyWALL product individually, using myZyXEL.com you have a single user profile where you can manage all your product registration and service activation.

# F03. Is there anything changed on myZyXEL.com because of the launch of ZyNOS v4.00? Which ZyWALL models can be registered via myZyXEL.com?

Yes. Because the launch of ZyNOS v4.00, we are proudly to introduce the new registration flow on myZyXEL.com. However, you can still register devices running older firmware. Please refer to the following table for model mappings.

	Dovice Degistration	AV+IDP Service	Anti-Spam Service	Content Filtering		
	Device Registration	Activation	Activation	Service Activation		
New Degistration	ZW5 (v4.00)	ZW5 (v4.00)	ZW5 (v4.00)	ZW5 (v4.00)		
New Registration Flow	ZW35 (v4.00)	ZW35 (v4.00)	ZW35 (v4.00)	ZW35 (v4.00)		
FIUW	ZW70 (v4.00)	ZW70 (v4.00)	ZW70 (v4.00)	ZW70 (v4.00)		
	ZW2 (v3.62)			ZW2 (v3.62)		
Previous	ZW5 (v3.64/v3.62)	N/A	N/A	ZW5 (v3.64/v3.62)		
<b>Registration Flow</b>	ZW35 (v3.64 or below)	N/A	IN/A	ZW35 (v3.64 or below)		
	ZW70 (v3.65 or below)			ZW70 (v3.65 or below)		

#### Model Mappings for Registration on myZyXEL.com

Note Devices running ZyNOS v4.00 and above dose NOT support the Previous Registration Flow.

## F04. What's the difference between new registration flow and previous registration? What's the advantage of new registration flow over the previous registration flow?

1. In new registration flow, the registration is processed within device's WebGUI. In previous registration flow, the registration is processed through hyperlink to myZyXEL.com in a separate browser window.

2. The new registration flow is easier to use for both experienced customers and new customers. In the new registration flow, it's no longer necessary to open another web browser window to register your device. Instead, the registration flow is embedded in device's WebGUI. Furthermore, customer is no longer required to manually input the MAC of the device because the MAC will be automatically sent to myZyXEL.com during the registration flow.

# F05. If I were new to myZyXEL.com, what are the required fields when I register my ZyWALL device on myZyXEL.com?

The required fields include: user name, password, valid email address and country.

F06. When using the new registration flow of myZyXEL.com for ZyNOS v4.0, do I have to create a new account if I were already a registered user on myZyXEL.com?

No, you don't have to re-create a user account on myZyXEL.com if you were a registered user. Your user profile is already stored on myZyXEL.com.

#### F07. What is mySecurityZone?

- 1. mySecurityZone is a free service portal. It's open to the public.
- 2. For public users, you can browse the latest security news and updates from ZSRT, access free resources and subscribe to our free newsletter.
- 3. For those ZyWALL product owners who have already registered on myZyXEL.com, you can additionally use the same username/password to login to mySecurityZone to view detail description for all policies of AV+IDP service and make queries. Furthermore, you automatically receive our advisories carrying latest security updates and valuable information.

#### Summary

In mySecurityZone you can:

- 1. Display, share ZyWALL security information, including AV/IDP policy, advisory, and resource
- 2. Search ZyWALL detailed product information, including AV/IDP policy, advisory, and resource
- 3. Receive ZyWALL advisory news by email

#### F08. What is Update Server?

Update Server is designed to serve the AV+IDP security service subscribers to assure their device is update so that is capable to handle latest threats from Internet.

When a ZyWALL device is scheduled to download the AV+IDP signature pack, the download request is pointed to the Update Server.

Update Server is hosted by ZyXEL and the capacity of Update Server is precisely calculated. After taking the following factors into consideration: bandwidth consumption, availability, geographically distribution of subscribers, we have decided to build the Update Server in IDCs in a globally distributed architecture plus 24x7 monitoring mechanism. This will fully assure the maximum quality of service for all security service subscribers.

#### F09. Who maintains mySecurityZone & Update Server?

It's maintained by ZyXEL Security Response Team (ZSRT) who manages backend support from the beginning of outbreak happen to attack sample collection, analyze it and output it as policy, and finally

make solution of advisory. ZSRT is formed as a group of security experts.

#### F10. What's the URL for these service portals?

myZyXEL.com http://www.myzyxel.com/myzyxel/

mySecurityZone https://mysecurity.zyxel.com/mysecurity/

For Update Server, there is no interactive login screen available since it communicates with ZyWALL devices only.

### G. Anti-Virus FAQ

### G01. Why should I need a gateway Anti-Virus solution while I already deployed the Anti-Virus software on each desktop/laptop?

Gateway Anti-Virus feature is typically deployed on the central gateway in a corporate network. Therefore, it's highly manageable and IT staff can enforce corporate content security policy against commonly used protocols including SMTP, pop3, http and ftp.

On the other hand, client-based AV solution is designed to protect the endpoint inside corporate network. It requires software installation on each client and higher managerial overhead because of its nature. For best protection, modern security-aware companies tend to deploy both solutions because these two solutions are pretty much complementary in nature.

#### G02. Why does ZyWALL bundle Anti-Virus and IDP feature together?

The IDP feature can stop live network attacks while the AV feature will scan, detect and destroy files that are infected with virus/worms. Armed with BOTH features, you are guaranteed to have the ultimate tool to guard your network from most types of attacks coming from any networks.

#### G03. Can I subscribe to the Anti-Virus service alone or IDP service alone?

No. Because the Anti-Virus and IDP services are bundled together, you can not subscribe to any one of them alone.

#### G04. What are the hardware requirements to run AV+IDP security service?

1. For ZyWALL 5 UTM, ZyWALL 35 UTM or ZyWALL 70 UTM owners, you don't have to acquire additional hardware accessories to activate the AV+IDP security service because the ZyWALL Turbo Card is already inside the package.

2. For existing ZyWALL 5, ZyWALL 35 or ZyWALL 70 owners, you are required to upgrade the firmware to ZyNOS v4.00 or above f/w and get a ZyWALL Turbo Card and insert it into your own device. You can not activate the AV+IDP security service when the ZyWALL Turbo Card is not present on the device.

For detailed information on how to acquire a trial ZyWALL Turbo Card, please contact your local reseller.

# G05. Now I know that the ZyWALL Turbo Card is a must when use AV+IDP service; but what exactly I can benefit from the ZyWALL Turbo Card?

With ZyWALL Turbo Card inserted, customers can enjoy ZyXEL's unique SecuASIC technology which boosts up the performance of AV+IDP inspection while maintaining unmatched protection against network security threats.

#### G06. How do I keep signatures of AV+IDP service updated?

We recommend you configuring your device to automatically update the signature on an hourly basis so that the device will check with our Update Server to see if there is new signature available. However, you could still change the update interval as you wish and could force manual update at any given time.

#### G07. How often does ZyXEL release signatures of AV+IDP security service?

ZyXEL is managing to release the AV+IDP signature packs at least 5 times a week on a regular basis. Those signatures are fully tested and the quality is assured.

Once new virus is spreading, ZyXEL will release the virus signature as fast as it can. Minimizing the impact of new virus is always the first priority for our AV+IDP service subscribers.

# G08. Will the traffic coming in through the VPN tunnel also be scanned by Anti-Virus, IDP and Anti-Spam feature in ZyWALL ZyNOS v4.0?

No, VPN traffic will not be inspected by be scanned by Anti-Virus, IDP and Anti-Spam module. However, we manage to support this feature in the forthcoming ZyNOS firmware.

### H. IDP FAQ

#### H01. Why does ZyWALL bundle Anti-Virus and IDP feature together?

The IDP feature can stop live network attacks while the AV feature will scan, detect and destroy files that are infected with virus/worms. Armed with BOTH features, you are guaranteed to have the ultimate tool to guard your network from most types of attacks coming from any networks.

#### H02. Can I subscribe to the Anti-Virus service alone or IDP service alone?

No. Because the Anti-Virus and IDP services are bundled together, you can not subscribe to any one of them alone.

#### H03. What are the hardware requirements to run AV+IDP security service?

1. For ZyWALL 5 UTM, ZyWALL 35 UTM or ZyWALL 70 UTM owners, you don't have to acquire additional hardware accessories to activate the AV+IDP security service because the ZyWALL Turbo Card is already inside the package.

2. For existing ZyWALL 5, ZyWALL 35 or ZyWALL 70 owners, you are required to upgrade the firmware to ZyNOS v4.01 and get a ZyWALL Turbo Card and insert it into your own device. You can not activate the AV+IDP security service when the ZyWALL Turbo Card is not present on the device.

For detailed information on how to acquire a trial ZyWALL Turbo Card, please contact your local reseller.

# H04. Now I know that the ZyWALL Turbo Card is a must when use AV+IDP service; but what exactly I can benefit from the ZyWALL Turbo Card?

With ZyWALL Turbo Card inserted, customers can enjoy ZyXEL's unique SecuASIC technology which boosts up the performance of AV+IDP inspection while maintaining unmatched protection against network security threats.

# H05. Could I duplicate the IDP feature's policy settings from one ZyWALL device to another?

Yes. In ZyNOS v4.01, you can always backup the IDP feature's policy settings to your desktop PC. Afterwards, from within WebGUI of another device, you can restore the backup file so that the IDP

feature's policy settings are duplicated and you will have same IDP policy settings on both ZyWALL devices.

#### H06. How do I keep signatures of AV+IDP service updated?

We recommend you configuring your device to automatically update the signature on an hourly basis so that the device will check with our Update Server to see if there is new signature available. However, you could still change the update interval as you wish and could force manual update at any given time.

#### H07. How often does ZyXEL release signatures of AV+IDP security service?

ZyXEL is managing to release the AV+IDP signature packs at least 5 times a week on a regular basis. Those signatures are fully tested and the quality is assured.

Once new virus is spreading, ZyXEL will release the virus signature as fast as it can. Minimizing the impact of new virus is always the first priority for our AV+IDP service subscribers.

# H08. Will the traffic coming in through the VPN tunnel also be scanned by Anti-Virus, IDP and Anti-Spam feature in ZyWALL ZyNOS v4.0?

No, VPN traffic will not be inspected by be scanned by Anti-Virus, IDP and Anti-Spam module. However, we manage to support this feature in the forthcoming ZyNOS firmware.

### I. Anti-Spam FAQ

# I01. What's the difference between gateway Anti-Spam and client-based Anti-Spam filter such as Microsoft Outlook's?

The major differences between the two are:

1. Sensitivity: ZyWALL's AS can adjust threshold while you can not adjust AS threshold in Outlook.

2. Phishing: ZyWALL's AS can detect phishing emails but Outlook's AS cannot detect phishing emails.

3. Outlook's AS filter is updated monthly with Windows Update, while ZyWALL's AS is updated in real-time.

Furthermore, ZyWALL's Anti-Spam feature is complementary with client-based Anti-Spam filter.

#### 102. A customer already has her/his own exchange server including the Anti-Spam

# software from other vendors; is there any good reason for her/him to use ZyXEL's Anti-Spam service in addition to the current solution?

Yes, the reasons are:

1. Complementary filtering

The tagged-spam filtered by spam software will be tagged again by ZyWALL's Anti-Spam. But those undetected spam emails can be detected by ZyWALL's Anti-Spam feature.

2. Phishing

Not every spam software can detect phishing emails. The Anti-Spam service of ZyWALL can detect phishing emails.

### I03. What happens when an email with large attachment in size, e.g. 5MB, is downloaded which has virus in it?

ZyWALL's Anti-Virus feature doesn't care the file size. We have implemented a special algorithm to handle this condition – file with attachment of any size can be scanned by Anti-Virus feature of ZyWALL UTM.

# 104. What happens if the virus is in the last part of the email message and the email receiver already got a part of the contaminated file in her/his laptop or desktop?

Even the virus hidden in the last part of a specific file, we still can detect and then destroy this part. As a result, the user will get a file but it can't be accessed (read, write or execute). Thus, the laptop/desktop won't be infected by this virus.

# I05. Will the traffic coming in through the VPN tunnel also be scanned by Anti-Virus, IDP and Anti-Spam feature in ZyWALL ZyNOS v4.0?

No, VPN traffic will not be inspected by be scanned by Anti-Virus, IDP and Anti-Spam module. However, we manage to support this feature in the forthcoming ZyNOS firmware.

# **I06.** In ZyWALL's Anti-Spam feature, what's your recommendation to handle identified spam emails?

1. There two actions ZyWALL can take against identified spam emails: to block or to tag.

2. Pros and Cons

If you choose to block them, then you have no control over false-positives.

If you choose to tag them, then you still have the spam email traffic on your mail server and everybody has to set a rule in outlook to filter the spam emails into a dedicated folder.

3. Recommendation

Most IT managers choose "tag" spam emails, which is also our recommendation although ZyWALL/Mailshell Anti-Spam technology performs very low false-positive.

#### **107.** What's the specification of Anti-Spam feature in ZyNOS v4.01? Specifications of Anti-Spam feature

Supported protocols	POP3 and SMTP protocol		
Action on spam emails	For Pop3, it can "tag" the spam email;		
	For SMTP, it can do "tag" and "block".		
Default Setting	Enable Tag with [SPAM]/[PHISHING] subject		
Maximum concurrent sessions	ZyWALL 5: 5		
	ZyWALL 35: 15		
	ZyWALL 70: 30		

#### 108. How do I keep signatures of Anti-Spam service update?

From the current design, there is no local spam signature database maintained on the ZyWALL UTM devices. As a result, you don't have to update the AS signature for the device. The transactions and queries between AS-enabled ZyWALL devices and our rating server are taking place dynamically and automatically in the background.

However, you may want to maintain your own black list/white list on device to maximize the effectiveness of the Anti-Spam security service.

### J. Content Filter FAQ

#### J01. What's the operation between ZyXEL appliance and BlueCoat data center?

Whenever a PC behind ZyXEL appliance issues HTTP requests to some public WEB server. ZyXEL appliance will forward the request to the targeted WEB server, but also issue an categorization query to BlueCoat data center. When the HTTP response is back to ZyXEL appliance, the appliance will hold the response for a while, and wait for the query result from the BlueCoat data center. If the query is not back within 10 seconds (by default setting), ZyXEL appliance will block (by default setting) the HTTP response to the PC. If the query is back, ZyXEL appliance will drop or forward the request according to

the Content Filtering policy set in the appliance. The result of categorization query will be cached in ZyXEL appliance. Later on, HTTP requests to the same WEB server will be inspected by local cache.

#### J02. How many entries can the cache of Web Site Auto Categorization keep at most?

ZyXEL appliance can keep 1024 entries in the cache at most. Entries that are used less frequently will be overwritten first when the cache is full. Contents inside the cache will be cleared out after rebooting.

#### J03. Can I specify the time out value of the query response from BlueCoat data center?

Yes, you can change it on ZyXEL appliance. The default value of the time out is 10 seconds.

### J04. Can I decide whether to forward or drop the HTTP response if the query to BlueCoat data center is timed out?

Yes, you can set the policy, drop or forward, when query is timed out. The default policy is block.

#### J05. How to register for BlueCoat service?

Either for free trial purpose or if you get PIN code by purchasing iCard, you need to initiate registration process from ZyXEL appliance by clicking **Registration and Reports** button from content Filter-> Categories page.

#### J06. Why can't I make registration successfully?

Since the Registration job is between ZyXEL appliance and Http://myZyXEL.com server. Please make sure your Internet connection from ZyXEL appliance is ok first, and keep the connection between them online during the registration process. Since once the registration is granted on the\_Http://myZyXEL.com server, Http://myZyXEL.com needs to feedback the result (either Successful or Fail) to ZyXEL appliance.

#### J07. What services can I get with Trial Registration?

With Trial Registration, you can get Web Site Auto Categorization, and Content Filtering Report services.

#### J08. What types of content filter does ZyWALL provide?

ZyWALL supports three types of content filtering.

- Restrict Web Data including ActiveX, Java Applet, Cookie, Web proxy
- URL keywords blocking
- BlueCoat filter list

#### J09. What are the primary features of ZyXEL Content Filtering?

- Blocking or Forwarding Policy Management (ZyXEL appliance)
- Monitoring (BlueCoat)
- Real-time URL Rating (BlueCoat)
- Real-Time Reporting (BlueCoat)

# J10. Who needs ZyXEL Content Filtering? Is ZyXEL Content Filtering for small companies or for large corporations?

All businesses can benefit from using the ZyXEL Content Filtering solution

ZyXEL Content Filtering helps organizations manage, monitor, and report on users' Internet activity regardless of their location within the organization. Almost any organization — business, government, or school — can benefit from BlueCoat's centrally managed, web-based filtering service. Consider the following:

- 30 to 40% of Internet surfing during work hours is not business related.

- In some companies as much as 70% of bandwidth is consumed by non-productive pursuits.

- 68% of all Internet porn traffic occurs during the 9 to 5 workday.

- 53% of teens have encountered offensive Web sites that include pornography, hate, or violence. Of these, 91% unintentionally found the offensive sites while searching the Web.

ZyXEL Content Filtering is helpful to improve productivity, minimize legal liability, and conserve costly Internet bandwidth within the organization. BlueCoat provides the most complete and accurate Internet filtering solution of any Internet management provider and enables companies to better manage, secure and protect their Internet investment.

#### J11. Can I have different policies in effect for different times of the day or week?

Yes, but only one blocking period of time is supported currently on ZyXEL appliance.

#### J12. How many policies can I create?

Two. One is for all users, the other is exempting zone. With exempting zone, you can define a specific range of IP exempting from the policy for all users.

#### J13. Can I create my own categories?

No, you can't create your own policies other than the 52 categories BlueCoat provides.

#### J14. Can I override (block or allow) certain URLs regardless of the rating?

Yes, you can use key word blocking to override ratings in the BlueCoat database.

#### J15. How many URL keywords does ZyWALL support?

64 keywords are supported.

#### J16. How do I keep database of Content Filtering service updated?

From the current design, there is no local Content Filtering signature database stored on the ZyWALL devices.

As a result, you don't have to worry about the signature update of ZyWALL devices since it's not required. The transactions and queries between CF-enabled ZyWALL devices and our dynamic database server are taking place dynamically and automatically in the background.

However, you may want to maintain your own URL/keyword list on device to maximize the effectiveness of the Content Filtering service.

#### J17. What is BlueCoat Filter list?

BlueCoat (http://www.cerberian.com) provides Internet content filtering service through an outsourced model to original equipment manufacturers (OEMs) and service providers. With the BlueCoat Integration Kit, ZyXEL integrates the BlueCoat content filtering service into ZyXEL appliances, such as ZyWALL, Prestige, ZyAir series.

#### J18. How many ratings does the BlueCoat database contain?

BlueCoat database contains 4.3 million ratings. The BlueCoat database contains about 4.3 million ratings. Because BlueCoat rates sites at the domain or directory level, the database actually covers hundreds of millions of unique web pages.

#### J19. How often does BlueCoat update the database?

BlueCoat continuously updates the ratings database, but BlueCoat's outsourced model does not require customers to update a local database.

Unlike other Internet content filtering solutions, BlueCoat's outsourced solution does not require clients to

receive large database updates daily or weekly. Instead, BlueCoat customers all access the same ratings database. When a user requests a URL not contained in the database, the BlueCoat solution uses Dynamic Real-time Rating to assign a rating to that page. All unrated URLs are further analyzed by background technologies and human raters.

#### J20. How do I locate sites to block?

BlueCoat provides category ratings for Web sites. Based on the category rating from BlueCoat, users of ZyXEL appliances then define blocking/forwarding policy in WEB GUI. Do humans review the web sites?

BlueCoat uses expert Web content raters to train the ratings technology.

Initially, category experts create a list of URLs that represent good content for each category. The ratings technology then uses this initial set of pages to recognize content similar to those initial pages. Through BlueCoat's internal processes, the ratings technology learns to better categorize pages as it rates more and more user requests. The BlueCoat staff also continually adds new pages to all categories and evaluates any pages that the rating process could not recognize. Users can request BlueCoat staff to rate specific new pages or review automatic ratings assigned by the technology. Through this process, the ratings technology becomes more accurate at categorizing future user requests.

#### J21. Do humans review the ratings?

BlueCoat's Web content raters periodically review each content area. They also examine pages based on categorization requests from end-users.

BlueCoat periodically reviews certain content areas to fine tune the ability of the ratings technology to recognize specific types of content. Also, when users believe a page has received an incorrect rating, BlueCoat rating experts will review the categories assigned and make changes as necessary. BlueCoat also uses the human-rated sites to further train and improve the content analysis system.

#### J22. How can I do if I find a WEB site is mis-categorized?

When you find a web site is not categorized as you expect, you can report to either <a href="mailto:support@zyxel.com.tw">support@zyxel.com.tw</a> or BlueCoat <a href="mailto:Site Submissions">Site Submissions</a>.

#### J23. How many and what categories do you provide?

ZyXEL Content Filtering provides 52 categories.

### ZyXEL

We currently recognizes the following 52 categories:

Potential Liable & Objectionable Content Categories

- · Adult/Mature Content
- $\cdot \ Alcohol/Tobacco$
- $\cdot \ Gambling$
- · Hacking/Proxy Avoidance Systems
- · Illegal Drugs
- $\cdot$  Illegal/Questionable
- · Intimate Apparel/Swimsuit
- $\cdot$  Nudity
- · Pornography
- $\cdot$  Sex Education
- · Violence/Hate/Racism
- · Weapons

#### Potential Non-Productive Categories

- $\cdot$  Abortion
- · Arts/Entertainment
- $\cdot$  Auctions
- · Brokerage/Trading
- · Business & Economy
- $\cdot$  Chat/Instant Messaging
- $\cdot$  Computers/Internet
- $\cdot$  Cult/Occult
- · Cultural Institutions
- · Education
- $\cdot$  Email
- · Financial Services
- $\cdot$  For Kids
- · Games
- · Gay & Lesbian
- $\cdot$  Government/Legal
- · Health
- · Humor/Jokes
- · Job Search/Careers
- · Military
- · News & Media
- $\cdot$  Newsgroups

- $\cdot$  Pay to surf sites
- · Personals & Dating
- · Political/Activist Groups
- $\cdot$  Real Estate
- $\cdot \ Reference$
- · Religion
- · Restaurants/Dining/Food
- · Search Engines and Portals
- · Shopping
- · Society & Lifestyle
- $\cdot$  Software Downloads
- $\cdot \ Sports/Recreation/Hobbies$
- · Streaming Media/MP3
- · Travel
- $\cdot$  Vehicles
- · Web Advertisements
- · Web Communications
- $\cdot$  Web Hosting

#### J24. How does the ZyXEL content filtering handle dynamically generated sites?

We use BlueCoat's Dynamic Real-Time Rating service to accurately categorize dynamic content. Because BlueCoat provides Dynamic Real-Time Rating technology, most dynamic sites receive the correct rating. BlueCoat's database continually reviews the ratings of stored URLs to ensure that the content has not changed.

# J25. Does BlueCoat have more than one data center? Is the BlueCoat Web Filter geographically load balanced?

Yes, BlueCoat provides several, geographically distributed data centers to meet the demand of users around the world.

#### J26. Who can generate and view reports on BlueCoat WEB site?

Anyone with the administration username and password can view and generate reports.

#### J27. How can I get Content Filtering report?

You can get report for content filtering by clicking **Register** button from ZyXEL appliance's WEB GUI, and then you will be redirected to http://myZyXEL.com web server. By clicking **Content Filtering** 

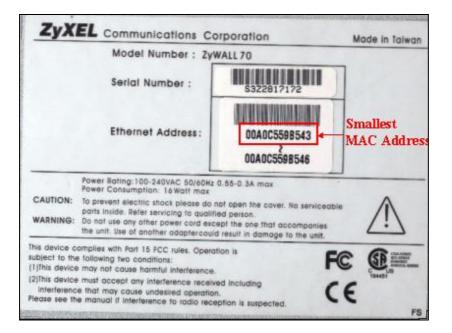
**Report**, the WEB interface of BlueCoat reporting system will pop out. By entering the MAC address you registered to Http://myZyXEL.com web server, which you can check from **Registration Status** of Http://myZyXEL.com server, and password you specified when doing registration, you can log into BlueCoat reporting system.

#### J28. Can I change the password for BlueCoat service?

Yes, you can click **Register** button from ZyXEL appliance's WEB GUI, then Http://myZyXEL.com web page would popped out. You can change password in user profile.

#### J29. Which User Name & Password should I input for Content Filtering report?

The User Name is the smallest Ethernet MAC address of your device. To identify check the sticker in the bottom of the device as below,



password is the password to login Http://myZyXEL.com.

# J30. My device can't get connected to Http://myZyXEL.com, so I can't get into Registration page. What should I check?

 Please check the Internet Access is ok via launching Internet Browser and connect to a public WEB site.
 If your ZyWALL is using Static (or Fixed) WAN IP address, please make sure that you have configured DNS server's IP address for the device in "System->General->System DNS Servers" or "Maintenance->General->System DNS Server".

### K. IPSec FAQ

#### K01. How many VPN tunnels are supported on ZyWALL?

Following table illustrates how many VPN tunnels are supported on ZyWALL5/35/70 with 3.64 f/w. For example: User can configure up to 120 VPN tunnel (rules) on ZW70. But only 100 concurrent VPN tunnels can be used at the same time.

Model Name	ZW5	ZW35	ZW70
Version	3.62(XD.0)	3.64(WZ.0)	3.64(WM.0)
VPN			
VPN Tunnels (Simultaneously usable)	10	35	100
VPN Tunnels (User can configure)	10	40	120

#### K02. How to count my VPN tunnels on ZyWALL?

On 3.64, multiple Network Policies (IKE Phase 2) can be mapped to same Gateway policy (IKE Phase 1). ZyWALL counts the Network policies as VPN tunnels.

In following example, two network policies, Netowrk\_1 & Network\_2 are mapped to same gateway policy, Gateway\_1. In this case, this will be counted as two VPN tunnels.

Rules (IKE)	VPN Rules (Mar	ual) SA Monitor	Global Setting	
VPN Rules				
			2.0	
	Local		ternet	Remote
N	etwork	VP	N Tunnel	Network
			Remote Gatew	
# VPN F	Rules	My ZyWALL	Remote Gatew	~ *
	Rules eway_1)	Ny ZyWALL	Remote Gatew 2.2.2.2	້ ອີບີ ແ <sub>ນ</sub> ນີ
□ 1 Gate		€⊋1.1.1.1 ~~ 192.168.1.0 /	©2.2.2.2 192.168.11.0 /	` *
■ 1 Gate	eway_1	©1.1.1.1	<b>⊗2.2.2.2</b>	5° (1) (1)

#### K03. What is VPN?

A VPN gives users a secure link to access corporate network over the Internet or other public or private networks without the expense of lease lines. A secure VPN is a combination of tunneling, encryption, authentication, access control and auditing technologies/services used to transport traffic over the Internet or any insecure network that uses the TCP/IP protocol suite for communication.

#### K04. Why do I need VPN?

There are some reasons to use a VPN. The most common reasons are because of security and cost.

Security

1). Authentication

With authentication, VPN receiver can verify the source of packets and guarantee the data integrity.

2). Encryption

With encryption, VPN guarantees the confidentiality of the original user data.

Cost

1). Cut long distance phone charges

Because users typically dial the their local ISP for VPN, thus, long distance phone charge is reduced than making a long direct connection to the remote office.

2).Reducing number of access lines

Many companies pay monthly charges for two types access lines: (1) high-speed links for their Internet access and (2) frame relay, ISDN Primary Rate Interface or T1 lines to carry data. A VPN may allow a company to carry the data traffic over its Internet access lines, thus reducing the need for some installed lines.

#### K05. What are most common VPN protocols?

There are currently three major tunneling protocols for VPNs. They are Point-to-Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP) and Internet Protocol Security (IPSec).

#### K06. What is PPTP?

PPTP is a tunneling protocol defined by the PPTP forum that allows PPP packets to be encapsulated within Internet Protocol (IP) packets and forwarded over any IP network, including the Internet itself. The PPTP is supported in Windows NT and Windows 98 already. For Windows 95, it needs to be upgraded by the Dial-Up Networking 1.2 upgrade.

#### K07. What is L2TP?

Layer Two Tunneling Protocol (L2TP) is an extension of the Point-to-Point Tunneling Protocol (PPTP) used by an Internet service provider (ISP) to enable the operation of a virtual private network (VPN) over the Internet.

#### K08. What is IPSec?

IPSec is a set of IP extensions developed by IETF (Internet Engineering Task Force) to provide security services compatible with the existing IP standard (IPv.4) and also the upcoming one (IPv.6). In addition, IPSec can protect any protocol that runs on top of IP, for instance TCP, UDP, and ICMP. The IPSec provides cryptographic security services. These services allow for authentication, integrity, access control, and confidentiality. IPSec allows for the information exchanged between remote sites to be encrypted and verified. You can create encrypted tunnels (VPNs), or just do encryption between computers. Since you have so many options, IPSec is truly the most extensible and complete network security solution. What secure protocols does IPSec support?

There are two protocols provided by IPSec, they are AH (Authentication Header, protocol number 51) and ESP (Encapsulated Security Payload, protocol number 50).

What are the differences between 'Transport mode' and 'Tunnel mode?

The IPSec protocols (AH and ESP) can be used to protect either an entire IP payload or only the upper-layer protocols of an IP payload. Transport mode is mainly for an IP host to protect the data

generated locally, while tunnel mode is for security gateway to provide IPSec service for other machines lacking of IPSec capability.

In this case, Transport mode only protects the upper-layer protocols of IP payload (user data). Tunneling mode protects the entire IP payload including user data.

There is no restriction that the IPSec hosts and the security gateway must be separate machines. Both IPSec protocols, AH and ESP, can operate in either transport mode or tunnel mode.

#### K09. What is SA?

A Security Association (SA) is a contract between two parties indicating what security parameters, such as keys and algorithms they will use.

What is IKE?

IKE is short for Internet Key Exchange. Key Management allows you to determine whether to use IKE (ISAKMP) or manual key configuration to set up a VPN.

There are two phases in every IKE negotiation- phase 1 (Authentication) and phase 2 (Key Exchange). Phase 1 establishes an IKE SA and phase 2 uses that SA to negotiate SAs for IPSec.

#### K10. What is Pre-Shared Key?

A pre-shared key identifies a communicating party during a phase 1 IKE negotiation. It is called 'Pre-shared' because you have to share it with another party before you can communicate with them over a secure connection.

What are the differences between IKE and manual key VPN?

The only difference between IKE and manual key is how the encryption keys and SPIs are determined. For IKE VPN, the key and SPIs are negotiated from one VPN gateway to the other. Afterward, two VPN gateways use this negotiated keys and SPIs to send packets between two networks.

For manual key VPN, the encryption key, authentication key (if needed), and SPIs are predetermined by the administrator when configuring the security association.

IKE is more secure than manual key, because IKE negotiation can generate new keys and SPIs randomly for the VPN connection.

#### K11. What is Phase 1 ID for?

In IKE phase 1 negotiation, IP address of remote peer is treated as an indicator to decide which VPN rule must be used to serve the incoming request. However, in some application, remote VPN box or client software is using an IP address dynamically assigned from ISP, so ZyWALL needs additional information

to make the decision. Such additional information is what we call phase 1 ID. In the IKE payload, there are local and peer ID field to achieve this.

#### K12. What are Local ID and Peer ID?

Local ID and Peer ID are used in IKE phase 1 negotiation. It's in FQDN(Fully Qualified Domain Name) format, IKE standard takes it as one type of Phase 1 ID.

Phase 1 ID is identification for each VPN peer. The type of Phase 1 ID may be IP/FQDN (DNS)/User FQDN (E-mail). The content of Phase 1 ID depends on the Phase 1 ID type. The following is an example for how to configure phase 1 ID.

ID type Content

\_\_\_\_\_

IP 202.132.154.1 DNS www.zyxel.com E-mail support@zyxel.com.tw

Please note that, in ZyWALL, if "DNS" or "E-mail" type is chosen, you can still use a random string as the content, such as "this\_is\_zywall". It's not neccessary to follow the format exactly. By default, ZyWALL takes IP as phase 1 ID type for itself and it's remote peer. But if its remote peer is using DNS or E-mail, you have to adjust the settings to pass phase 1 ID checking. When should I use FQDN?

If your VPN connection is ZyWALL to ZyWALL, and both of them have static IP address, and there is no NAT router in between, you can ignore this option. Just leave Local/Peer ID type as IP, and then skip this option.

If either side of VPN tunneling end point is using dynamic IP address, you may need to configure ID for the one with dynamic IP address. And in this case, "Aggressive mode" is recommended to be applied in phase 1 negotiation.

#### K13. Is my ZyWALL ready for IPSec VPN?

IPSec VPN is available for ZyWALL since ZyNOS V3.50. It is free upgrade, no registration is needed. By upgrading the firmware and also configurations (romfile) to ZyNOS V3.50, the IPSec VPN capability is ready in your ZyWALL. You then can configure VPN via web configurator. Please download the firmware from our web site.

#### K14. How do I configure ZyWALL VPN?

You can configure ZyWALL for VPN via web GUI. ZyWALL 1 supports Web only.

#### K15. What VPN protocols are supported by ZyWALL?

All ZyWALL series support ESP (protocol number 50) and AH (protocol number 51).

#### K16. What types of encryption does ZyWALL VPN support?

ZyWALL supports 56-bit DES and 168-bit 3DES.

#### K17. What types of authentication does ZyWALL VPN support?

VPN vendors support a number of different authentication methods. ZyWALL VPN supports both SHA1 and MD5.

AH provides authentication, integrity, and replay protection (but not confidentiality). Its main difference with ESP is that AH also secures parts of the IP header of the packet (like the source/destination addresses), but ESP does not.

ESP can provide authentication, integrity, replay protection, and confidentiality of the data (it secures everything in the packet that follows the header). Replay protection requires authentication and integrity (these two go always together). Confidentiality

(encryption) can be used with or without authentication/integrity. Similarly, one could use authentication/integrity with or without confidentiality.

#### K18. I am planning my ZyWALL-to-ZyWALL VPN configuration. What do I need to know?

First of all, both ZyWALL must have VPN capabilities. Please check the firmware version, V3.50 or later has the VPN capability. If your ZyWALL is capable of VPN, you can find the VPN options in **Advanced>VPN** tab.

For configuring a 'box-to-box VPN', there are some tips:

If there is a NAT router running in the front of ZyWALL, please make sure the NAT router supports to pass through IPSec.

In NAT case (either run on the frond end router, or in ZyWALL VPN box), only IPSec ESP tunneling mode is supported since NAT against AH mode.

**Source IP/Destination IP**-- Please do not number the LANs (local and remote) using the same exact range of private IP addresses. This will make VPN destination addresses and the local LAN addresses are

### ZyXEL

indistinguishable, and VPN will not work.

**Secure Gateway IP Address** -- This must be a public, routable IP address, private IP is not allowed. That means it can not be in the 10.x.x.x subnet, the 192.168.x.x subnet, nor in the range 172.16.0.0 - 172.31.255.255 (these address ranges are reserved by internet standard for private LAN numberings behind NAT devices). It is usually a static IP so that we can pre-configure it in ZyWALL for making VPN connections. If it is a dynamic IP given by ISP, you still can configure this IP address after the remote ZyWALL is on-line and its WAN IP is available from ISP.

#### K19. Does ZyWALL support dynamic secure gateway IP?

If the remote VPN gateways uses dynamic IP, we enter **0.0.0.0** as the **Secure Gateway IP Address** in ZyWALL. In this case, the VPN connection can only be initiated from dynamic side to fixed side in order to update its dynamic IP to the fixed side. However, if both gateways use dynamic IP addresses, it is no way to establish VPN connection at all.

#### K20. What VPN gateway that has been tested with ZyWALL successfully?

We have tested ZyWALL successfully with the following third party VPN gateways. Cisco 1720 Router, IOS 12.2(2)XH, IP/ADSL/FW/IDS PLUS IPSEC 3DES NetScreen 5, ScreenOS 2.6.0r6 SonicWALL SOHO 2 WatchGuard Firebox II ZyXEL ZyWALL 100 Avaya VPN Netopia VPN III VPN

#### K21. What VPN software that has been tested with ZyWALL successfully?

We have tested ZyWALL successfully with the following third party VPN software. SafeNet Soft-PK, 3DES edition Checkpoint Software SSH Sentinel, 1.4 SecGo IPSec for Windows F-Secure IPSec for Windows KAME IPSec for UNIX Nortel IPSec for UNIX

### ZyXEL

Intel VPN, v. 6.90 FreeS/WAN for Linux SSH Remote ISAKMP Testing Page, (http://isakmp-test.ssh.fi/cgi-bin/nph-isakmp-test) Windows 2000, Windows XP IPSec

#### K22. Will ZyXEL support Secure Remote Management?

Yes, we will support it and we are working on it currently.

#### K23. Does ZyWALL VPN support NetBIOS broadcast?

Yes, the ZyWALL does support NetBIOS broadcast over VPN.

#### K24. Is the host behind NAT allowed to use IPSec?

NAT Condition	Supported IPSec Protocol
VPN Gateway embedded NAT	AH tunnel mode, ESP tunnel mode
VPN client/gateway behind NAT <sup>*</sup>	ESP tunnel mode
NAT in Transport mode	None

\* The NAT router must support IPSec pass through. For example, for ZyWALL NAT routers, IPSec pass through is supported since ZyNOS 3.21. The default port and the client IP have to be specified in NAT menu Server Setup.

#### K25. How do I configure ZyWALL with NAT for internal servers?

Generally, without IPSec, to configure an internal server for outside access, we need to configure the server private IP and its service port in NAT Server Table.

However, if both NAT and IPSec is enabled in ZyWALL, the edit of the table is necessary only if the connection is a non-secure connections. For secure connections, none NAT server settings are required since private IP is reachable in the VPN case.

For example:

host----ZyWALL(NAT)----ADSL Modem----Internet----Secure host

Non-secure host

#### K26. I am planning my ZyWALL behind a NAT router. What do I need to know?

Some tips for this:

The NAT router must support to pass through IPSec protocol. Only ESP tunnel mode is possible to work in NAT case. In the NAT router is ZyWALL NAT router supporting IPSec pass through, default port and the ZyWALL WAN IP must be configured in NAT Server Table.

WAN IP of the NAT router is the tunneling endpoint for this case, not the WAN IP of ZyWALL.

If firewall is turned on in ZyWALL, you must forward IKE port in Internet interface.

If NAT are also enabled in ZyWALL, NAT server is required for non-secure connections, NAT server is not required for secure connections and the physical private IP is used.

For example:

host----ZyWALL----NAT Router----Internet----Secure host

Non-secure host

#### K27. Where can I configure Phase 1 ID in ZyWALL?

Phase 1 ID can be configured in VPN setup menu as following ..

Property	
Name	gate 1
ateway Policy Information	
Ny ZyWALL	0.0.0.0
Remote Gateway Address	172.22.1.67
uthentication Key	
Pre-Shared Key	12345678
C Certificate	auto_generated_self_signed_cert 🚩 (See My Certificates)
Local ID Type	
Content	
Peer ID Type	
Content	
umentication For Activating VPN	
Authenticated By	ZyWALL
User Name	test
Password	••••
KE Proposal	
Negotiation Mode	Main 🔽
Encryption Algorithm	DES 🔽
Authentication Algorithm	MD5 🔽
SA Life Time (Seconds)	28800
Key Group	DH1 💌
Enable Multiple Proposals	
ssociated Network Policies	
# Name	Local Network Remote Network
vpn1	(1) 192.168.0.0 / 255.255.255.0
A	pply Cancel

#### K28. How can I keep a tunnel alive?

To keep a tunnel alive, you can check "**Nailed-up**" option when configuring your VPN tunnel. With this option, the ZyWALL will keep IPSec tunnel up at all time. With "**Nailed-up**", the ZyWALL will try to establish whenever tunnel is terminated due to any unknown reason.

### K29. Single, Range, Subnet, which types of IP address does ZyWALL support in VPN/IPSec?

All ZyWALL series support single, range, and subnet configuration for VPN IPSec. In other words, you can specify a single PC, a range of PCs or even a network of PCs to utilize the VPN/IPSec service.

#### K30. Does ZyWALL support IPSec pass-through?

Yes, ZyWALL can support IPSec pass-through. ZyWALL series don't only support IPSec/VPN gateway, it can also be a NAT router supporting IPSec pass-through.

If the VPN connection is initiated from the security gateway behind ZyWALL, no configuration is necessary for neither NAT nor Firewall.

If the VPN connection is initiated from the security gateway outside of ZyWALL, NAT port forwarding and Firewall forwarding are necessary.

To configure NAT port forwarding, please go to WEB interface, **Setup/ "NAT"**, put the secure gateway's IP address in default server.

To configure Firewall forwarding, please go to WEB interface, **Setup/Firewall**, select Packet Direction to **WAN to LAN**, and create a firewall rule the forwards IKE(UDP:500).

# K31. Can ZyWALL behave as a NAT router supporting IPSec pass through and an IPSec gateway simultaneously?

No, ZyWALL can't support them simultaneously. You need to choose either one. If ZyWALL is to support IPSec pass through, you have to disable the VPN function on ZyWALL. To disable it, you can either deactivate each VPN rule or issue a CI command, "**IPSec switch off**".

# K32. Will the traffic coming in through the VPN tunnel also be scanned by Anti-Virus, IDP and Anti-Spam feature in ZyWALL ZyNOS v4.0?

No, VPN traffic will not be inspected by be scanned by Anti-Virus, IDP and Anti-Spam module. However, we manage to support this feature in the forthcoming ZyNOS firmware.

### L. PKI FAQ

#### L01. Basic Cryptography concept

Encryption and decryption are two major operations involved in cryptography. Whenever we would like to send some secret over an insecure media, such as Internet, we may encrypt the secret before sending it out. The receiver thus needs the corresponding decryption key to recover the encrypted secrete. We need to have keys for both encryption and decryption. The key used to encrypt data is called the encryption key, and the key for decryption is called the decryption key.

Cryptography can be categorized into two types, *symmetric* and *asymmetric* cryptography. For symmetric cryptography, the encryption key is the same with the decryption. Otherwise, we the cryptography as asymmetric.

Symmetric cryptography, such as DES, 3DES, AES, is normally used for data transmission, since it requires less computation power than asymmetric cryptography. The task of privately choosing a key before communicating, however, can be problematic. Applications in real case may use asymmetric cryptography for to protect distribution of keys (symmetric), and uses symmetric cryptography for data transmission.

Asymmetric cryptography solves the key exchange problem by defining an algorithm which uses two keys, each of which can be used to encrypt a message. If one key is used to encrypt a message, then the other must be used to decrypt it. This makes it possible to receive secure messages by simply publishing one key (the public key) and keeping the other secret (the private key).

#### L02. What is PKI?

PKI is acronym of Public Key Infrastructure. A PKI is a comprehensive system of policies, processes, and technologies working together to enable users of the Internet to exchange information securely and confidentially. Public Key Infrastructures are based on the use of cryptography – the scrambling of information by a mathematical formula and a virtual key so that it can only be decoded by an authorized party using a related key.

A PKI uses pairs of cryptographic keys provided by a trusted third party known as a Certification Authority (CA). Central to the workings of a PKI, a CA issues digital certificates that positively identify the holder's identity. A Certification Authority maintains accessible directories of valid certificates, and a list of certificates it has revoked.

#### L03. What are the security services PKI provides?

PKI brings to the electronic world the security and confidentiality features provided by the physical



documents, hand-written signatures, sealed envelopes and established trust relationships of traditional, paper-based transactions. These features are:

Confidentiality: Ensures than only intended recipients can read files.

Data Integrity: Ensures that files cannot be changed without detection.

Authentication: Ensures that participants in an electronic transaction are who they claim to be.

Non-repudiation: Prevents participants from denying involvement in an electronic transaction.

#### L04. What are the main elements of a PKI?

A PKI includes: A Certification Authority Digital certificates Mathematically related key pairs, each comprising a private key and a public key These elements work within a formal structure defined by: Certificate Policies A Certification Practice Statement.

#### L05. What is a Certification Authority?

A Certification Authority is a trusted third party that verifies the identity of an applicant registering for a digital certificate. Once a Certification Authority is satisfied as to the authenticity of an applicant's identity, it issues that person a digital certificate binding his or her identity to a public key. (Digital certificates are also issued to organizations and devices, but we will focus on people for the purposes of this discussion.)

#### L06. What is a digital certificate?

An electronic credential that vouches for the holder's identity, a digital certificate has characteristics similar to those of a passport – it has identifying information, is forgery-proof, and is issued by a trusted third party. Digital certificates are published in on-line directories. Typically, a digital certificate contains:

The user's distinguished name (a unique identifier)

The issuing Certification Authority's distinguished name

The user's public key

The validity period

The certificate's serial number

The issuing Certification Authority's digital signature is for verifying the information in the digital certificate.

#### L07. What are public and private keys, and what is their relationship?

A PKI uses asymmetric cryptography to encrypt and decrypt information. In asymmetric cryptography, encryption is done by a freely available public key, and decryption is done by a closely guarded private key. Although the public and private keys in a particular key pair are mathematically related, it is impossible to determine one key from the other. Each key in an asymmetric key pair performs a function that only the other can undo.

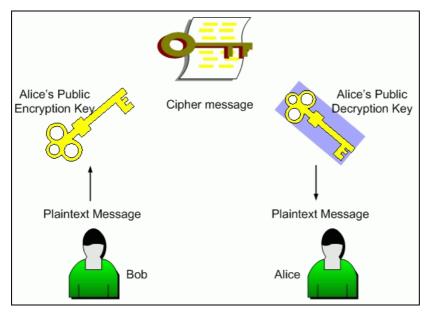
#### L08. What are Certificate Policies (CPs)?

Certification Authorities issue digital certificates that are appropriate to specific purposes or applications. For example, in the Government of Canada Public Key Infrastructure, digital certificates for data confidentiality are different from those used for digital signatures. Certificate Policies describe the rules governing the different uses of these certificates.

#### L09. How does a PKI ensure data confidentiality?

Users' public keys are published in an accessible directory. A person wishing to send an encrypted message uses the recipient's public key to scramble the information in the message. Only the recipient's private key can decrypt the message.

So, if Bob wants to send a confidential message to Alice, his PKI software finds Alice's public key in the directory where it is published, and he uses it to encrypt his message. When Alice receives the encrypted message, she uses her private key to decrypt it. Because Alice keeps her private key secret, Bob can be assured that, even if his message were to be intercepted, only Alice can read it.



#### L10. What is a digital signature?

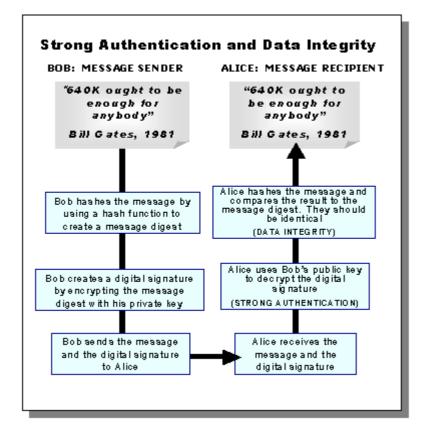
Not to be confused with a digitized signature (a scan of a hand-written signature), a digital signature can be used with either encrypted or unencrypted messages to confirm the sender's identity and ensure the recipient that the message content has not been changed in transmission. Digital signatures incorporate the characteristics of hand-written signatures in that they can only be generated by the signer, are verifiable, and cannot easily be imitated or repudiated.

#### L11. How does a digital signature work?

Suppose that the famous Bob and Alice wish to correspond electronically. Bob wants to assure Alice that he originated the electronic message, and that its contents have not been tampered with. He does so by signing the message with a digital signature.

When Bob clicks on the digital signature option on his e-mail application, special software applies a mathematical formula known as a hash function to the message, converting it to a fixed-length string of characters called a message digest. The digest acts as a "digital fingerprint" of the original message. If the original message is changed in any way, it will not produce the same message digest when the hash function is applied. Bob's software then encrypts the message digest with his private key, producing a digital signature of the message. He transmits the message and digital signature to Alice. Alice uses Bob's public key to decrypt the digital signature, revealing the message digest. Since only Bob's public key can decrypt the digital signature, she is able to verify that Bob was the sender of the message. This verification process also tells Alice's software which hash function was used to create the message digest of Bob's original message. To verify the message content, Alice's software applies the hash function to the message has not been changed and she is assured of its integrity. (If Bob had wanted to ensure the confidentiality of his message, he could have encrypted it with Alice's public key before applying the hash function to the message.)

The best thing about all these encryption, decryption, verifying and authenticating processes is that special software does them all transparently, so that Bob and Alice receive the assurances they need without having actually to engage in computations themselves.



#### L12. Does ZyXEL provide CA service?

No, ZyXEL doesn't maintain CA service for customers, customers need to find CA server (trusted 3rd party) in order to use PKI functionality on ZyWALL.

# L13. What if customers don't have access to CA service, but would like to use PKI function?

ZyXEL VPN solution provides a mechanism called "self-signed" Certificate. If you don't have access CA service, but would like to use PKI function, please use the self-signed Certificate. Check here for how to configure it.

#### L14. How can I have Self-signed certificate for ZyXEL appliance?

Each ZyXEL appliance would provide a Self-signed certificate along with default configuration file. You can check content of Self-signed certificate in WEB GUI.

#### L15. Can I create self-signed certificates in addition to the default one?

Yes, you can create self-signed certificates of your own by selecting self-signed category when creating My Certificates.

#### L16. Will Self-signed certificate be erased if I reset to default configuration file?

Yes, the original Self-signed certificate will be erased. But ZyXEL appliance will create a new self-signed certificate at it's first boot-up time after resetting the configuration. But the new self-signed certificate is different from the original one. So users also need to export the new self-signed certificate to appliance's peer if they would like to use PKI for VPN.

# L17. Will certificates stored in ZyXEL appliance be erased if I reset to default configuration file?

Yes, My Certificates, Trusted CAs' Certificates, and Trusted Remote's Certificates will be totally erased after erasing configuration files. Users need to enroll My Certificates and import Trusted CA's certificates & Trusted Remote's certificates again.

#### L18. What can I do prior to reset appliance's configuration?

You can export Trusted CA's certificates and Trusted Remote's certificates before resetting configuration to the local computer. Then import them back to ZyXEL appliance.

# L19. If I export My Certificates from ZyXEL appliance, save them locally, and then import them back after resetting the configuration file, can I reuse the imported My Certificates ?

No, you can't reuse them. Each certificate stored in My Certificates has corresponding private key. When you erase the configuration, the corresponding private keys are also deleted. So you can't reuse the certificates by importing them afterward.

### M. Dual WAN Auto Fail-over/Fail-back and Load Balance FAQ

#### M01. How do ZyWALLs dispatch outgoing sessions to different WAN connections?

When load-balance is enabled on ZyWALLs which have multiple WAN connections (e.g. ZyWALL 35/70/1000), the ZyWALL will dispatch the outgoing traffic which refers to default route (no policy route or static route applied to it). The traffic will be forwarded to the wan connections according the load-balance algorithms selected (e.g. Spiller-Over, Weighted Round Robin, or Least-Load First). When the outgoing session is dispatched to a specific wan connection (e.g. WAN1 or WAN2), the session will be fixed on this connection until it is terminated by the hosts or servers.

#### M02. Can ZyWALL support VPN load balancing?

No, because when using IPSec VPN, you need to specify source/destination security gateways, thus ZW can NOT dynamically change gateway (WAN) to go in/out. And with Load balancing mechanism, session manager in ZyWALL will decide each session will go to primary WAN or secondary WAN. That is, one session may possible to be sent via primary WAN or secondary WAN. In this way, it may cause the gateway is not the same as defined in VPN rule.

As for ZyWALL v3.64, we only supports BWM and fail-over for VPN tunnel.

### N. Bandwidth Management FAQ

# N01. How many class can I create in ZyWALL Bandwidth Management class tree? And, what is the max depth of a class?

Number of classes and max depth of a class supported on ZyWALL's Bandwidth management is model specific.

(1) Max depth of a classes

ZyWALL 70: 5 ZyWALL 35: 3 ZyWALL 5: 1

(2) Number of classes

ZyWALL 70: 100 ZyWALL 35: 50 ZyWALL 5: 20

### O. Wireless FAQ

#### O01. Which wireless cards does it support in ZyWALL 5/35/70?

(ZW1000 doesn't support wireless function)

Following table illustrates which wireless cards are supported by ZyWALL. For example: B-120/G-100/G-110 are supported on ZW70 since firmware 3.63 and later.

	B-100	B-101	B-120	G-100	G-110
ZW5	3.62	3.62	3.62	3.62	3.62
ZW35	3.62	3.62	3.62	3.62	3.62
ZW70	3.62	3.62	3.63	3.63	3.63

### **O02.** Which wireless security option can I use while using related wireless cards? (ZW1000 doesn't support wireless function)

When wireless cards are inserted to the slot of ZyWALL, the only related security options are supported. For example, using a B-100 wireless card means that "Static WEP" is supported but "WPA-PSK", "WPA" & "802.1x+" Dynamic WEP" are not supported.

	B-100	B-101	B-120	G-100	G-110
No Security	О	0	0	0	Ο
Static WEP	О	0	0	0	0
WPA-PSK	X	X	0	0	Ο
WPA	X	X	0	0	0
802.1x + Dynamic WEP	X	X	0	0	Ο
802.1x + Static WEP	О	0	0	0	0
802.1x + No WEP	О	0	0	0	0
No Access 802.1x + Static WEP	0	0	0	0	0
No Access 802.1x + No WEP	0	0	0	0	0

Please Note:

"X" means NOT support

"O" means support

If "WPA" is selected, external radius must be used for authentication.

If "802.1x+ Dynamic WEP" is selected, external radius must be used for authentication.