

ZyWALL USG Series

Unified Security Gateway

Version 4.10 Edition 1, 05/2014

Application Notes

Copyright \circledast 2014 ZyXEL Communications Corporation

Table of Contents

Scenario 1 — Connecting your USG to the Internet	4
1.1 Application Scenario	4
1.2 Configuration Guide	4
Scenario 2 — WAN Load Balancing and Customized Usage of WAN	
Connection for Specific Traffic Dual WAN setting	8
2.1 Application Scenario	8
2.2 Configuration Guide	8
Scenario 3 — How to configure NAT if you have Internet-facing public	C
servers	13
3.1 Application Scenario	13
3.2 Configuration Guide	13
Scenario 4 — Secure site-to-site connections by using IPSec VPN – I	Pv4
with IKEv2 / IPv6	17
4.1 Application Scenario	17
4.2 Configuration Guide	17
Scenario 5 — Connect to USG by using IPSec IKEv2 in Windows 7	25
5.1 Application Scenario	25
5.2 Configuration Guide	25
Scenario 6 — GRE over IPSec VPN tunnel –VPN fail over	40
6.1 Application scenario	40
6.2 Configuration Guide	40
Scenario 7 - Deploying SSL VPN for Tele-workers to Access Compan	У
Resources –SSL VPN with Apple Mac OSX	
7.1 Application Scenario	54
7.2 Configuration Guide	54
Scenario 8 — Reserving Highest Bandwidth Management Priority for	
VoIP traffic	
8.1 Application Scenario	
8.2 Configuration Guide	
Scenario 9 - Reserving Highest Bandwidth Management Priority for a	
Superior User and Control Session per Host – BWM Per IP or Per Use	
9.1 Application Scenario	
9.2 Configuration Guide	
Scenario 10 - Using USG to Control Popular Applications – APP patro	
10.1 Application Scenario	
10.2 Configuration Guide	66

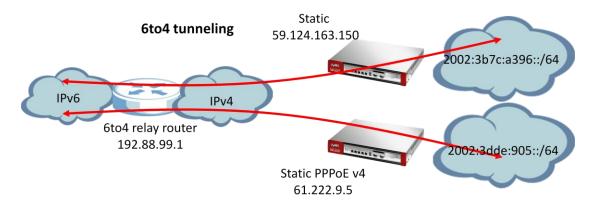
70
.71
.71
74
.74
.74
.77
.77
.77
90
.90
.90
95
.95
.95

Tut	orial	1: How to Set Up Your Network	98
	1.1	Vizard Overview	98
	1.2	How to Configure Interfaces, Port Roles, and Zones	98
	1.3	How to Configure a Cellular Interface	101
	1.4	How to Set Up a Wireless LAN	103
	1.6	How to Set Up IPv6 Interfaces For Pure IPv6 Routing	108
	1.7	How to Set Up an IPv6 6to4 Tunnel	113
	1.8	How to Set Up an IPv6-in-IPv4 Tunnel	117
Tut	orial	2: Protecting Your Network	121
	2.1	Firewall	121
	2.2	User-aware Access Control	122
	2.3	Device and Service Registration	123
	2.4	Anti-Virus Policy Configuration	124
	2.5	IDP Profile Configuration	126
	2.6	ADP Profile Configuration	127
	2.7	Content Filter Profile Configuration	129
	2.8	Viewing Content Filter Reports	131
	2.97	Anti-Spam Policy Configuration	134
Tut	orial	3: Create Secure Connections Across the Internet	136
	3.1	IPSec VPN	136
	3.2	VPN Concentrator Example	138
	3.3	Hub-and-spoke IPSec VPN Without VPN Concentrator	140
	3.4	USG IPSec VPN Client Configuration Provisioning	142
	3.58	SSL VPN	144
	3.6L	2TP VPN with Android, iOS, and Windows	145
Tut	orial	4: Managing Traffic	159
	4.1⊦	low to Configure Bandwidth Management	159
	4.2	How to Configure a Trunk for WAN Load Balancing	166
	4.3	How to Use Multiple Static Public WAN IP Addresses for	
	LAN	-to-WAN Traffic	168
	4.4⊦	low to Use Device HA to Backup Your USG	169
	4.5H	low to Configure DNS Inbound Load Balancing	173
	4.6	How to Allow Public Access to a Web Server	189
		low to Manage Voice Traffic	
	4.8H	low to Limit Web Surfing and MSN to Specific People	197

Scenario 1 — Connecting your USG to the Internet

1.1 Application Scenario

Nowadays, many Internet service providers offer an IPv6 environment. With an IPv6 feature enabled on the USG, it can assign an IPv6 address to clients and pass IPv6 traffic through IPv4 environment to access a remote IPv6 network.



1.2 Configuration Guide

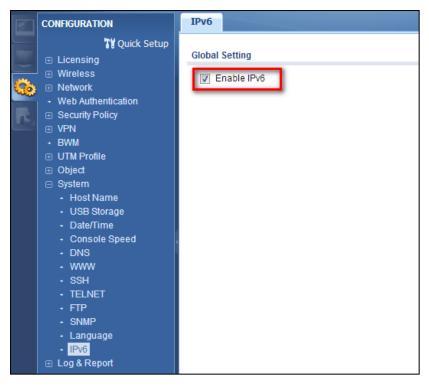
Network conditions:

<u>USG:</u> WAN1: 61.222.9.5(Static PPPoE v4) Or WAN1: 59.124.163.150(Static)

Goal to achieve:

A USG will assign an IPv6 IP addresses to the clients, which are behind it, and the clients can access a remote IPv6 network by using the USG 6to4 tunnel.

USG configuration Step 1: Configuration > System > IPv6 > Click Enable IPv6



Step 2: Setting the static IP on WAN1

Configuration > Interface > Ethernet > double-click on WAN1 interface and configure with static IP address 59.124.163.150.

	CONFIGURATION	Port Role	Ethernet	РРР	Cellular	Tunnel	VLAN	Bridge	Trunk			
	₩ Quick Setup Licensing Wireless	Configurat										
Ô	 Network Interface 		👕 Remove 🤪 tatus	Activate Nam			Virtual Inte ddress	rface ा 🛅 Ob	oject Refer	ence	Mask	
R,	RoutingDDNS	1	2	want wan2			(TIC 59.12 CP 10.59	24.163.150 3.82			255.255.255.224 255.255.255.0	
	 NAT HTTP Redirect 	3 (• •	lan1			TIC 192.1				255.255.255.0	
	 ALG IP/MAC Binding 	4 (2	lan2 dmz			TIC 192.1				255.255.255.0 255.255.255.0	
	DNS Inbound LB Web Authentication		Page 1 of :	1	Show 50						200.200.200.0	

Step 3: Setting IPv6 IP address on LAN1

 Configuration > Interface > Ethernet > double-click LAN1 interface in IPv6 configuration.

🥜 Edit Ethernet	Tunnel VLAN Bridge Trunk
IPv6 View 🔻 🏢 Show Advanced Settings 🖥	■Create new Object
General Settings	
Enable Interface	
General IPv6 Setting	
🔽 Enable IPv6 🔒	
Interface Properties	
Interface Type:	internal
Interface Name:	lan1
Port:	P3, P4, P5, P6
Zone:	LAN1
MAC Address:	B0:B2:DC:70:C1:D8

- (2) Convert WAN1 IP address to hexadecimal. 59.124.163.150(Decimal) = 3b7c:a396(Hex). Fill-in 2002:3b7c:a396::1/128 in the prefix table as the LAN interface IPv6 address.
- (3) Check the IPv6 Router Advertisement Setting box and add the prefix in the Advertised Prefix Table.

Edit Ethernet	
IPv6 View 🔻 🎹 Show Advanced Settings	; 🛅 Create new Object
IGMP Downstream	
IPv6 Address Assignment	
Enable Stateless Address Auto-cor	nfiguration (SLAAC)
Link-Local Address:	fe80::b2b2:dcff:fe70:c1d8/64
IPv6 Address/Prefix Length:	2002:3b7c:a396::1/12 (Optional)
DHCPv6 Setting	
DHCPv6:	N/A
IPv6 Router Advertisement Setting	
Enable Router Advertisement	
Router Preference:	Medium 👻
Advertised Prefix Table	💿 Add 🔀 Edit 🃋 Remove
	# IPv6 Addrose/Profix Longth
	1 2002:3b7c:a396::/64
	Page 1 of 1 Page Show 50 ritems Displaying 1 - 1 of 1

Step 4: Enable 6 to 4 tunnel.

(1) **Configuration > Interface>Tunnel >** Click on the **Add** button.

2	CONFIGURATION	Port Role	Ethernet	РРР	Cellular	Tunnel	VLAN	Bridge	Trunk
	7¥ Quick Setup	Configuratio	on 2 Edit 📺 Ren	nove 💡	Activate 🖗 🛙	Inactivate 🛙	Object Re	eference	
			atus Name Page 1 of	1 ▶ ₽	IP Addre			Tu	nnel Mode

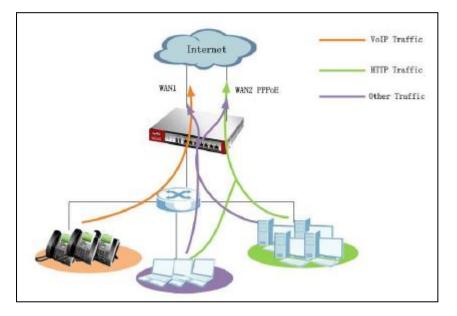
- (2) Select the 6to4 in that Tunnel Mode.
- (3) Check the Prefix in the 6tp4 tunnel Parameter.
- (4) Select the WAN1 interface as the gateway in the Gateway Setting.

) Edit Tunnel			?
Show Advanced Settings			
Enable			
Interface Properties			
Interface Name:	tunnel0		
Zone:	TUNNEL	v 1	
Tunnel Mode:	6to4	*	
IPv6 Address Assignment		_	
IPv6 Address/Prefix Length:			(Optional)
Metric:	0 (0-15)		
6to4 Tunnel Parameter			
6to4 Prefix:	2002::/16		
Relay Router:	192.88.99.1		(Optional)
NOTE: traffic destinated to the Gateway Settings My Address	non-6to4 prefix domain tunnels	to the relay router	
Interface	wan1	Static 59.124.163.150/2	255.255.255.224
			OK Cancel

Scenario 2 — WAN Load Balancing and Customized Usage of WAN Connection for Specific Traffic --Dual WAN setting

2.1 Application Scenario

The company has two WAN connections for sharing outbound internet traffic. WAN1 uses a static IP address, and WAN2 uses a PPPoE connection. Since WAN1 ISP is also the company's VoIP provider, the network administrator wants VoIP traffic primarily sent out over WAN1. In case WAN1 is down, the VoIP traffic can still go out over WAN2 PPPoE connection. The network administrator also wants HTTP traffic sent over WAN2 PPPoE connection primarily. In case WAN2 PPPoE is down, LAN users can still surf Internet over WAN1. For all other types of traffic, administrator needs the two WAN connections to share the outbound traffic load, performing load balancing.



2.2 Configuration Guide

Goals to achieve:

1) VoIP traffic goes out primarily through WAN1. In case WAN1 is down, it will go out via WAN2 PPPoE connection.

2) HTTP traffic goes out primarily through WAN2 PPPoE connection. In case WAN2 PPPoE is down, it will go out via WAN1.

3) All other traffic goes out via WAN trunk performing Load Balancing with Least

Load Balancing algorithm.

USG configuration

Step 1. Configure a PPPoE account on WAN2 interface.

(1) Go to **CONFIGURATION > Object > ISP Account,** add a PPPoE account:

CONFIGURATION	ISP Account	Z Edit ISP Account Rule		? 🗙
™ Quick Setup ■ Licensing ■ Wireless ■ Network ■ Security Policy ■ WM ■ UTM Profile ■ Object • Zone • User/Group • Application • Address • Service • Schedule • Address • Address • Schedule • Address • Address • Schedule • Address • Address • Address • Address • Schedule • Address • Address	Configuration	Profile Name: Protocol: Authentication Type: User Name : Password: Retype to Confirm: Service Name: Compression Idle timeout:	WAN2_PPPoE_ACCO pppoe Chap/PAP my_account	(Optional) (Seconds)
ISP Account SSL Application				

(2) Go to **CONFIGURATION > Network > Interface > PPP**, add a new PPP

interface, which is based on WAN 2 interface:

Edit PPPoE/PPTP		
IPv4/IPv6 View 🔻 🎹 Show Advanced Sett	ings 🛅 Create new Objec	t
General Settings		
Enable Interface		
General IPv6 Setting		
🔲 Enable IPv6 👔		
Interface Properties		
Interface Name:	wan2_ppp	
Base Interface:	wan2	
Zone:	WAN	
Description:		(Optional)
Connectivity		
Nailed-Up		
Dial-on-Demand		
ISP Setting		
Account Profile:	WAN2_PPPoE_A(💙	
Protocol:	pppoe	
User Name :	74823078@hinet.net	

Step 2. Go to **CONFIGURATION > Network > Interface > Trunk**. Add WAN Trunks.

(1) Add WAN trunk for VoIP traffic — Set WAN1 as Active mode, while setting WAN2_ppp as Passive mode.

Add 1	Trunk						?
Nam	ne:	WAN_tru	unk_Vo	[P			
Load	d Balancing Algorithm:	Least Lo	Least Load First				
Load	d Balancing Index(es):	Outbour	d		-		
0	Add 🛃 Edit 🍵 Remove	⊌N Move					
#	Member	Mode		Egress Ba	ndwidt	h	
1	wan1	Active		1048576	ops		1
2	wan2_ppp	Passive		1048576	obps		
14		▶ ▶ Show 50	✓ ite	ms		No data to display	1

(2) Add WAN trunk for HTTP traffic — Set WAN2_ppp as Active mode, while setting WAN1 as Passive mode.

Add 1	Frunk						?
Nam	e:	WAN	I_trunk_HT	ГР			
Load Balancing Algorithm:			t Load First		~		
Load	Balancing Index(es):	Outb	ound		~		
0	Add 🛃 Edit 🍵 Remove	Move 📢					
#	Member	Mode		Egress B	andwidth	1	
1	wan1	Passive		1048576	kbps		
2	wan2_ppp	Active		1048576	kbps		
14		▶ Show	50 🔻 iter	ms		No data to display	

(3) Use SYSTEM_DEFAULT_WAN_TRUNK to perform load balancing for all other traffic.

S	System Default										
🖉 Edit ा Object Reference											
	#	Name	Algorithm								
	1	SYSTEM_DEFAULT_WAN_TRUNK	llf								
	I I of 1 ▶ ▶I Show 50 v items										

Step 3. Go to CONFIGURATION > Network > Routing > Policy Route, add policy

routes for VoIP traffic and HTTP traffic.

- (1) Add a policy route for VoIP traffic:
 - Source: LAN1_subnet
 - Destination: Any

Service: SIP

Next Hop: select the newly created WAN trunk WAN_Trunk_VoIP

Add Policy Route		? >
🏢 Show Advanced Settings 🛅 Creat	te new Object 🔹	
Criteria		
User:	any 💌	
Incoming:	any (Excluding ZyWALL)	
Source Address:	LAN1_SUBNET	
Destination Address:	any 👻	
DSCP Code:	any 👻	
Schedule:	none 💌	
Service:	SIP	
Next-Hop		
Туре:	Trunk	
Trunk:	WAN_trunk_VoIP 🗸	
DSCD Marking		

Please note that to make sure this policy route applies to all VoIP traffic, including both the SIP signaling and RTP (voice data), we need to enable SIP ALG.

CONFIGURATION	ALG	
₩ Quick Setup	SIP Settings	
	Enable SIP ALG	
 Interface Routing 	Enable SIP Transformations Enable Configure SIP Inactivity Timeout	
+ DDNS + NAT	Enable Configure SIP Inactivity Timeout SIP Media Inactivity Timeout :	120 (seconds)
HTTP Redirect ALG	SIP Signaling Inactivity Timeout :	1800 (seconds)
+ IP/MAC Binding	Restrict Peer to Peer Signaling Connection Restrict Peer to Peer Media Connection	
ONS Inbound LB Web Authentication Security Policy	SIP Signaling Port :	O Add ≥ Edit [™] Remove
⊕ VPN		# Port ▲ 1 5060
 BWM ⊕ UTM Profile 		1 5060

Go to **Configuration > Network > ALG**, enable SIP ALG.

(2) Add a policy route for HTTP traffic:

Source: LAN1_subnet Destination: Any Service: HTTP Next Hop: Select the newly created WAN trunk WAN_Trunk_HTTP.

O Add Policy Route		? 🗙
🔢 Show Advanced Settings 🛅 Create new Ob	ject•	
Criteria		
User:	any	v
Incoming:	any (Excluding ZyWALL)	
Source Address:	LAN1_SUBNET	×
Destination Address:	any	¥
DSCP Code:	any	×
Schedule:	none	¥
Service:	нттр	¥
Next-Hop		
Type:	Trunk	v
Trunk:	WAN_trunk_HTTP	¥

(3) For all other traffic, use SYSTEM_DEFAULT_WAN_TRUNK to perform load balancing. Go to Configuration > Network > Interface > Trunk. Click on Show Advanced Settings.

CONFIGURATION	Port Role	Ethernet	РРР	Cellular	Tunnel	VLAN	Bridge	Trunk		
📲 Quick Setup	Show Adv	anced Setting	5							
E Licensing										
⊕ Wireless	Configurati	on								
Network										
Interface	Disconnect Connections Before Falling Back									
+ Routing										
+ DDNS	Default WA	N Trunk								

Make sure **Default SNAT** is enabled. Select

SYSTEM_DEFAULT_WAN_TRUNK in Default Trunk Selection.

Default WAN Trunk	
Enable Default SNAT Default Trunk Selection	
SYSTEM_DEFAULT_WAN_TRUNK	
User Configured Trunk WAN_trunk_HTTP	*

Scenario 3 — How to Configure NAT if you have

Internet-facing Public Servers

3.1 Application Scenario

It is a common practice to place company servers behind the USG's protection; while at the same time letting WAN side clients/servers access the intranet servers. To give an example, the company may have an internal FTP server, which needs to be accessible from the Internet as well. To fulfill this requirement, the user can configure a NAT mapping rule to forward the traffic from the Internet side to intranet side. This feature does not only ensure service availability, but also helps avoid exposing the server's real IP address from being attacked.

3.2 Configuration Guide

Goal to achieve:

User Tom can access the Internet FTP server by accessing the Internet-facing the WAN IP address.

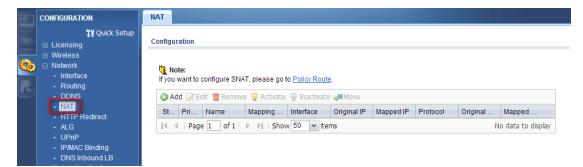
Network Conditions: USG-50:

- WAN IP: 59.124.163.152
- FTP server IP: 192.168.50.33



Configuration

Step 1. Go to **CONFIGURATION > Network > NAT** to open the configuration screen.



Step 2. Click on the **Add** button to create a mapping rule.

Step 3. In this page, the user needs to configure:

- Rule's name
- Select Virtual Server type to let USG-50 do packet forwarding
- Fill-in the Original IP (WAN IP) address
- Fill-in the **Mapped IP** (Internal FTP server IP) address

- Select the service to be mapped (FTP); the ports will be selected automatically

					?
Create new Object -					
eneral Settings					
Enable Rule					
Rule Name:	FTP				
ort Mapping Type		_			
Classification:	Virtual Server	1:1 NAT	e	Many 1:1 NAT	
		1.119231		y many it river	
lapping Rule					
Incoming Interface:	wan1	~		1	
Original IP:	User Defined	~			
Original IP: User-Defined Original IP:	User Defined 59.124.163.152	_	Address)		
		_	Address)		
User-Defined Original IP:	59.124.163.152	(IP)	Address) Address)		
User-Defined Original IP: Mapped IP:	59.124.163.152 User Defined	(IP)			
User-Defined Original IP: Mapped IP: User-Defined Mapped IP:	59.124.163.152 User Defined 192.168.50.33	(IP) (IP)			

Step 4. Go to **CONFIGURATION > Security Policy > Policy Control** to open the firewall configuration screen.

Here assume the user already assigned the WAN interface to WAN zone and LAN interface to LAN1 zone.

Step 5. Click on the **Add** button to create a firewall rule to enable the FTP service to pass from WAN to LAN1.

CONFIGURATION	Policy										
₩ Quick Setup Licensing	General	Setting	s								
■ Wireless	I Enable Policy Control										
 ⊟ Network	V En	Jable Po	oncy Control								
Interface	IPv4 Cor	nfigurat	ion								
+ Routing		-									
DDNS	📄 All	ow Asyr	mmetrical Route	•							
• NAT • HTTP Redirect	O Ac	dd 📝 E	dit 🍵 Remove	Q Activate	Inactivate 📣	Move					
+ ALG	Pri	-	Name	From	То	IPv4 Source	IPv4 Desti	Service	User	Schedule	Act UTM Profile
+ UPnP	1	0.0	LAN1 Out		any (Exclu	any	any	any	any	none	allow
 IP/MAC Binding 			-								
 DNS Inbound LB 	2	9	LAN2_Out		any (Exclu	any	any	any	any	none	allow
+ Web Authentication	3	9	DMZ_to_W	■ DMZ	■ WAN	any	any	any	any	none	allow
Security Policy	4	0	IPSec_VP	IPSec_VPN	any (Exclu	any	any	any	any	none	allow
Policy Control ADP	5	0	SSL_VPN	SSL_VPN	any (Exclu	any	any	any	any	none	allow
Session Control	6	0	TUNNEL	TUNNEL	any (Exclu	any	any	any	any	none	allow
	7	0	LAN1_to	■LAN1	ZyWALL	any	any	any	any	none	allow
+ BWM	8	0	LAN2_to	■LAN2	ZvWALL	anv	any	any	anv	none	allow
UTM Profile	9		DMZ to D		ZvWALL	any		Default	any		allow
Device HA Object		9			· ·		any			none	
⊕ System	10	9	WAN_to_D		ZyWALL	any	any	Default	any	none	allow
	11	9	IPSec_VP	IPSec_VPN	ZyWALL	any	any	any	any	none	allow
	12	9	SSL VPN	SSL VPN	ZyWALL	any	any	any	any	none	allow

Step 6. The user can create an address object for the internal FTP server for further configuration usage. Click on **Create new Object** for this function.

Edit Address Rule In	Zedit Address Rule Internal_FTP								
Name:	Internal_FTP								
Address Type:	HOST	~							
IP Address:	192.168.50.33								
		OK Can	cel						

Step 7. Configure the rule to:

- Allow access from WAN to LAN1
- Source IP address is not specific
- Destination IP address is the FTP server's address
- Select FTP service (with port 20/21) to be enabled
- Select the **allow** action for matched packets

Add corresponding					t Refer ? (
Create new Object -					
Enable					
Name:	For_FTP				
Description:		(Optional)			
From:	WAN	~			
то:	LAN1	*			
Source:	any	~			
Destination:	Internal_FTP	~			
Service:	FTP	*			
User:	any	~			
Schedule:	none	*			
Action:	allow	~			
Log matched traffic:	no	~			
UTM Profile					
Application Patrol:	none	~	Log:		~
Content Filter:	none	~	Log:		~
IDP:	none	~	Log:		~
Anti-Virus:	none	~	Log:		~
Anti-Spam:	none	~	Log:		~
SSL Inspection:	none	~	Log:		×
			C		_
			_	OK	Cancel

Step 8: Click on the **OK** button, you will see the rule in policy control.

	CONFIGURATION	Ро	olicy										
	T¥ Quick Setup ■ Licensing ● Wireless ● Network • Interface		🔽 En:	Settings able Pol figuratio	icy Control								
R.	Routing DDNS NAT				nmetrical Route	Q Activate Q	Inactivate 🔊	Move					
	 HTTP Redirect ALG 		Pri	Sta	Name	From	То	IPv4 Source	IPv4 Desti	Service	User	Schedule	Act UTM Profile
	UPnP		1	9	For_FTP	■ WAN	■LAN1	any	Internal	■FTP	any	none	allow
	 IP/MAC Binding DNS Inbound LB 		2	9	LAN1_Out	■LAN1	any (Exclu	any	any	any	any	none	allow
	Web Authentication		3	9	LAN2_Out	LAN2	any (Exclu	any	any	any	any	none	allow
	Security Policy		4	0	DMZ_to_W	■ DMZ	■ WAN	any	any	any	any	none	allow
	Policy Control ADP		5	9	IPSec_VP	IPSec_VPN	any (Exclu	any	any	any	any	none	allow
	Session Control		6	9	SSL_VPN	SSL_VPN	any (Exclu	any	any	any	any	none	allow
	VPN		7		TUNNEL	TUNNEL	any (Exclu	any	any	any	any	none	allow
	BWM		8		LAN1_to	■LAN1	ZyWALL	any	any	any	any	none	allow
	OTM Profile Orevice HA		9	9	LAN2_to	■LAN2	ZyWALL	any	any	any	any	none	allow
	Object		10	0	DMZ_to_D	= DMZ	ZyWALL	any	any	■ Default	any	none	allow
	 Zone 			~	1074 KL 44 15		-			m			-0

Scenario 4 — Secure Site-to-site Connections using IPSec VPN – IPv4 with IKEv2 / IPv6

4.1 Application Scenario

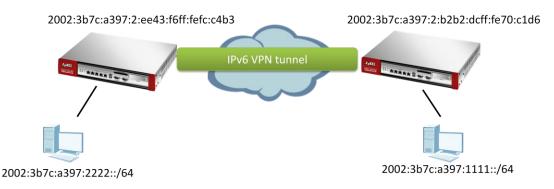
IPv4 with IKEv2

We want to use IKEv2 to establish a VPN tunnel between the HQ and Branch Office.



IPv6 (with IKEv2 only)

ISP has changed the environment to IPv6. We applied for IPv6 address pool for internal use. So we have to change use the IPv6 address to establish an VPN tunnel between the USG.



4.2 Configuration Guide

IPv4

Network Conditions:

USG-40W with static WAN:

- WAN IP: 59.124.163.155
- Local subnet: 192.168.100.0/24

USG-40W with PPPOE WAN:

- PPPOE IP: 220.137.67.76
- Local subnet: 192.168.200.0/24

IPSec VPN Conditions:

Phase 1:	Phase 2:
IKE version: IKEv2	Active Protocol: ESP
Authentication: 1234567890	Encapsulation Mode: Tunnel
Local/Peer ID type: IPv4 0.0.0.0 / Any	Encryption Algorithm: DES
Encryption Algorithm: 3DES	Authentication Algorithm: SHA1
Authentication Algorithm: MD5	Perfect Forward Secrecy: None
Key Group: DH1	

Goal to achieve:

Establish an IPSec VPN tunnel between two USGs with the above configuration.

Step 1. Go to **CONFIGURATION > VPN > IPSec VPN > VPN Gateway** to open the configuration screen.

Step 2. Click on the Add button to add a VPN gateway rule.

Z	YXEL USG40W					Welcome admin Logout	?Help Z About	🖣 Site Map	CObject Reference	🖵 Console	ធា
	CONFIGURATION	VPN Connection VPN Gateway	Concentrator	Configuration Provisioning							
	₩ Quick Setup ■ Licensing ■ Wireless ■ Network	IPv4 Configuration	vate 😨 Inactivate	e 🕞 Object Reference							
000	Web Authentication	# § Add a new rule 🕽		My Address	Secure Ga	teway	VPN Connection			KE Vers	
R	 Security Policy VPN IPSec VPN SSL VPN 	4	Show 50 🖌 ite	ms					No d	lata to display	

Step 3. To configure the VPN gateway rule, the user needs to fill-in:

- VPN gateway name
- Enable IKEv2 protocol
- Gateway address; both local (My Address) and peer (Peer GW Address)
- Authentication setting
 - Pre-Shared Key
 - ID Type setting (Local and Peer side)
- Phase-1 setting
 - Negotiation mode
 - Encryption algorithm
 - Authentication algorithm
 - Key Group

Add VPN Gateway						?
🔲 Hide Advanced Settings 🔚 Create r	new Object 🔹					
General Settings						
VPN Gateway Name:	To_PPPOE	40W/ GW	1			
IKE Version	[IU_rrroc	1010_011				
IKEv2						
Gateway Settings						
My Address	-		1.3			
Interface	wan1		*	Static :	59.124.163.155/255.255.255.224	
Domain Name / IPv4						
Peer Gateway Address						
Static Address 1	Primary	220.137.67	.76			
	Secondary	0.0.0.0				
Fall back to Primary Peer Ga		ossible	(60.9	6 <mark>40</mark> 0 sec	anda)	
Fall Back Check Interval:	300		(00-0	0400 Sec	onas)	
🔘 Dynamic Address 🛛 👔						
Authentication						
Pre-Shared Key	123456789	0				
unmasked	10					
Certificate	default		~	(See <u>My</u>		
Local ID Type:	IPv4		~			
Content:	0.0.0.0					
Peer ID Type:	Any		~			
Content:						
Diverse & Configuration						
Phase 1 Settings						1
SA Life Time:	86400			- 3000000) Seconds)	
Proposal	There is a second	Edit 🎁 Rem			-	
			uthenti	cation		
	1 3DE	5 M	ID5			
Key Group:	DH1		~			
	-					
Extended Authentication Protocol						
Enable Extended Authentication	184 - 9 Karris (185 August)					
Allowed Auth Method:	mschapv2					
Server Mode						
AAA Method:	default		~			
Allowed User:	any		~			
Client Mode	-					

Step 4. Go to **CONFIGURATION > VPN > IPSec VPN > VPN Connection** to open the configuration screen to configure the phase-2 rule.

Step 5. Click on the **Add** button to add a rule.

Z	ZyXEL USG40W						Welcome admin Logout	?Help	Z About	🕈 Site Map	CObject Reference	🖵 Console	ചവ
E	CONFIGURATION	VPN Connection	VPN Gateway	Concentrator	Configuration Provisioning								
	11 Quck Setup 2 Licensing 3 Network 3 Web Authentication 3 Security Policy 4 VPN 4 USAN VPN 5 SUVPN 5 S	Ignore "Don't Fi		Pheader 💽 te 🎯 Inactivate	මු, Connect මු, Disconnect ැ PN Gateway 115	Object: Reference	Encapsulation	Algo	orithm		Policy No d	iata to display	

Step 6. To configure the phase-2 rule, the user needs to fill-in:

- VPN connection name
- VPN gateway selection

-Policy for

- Local network side
- Remote network side

- Phase-2 settings

- Active protocol
- Encapsulation mode
- Encryption algorithm
- Authentication algorithm
- Perfect Forward Secrecy

Add VPN Connection					?
Hide Advanced Settings	🔄 Create new	Object 🕶			
General Settings					
🔽 Enable	_			_	
Connection Name:		To_PPPOE40W_VPN			
Nailed-Up					
Enable Replay Detect	tion				
Enable NetBIOS broa	dcast over IPS	ес			
MSS Adjustment					
Custom Size			(200 - 1	460 Bytes)	
Auto					
Varrowed					
VPN Gateway					
Application Scenario					
Site-to-site					
Site-to-site with D	ynamic Peer				
Remote Access (\$					
Remote Access (
VPN Gateway:	10	Co_PPPOE40W_GW	▼ w	an1 220.137.67.76, 0.0.0.0	
Policy					
Local policy:	L.	AN1_SUBNET	× II	ITERFACE SUBNET, 192.168.100.0/24	
Remote policy:		PPOE40W_LAN	1000	UBNET, 192.168.200.0/24	
Enable GRE over IPS			- P		
Concernent and the second	ec				
Policy Enforcement					
Phase 2 Setting					
SA Life Time:	5	86400	(180 - 3	000000 Seconds)	
Active Protocol:		SP	~		
			ALC: NO.		
Encapsulation:	-	Funnel	~		
Proposal		🗿 Add 🔜 Edit 🍵 Rem	love		
	102				
		# Encryption	Authe	ntication	
	1		Authe SHA1	ntication	
	1	DES	SHA1		
Perfect Forward Secrecy	1		1 Martine Contraction		
	1	DES	SHA1		
Related Settings	(PFS): r	DES	SHA1		
	(PFS): r	DES	SHA1		
Related Settings	(PFS): r	DES	SHA1		
Related Settings Zone: Connectivity Check	(PFS): r	DES	SHA1		
Related Settings Zone: Connectivity Check	(PFS): r	DES ione PSec_VPN	SHA1		
Related Settings Zone: Connectivity Check Enable Connectivity C Check Method:	(PFS): r	DES ione PSec_VPN	SHA1		
Related Settings Zone: Connectivity Check Enable Connectivity C Check Method: Check Period:	(PFS): r I Check I	DES ione PSec_VPN	SHA1		
Related Settings Zone: Connectivity Check Enable Connectivity C Check Method: Check Period: Check Timeout:	(PFS): r	DES Ione PSec_VPN 5 (5-600 Seco 6 (1-10 Secon	SHA1		
Related Settings Zone: Connectivity Check Enable Connectivity C Check Method: Check Period:	(PFS): r	DES ione PSec_VPN	SHA1		
Related Settings Zone: Connectivity Check Enable Connectivity C Check Method: Check Period: Check Timeout:	(PFS): r	DES Ione PSec_VPN 5 (5-600 Seco 6 (1-10 Secon	SHA1		
Related Settings Zone: Connectivity Check Enable Connectivity O Check Method: Check Period: Check Timeout: Check Timeout: Check Fail Tolerance: © Check This Addree	(PFS): r I Check I	DES Ione PSec_VPN 5 (5-600 Seco 6 (1-10 Secon	SHA1		
Related Settings Zone: Connectivity Check Enable Connectivity O Check Method: Check Period: Check Timeout: Check Timeout: Check Fail Tolerance: © Check This Addree	(PFS): r I Check I	DES none PSec_VPN 6 (5-600 Seco 6 (1-10 Secon (1-10)	SHA1		
Related Settings Zone: Connectivity Check Enable Connectivity C Check Method: Check Period: Check Period: Check Timeout: Check Fail Tolerance: Check This Addre Check the First ar	(PFS): r I Check I Ss d Last IP Addre	DES none PSec_VPN 6 (5-600 Seco 6 (1-10 Secon (1-10)	SHA1		
Related Settings Zone: Connectivity Check Enable Connectivity O Check Method: Check Period: Check Timeout: Check Fall Tolerance: © Check This Addre @ Check the First an	(PFS): r I Check I Ss d Last IP Addre	DES none PSec_VPN 6 (5-600 Seco 6 (1-10 Secon (1-10)	SHA1		
Related Settings Zone: Connectivity Check Enable Connectivity C Check Method: Check Period: Check Period: Check Timeout: Check Fail Tolerance: Check This Addre Check the First ar	(PFS): r I Check I Ss d Last IP Addre	DES none PSec_VPN 6 (5-600 Seco 6 (1-10 Secon (1-10)	SHA1		
Related Settings Zone: Connectivity Check Enable Connectivity C Check Method: Check Period: Check Timeout: Check Timeout: Check Timeout: Check Timeout: Check This Addre © Check the First ar Log Inbound/Outbound traffic F	(PFS): r I Check I Ss d Last IP Addre	DES none PSec_VPN 6 (5-600 Seco 6 (1-10 Secon (1-10)	SHA1		
Related Settings Zone: Connectivity Check Enable Connectivity O Check Method: Check Period: Check Timeout: Check Tail Tolerance: Check Tail Tolerance: Check This Addre Check the First ar Log Inbound/Outbound traffic I Outbound Traffic	(PFS): r I Check I SS Ind Last IP Addre	DES none PSec_VPN 6 (5-600 Seco 6 (1-10 Secon (1-10)	SHA1		
Related Settings Zone: Connectivity Check Enable Connectivity Of Check Method: Check Period: Check Timeout: Check Timeout: Check Tail Tolerance: Check This Addre Check the First ar Log Inbound/Outbound traffic M Outbound Traffic	(PFS): r I Check I SS Ind Last IP Addre	DES none PSec_VPN 6 (5-600 Second (1-10 Second (1-10) ess in the Remote Polic	SHA1		
Related Settings Zone: Connectivity Check Enable Connectivity Oneck Check Method: Check Period: Check Period: Check Timeout: Check Tall Tolerance: Check Tall Tolerance: Check the First ar Check the First ar Dog Inbound/Outbound traffic M Outbound Traffic Source NAT Source:	(PFS): r I Check I SS Ind Last IP Addre NAT	DES ione PSec_VPN 5 (5-600 Seco 6 (1-10 Secon (1-10) ess in the Remote Polic	SHA1		
Related Settings Zone: Connectivity Check Enable Connectivity Check Enable Connectivity C Check Method: Check Period: Check Timeout: Check Tail Tolerance: Check This Addre Check the First ar Log Inbound/Outbound traffic M Outbound Traffic Source NAT Source: Destination:	(PFS): r I Check I SS Ind Last IP Addre IAT	DES	SHA1		
Related Settings Zone: Connectivity Check Enable Connectivity Check Enable Connectivity Check Check Method: Check Period: Check Timeout: Check Fail Tolerance: Check This Addre Check this Addre Source NAT Source: Destination: SNAT: Inbound Traffic	(PFS): r I Check I SS Ind Last IP Addre IAT	DES ione PSec_VPN 5 (5-600 Seco 6 (1-10 Secon (1-10) ess in the Remote Polic	SHA1		
Related Settings Zone: Connectivity Check Enable Connectivity Check Enable Connectivity Check Check Method: Check Period: Check Timeout: Check Tail Tolerance: Check This Addre Check This Addre Check the First ar Log Inbound/Outbound traffic M Outbound Traffic Source: Destination: SNAT: Inbound Traffic Source NAT	(PFS): r I Check I SS Md Last IP Addr NAT	DES ione PSec_VPN 5 (5-600 Seco 6 (1-10 Secon (1-10) ess in the Remote Polic Please select one Please select one	SHA1		
Related Settings Zone: Connectivity Check Enable Connectivity C Check Method: Check Period: Check Period: Check Timeout: Check Tail Tolerance: Check This Addre Check the First ar Log Inbound/Outbound traffic I Cottbound Traffic Source: Destination: SNAT: Inbound Traffic Source NAT Source NAT Source NAT	(PFS): r I Check I SS Ind Last IP Addre MAT	DES Ione PSec_VPN 5 (5-600 Seco 6 (1-10 Secon (1-10) ess in the Remote Polic Please select one Please select one Please select one	SHA1		
Related Settings Zone: Zone: Connectivity Check Enable Connectivity C Check Method: Check Period: Check Period: Check Timeout: Check Fail Tolerance: Check This Addre Check the First ar Log Inbound/Outbound traffic M Outbound Traffic Source: Destination: Source NAT Source: Destination:	(PFS): r I Check I Sss ad Last IP Addre NAT	DES	SHA1		
Related Settings Zone: Connectivity Check Enable Connectivity C Check Method: Check Period: Check Period: Check Timeout: Check Fail Tolerance: Check This Addre Check the First ar Log Inbound/Outbound traffic M Outbound Traffic Source: Destination: SNAT: Inbound Traffic Source NAT Source: Destination: SNAT:	(PFS): r I Check I Sss ad Last IP Addre NAT	DES Ione PSec_VPN 5 (5-600 Seco 6 (1-10 Secon (1-10) ess in the Remote Polic Please select one Please select one Please select one	SHA1		
Related Settings Zone: Connectivity Check Enable Connectivity C Check Method: Check Period: Check Period: Check Timeout: Check Tail Tolerance: Check Tail Tolerance: Check This Addre Check the First ar Log Inbound/Outbound traffic M Outbound Traffic Source: Destination: SNAT: Inbound Traffic Source: Destination: SNAT:	(PFS): r I Check I SS Ind Last IP Addre IAT	DES	SHA1		
Related Settings Zone: Connectivity Check Enable Connectivity C Check Method: Check Period: Check Period: Check Timeout: Check Fail Tolerance: Check This Addre Check the First ar Log Inbound/Outbound traffic M Outbound Traffic Source: Destination: SNAT: Inbound Traffic Source NAT Source: Destination: SNAT:	(PFS): r I Check I SS Ind Last IP Addre IAT	DES	SHA1	Name or IP Address)	

Step 7. After setting the rule, the user can select the rule and click on the **Connect** button to establish the VPN link. Once the tunnel is established, a **connected** icon will be displayed in front of the rule.

ZyXEL USG40W			Welcome ad	min <u>Logout</u> ?He	Help Z About 🛉 Site Map	CObject Reference	🖵 Console 🖸	a
CONFIGURATION	VPN Connection VPN	N Gateway Concentrator Configuration	n Provisioning					
7¥ Quick Setup ⊞ Licensing	Global Setting							
Wireless Network Interface	and the second s	control dynamic IPSec rules ent' setting in IP header 🛛 🛐						
Routing DDNS	IPv4 Configuration							
NAT HTTP Redirect	🔕 Add 📝 Edit 🍟 Rem	nove 💡 Activate 🖗 Inactivate 🍓 Connect 🙀	b Disconnect 📷 Object Reference					
	# Status	Name	VPN Gateway		Policy			
UPnP IP/MAC Binding	1 💡 🚱	To_PPPOE40W_VPN	To_PPPOE40W_GW		LAN1_SUBNET	7- PPPOE40W_LAN		
IP/MAC Binding DNS Inbound LB	14 4 Page 1 of 7	1 🕨 🕅 Show 50 💙 items				Displayin	ng 1 - 1 of 1	
Web Authentication								

Step 8. When the VPN tunnel is established, the user can find the SA information on **MONITOR > VPN MONITOR > IPSec**.

IPv6

Step 1. Add an IPV6 VPN phase I on USG1. Go to CONFIGURATION > VPN > IPSec

VPN > VPN Gateway.

My Address: 2002:3b7c:a397:2:ee43:f6ff:fefc:c4b3

Peer Gateway Address: 2002:3b7c:a397:2:b2b2:dcff:fe70:c1d6

Pre-Shared Key: 12345678

Add VPN Gateway			? ×
III Show Advanced Settings			
General Settings			- 11
Enable			
VPN Gateway Name:	USG1_GW		
Gateway Settings			
Ny Addrose			- 11
IPv6:	2002:3b7c:	a397:2:ee43:f6ff:fefc:c4b3	
Peer Gateway Address			
Static Address	Primary	2002:3b7c:a397:2:b2b2:dcff:fe70:c1d6	
	Secondary	::	
Fall back to Primary Peer Ga	ateway when po	ossible	
Fall Back Check Interval:	300	(60-86400 seconds)	
O Dynamic Address			
Authentication			
Pre-Shared Key	•••••		
unmasked			
Certificate	default	✓ (See <u>My Certificates</u>)	
		OK Cance	el

Step 2. Add an IPv6 VPN phase II on USG1. Go to CONFIGURATION > VPN > IPSec

VPN > VPN Connection.

VPN Gateway: USG1_GW

Local policy: 2002:3b7c:a397:2222::/64

Remote policy: 2002:3b7c:a397:1111::/64

Add VPN Connection				? ×
🔟 Show Advanced Settings 🛅 Create n	ew Object•			
General Settings				
Enable				
Connection Name:	USG1_Conn			
VPN Gateway				
Application Scenario				
 Site-to-site Site-to-site with Dynamic Peer 				
 Remote Access (Server Role) 				
Remote Access (Client Role)				
VPN Gateway:	USG1_GW	*	2002:3b7c:a397:2:ee43:f6ff.fefc:c4b3 2002:3b7c:a397:2:b2b2:dcff:	fe70:c1d6, ::
Policy				
Local policy:	LAN1_SUBNET_DHCPv6	~	INTERFACE SUBNET, 2002:3b7c:a397:2222::1/64(DHCPv6)	
Remote policy:	remote_v6	~	SUBNET, 2002:3b7c:a397:1111::/64	
Phase 2 Setting				
SA Life Time:	86400	(180	- 3000000 Seconds)	

Step 3. Add an IPV6 VPN phase I on USG2. Go to **CONFIGURATION > VPN > IPSec**

VPN > VPN Gateway.

My Address: 2002:3b7c:a397:2:b2b2:dcff:fe70:c1d6

Peer Gateway Address: 2002:3b7c:a397:2:ee43:f6ff:fefc:c4b3

Pre-Shared Key: 12345678

Add VPN Gateway			? X
Show Advanced Settings			
General Settings			
Enable			
VPN Gateway Name:	USG2_GW		
Gateway Settings			
My Address			
IPv6:	2002:3b7c	:a397:2:b2b2:dcff:fe70:c1d6	
Peer Gateway Address			
Static Address	Primary	2002:3b7c:a397:2:ee43:f6ff:fefc:c4b3	
	Secondary	::	
Fall back to Primary Peer 0	ateway when p	ossible	
Fall Back Check Interval:	300	(60-86400 seconds)	
Oynamic Address			
Authentication			
Pre-Shared Key	•••••		
🔲 unmasked			
Certificate	default	 (See <u>My Certificates</u>) 	

Step 4. Add an IPV6 VPN phase II on USG2. Go to **CONFIGURATION > VPN > IPSec**

VPN > VPN Connection.

VPN Gateway: USG2_GW

Local policy: 2002:3b7c:a397:1111::/64

Remote policy: 2002:3b7c:a397:2222::/64

Add VPN Connection		
Show Advanced Settings 🛅	Create new Object •	
General Settings		
V Enable		
Connection Name:	USG2_Conn	
PN Gateway		
Application Scenario		
Site-to-site		
Site-to-site with Dyna	imic Peer	
Remote Access (Ser	ver Role)	
Remote Access (Clie	ent Role)	
VPN Gateway:	USG2_GW	2002:3b7c:a397:2:b2b2:dcff.fe70:c1d6 2002:3b7c:a397:2:ee43:f6ff.fefc:c4b
olicy		
Local policy:	LAN1_SUBNET_DHCPv6	INTERFACE SUBNET, 2002:3b7c:a397:1111::1/64(DHCPv6)
Remote policy:	remote <u>v6</u>	SUBNET, 2002:3b7c:a397:2222::/64
Phase 2 Setting		
SA Life Time:	86400 (1	80 - 3000000 Seconds)

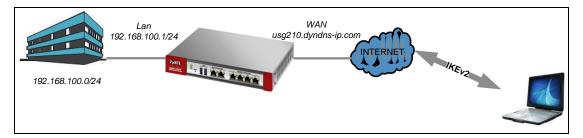
Step 5. When the VPN tunnel is established, the user can find the SA information on

MONITOR > VPN MONITOR > IPSec.

Scenario 5 — Connect to USG using IPSec

IKEv2 in Windows 7

5.1 Application Scenario



Windows 7 supports IPSec IKEv2 with certificate authentication.

This section provides information on how to configure the IKEv2 (Internet Key Exchange) on a Windows 7 PC via certificates.

5.2 Configuration Guide

Network Conditions:

USG 210:

- WAN1 IP: usg210.dyndns-ip.com
- Local subnet: 192.168.100.0/24

USG-210 VPN Conditions:

Phase 1:

- Authentication Method: Certificate
- Local /Peer ID type: DNS / Any
- Encryption and Authentication Algorithm: 3DES/SHA1, AES128/MD5, AES128/SHA1
- Key Group: DH2

Goal to achieve:

Establish an IPSec VPN tunnel from Windows 7 using IKEv2 protocol.

Step 1. Go to **CONFIGURATION > Object > Certificate > My Certificates tab** to add a new certificate for Windows clients.

Name:	CER_For_Windows					
bject Information						
Host IP Address						
Host Domain Name	usg210.dyndns-ip.com	Mus	t select and fill in FQDN			
🔘 E-Mail						
Organizational Unit:		(Optional)				
Organization:		(Opt	ional)			
Town (City):		(Optional)				
State (Province):		(Opt	ional)			
Country:		(Opt	ional)			
Кеу Туре:	RSA	~				
Key Length:	2048	~	bits			
Extended Key Usage						
Server Authentication Client Authentication iKEIntermediate	ust select iKEIntermediate					

Step 2. Go to **CONFIGURATION > Object > User/Group** to create a user account. Add this account into IKEv2 users group object. This group object will be used in IPSec VPN phase-1 EAP (Extended Authentication Protocol) field.

ZyXEL USG210			Welcome admin Logout ?Help Z About \$Site M	ap 🖙 Object Reference 🖵 Console 🛙
CONFIGURATION	User Group Setting			
TV Quick Setup	Configuration			
Wireless	🔘 Add 📝 Edit 🍟 Remove 🔚 Object Refer	ence		
 Network Web Authentication 	# User Name	User Type	Description	Reference
Security Policy	1 admin	admin	Administration account	0
VPN	2 Idap-users	ext-user	External LDAP Users	0
BWM UTM Profile	3 radius-users	ext-user	External RADIUS Users	0
Device HA	4 ad-users	ext-user	External AD Users	0
Object	5 spark	user	Local User	0
Zone User/Group	4 4 Page 1 of 1 ▶ ▶ Show 50) 🗸 items		Displaying 1 - 5 of 5
CONFIGURATION TY Quick Se Licensing Wireless	Configuration			
Network	🔘 Add 📝 Edit 🍟 Remove 🏣 Obj	ect Reference		
Web Authentication	# Group Name 🔺	Description	Member	
	1 IKEv2_users		spark	
VPN BWM	4 4 Page 1 of 1 ▶ ▶	Show 50 👻 items		
	Z Edit Group IKEv2_users		? ×	
	Configuration			
	comguration		-	
- User/Group	Name: IKEv2_	users		
	Description:	(Optional)		
 Application Address 				
- Service	Member List			
	Available	Member		
	Object	Object		
	ad-users Idap-users	spark		
 Certificate ISP Account 	radius-users			
 ISP Account SSL Application 	Tadius-users	•		
		+		

Step 3. Go to **CONFIGURATION > VPN > IPSec VPN > VPN Gateway** to open the configuration screen.

Step 4. Click on the Add button to add a VPN gateway rule.

ZyXEL USG210							Welcome admin <u>Logo</u>	<u>it</u> YHelp Z About T Site Map G	🛛 Object Reference 🚽 Console 📼
CONFIGURATION	V	PN Conr	nection	VPN Gateway	Concentrator	Configuration Provisioning			
T¥ Quick Setu E Licensing Wireless		IPv4 Configuration							
Writeless Network Web Authentication			d Z Edit	TRemove 💡 Activ	zate 🖗 Inactivate	My Address	Secure Gateway	VPN Connection	IKE Ver
Security Policy		1	P	Windows_IKEv2_	GW	a wan1_ppp	0.0.0.0	For_Windows_Clinet_Conn	IKEv2
 VPN IPSec VPN SSL VPN SSL VPN L2TP VPN RWM 		14 4	Page 1	of1 ▶ ▶ !	Show 50 👻 ter	ns			Displaying 1 - 1 of 1

Step 5. To configure the VPN gateway rule, the user needs to fill-in:

- VPN gateway name:
- IKE Version: IKEv2
- Gateway address: both local (My Address) and peer (Dynamic Address)
- Authentication setting:
 - Certificate
- Phase-1 setting
 - Encryption and Authentication Algorithm:
 - 1) 3DES / SHA1
 - 2) AES128 / MD5
 - 3) AES128 / SHA1
 - 4) Key Group DH2
- Extended Authentication Protocol:
 - Enable Extended Authentication Protocol Server Mode
 - AAA Method: default
 - Allowed User: IKEv2_users

Hide Advanced Settings 🛅 Create	e new Object 🗸
eneral Settings	
Enable	
VPN Gateway Name:	Windows_IKEv2_GW
KE Version	
IKEv1 IKEv2	
Ay Address Interface	wan1_ppp
Domain Name / IPv4	
Peer Gateway Address	
Static Address 1	Primary 0.0.0.0
	Secondary 0.0.0.0
Fall back to Primary Peer (Gateway when possible
Fall Back Check Interval:	300 (60-86400 seconds)
Oynamic Address]
	J
uthentication	
Pre-Shared Key	000000000
unmasked	
Oertificate	CER_For_Windows Y (See <u>My Certificates</u>)
Local ID Type:	DNS
Content:	usg210.dyndns-ip.com
Peer ID Type:	Any 👻
Content:	
lboos & Cattings	
hase 1 Settings SA Life Time:	86400 (180 - 3000000 Seconds)
Proposal	
	🐼 Add 🔜 Edit 🧃 Remove
	# Encryption _ Authentication 1 3DES SHA1
	2 AES128 MD5
	3 AES128 SHA1
X1811 (1965)	
Key Group:	DH2
xtended Authentication Protocol	
Enable Extended Authenticatio	on Protocol 🛐
Allowed Auth Method:	mschapv2
 Server Mode 	Histripy2
AAA Method:	default 🗸
Allowed User:	
	IKEv2_users
Client Mode	
User Name : Password:	

Step 6. Go to **CONFIGURATION > Object > Address** to create an address object. This

ZyXEL USG210 CONFIGURATION Address Group IPv4 A ss Configuration 🛇 Add 📝 Edit 🍵 Remove 🔚 Object Reference Name -DMZ_SUBNET dmz-192.168.3.0/24 ACE SUBNE 192.88.99.1 IP6to4-Relay lan1-192.168.100.0/24 lan2-192.168.2.0/24 wan1_ppp-111.250.186.198 LAN1_SUBNET INTERFACE SUBNET INTERFACE SUBNET TERFACE IP Page 1 of 1 🕨 🕅 Show 50 Edit Address Rule Windo ws_Client_F Name Windows_Client_Pool Address Type: RANGE * Starting IP Address: 172.16.1.10 End IP Address: 172.16.1.20 OK Cancel

address object's IP address will be assigned to the Windows IKEv2 client's machine.

Step 7. Go to **CONFIGURATION > VPN > IPSec VPN > VPN Connection** to open the configuration screen to configure the phase-2 rule.

Step 8. Click on the **Add** button to add a rule.

Z	YXEL USG210			Wekome admin <u>Loqout</u>	?Help Z About	Site Map GObject Reference	🖵 Console 🖾 CLI			
	CONFIGURATION	VPN Connection	VPN Gateway Concentrator Config	uration Provisioning						
0	TV Quick Setup E Licensing Wireless Network Web Authentication Security Policy VPN		ute to control dynamic IPSec rules ragment' setting in IP header 🛛 🚦							
	IPSecVPN SSLVPN	IPBecVPNI Sa VPNI Sa VPNI S								
	L2TP VPN	# Status	Name	VPN Gateway	F	Policy				
	BWM UTM Profile	1 💡 🗞	For_Windows_Clinet_Conn	Windows_IKEv2_GW		LAN1_SUBNET/				
	Device HA	14 4 Page 1	of 1 > > Show 50 vitems			Display	ring 1 - 1 of 1			

Step 9. To configure the phase-2 rule, the user needs to fill-in:

- VPN connection name
- VPN gateway selection
- Policy for
 - Local network side
- Configuration Payload
 - Enable Configuration Payload
 IP Address Pool:
- Phase-2 setting
 - Active protocol
 - Encapsulation mode
 - Encryption algorithm
 - Authentication algorithm
 - Perfect Forward Secrecy

Edit VPN Connection For_Window	ws_Clinet_Conn				
Hide Advanced Settings 🛅 Create i	new Object +				
General Settings					
Enable					
Connection Name:	For_Windows_Clinet_C	onn			
Nailed-Up					
Enable Replay Detection					
Enable NetBIOS broadcast over	IPSec				
MSS Adjustment					
Custom Size	0	(200) - 1460 Bytes)		
Auto					
Varrowed					
VPN Gateway					
Application Scenario					
Site-to-site					
Site-to-site with Dynamic Pe	er				
Remote Access (Server Role	e)				
Remote Access (Client Role	ə)				
VPN Gateway:	Windows_IKEv2_GW	~	wan1_ppp 0.0.0.0, 0	0.0.0	
	d.				
Policy					
Local policy:	LAN1_SUBNET	~	INTERFACE SUBNET	, 192.168.100.0/24	
Enable GRE over IPSec					
Configuration Payload					
		_			
Enable Configuration Payload		-			
IP Address Pool:	Windows_Client_Pool	~	RANGE, 172.16.1.10-	172.16.1.20	
First DNS Server (Optional):	1.1.1.1				
Second DNS Server (Optional):	2.2.2.2				
First WINS Server (Optional):	3.3.3.3				
Second WINS Server (Optional):	4.4.4.4				
Phase 2 Setting					
SA Life Time:	86400	(180	0 - 3000000 Seconds)	en	
Active Protocol:	ESP	~			
Encapsulation:	Tunnel	~			
Proposal	🗿 Add 🔜 Edit. 🍵 Rei	move			
	# Encryption	1	uthentication		
	1 3DES		HA1		
	2 AES128		HA256		
	3 AES256	SI	HA1		
			-		
Perfect Forward Secrecy (PFS):	none	*			
Related Settings					
		11.51	-		
Zone:	IPSec_VPN	~			
Connectivity Check					
	1				
Check Method:	licmp	~			
Check Period:	(5-600 Sec				
Check Timeout:	(1-10 Seco	nas)			
Check Fail Tolerance:	(1-10)				
Check This Address		(Do)	main Name or IP Addres	5)	
Check the First and Last IP /	Address in the Remote Poli	су			
E Log					
Inbound/Outbound traffic NAT					
Outbound Traffic					
Source NAT					
		~			
Source:		~			
Source: Destination:	Please select one				
	Please select one Please select one	~			
Destination:		~			
Destination: SNAT:		~			
Destination: SNAT: Inbound Traffic		~			
Destination: SNAT: Inbound Traffic Source NAT		*			
Destination: SNAT: Inbound Traffic Source NAT Source:		> > >			
Destination: SNAT: Inbound Traffic Source NAT Source: Destination: SNAT:		> > > >			
Destination: SNAT: Inbound Traffic Source NAT Source: Destination: SNAT: Destination NAT		> > > >			
Destination: SNAT: Inbound Traffic Source NAT Source: Destination: SNAT:	Please select one Please select one Please select one Please select one	× × ×	nal Port S Original Po		

30

Step 10. Export the certificate, which was generated in step 1, and save it to the Windows 7 machine.

onfiguration	
Name:	CER_For_Windows
ertification Path	
CN=usg210.dyndns-ip.com Validation Result=self-signed	
Refresh	
ertificate Information	
Туре:	Self-signed X.509 Certificate
Version:	V3
Serial Number:	1396161402
Subject:	CN=usg210.dyndns-ip.com
Issuer:	CN=usg210.dyndns-ip.com
Signature Algorithm:	rsa-pkcs1-sha1
Valid From:	2014-03-30 06:36:42 GMT
Valid To:	2017-03-29 06:36:42 GMT
Key Algorithm:	rsaEncryption (2048 bits)
Subject Alternative Name:	usg210.dyndns-ip.com
Key Usage:	DigitalSignature, KeyEncipherment, DataEncipherment, KeyCertSign
Extended Key Usage:	ServerAuthentication, ClientAuthentication, iKEIntermediate
Basic Constraint:	Subject Type=CA, Path Length Constraint=1
MD5 Fingerprint:	eb:1e:f0:f9:e5:ca:04:81:5e:0f:fc:48:d5:8c:e9:34
SHA1 Fingerprint:	ec:8e:71:ef:ef:66:d9:f1:b2:a6:59:93:e8:ee:a3:93:b5:79:35:44
ertificate in PEM (Base-64) Enc	oded Format
BEGIN X509 CERTIFICATE	
2cyMTAuZHluZG5zLWlwLmNvb	TAeFw0xNDAzMzAwNjM2NDJaFw0xNzAzMjkwNjM2 ZzIxMC5keW5kbnMtaXAuY29tMIIBIjANBgkghkiG
	Password:

Step 11. In the Windows 7 machine, go to Start > mmc >

Programs (1)	
See more results mmc ×	Shut down

Step 12. In the mmc console, click on File > Add/Remove Snap-in... >

	ile1 - [Console Root]			
	Action View Favorite	s Window Help Ctrl+N		- 8
	New	Ctrl+N Ctrl+O		
	Open Save	Ctrl+S		Actions
	Save As	Ctil+3	tems to show in this view.	Console Root
				More Actions
	Add/Remove Snap-in	Ctrl+M		
(Options			
1	1 C:\Windows\system32\compmgmt			
I	Exit			
			_	
bles yo	o <mark>u to add snap-ins to or re</mark> r	nove them from the shap-	in console.	

OK

Cancel

Step 13. In the left panel, select the Certificates and click on the Add button. X Add or Remove Snap-ins -You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled. Available snap-ins: Selected snap-ins: Vendor Console Root . Edit Extensions... Snap-in ActiveX Control Microsoft Cor... Remove Authorization Manager Microsoft Cor... Certificates Microsoft Cor... Е Component Services Microsoft Cor... Move Up Ecomputer Managem... Microsoft Cor... Move Down -Device Manager Microsoft Cor... Add > Disk Management Microsoft and... Event Viewer Microsoft Cor... Folder Microsoft Cor... Group Policy Object ... Microsoft Cor... IP Security Monitor Microsoft Cor... 😓 IP Security Policy M... Microsoft Cor... Link to Web Address Microsoft Cor... Advanced... Description: The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

Step 14. Select the **Computer account > Next button > select Local computer > Finish** button **> OK** button.

ertifica	ates snap-in	and addresses.	or or share			×
	s snap in will alway	s manage certifica	tes for:			
	My user account					
_	Service account					
0	Computer account					
-						
			1	< Back	Next >	Cancel
			-		TTSML F	00/100

his snap-in will always mar	nage:
) Local computer: (the c	omputer this console is running on)
) Another computer:	Browse

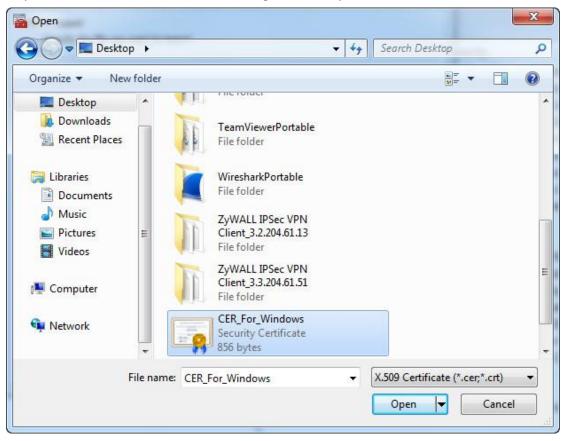
vailable snap-ins: Snap-in	Vendor	*	Ĩ	elected snap-ins: Console Root	Edit Extensions
ActiveX Control	Microsoft Cor Microsoft Cor			Certificates (Local Computer)	Remove
Certificates	Microsoft Cor Microsoft Cor	ш			Move Up
Computer Managem Device Manager Disk Management	Microsoft Cor Microsoft Cor Microsoft and		Add >	[Move Down
Event Viewer Folder	Microsoft Cor Microsoft Cor				
Group Policy Object	Microsoft Cor				
IP Security Policy M		-			Advanced
escription:					

Step 15. Open up the **Certificates (Local Computer) > Trusted Root Certification Authorities >** right-click on **Certificate > All Tasks > Import**.

ZyXEL – USG Application Notes

onsole Root	Issued To	Issued By	Expiration Date	Intended P	Actions
Image: Section of the section of	re ert High Assurance EV Ro st.net Certification Author x Secure Certificate Author ust Global CA ISign Root CA iyberTrust Global Root	Class 3 Public Primary Certificatio Copyright (c) 1997 Microsoft Corp. DigiCert Assured ID Root CA DigiCert High Assurance EV Root Entrust.net Certification Authority Equifax Secure Certificate Authority GeoTrust Global CA GlobalSign Root CA GTE CyberTrust Global Root Microsoft Authenticode(tm) Root Microsoft Root Certificate Authori NO LIABILITY ACCEPTED, (c)97 V Thawte Premium Server CA Thawte Timestampi CA usg210.dyndns-ip.com UTN - DATACorp SGC	2004/1/8 2021/1/1 2021/1/1 2017/3/29 2019/6/25	Intended P Server Autl Secure Em: Secure Em: Secure Em: Time Stam Server Autl Server Autl Server Autl Secure Em: Secure Em: <all> Time Stam Server Autl Secure Em: <all></all></all>	Actions Certificates More Actions

Step 16. Select the certificate, which was generated by the USG.



Step 17. Create the Windows IPSec connection profile.

🚱 📠 Connect to a Workpla	ace	
Type the Internet a	ddress to connect to	
Your network administra	ator can give you this address.	
Internet address:	usg210.dyndns-ip.com	
Destination name:	IKEv2 Connection	
This option allow	l ple to use this connection vs anyone with access to this computer to use this conne ow; just set it up so I can connect later	ction.
	(Next Cancel

Connect to a Workpla	ice	
Type your user nar	ne and password	
User name:	spark	1
Password:	1234	1
	Show characters	
	Remember this password	1
Domain (optional):		
		Create

Step 18. Modify the IPSec connection profile. Go to **Security** > **Type of VPN:** IKEv2

Data encryption: Requires encryption (disconnect if server declines) **Authentication:** Use Extensible Authentication Protocol (EAP)

eneral Options Security	Networking Sharing
Type of VPN:	
IKEv2	
)ata encryption:	Advanced settin
Require encryption (disconr	nect if server declines)
Authentication Use Extensible Authent	tication Protocol (EAP)
Microsoft: Secured pas	ssword (EAP-MSCHAP v2) (encry) 🤜
	Flopenies
Use machine certificate	Properties

Step 19. Modify IPSec connection profile. Go to **Networking** > and disable the **TCP/IPv6** checkbox.

Note: USG 4.10 firmware does not support multiple proposals. It only supports IPv4 proposal selection.

	urity Networking Sha	aring
This connection uses th	ie following items:	
Martin and States	ol Version 6 (TCP/IPv6)	Ū
	ol Version 4 (TCP/IPv4)	tunda
Client for Micros	Sharing for Microsoft Ne oft Networks	etworks
Install	Uninstall	Properties
Description		
TCP/IP version 6. Th	ne latest version of the i	nternet protocol
that provides commun networks.	nication across diverse	interconnected
HELWOIKS.		

Step 20. Establish the IPSec tunnel from the Windows 7 machine, and the tunnel will be established successfully.



ZyXEL – USG Application Notes

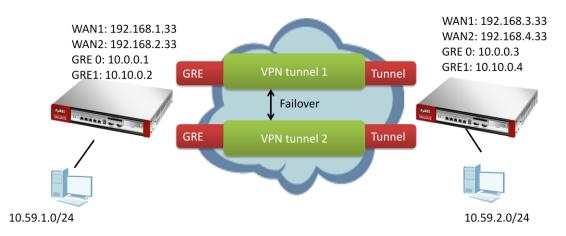
General Details		Network Connection Deta	ls:
Connection		Property	Value
IPv4 Connectivity: IPv6 Connectivity: Media State:	No network access No network access Connected	Connection-specific DN. Description Physical Address DHCP Enabled	IKEv2 Connection
Duration:	00:00:38	IPv4 Address IPv4 Subnet Mask IPv4 Default Gateway	172.16.1.14 255.255.255.255
Activity		IPv4 DNS Servers	1.1.1.1 2.2.2.2 3.3.3.3 4.4.4.4
Sent — Sent — Sent —	Received	NetBIOS over Topip En.	Yes
Compression: 0 %	0 %		
Errors: 0	0	v	
Properties Disconnect Dia	agnose	ic	

Scenario 6 — GRE over IPSec VPN

Tunnel –VPN Failover

6.1 Application scenario

We want to use VPN tunnels to transfer important files between the branch Office and HQ. To prevent the network from getting disconnected, we configure four WAN interfaces to do redundancy. Now, we want to establish two VPN tunnels between the two USGs to perform failover, to ensure that the transfer will not be interrupted when the first connection encounters a problem. This will create a stable environment for the transfer.



6.2 Configuration Guide

Network conditions:

USG1

- WAN1 IP: 192.168.1.33
- WAN2 IP: 192.168.2.33
- GRE tunnel interface1: 10.0.0.1
- GRE tunnel interface2: 10.10.0.2

USG2

- WAN1 IP: 192.168.3.33
- WAN2 IP: 192.168.4.33
- GRE tunnel interface1: 10.0.0.3
- GRE tunnel interface2: 10.10.0.4

Goals to achieve:

Use GRE over IPSec VPN to perform the VPN fail-over. USG configuration Step 1. Add two GRE tunnels on USG1. Go to CONFIGURATION > Tunnel.

Add the first tunnel IP Address: 10.0.0.1, Subnet Mask: 255.255.255.0 My Address: WAN1, Remote Gateway Address: 192.168.3.33

🔾 Edit Tunnel	Turned Distance Income		?
Show Advanced Settings			
General Settings			
Enable			
Interface Properties			
Interface Name:	tunnel0		
Zone:	TUNNEL	▼ 1	
Tunnel Mode:	GRE	~	
IP Address Assignment			
IP Address:	10.0.0.1		
Subnet Mask:	255.255.255.0		
Metric:	0 (0-15)		
Gateway Settings			
My Address			
Interface	wan1	 DHCP client 192.168.1.33/25 	5.255.255.0
IP Address	0.0.00		
Remote Gateway Address:	192.168.3.33]	

Place a check in the **Enable Connectivity Check** checkbox. Ensure that the Address is the remote GRE tunnel interface.

📀 Edit Tunnel	Turner 1	an I an I a c		? X
Show Advanced Settings				
Connectivity Check				
Enable Connectivity Check				
Check Method:	icmp	~		
Check Period:	10	(5-600 seconds)		
Check Timeout:	3	(1-10 seconds)		
Check Fail Tolerance:	3	(1-10)		
Check this address:	10.0.0.3	3	(Domain Name or IP Address)	
Related Setting Configure <u>WAN_TRUNK</u> Configure <u>Policy Route</u>				-

b. Add the second tunnel

IP Address: 10.10.0.2, Subnet Mask: 255.255.255.0 My Address: WAN2, Remote Gateway Address: 192.168.4.33

O Edit Tunnel approved Caluar a	Tunnel VLAN Bridge Trunk	? ×
Show Advanced Settings		
General Settings		
🕼 Enable		
Interface Properties		
Interface Name:	tunnel1	
Zone:	TUNNEL	
Tunnel Mode:	GRE	
IP Address Assignment		
IP Address:	10.10.0.2	
Subnet Mask:	255.255.255.0	
Metric:	0 (0-15)	
Gateway Settings		
My Address		
Interface	wan2 DHCP client 192.168.2.33/255.255.255.0	
IP Address	0.0.0.0	
Remote Gateway Address:	192.168.4.33	

Place a check in the **Enable Connectivity Check** checkbox. Ensure that the Address is the remote GRE tunnel interface.

nectivity Check		
Enable Connectivity Check		
Check Method:	icmp 🗸	
Check Period:	10 (5-600 seconds)	
Check Timeout:	3 (1-10 seconds)	
Check Fail Tolerance:	3 (1-10)	
Check this address:	10.10.0.4	(Domain Name or IP Address)

Step 2. Add a GRE tunnel trunk on USG1. Go to CONFIGURATION > Network > Interface > Trunk.
 gre_trunk member:
 tunnel0: Active
 tunnel1: Passive

	CONFIGURATION	Port Role	Ethernet	РРР	Cellular	Tunnel	VLAN	Bridge	Trunk		
	📲 Quick Setup	🛄 Show Adv	anced Setting	;							
@	 Licensing Wireless Network Interface Routing 	Configurati	on nnect Connect	ions Befo	re Falling Ba	ack 🚺					
	+ DDNS	Default WA	N Trunk	k							
	• NAT • HTTP Redirect • ALG	Oefault Trunk Selection SYSTEM_DEFAULT_WAN_TRUNK									
	IP/MAC Binding DNS Inbound LB Web Authentication	User Config	ser Configured Juration	Trunk	Please s	elect one		*			
	 Becurity Policy ♥ VPN ♥ BWM ♥ UTN Parafile 		🖉 Edit 🍵 Rer	nove ा 📑	Object Refer	rence	Algo	rithm			
	⊕ Object										
0	Add Trunk									? ×	
0	Name:		gre_tru	ink							
	Load Balancing Algorithr	m:	Least L	oad Firs	st	~					
	Load Balancing Index(e	5):	Outbou	ınd		~					
a contraction of the second	🔘 Add 🛃 Edit 🍵 Rer	move 📣 Me	ove								
	# Member	Mo	de		Egres	s Bandwi	dth				
	1 tunnel0	Act	ive		10485	576 kbps					
	2 tunnel1	Pa	ssive		10485	576 kbps					
	d d Page 1 of	1 🕨 🕅	Show 50	V	tems		No	data to d	isplay		

Step3. Add two IPSec VPN tunnels on USG1. Go to **CONFIGURATION > VPN > IPSec VPN**.

Add two VPN gateway policies.
 First VPN Gateway policy (USG1 wan1 to USG2 wan1)
 My Address: wan1, Peer Gateway Address: 192.168.3.33
 Pre-Shared Key: 12345678

Edit VPN Gateway GRE0_GW	Configura	ition Provisioning	? X
🔟 Show Advanced Settings 🛅 Create n	ew Object 🕶		
General Settings			
Enable			
VPN Gateway Name:	GRE0_GW		
IKE Version			
IKEv1			
IKEv2			
Gateway Settings			- 11
My Address			
Interface	wan1	DHCP client 192.168.1.33/255.255.255.0	
Domain Name / IPv4			
Peer Gateway Address			
Static Address []	Primary	192.168.3.33	
	Secondary	0.0.0.0	
Fall back to Primary Peer Gate	way when po	ossible	
Fall Back Check Interval:	300	(60-86400 seconds)	
Dynamic Address 1			
Authentication			- 11
Pre-Shared Key	•••••		

Secondary Gateway policy (USG1 wan2 to USG2 wan2) My Address: wan2, Peer Gateway Address: 192.168.4.33 Pre-Shared Key: 12345678

Edit VPN Gateway GRE1_GW	Configura	ation Provisioning	?	×
💷 Show Advanced Settings 🛅 Create r	new Object •			
Enable				
VPN Gateway Name:	GRE1_GW			
IKE Version				
IKEv1				
IKEv2				
Gateway Settings				
My Address				
 Interface 	wan2	 DHCP client 192.168.2.33/255.255.255.0 		
Domain Name / IPv4				
Peer Gateway Address				
Static Address 1	Primary	192.168.4.33		
	Secondary	0.0.0.0		
Fall back to Primary Peer Gat	eway when po	ossible		
Fall Back Check Interval:	300	(60-86400 seconds)		
Dynamic Address				
Authentication				
Pre-Shared Key	•••••			
h Add two VPN Conr	ections			-

b. Add two VPN Connections
 First VPN Connection
 Enable Nailed-Up
 Application Scenario: Site-to-Site
 VPN Gateway: GRE0_GW
 Local policy: 192.168.1.33
 Remote policy: 192.168.3.33

Enable GRE over IPSec

Edit VPN Connection GRE0_Conn	Concentrator L Config	uration Provisioning	? ×
Hide Advanced Settings 🛅 Create ne	w Object •	unadon Providenting	
General Settings			
Enable			
Connection Name:	GRE0_Conn		
Nailed-Up			
Enable Replay Detection			
Enable NetBIOS broadcast over IF	Sec		
MSS Adjustment			
Custom Size	0	(200 - 1460 Bytes)	
Auto			
VPN Gateway			
Application Scenario			
Site-to-site			
Site-to-site with Dynamic Peer			
Remote Access (Server Role)			
Remote Access (Client Role)			
VPN Gateway:	GRE0_GW	 wan1 192.168.3.33, 0.0.0.0 	
Edit VPN Connection GRE0_Conn			
			2 X
	w Object+	uration Provisioning	? 🗙
Hide Advanced Settings 🔚 Create ne	w Object •	uration Provisioning	? ×
Hide Advanced Settings 🛅 Create ne	1	HOST 102 168 1 33	? ×
Hide Advanced Settings Create ne Policy Local policy:	local_gre0	HOST, 192.168.1.33	? ×
Hide Advanced Settings Create ne Policy Local policy: Remote policy:	1		? ×
Hide Advanced Settings Create ne Policy Local policy: Remote policy: C Enable GRE over IPSec	local_gre0		? ×
Hide Advanced Settings Create ne Policy Local policy: Remote policy: Create ne Policy Local policy: Remote policy: Policy Enforcement	local_gre0		? ×
Hide Advanced Settings Create ne Policy Local policy: Remote policy: C Enable GRE over IPSec	local_gre0	HOST, 192.168.3.33	? ×
Hide Advanced Settings Create ne Policy Local policy: Remote policy: Policy Enable GRE over IPSec Policy Enforcement Phase 2 Setting SA Life Time:	local_gre0 remote_gre0 86400	HOST, 192.168.3.33	? ×
Hide Advanced Settings Create ne Policy Local policy: Remote policy: Catable GRE over IPSec Policy Enable GRE over IPSec Policy Enforcement Phase 2 Setting	local_gre0 remote_gre0	 HOST, 192.168.3.33 (180 - 3000000 Seconds) 	? ×
 Hide Advanced Settings Create ne Policy Local policy: Remote policy: Enable GRE over IPSec Policy Enforcement Phase 2 Setting SA Life Time: Active Protocol: Encapsulation: 	local_gre0 remote_gre0 86400 ESP Tunnel	 HOST, 192.168.3.33 (180 - 3000000 Seconds) 	? ×
Hide Advanced Settings Create ne Policy Local policy: Remote policy: Policy Enable GRE over IPSec Policy Enforcement Phase 2 Setting SA Life Time: Active Protocol:	local_gre0 remote_gre0 86400 ESP	 HOST, 192.168.3.33 (180 - 3000000 Seconds) 	? ×
 Hide Advanced Settings Create ne Policy Local policy: Remote policy: Enable GRE over IPSec Policy Enforcement Phase 2 Setting SA Life Time: Active Protocol: Encapsulation: 	local_gre0 remote_gre0 86400 ESP Tunnel Add ZEdit TRe # Encryption	 HOST, 192.168.3.33 (180 - 3000000 Seconds) 	
 Hide Advanced Settings Create ne Policy Local policy: Remote policy: Enable GRE over IPSec Policy Enforcement Phase 2 Setting SA Life Time: Active Protocol: Encapsulation: 	local_gre0 remote_gre0 86400 ESP Tunnel Add ZEdit TRe	HOST, 192.168.3.33 (180 - 3000000 Seconds)	
 Hide Advanced Settings Create ne Policy Local policy: Remote policy: Enable GRE over IPSec Policy Enforcement Phase 2 Setting SA Life Time: Active Protocol: Encapsulation: Proposal	local_gre0 remote_gre0 86400 ESP Tunnel Add ZEdit TRe # Encryption	 HOST, 192.168.3.33 (180 - 3000000 Seconds) 	
 Hide Advanced Settings Create ne Policy Local policy: Remote policy: Enable GRE over IPSec Policy Enforcement Phase 2 Setting SA Life Time: Active Protocol: Encapsulation: 	local_gre0 remote_gre0 86400 ESP Tunnel Add ZEdit TRE # Encryption 1 DES	 HOST, 192.168.3.33 (180 - 3000000 Seconds) Authentication SHA1 	
 Hide Advanced Settings Create ne Policy Local policy: Remote policy: Enable GRE over IPSec Policy Enforcement Phase 2 Setting SA Life Time: Active Protocol: Encapsulation: Proposal	local_gre0 remote_gre0 86400 ESP Tunnel Add ZEdit TRE # Encryption 1 DES	 HOST, 192.168.3.33 (180 - 3000000 Seconds) Authentication SHA1 	
 Hide Advanced Settings Create net Policy Local policy: Remote policy: Penable GRE over IPSec Policy Enforcement Phase 2 Setting SA Life Time: Active Protocol: Encapsulation: Proposal Perfect Forward Secrecy (PFS):	local_gre0 remote_gre0 86400 ESP Tunnel Add ZEdit TRE # Encryption 1 DES	 HOST, 192.168.3.33 (180 - 3000000 Seconds) Authentication SHA1 	
 Hide Advanced Settings Create ne Policy Local policy: Remote policy: Enable GRE over IPSec Policy Enforcement Phase 2 Setting SA Life Time: Active Protocol: Encapsulation: Proposal Perfect Forward Secrecy (PFS): Related Settings	local_gre0 remote_gre0 86400 ESP Tunnel ③ Add ⊇ Edit 1 Re # Encryption 1 DES none	 HOST, 192.168.3.33 (180 - 3000000 Seconds) Authentication SHA1 	? ×

Second VPN Connection Enable Nailed-Up Application Scenario: Site-to-Site VPN Gateway: GRE1_GW Local policy: 192.168.2.33 Remote policy: 192.168.4.33 Enable GRE over IPSec

Edit VPN Connection GRE1_Conr	Concentrator Confol	ration	Provisioning	? 🗙
🔲 Hide Advanced Settings 🛅 Create	new Object •			
-				1
General Settings				
V Enable				
Connection Name:	GRE1_Conn			
Nailed-Up				
Enable Replay Detection				
Enable NetBIOS broadcast over	r IPSec			
MSS Adjustment		/200	- 1460 Bytes)	
Custom Size	0	(200	- 1400 Bytes)	
Auto				
VPN Gateway				
Application Scenario				
 Site-to-site 				
Site-to-site with Dynamic Period	er			
Remote Access (Server Rol	le)			
Remote Access (Client Role	e)			
VPN Gateway:	GRE1_GW	~	wan2 192.168.4.33, 0.0.0.0	
Edit VPN Connection GRE1_Conn			Provisioning	? 🗙
Hide Advanced Settings 🔄 Create	new Object*			
		1921		
Local policy:	local_gre1	*	HOST, 192.168.2.33	
Remote policy:	remote_gre1		HOST, 192.168.4.33	
Enable GRE over IPSec Policy Enforcement				
- Folicy Enforcement				
Phase 2 Setting				
SA Life Time:	86400	(180	- 3000000 Seconds)	9
Active Protocol:	ESP	~		
Encapsulation:	Tunnel	~		
Proposal	💿 Add 🔜 Edit 🍵 Rem	ove		
	# Encryption		thentication	
	1 DES	SH	IA1	
Perfect Forward Secrecy (PFS):	none	×	E	
			-	
Related Settings				
Zone:	IPSec_VPN	~	1	
Zone:	IPSec_VPN	*	•	OK Cancel

Step 4. Add a policy routes on USG1. Go to **CONFIGURATION> Network > Routing**.

Source: LAN1_Subnet Destination: Remote subnet Next-Hop: gre_trunk SNAT: none

Add Policy Route			? X
🏢 Show Advanced Settings 🛅 Create new Obje	ect▼		
Configuration			
Enable			
Description:		(Optional)	
Criteria			
User:	any	~	
Incoming:	any (Excluding ZyWALL)	~	
Source Address:	LAN1_SUBNET	×	
Destination Address:	remote_11	~	
DSCP Code:	any	*	
Schedule:	none	*	
Service:	any	•	
Next-Hop			
Type:	Trunk	×	
Trunk:	gre_trunk	*	
		OK Canc	el

Step5. Add two GRE tunnels on the USG2. **Go to CONFIGURATION > Tunnel**.

a. Add first tunnel

IP Address: 10.0.0.3, Subnet Mask: 255.255.255.0

			_	-		
NΛ	/ Address [.]	$W/\Delta N1$	Remote	Gateway	/ Address:	192.168.1.33
	/ / / / / / / / / / / / / / / / / / / /	vv/((v±)	nemote	Guteway	/ / / / / / / / / / / / / / / /	192.100.1.99

Add Tunnel	Tunnel VLAN Bridge Trunk	? >
III Show Advanced Settings		
General Settings		
💟 Enable		
Interface Properties		
Interface Name:	tunnel0	
Zone:	TUNNEL 👻 🚺	
Tunnel Mode:	GRE 👻	
IP Address Assignment		
IP Address:	10.0.03	
Subnet Mask:	255.255.255.0	
Metric:	0 (0-15)	
Gateway Settings		
My Address		
Interface	wan1 Y DHCP client 192.168.	3.33/255.255.255.0
IP Address	0.0.0.0	
Remote Gateway Address:	192.168.1.33	

Place a check in the **Enable Connectivity** Check checkbox. Ensure that the Address is the remote GRE tunnel interface.

Egress Bandwidth:	1048576 Kbps		
onnectivity Check			
Enable Connectivity Check			
Check Method:	icmp 💌		
Check Period:	10 (5-600 seconds)		
Check Timeout:	3 (1-10 seconds)		
Check Fail Tolerance:	3 (1-10)		
Check this address:	10.0.0.1	(Domain Name or IP Address)	
elated Setting			
Configure WAN_TRUNK			
Configure Policy Route			

- b. Add Second tunnel
 - IP Address: 10.10.0.4, Subnet Mask: 255.255.255.0

IVIY AUULESS. WAINZ, NEITIULE UALEWAY AUULESS. 132.100.2.3.	My Address: WAN2	2, Remote Gateway	Address: 192.168.2.33
---	------------------	-------------------	-----------------------

Edit Tunnel ppp Celular		?
Show Advanced Settings		
General Settings		
Enable		
Interface Properties		
Interface Name:	tunnel1	
Zone:	TUNNEL	
Tunnel Mode:	GRE 👻	
IP Address Assignment IP Address: Subnet Mask:	10.10.0.4	
Bublice Hublin	200120012010	
Methe:	0 (0-15)	
	<u>0</u> (0-15)	
Gateway Settings My Address	0 (0-15)	
Gateway Settings	0 (8-15) wan2 ▼ DHCP client 192.168.4.33/255	.255.255.0
Gateway Settings My Address		.255.255.0

Place a check in the **Enable Connectivity** Check checkbox. Ensure that the Address is the remote GRE tunnel interface.

Enable Connectivity Check			
Check Method:	icmp 👻		
Check Period:	10 (5-600 seconds)		
Check Timeout:	3 (1-10 seconds)		
Check Fail Tolerance:	3 (1-10)		
Check this address:	10.10.0.2	(Domain Name or IP Address)	

Step6. Add a GRE tunnel trunk on USG2. Go to CONFIGURATION > Network > Interface > Trunk. gre_trunk member:

tunnel0: Active Tunnel1: Passive

	CONFIGURATION	Port Role	Ethernet	РРР	Cellular	Tunnel	VLAN	Bridge	Trunk
	📲 Quick Setup	Show Adv	anced Setting	5					
	 Licensing Wireless Network Interface Routing DDNS NAT HTTP Redirect ALG IP/MAC Binding 	Default WA Default Tr © SY	nnect Connect	ILT_WAN	_TRUNK	ack 👔		~	
	 DNS Inbound LB Web Authentication Becurity Policy VPN IPSec VPN SSL VPN L2TP VPN RWM 	# Na	Z Edit 📋 Rer		Object Refer		Algo	prithm	
0	Add Trunk								? ×
	Name: Load Balancing Algorith Load Balancing Index(e		gre_tru Least L Outbou	oad Firs	t	*			
1	O Add Z Edit								
	# Member	Mo	de		Egress	Bandwid	th		
	1 tunnel0	Act	ive		10485	76 kbps			
	2 tunnel1	Pa	ssive		10485	76 kbps			
	4 4 Page 1 of	1 ▶ ▶ 	Show 50	- it	ems		No da	sta to dis	hay

Step 7. Add two IPSec VPN tunnels on USG2. **Go to CONFIGURATION > VPN > IPSec VPN**.

а.	Add two VPN Gateways.
	First VPN Gateway
	My Address: wan1, Peer Gateway Address: 192.168.1.33
	Pro-Sharod Kov: 123/15678

The Sharea Rey. 1			
Add VPN Gateway	Configura	tion Provisioning	? ×
III Show Advanced Settings 🛅 Create	new Object•		
🔽 Enable			
VPN Gateway Name:	GRE0_GW		
IKE Version			
IKEv1			
IKEv2			
Gateway Settings			
			- 11
My Address Interface	wan1	DHCP client 192.168.3.33/255.255.255.0	
Domain Name / IPv4			
_			
Peer Gateway Address Static Address	Primary	192.168.1.33	
	Secondary	0.0.0.0	
Fall back to Primary Peer Gat			
Fall Back Check Interval:	300	(60-86400 seconds)	
Dynamic Address	500		
U Dynamic Address			
Authentication			
Pre-Shared Key	•••••		
Second VPN Gatev	wav		
	•		
My Address · wan 2) Door Ga	192 168 2 33	
		ateway Address: 192.168.2.33	
Pre-Shared Key: 12		ateway Address: 192.168.2.33	
Pre-Shared Key: 12 Add VPN Gateway	2345678	ateway Address: 192.168.2.33	? 🗙
Pre-Shared Key: 12 Add VPN Gateway Show Advanced Settings Create	2345678	ateway Address: 192.168.2.33	? ×
Pre-Shared Key: 12 Add VPN Gateway Show Advanced Settings Create Create	2345678	ateway Address: 192.168.2.33	? ×
Pre-Shared Key: 12 Add VPN Gateway Show Advanced Settings Create VPN Gateway Name:	2345678	ateway Address: 192.168.2.33	? ×
Pre-Shared Key: 12 Add VPN Gateway Show Advanced Settings Create Create	2345678	ateway Address: 192.168.2.33	? ×
Pre-Shared Key: 12 Add VPN Gateway Show Advanced Settings Create C Enable VPN Gateway Name: IKE Version	2345678	ateway Address: 192.168.2.33	? ×
Pre-Shared Key: 12 Add VPN Gateway Show Advanced Settings Create Finable VPN Gateway Name: IKE Version © IKEv1	2345678	ateway Address: 192.168.2.33	? ×
Pre-Shared Key: 12 Add VPN Gateway Show Advanced Settings Create Finable VPN Gateway Name: IKE Version © IKEv1	2345678	ateway Address: 192.168.2.33	? ×
Pre-Shared Key: 12	2345678	ateway Address: 192.168.2.33	? ×
Pre-Shared Key: 12 Add VPN Gateway Show Advanced Settings Create VPN Gateway Name: IKE Version IKE V1 KEv2 Gateway Settings	2345678	DHCP client 192.168.4.33/255.255.255.0	? ×
Pre-Shared Key: 12 Add VPN Gateway Show Advanced Settings Create VPN Gateway Name: IKE Version IKEV1 KEv2 Gateway Settings My Address	2345678 new Object+ GRE1_GW		? ×
Pre-Shared Key: 12 Add VPN Gateway Show Advanced Settings Create VPN Gateway Name: IKE Version IKEV1 IKEV2 Gateway Settings My Address Interface Domain Name / IPv4	2345678 new Object+ GRE1_GW		? ×
Pre-Shared Key: 12 Add VPN Gateway Show Advanced Settings Create VPN Gateway Name: IKE Version IKEV1 KEV2 Gateway Settings My Address IN Interface	2345678 new Object+ GRE1_GW		? ×
Pre-Shared Key: 12 Add VPN Gateway Show Advanced Settings Create VPN Gateway Name: IKE Version IKEv1 IKEv2 Gateway Settings My Address Interface Domain Name / IPv4 Peer Gateway Address	2345678 new Object+ GRE1_GW	DHCP client 192.168.4.33/255.255.255.0	? ×
Pre-Shared Key: 12 Add VPN Gateway Show Advanced Settings Create VPN Gateway Name: IKE Version IKEv1 IKEv2 Gateway Settings My Address Interface Domain Name / IPv4 Peer Gateway Address	2345678 new Object+ GRE1_GW wan2 Primary Secondary	DHCP client 192.168.4.33/255.255.255.0	? ×
Pre-Shared Key: 1: Add VPN Gateway Show Advanced Settings Create VPN Gateway Name: IKE Version IKE Version IKE V2 Gateway Settings My Address Interface Domain Name / IPv4 Peer Gateway Address Static Addres Static Addres Stat	2345678 new Object+ GRE1_GW wan2 Primary Secondary	DHCP client 192.168.4.33/255.255.255.0	? ×
Pre-Shared Key: 1: Add VPN Gateway Show Advanced Settings Create VPN Gateway Name: IKE Version IKE Version IKE V2 Gateway Settings My Address My Address Interface Domain Name / IPv4 Peer Gateway Address Static Address Fall back to Primary Peer Gat Fall Back Check Interval:	2345678 new Object GRE1_GW Wan2 Primary Secondary teway when po	DHCP client 192.168.4.33/255.255.255.0 192.168.2.33 0.0.0 ssible	? ×
Pre-Shared Key: 1: Add VPN Gateway Show Advanced Settings Create VPN Gateway Name: IKE Version IKE V1 IKEv2 Gateway Settings My Address Interface Domain Name / IPv4 Peer Gateway Address Static Address Fall back to Primary Peer Gat Fall Back Check Interval: Dynamic Address Static A	2345678 new Object GRE1_GW Wan2 Primary Secondary teway when po	DHCP client 192.168.4.33/255.255.255.0 192.168.2.33 0.0.0 ssible	? ×
Pre-Shared Key: 1: Add VPN Gateway Show Advanced Settings Create VPN Gateway Name: IKE Version IKE Version IKE V2 Gateway Settings My Address My Address Interface Domain Name / IPv4 Peer Gateway Address Static Address Fall back to Primary Peer Gat Fall Back Check Interval:	2345678 new Object GRE1_GW Wan2 Primary Secondary teway when po	DHCP client 192.168.4.33/255.255.255.0 192.168.2.33 0.0.0 ssible	? ×

b. Add two VPN Connections.
 First VPN connection
 Application Scenario: Site-to-Site
 VPN Gateway: GRE0_GW
 Local policy: 192.168.3.33

Remote policy: 192.168.1.33 Enable GRE over IPSec

Z Edit VPN Connection GRE0_Conn	oncentrator Configuration Provisioning	? ×
🔲 Hide Advanced Settings 🛅 Create ne	v Object▼	
General Settings		
Enable		
Connection Name:	GRE0_Conn	
Nailed-Up		
Enable Replay Detection		
Enable NetBIOS broadcast over IF	Sec	
MSS Adjustment		
Custom Size	0 (200 - 1460 Bytes)	
Auto		
VPN Gateway		
Application Scenario		
 Site-to-site 		
Site-to-site with Dynamic Peer		
Remote Access (Server Role)		
Remote Access (Client Role)		
VPN Gateway:	GRE0_GW van1 192.168.1.33, 0.0.0.0	1
		-
Fdit VPN Connection GRE0 Conn	ancontrator Configuration Dravisioning	? ×
Edit VPN Connection GRE0_Conn Hide Advanced Settings Greate ne	oncentrator Configuration Provisioning	? 🗙
Hide Advanced Settings 🛅 Create ne	orentator Contouration Provisioning	5 ×
Hide Advanced Settings 🔚 Create ne		3 ×
Hide Advanced Settings Create ne Policy Local policy:	local_gre0 Y HOST, 192.168.3.33	2 ×
Hide Advanced Settings Create ne Policy Local policy: Remote policy:		2 ×
Hide Advanced Settings Create ne Policy Local policy: Remote policy: V Enable GRE over IPSec	local_gre0 Y HOST, 192.168.3.33	3 ×
Hide Advanced Settings Create ne Policy Local policy: Remote policy:	local_gre0 Y HOST, 192.168.3.33	3 ×
Hide Advanced Settings Create ne Policy Local policy: Remote policy: V Enable GRE over IPSec	local_gre0 Y HOST, 192.168.3.33	2 ×
Hide Advanced Settings Create ne Policy Local policy: Remote policy: Enable GRE over IPSec Policy Enforcement	local_gre0 Y HOST, 192.168.3.33	2 ×
Hide Advanced Settings Create ne Policy Local policy: Remote policy: Plase 2 Setting Create ne	local_gre0 HOST, 192.168.3.33 remote gre0 HOST, 192.168.1.33	2 ×
Hide Advanced Settings Create ne Policy Local policy: Remote policy: C Enable GRE over IPSec Policy Enforcement Phase 2 Setting SA Life Time:	local_gre0	2 ×
Hide Advanced Settings Create ne Policy Local policy: Remote policy: Color Enable GRE over IPSec Policy Enforcement Phase 2 Setting SA Life Time: Active Protocol:	local_gre0 	2 ×
Hide Advanced Settings Create ne Policy Local policy: Remote policy: Color Enable GRE over IPSec Policy Enforcement Phase 2 Setting SA Life Time: Active Protocol: Encapsulation:	local_gre0	2 ×
Hide Advanced Settings Create ne Policy Local policy: Remote policy: Color Enable GRE over IPSec Policy Enforcement Phase 2 Setting SA Life Time: Active Protocol: Encapsulation:	local_gre0	2 ×
 Hide Advanced Settings Create ne Policy Local policy: Remote policy: Enable GRE over IPSec Policy Enforcement Phase 2 Setting SA Life Time: Active Protocol: Encapsulation: Proposal 	local_gre0 ▼ HOST, 192.168.3.33 remote_gre0 ▼ HOST, 192.168.1.33 86400 (180 - 3000000 Seconds) ESP ▼ Tunnel ▼ SAdd Zedt: Temove # Encryption 1 DES SHA1	2 ×
Hide Advanced Settings Create ne Policy Local policy: Remote policy: Color Enable GRE over IPSec Policy Enforcement Phase 2 Setting SA Life Time: Active Protocol: Encapsulation:	local_gre0 ▼ HOST, 192.168.3.33 remote_gre0 ▼ HOST, 192.168.1.33 HOST, 192.168.1.33 86400 (180 - 3000000 Seconds) ESP ▼ Tunnel ▼ @ Add @ Edit Remove # Encryption Authentication	
 Hide Advanced Settings Create ne Policy Local policy: Remote policy: Enable GRE over IPSec Policy Enforcement Phase 2 Setting SA Life Time: Active Protocol: Encapsulation: Proposal 	local_gre0 ▼ HOST, 192.168.3.33 remote_gre0 ▼ HOST, 192.168.1.33 86400 (180 - 3000000 Seconds) ESP ▼ Tunnel ▼ SAdd Zedt: Temove # Encryption 1 DES SHA1	
 Hide Advanced Settings Create ne Policy Local policy: Remote policy: Enable GRE over IPSec Policy Enforcement Phase 2 Setting SA Life Time: Active Protocol: Encapsulation: Proposal Perfect Forward Secrecy (PFS):	local_gre0 ▼ HOST, 192.168.3.33 remote_gre0 ▼ HOST, 192.168.1.33 86400 (180 - 3000000 Seconds) ESP ▼ Tunnel ▼ SAdd Zedt: Temove # Encryption 1 DES SHA1	

Second VPN connection Enable Nailed-Up Application Scenario: Site-to-Site VPN Gateway: GRE1_GW Local policy: 192.168.4.33 Remote policy: 192.168.2.33 Enable GRE over IPSec

Edit VPN Connection GRE1_Conr	Concentrator Config	ration Provisioning	? 🗙
🔲 Hide Advanced Settings 🔚 Create	new Object•		
General Settings			
V Enable			
Connection Name:	GRE1_Conn		
Nailed-Up			
Enable Replay Detection			
Enable NetBIOS broadcast over	r IPSec		
MSS Adjustment			
Custom Size	0	(200 - 1460 Bytes)	
 Auto 			
VPN Gateway			
Application Scenario			
Site-to-site			
Site-to-site with Dynamic Pe	er		
Remote Access (Server Rol	e)		
Remote Access (Client Role	e)		
VPN Gateway:	GRE1_GW	 wan2 192.168.2.33, 0.0.0.0 	
Edit VPN Connection GRE1_Conr	Concentrator Config	ration Provisioning	? ×
🔲 Hide Advanced Settings 🛅 Create	new Object •		
Policy			
Local policy:	local_gre1	➤ HOST, 192.168.4.33	
Remote policy:	remote are1	HOST, 192,168,2,33	
Enable GRE over IPSec			
Policy Enforcement			
Phase 2 Setting			
SA Life Time:	86400	(180 - 3000000 Seconds)	
Active Protocol:	ESP	*	
Encapsulation:	Tunnel	*	
Proposal	🔘 Add 🛃 Edit. 🃋 Rer	love	
	# Encryption	Authentication	
	1 DES	SHA1	
Perfect Forward Secrecy (PFS):	none	× 1	
Related Settings			
Zone:	IPSec_VPN	× 1	
			OK Cancel

Step 8. Add a policy routes on USG2. Go to **CONFIGURATION > Network > Routing**.

Source: LAN1_Subnet Destination: Remote subnet Next-Hop: gre_trunk SNAT: none

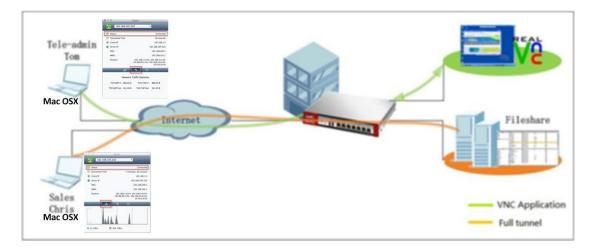
Add Policy Route		?)
Show Advanced Settings 🛅 Creat	e new Object▼	
Configuration		
V Enable		
Description:	(Optional)	
Criteria		
User:	any 👻	
Incoming:	any (Excluding ZyWALL)	
Source Address:	LAN1_SUBNET	
Destination Address:	remote_10	
DSCP Code:	any 👻	
Schedule:	none 💌	
Service:	any 👻	
lext-Hop		
Туре:	Trunk	
Trunk:	gre_trunk	

Scenario 7 - Deploying SSL VPN for Tele-workers to Access Company Resources –SSL VPN with Apple Mac OS X

7.1 Application Scenario

Tele-workers who work away from the office, sometimes need to access company resources in a secured way. USG supports hybrid VPN for client dial-up, and provides an SSL VPN function, which allowing tele-workers to access company resources through a secured VPN tunnel with little effort. All they need on their PC is a browser, and it only requires installation of additional SSL SecuExtender software. Besides, in SSL VPN, the network administrator can define different access rules to allow different users to access different company resources. In the USG 4.10 firmware, we have extended support for SSL VPN with Apple Mac OSX.

For example, the network administrator can configure an SSL VPN rule to allows the administrator to remotely control company servers by RDP or VNC through an SSL VPN tunnel. The administrator can also configure an SSL VPN Full tunnel rule to allow sales people to remotely access company file-share resources to conduct their daily tasks.



7.2 Configuration Guide

Step 1. Go to **Configuration > Object > Address**, add address object with "ssl_pool" (range 192.168.1.0~192.168.1.10).

YXEL USG40			Welcome admin <u>Loqout</u> ?Help Z About	Intermediate Provide the P
CONFIGURATION	Address Address Group			
TY Quick Setur				
Licensing	IPv4 Address Configuration			
Wireless	🔾 Add 📝 Edit 🏢 Remove 🖙 C	North Deferrer		
Network	V Add Z Edit 📑 Remove 👘 C	oject kererence		
Web Authentication	# Name 🔺	Туре	IPv4 Address	Reference
Security Policy	1 DMZ_SUBNET	INTERFACE SUBNET	dmz-192.168.3.0/24	0
VPN	2 IP6to4-Relay	HOST	192.88.99.1	0
- BWM	3 LAN1 SUBNET	INTERFACE SUBNET	lan1-192.168.1.0/24	1
UTM Profile	4 LAN2 SUBNET	INTERFACE SUBNET	lan2-192.168.2.0/24	2
Object	5 ssl_pool	RANGE	192.168.1.0-192.168.1.10	-
 Zone User/Group 	6 subnet_branch	SUBNET	192.168.10.0/24	1
AP Profile	7 vlan1	SUBNET	192.168.1.0/24	1
+ Application			192.108.1.0/24	· · · · · · · · · · · · · · · · · · ·
+ Address	≪ ≪ Page 1 of 1 ▶ ▶	Show 50 👻 items		Displaying 1 - 7 of
+ Service				
+ Schedule				
+ AAA Server				
 Auth. Method 				
Certificate				
 ISP Account 				
 SSL Application 				
System				
I Log & Roport				

Step 2. Go to **Configuration > Object > User/Group**, add an SSL VPN user account, e.g. "test".

CONFIGURATION	User	Group Setting			
TH Quick Setup					
Licensing	Configu	ration			
Wireless	Que	d 📝 Edit 🏢 Remove 🔚 Object Ref	aran ca		
Network	_				
Web Authentication	# 🔺	User Name	UserType	Description	Reference
 Security Policy 	1	admin	admin	Administration account	1
VPN	2	Idap-users	ext-user	External LDAP Users	0
• BWM	3	radius-users	ext-user	External RADIUS Users	0
 UTM Profile 	4	ad-users	ext-user	External AD Users	0
Object	5	user-phone	admin	Local User	1
- Zone	6		admin	Local User	1
User/Group AP Profile	0	user-pc			1
Application	/	test	user	Local User	1
Address	444	Page 1 of 1 🕨 🕅 Show	50 👻 items		Displaying 1 - 7 of 7
Service					
Schedule					
AAA Server					
+ Auth, Method					
Certificate					
- ISP Account					
 SSL Application 					
Log & Report					

Step 3. Go to **Configuration > Object > SSL Application**, add a web link with the URL for the SSL VPN client to access.

Z	YXEL USG40					Welcome admin <u>Loqout</u>	?Help Z Abou	t 📲 Site Map	Cobject Reference	🖵 Console 🛛
	CONFIGURATION Y Quick Setup Ucensing Wireless Network Web Authentication Security Policy VPN	SSL Application	Edit SSL Application Test Create new Object Object	t Web Appication		-	? ×		Display	ing 1 - 1 of 1
	BVM UTM Frolite UtM Frolite Dipled Sone SantGroup Application Address Santce Schnedule Control Address Santce Schnedule Genticate IsSF Account SSuperplication System		Web Application Server Type: Name: URL:	Weblink Y Test http://192.168.4.34]	OK	Cancel		USUR	

Step 4. Go to Configuration > VPN > SSL VPN > Access Privilege

(1) Add one SSL VPN rule and select User/Group Objects with "test" and SSL Application "Test" which you have already created.

7	YXEL USG40					?Help Z About ♣ Site Map
-	YAL USG40		O Edit Access Policy			? ×
12	CONFIGURATION	Access Privilege	🛅 Create new Object 🕶			
	CONFIGURATION Yu Quick Setup Licensing Wreless Network Web Authentication Security Policy VPN IPSac VPN L2TP VPN L2TP VPN UTM Profile Object System Log & Report	Access Policy St Access Polic	Configuration C	e test e object		cy Summary
					ОК	Cancel

(2) Enable **Network Extension (Full Tunnel Mode).** Choose the **Assign IP pool** with "ssl-pool" which you already create.

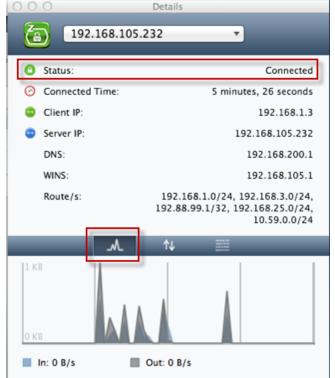
In the Network List, selected LAN1_Subnet.

7			Welcome admin <u>Logout</u>	?Help Z Abo
-	YXEL USG40		O Edit Access Policy	? ×
127	CONFIGURATION	Access Privilege	Create new Object -	
	Vy Quick Setup Licensing Wireless Network Security Policy VPN ISSE VPN ISSE VPN BWM UTM Profile Object System Log & Report	Access Policy St	Network Extension (Optional)	Cancel
				Cancel

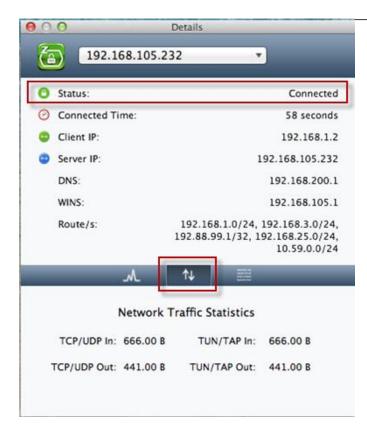
Step 5. Establish an SSL VPN on Apple Mac OS X

(1) When establishing an SSL VPN on Apple Mac OSX, the Status will become "Connected", and you can check the IP address information in the details.

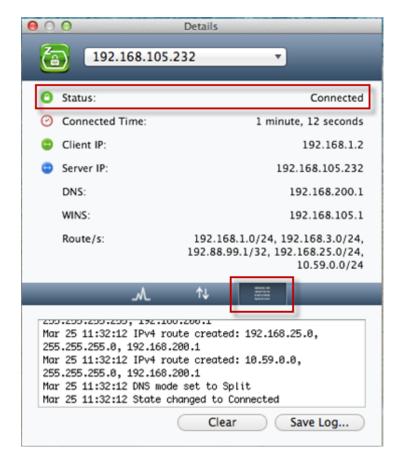
In the first tab – "Traffic Graph", it will automatically scale to match the maximum traffic rate.



(2) In the second tab – "Traffic", lists total data amounts that have passed through the VPN network adapter. These values are reset each time the connection is re-established.



(3) In the third tab – "Log", the log will contain important information if you are having trouble connecting.

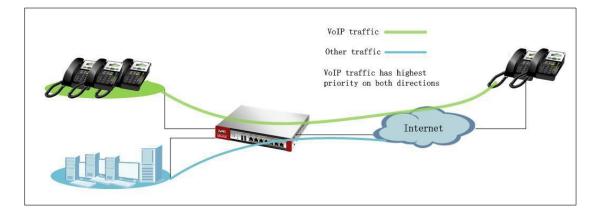


Scenario 8 — Reserving Highest Bandwidth Management Priority for VoIP traffic

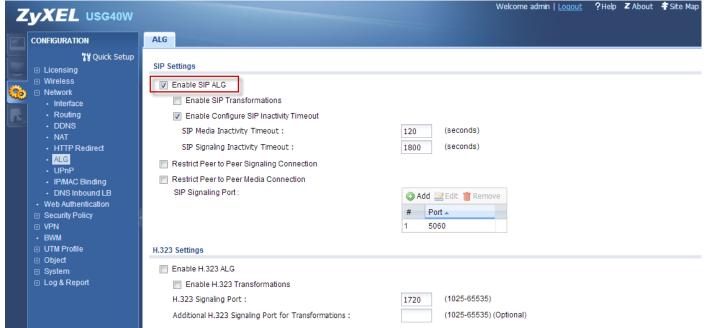
8.1 Application Scenario

In an enterprise network, there are various types of traffic. But the company Internet connection bandwidth is limited to a specific value. All this traffic will contend to use the limited bandwidth, which may result in some important traffic, for example, VoIP traffic getting slow or even starved. Therefore, intelligent bandwidth management for improved productivity becomes a matter of high concern for network administrators. ZyXEL USG provides Bandwidth Management (BWM) function to effectively manage bandwidth according to different flexible criteria.

VoIP traffic is quite sensitive to delay and jitter. Therefore, in an enterprise company, VoIP traffic should usually be awarded the highest priority over all other types of traffic.



8.2 Configuration Guide



Step 1. Go to Configuration > Network > ALG, enable SIP ALG.

Step 2. Go to **Configuration > BWM >** enable **BWM** and enable **Highest Bandwidth Priority for SIP Traffic >** Apply.

Enabling Highest Bandwidth Priority for SIP Traffic forces the device to give SIP traffic the highest bandwidth

priority. When this option is enabled the system ignores the bandwidth management settings of all application patrol rules for SIP traffic and does not record SIP traffic bandwidth usage statistics.

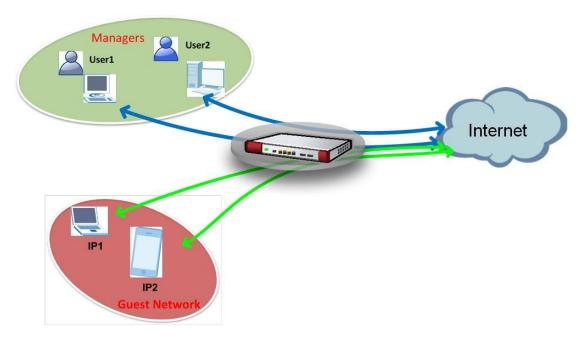
Z	YXEL USG40W								Wel	come admir	n <u>Loqout</u> ?H	lelp ZAł	pout 🛉 Si	ite Map 🗳 Object	Reference	🖵 Console	Ωα.
5	CONFIGURATION	BWM															
	₩ Quick Setup Licensing	BWM	ilobal Sett	ing													
	Wireless Network		nable BWI	M Highest Band	width Priority	for SIP Traffi											
R	Interface Routing DDNS		uration	- ingineer bana													
	• NAT • HTTP Redirect		dd 📝 Edi	t 📋 Remove	Q Activate	@ Inactivat	e 📣 Move										
	+ ALG	Sta	us Prio	Description	BWM Type	User	Schedule	Incoming Int	Outgoing Int	Source	Destination	DSCP	Service	BWM In/Pri/O	.t DSCP	Marking	
	+ UPnP		def		shared	any	none	any	any	any	any	any	Obj:any	no/7/no/7	preser	ve/pr	
	 IP/MAC Binding DNS Inbound LB 	14	🖣 Page	1 of 1 🕨	▶ I I Show	50 🔻 ite	ms								Displayi	ng 1 - 1 of :	1
	 Web Authentication 																
	Security Policy																
	• UTM Profile																
	⊕ Object																

Scenario 9 - Reserving Highest Bandwidth Management Priority for a Superior User and Control Session per Host – BWM Per IP or Per User

9.1 Application Scenario

In an enterprise network, there are various types of traffic. But the company Internet connection bandwidth is limited to a specific value. All this traffic will contend to use the limited bandwidth, which may result in some important traffic. Therefore, intelligent bandwidth management for improved productivity becomes a matter of high concern for network administrators. USG provides Bandwidth Management (BWM) function to effectively manage bandwidth according to different flexible criteria.

In the USG 4.10 firmware, we have extended the BWM function for a superior user and control session per host by only adding one rule. Then the USG can control Per IP or Per User to use the limited bandwidth individually. Among all the traffic in the company network, sometimes we need to a assign higher priority to some superior users to keep their important work going on smoothly. For example, the general managers need to surf the Internet smoothly to conduct their daily tasks. Therefore, the network administrator should use the bandwidth management function to prioritize the managers' Internet traffic, and guarantee a minimum bandwidth for their own traffic by IP address or by user account.



9.2 Configuration Guide

BWM Per IP

Step 1. Go to **Configuration > BWM >** add the policy to limit the Bandwidth by BWM type –Per-Source-IP.

(1) BWM Type : Per-Source-IP, Source: LAN1_SUBNET

Note: Object source IP address must belong to class C range which amount can't over 256 users.

Z	YXEL USG40				Welcome user-phone <u>Logout</u>	?Help ZAbout	🕈 Site	Map 🗳 Object Re	ference 🖙 Console
	CONFIGURATION TV Quick Setup Licensing Wireless	BW/4 BW/M Global Enable En Configuratic Status P Status P Status P	Configuration Enable Description: BWM Type: Criteria	Coption Shared Option Shared Peruser any any Atti_SUBNET v any any Service Object any Y	tai)	2 ×	cee	BWM In/Pri/Out. 2000/1/2000/1 no/7/no/7	DSCP Marking preserveipr preserveipr Dsplaying 1 - 2 of 2
					ОК	Cancel			

(2) Inbound = 2000Kbps, Out bound = 2000Kbps, Priority = 1

Z	YXEL USG40					Logout ?He	p Z About 🖣	Site Map GObje	ct Reference 🖙 Console 🕻
12	CONFIGURATION	BWM							
	Y Quick Setup Ucensing Wreless Interface Routing DDNS NAT HTTP Redired AG PMAC Binding DNS hound LB Web AuthentLation Security Policy UPAN WPA WMMI Oped System Log & Report	BWM Globa Enabl Configurati Status 4	Service Object:	Maximize Bandwidth Usage	disabled) Priority: Maximum: disabled) Priority: Maximum:	1 0 kb		ny 2000/1/200 ny 1000/7/100	
			Related Setting				- 11		
			Log	no			_ []		
					(ОК	Cancel		

Step 2. Go to **Configuration > BWM >** Enable BWM function.

ZyXEL USG40						Welcome	user-phone	Logout ?F	ielp Z Ab	out 🕈 Site	Map 📮 Object Re	ference 🛛 🖵 Console
CONFIGURATION	BWM											
TY Quick Setup • Licensing • Wireless • Network • Security Policy • VPN • WWI	BWM Global Setting											
 UTM Profile Object Zone User/Group 	③ Add		User	Schedule none none	Incoming Int any any	Outgoing Int any any	Source	Destination any any	DSCP any any	Service Obj:any Obj:any	BWM In/Pri/Out 2000/1/2000/1 no/7/no/7	DSCP Marking preserve/pr
AP Profile Application Address Service Schedule AA3 Server		▶ ▶∥ Show			urry	ur ry	401 Y J	urry.	erry	***;**ij		Displaying 1 - 2 of
Auth. Method Certificate ISP Account SSL Application System												

Step 3. Use the PC's IP address of "192.168.1.33" to connect to the USG. Visit the website <u>http://www.speedtest.net/</u> to test the speed.

The test result is around 2 Mbps, which is the same as our setup to manage per source IP 2 Mbps.

PING 18 ms	UPLOAD SPEED 1.91 Mbps UPLOAD SPEED 1.89 Mbps
	SHARE THIS RESULT
	Are you on CHTD, Chunghwa Telecom Co., Ltd.? Take our Broadband Internet Survey! GET A FREE OOKLA SPEEDTEST ACCOUNT Your Email Address
	CREATE
	Being togged in would allow you to start a Speed Wave here!
114.34.247.205 CHTD, Chunghwe Telecom Co., Ltd. Rate Your ISP	TEST AGAIN NEW SERVER Hosted by Taiwan Fixed Network

Step 4. Use the PC's IP address of "192.168.1.40" to connect to the USG. Visit the website <u>http://www.speedtest.net/</u>" to test the speed.

The test result is around 2 Mbps, which is the same as our setup to manage per source IP 2 Mbps.



BWM Per User-

Step 1. Go to **Configuration > Object > User/Group**.

(1) Add one user name as "user-phone", and add another user name as "user-pc".

ZyXEL USG4			Welcome admin Logout ?Help Z About ?Site Map	Console Discrimination Console
CONFIGURATION	User Group Setting			
TV Quick S	Setup Configuration			
 Wireless Network 	🛇 Add 📝 Edit 🃋 Remove 🔚 Object Reference	e		
Web Authentication	# Juser Name	User Type	Description	Reference
Security Policy	1 admin	admin	Administration account	1
VPN	2 Idap-users	ext-user	External LDAP Users	0
BWM	3 radius-users	ext-user	External RADIUS Users	0
UTM Profile Object	4 ad-users	ext-user	External AD Users	0
- Zone	5 user-phone	admin	Local User	1
 User/Group 	6 user-pc	admin	Local User	1
 AP Profile 		✓ items		Displaying 1 - 6 of
 Application 				
- Address - Service				
 Schedule 				
 AAA Server 				
 Auth. Method 				
 Certificate 				
 ISP Account 				
 SSL Application System 				
System				

(2) Add these two accounts "user-phone" and "user-pc" into the group as "user_local".

10/	CONFIGURATION	User Group Sett	ng	
	W Quick Setup	Configuration	Z Edit Group user_local	
	Wirkless Network Interface Routing DDNS NAT NAT ALG UPMAC Einding DNS inbound LB Web Authentication Security Policy WN EWM	Add 2 Edt 1 Rer # Group Name - 1 user_local H 4 Page 1 of	Name: user_local Description: (Optional) rphone	Reference 1 Displaying 1 - 1 of 1
	UTM Profile Object Zone Usernstoon AP Profile Application Address Schedule Schedule AAX Server Auth Method		OK_Cancel	

Step 2. Go to **Configuration > BWM >** Add the policy to limit the Bandwidth by BWM type – Per user. (1) BWM Type : Per user, User: user_local

CONFIGURATION	BWM	O Add Policy		? X			
	BWM Global	🛅 Create new Object 🕶		_			
	💟 Enable	Configuration		- 11			
	🔳 En:	Enable					
 Security Policy VPN 	Configuratio	Description:	(Optional)				
BWM UTM Profile	🔘 Add 🛃	BWM Type:	Shared Per user Per-Source-IP				
	Status P	Criteria			ce BV	VM In/Pri/Out	DSCP Marking
	<u> 9</u> 1	User:	user_local		any 20	000/1/2000/1	preserve/pr
	d	Schedule:	none		any no	0/7/no/7	preserve/pr
		Incoming Interface:	any 💌				Displaying 1 - 2
		Outgoing Interface:	any 👻				
		Source:	any 👻				
		Destination:	any 👻				
		DSCP Code:	any 🗸				
		Service Type:	Service Object Application Object				
		A		_			

(2) Inbound=2000Kbps, Out bound=2000Kbps, Priority =1

Z	YXEL USG40				Welcome user-phone <u>Logout</u>	?Help ZAbout	T Site N	lap 📮 Object Ref	erence 🗣 Console 🖪
197	CONFIGURATION	BWM							
	TV Quick Setup Ucensing Wrieless Notify During DDNS DDNS DDNS NAT HTTP Redired ALS PHAAC Binding DNS hound LB Web Authentication Beauth Policy VPN WwM Wrieles DVS horide Dyned Dyne	BWM Globa Enabl Enabl Configurati Add Status i Q Q Q Q Q Q Q Q Q Q Q Q Q Q Q Q Q Q Q	Per a seta a	any Inbound Marking: preserve Outbound Marking: preserve Inbound: 2000 kbps (0: di Maximize Bandwidh Usage Outbound: 2000 kbps (0: di Maximize Bandwidh Usage	sabled) Priority: 1 Maximum: 0	kbps kbps	any any	BWM In/Pri/Out 2000/1/2000/1 1000/7/1000/7 no/7/no/7	DSCP Marking preservelpr preservelpr Deplaying 1 - 3 of 3
			Related Setting						
			Log	no 👻					
					ОК	Cancel			

Step 3. Go to **Configuration > BWM > Enable BWM function**.

_	XEL USG40							weicome	user-phone		Help 4 AD	out 🖜 Site Ma	р чеорјест кег	erence 🖙 Console
C	CONFIGURATION	BWM												
	Tt Quick Setup . Licensing . Writess . Network . Web Authentication . Security Policy . VPN . WPN . UVM . UVH . ONject	Configura	bal Setting ble BWM Enable Highest Band ttion 1 2 Edit TRemove Prio Description	Q Activate		Move Schedule	Incoming Int	Outgoing Int	Source	Destination	Deck	Santon	3WM In/Pri/Out	DSCP Marking
	⊡ System	Q	1	per-user	suser_lo		any	any	any	any	any		2000/1/2000/1	preserve/pr
(Log & Report		def	shared	any	none	any	any	any	any	any	Obj:any i	10/7/no/7	preserve/pr
		14 4	Page 1 of 1	► 🕅 Show	50 👻 item	15								Displaying 1 - 2 of 2

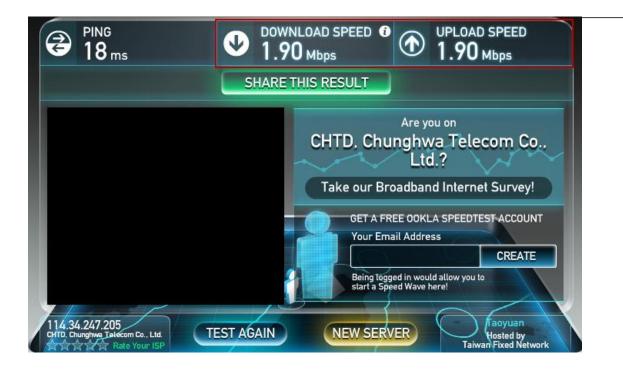
Step 4. Verify with the "user-phone" account.

(1) Enter the "user-phone" user name and password and Login.

USG40	Enter User Name/Passw	rord and click to login.
	User Name:	user-phone
	Password:	
	One-Time Password:	(Optional)
	(max. 63 alphanumeric, prin	table characters and no spaces)
	(max. 63 alphanumeric, prin	table characters and no spaces)

(2) Visit the website "<u>http://www.speedtest.net/</u>" to test the speed.

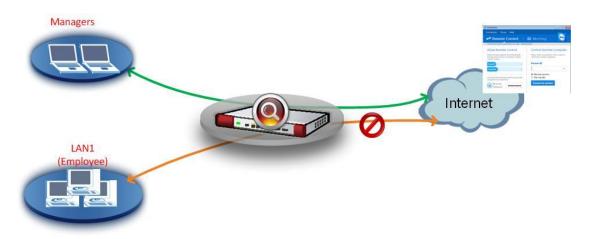
The test result is around 2 Mbps, which is the same as our setup to manage per user 2 Mbps.



Scenario 10 - Using USG to Control Popular Applications – APP Patrol

10.1 Application Scenario

In the company, the network administrator will need to control access to the Internet for internal managers and employees. The USG's Application Patrol function can take corresponding actions according to the configuration in App Patrol. For example, if the general managers need to execute the Teamviewer application to access the customer's side to conduct their daily work, then the network administrator can use the Firewall to drop other employee that are not allowed to use this type of application, and allow only managers to execute Teamviewer application.



10.2 Configuration Guide

Step 1. Go to **Configuration > Object > Application > Add Application Rule** For example Name: Teamviewer

ZyXEL USG40	Wekome admin Looput ?Heb Z Abou	t 🕈 Site Map 📮 Object Reference 💂 Console
COMFIGURATION If Quick Setup Classing Writess Network Network Security Policy VYPA UTIA Profile Cobject Zone User(Group A PFrofile Security Profile Security Profile Cobject Schedule Address Service Schedule Address Service Schedule Address Service Schedule Securit Structure Address Service Schedule Securit Structure S	Application Application Group Configuration It Application Rule Teamviewer Image: Configuration It Application Rule Teamviewer Image: Configuration It Application Rule Teamviewer Image: Configuration It Application Image: Configuration It Configuration Image: Configuration It Configuration	

NOTE: You need to register the IDP/App Patrol license to use App Patrol.

Step 2. Please add **Application Object > Search By Service >** insert "teamviewer" > select all to control all teamviewer applications > and then click on the **OK** button.

Add Application Object		? 🗙
Query		
Search:	By Service 💌 teamviewe	er Search
Query Result		
# 🔽 Category	Application	
Image: Constraint of the second sec	TeamViewer (communicate)	
Page 1 of 1 > > Show	TeamViewer (access)	Displaying 1 - 2 of 2
		OK Cancel

Step 3. Go to **Configuration > UTM Profile > App Patrol > Profile > Add rule** For example Name: teamviewer_rule.

Z	YXEL USG40			?Help Z Abou	t 📲 Site Map	CObject Reference	Gonsole
127	CONFIGURATION	Profile					
	IV Quick Setup Ucrensing Writess When Network Gezurty Policy PYP SWM Umf Profile Content Filter Dig Anti-Spam Object System Log & Report	Profile Management Add @ Edt @ Remove @ Name Leansever_rule License License Status: Licen License Type: Stan Signature Information Current Version: 3.1.4 Released Date: 2013 Undate Signatures	Name: teamviewer_rule Description: Profile Management Add @ Edt Remove # Application _ Action Log		Reference 1	Display	ng 1 - 1 of 1

Step 4. Go to Profile Management > Add Application

For example

Application: choose the application object of "Teamviewer" which you have already created. Action: drop

Log: log > ok.

Reference 1 Displaying 1 - 1 of 1
() X

Step 5. Go to **Configuration > Security policy > Policy Control > Policy > Add corresponding > Enable rule** For example

Name: teamviewer_drop

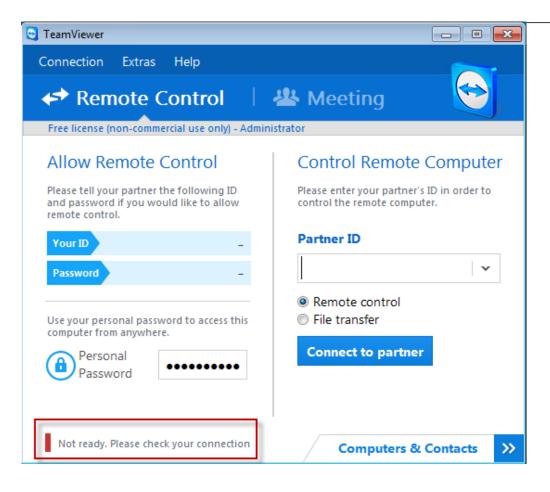
From: LAN1

UTM Profiles: Enable Application Patrol: choose the application profile of "teamviewer_rule" which you have already created.

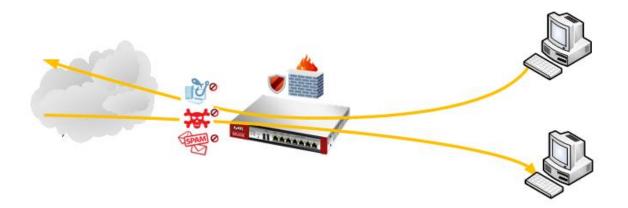
Log: by profile > ok > Enable Policy Control, and then App Patrol will work.

Z	YXEL USG40				welcome autimit <u>coquuc</u>	ineh TVDO	с токенар с	
5	CONFIGURATION	Policy						
	₩ Quick Setup □ Licensing	General Settings						
Ö	 → Registration → Signature Update 	Enable Policy Control	Edit Policy1 Create new Object+			? ×		
		IPv4 Configuration	Enable			•		
	 Interface Routing 	Allow Asymmetrical Ro	Name:	teamviewer_drop				
	+ DDNS	🔘 Add 📝 Edit. 🎁 Remo	Description.	-	(Optional)			
	 NAT HTTP Redirect 	Prior Status Name	From: To:	LAN1	~		Schedule none	Action UTM Profile
	 ALG IP/MAC Binding 	2 💡 Secure-		any (Excluding ZyWALL) any	~		none	allow
	ONS Inbound LB Web Authentication	3 9 Secure- 4 9 Secure-	P Destination:	any	~		none	allow
	Security Policy Policy Control	5 Secure-	Service:	any	*		none	allow
	+ ADP	6 🤪 Secure		ony	*		none	allow
	 → Session Control ⊕ VPN 	7 9 Secure- 8 9 Secure-		none allow	*		none	allow
	• BWM □ UTM Profile	9 @ Secure-			~		none	allow
	App Patrol Content Filter	10 🤪 Secure-	UTM Profiles				none	allow
	IDP Anti-Virus	11 G Secure- 12 G Secure-		teamviewer_rule	✓ Log: by profile ▼		none	allow
	+ Anti-Spam	13 Q Secure-		none	✓ Log: by profile ~	-	none	allow
	 ⊃ Object → Zone → User/Group 		ram.		ок с	ancel		

Step 6. Connect to the PC under USG LAN1, then teamviewer application will not open. But from other interface can, it can open.



Scenario 11 – Configure Unified Policy (Firewall Policy + UTM Profile)



Introduction:

The unified policy is merging with firewall rule and UTM functions. The flow will check the firewall rule first, and then check the UTM function. If the packets are already dropped by the firewall rule, then it will not check the UTM rule any more. The behavior of policy control is to check for the Initiator source IP address. For example, if you would like to block LAN1 users from downloading file from the Internet, then you should block From: LAN, To: WAN, Service: FTP, Action: deny.

If the packets are already dropped by the firewall rule, then it will not check the UTM rule any more.

Add corresponding							
i	Create new Object -						
	Enable						
	Name:	test					
	Description:		(Optional)				
	From:	LAN1	~				
	To:	WAN	~				
	Source:	any	~				
	Destination:	any	~				
	Service:	any	~				
	User:	any	~				
	Schedule:	none	•				
	Action:	deny	*				
	Log denied traffic:	no	*				
Е							
7							
B							
			Apply OK Cance				

If the packets are allowed by the firewall rule, then you can select the UTM profile to control sessions.

Add corresponding			?	×					
Ereate new Object +									
Enable									
Name:	test								
Description:		(Optional)							
From:	LAN1	~							
To:	WAN	*							
Source:	any	*							
Destination:	any	*							
Service:	any	*							
User:	any	*							
Schedule:	none	*							
Action:	allow	*							
Log matched traffic:	no	*							
UTM Profile									
Application Patrol:	none	~	Log:		~				
Content Filter:									
	none	~	Log:						
IDP:	none	~	Log:						
Anti-Virus:	none	*	Log:		~				
Anti-Spam:	none	*	Log:		×				
SSL Inspection:	none	*	Log:	by profile	×				
				ОК		-			
				UK	Cancel	J			

11.1 Application Scenario

The customer wants to block Skype and all social networks in LAN1.



11.2 Configuration Guide

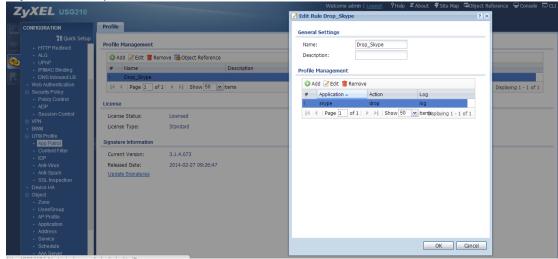
(1) Add a Skype object in Application.

Go to **Configuration > Object > Application**, and click on the "**Add**" button.

Z	YXEL USG210		Welcome admini <u>Lodout</u> ?Hep < About 1 Site Map UWObject Keference See
1	CONFIGURATION	Application Application Group	
	Uuick Setup	Configuration	
6	- ALG - UPnP	③ Add 📝 Edit 🍵 Remove 🖷 Object Reference	Edit Application Rule skype ? ×
	 IP/MAC Binding DNS Inbound LB 	# Name Description 1 skype New Create	Name: skype Description: New Create (Optional)
	Web Authentication Security Policy Policy Control	4	Description: New Create (Optional) O Add Tremove
	ADP Session Control	License License Status: Licensed	# Category Application 1 Voice over IP Skype (authority)
		License Type: Standard	2 Voice over IP Skype (media) 3 Voice over IP Skype (media)
	UTM Profile Device HA	Signature Information	Image: Second and the secon
	 Object Zone User/Group 	Current 3.1.4.073 Version:	
	AP Profile	Released Date: 2014-02-27 09:26:47	
	Application Address	Update Signatures	
	ServiceSchedule		
	 AAA Server Auth. Method 		
	 Certificate ISP Account 		OK Cancel
	SSL Application		

(2) Add to the App Patrol profile

Go to **Configuration** > **UTM profile** > **App Patrol**, and click on the "**Add**" button to add the application object into the profile.



Add a social network in Content Filter function to drop social networks.

ZyXEL USG210		Edit Filter Profile Social_n	etwork		🖙 Object Reference 🖙 Co 🍙
		Category Service Cust	om Service		
CONFIGURATION		General Settings			
HTTP Redirect	General Settings	License Status:	Licensed		
- ALG	Enable Content Filter Report Service	License Type:	Standard		
IP/MAC Binding DNS Inbound LB	Content Filter Category Service Timeou	Name: Description:	Social_network (Optional)		
Web Authentication Security Policy	Message to display when a site is block				
Policy Control	Denied Access Message:	Enable Content Filter C	ategory Service		
+ ADP		Action for Unsafe Web	Pages: Warn 👻	E Log	
→ Session Control	Redirect URL:	Action for Managed W	eb Pages: Block V	E Log	
- BWM	Profile Management	Action for Unrated We	b Pages: Warn Y	E Log	
 UTM Profile 			Server Is Unavailable: Warn	E Log	
 App Patrol 	🔘 Add 📝 Edit 🍵 Remove 🔚 Object	Action when category	Server is offavaliable: Warri	Log	
Content Filter IDP	# Name 🔺	Select Categories			
- Anti-Virus	1 Social_network				
- Anti-Spam	4 4 Page 1 of 1 ▶ ▶ Sh	Select All Categories	Clear All Categories		
 SSL Inspection Device HA 	Content Filter Category Service License				
 Device HA Object 		Security Threat (unsafe)			
- Zone	License Status:	Anonymizers	Botnets	Compromised	
- User/Group	License Type:	Malware	Network Errors	Parked Domains	
 AP Profile Application 	Expiration Date:	Phishing & Fraud	Spam Sites		
Address					
- Service		Managed Categories			
- Schedule	-				OK Cancel
 AAA Server 					

(4) Add a SSL inspection rule to drop the SSL web site to access the social network.

Go to **Configuration** > **UTM Profile** > **SSL Inspection** > **Profile**, and click on the "**Add**" button to add a SSL Inspection profile.

Z	YXEL USG210		Welcome admin <u>Loqout</u> ?Help Z About	t 🕈 Site Map 🗣 Object Reference 🗣 Console 🖾 CLI
2	CONFIGURATION	Profile Exclude List Profile Management		
	HTTP Redirect ALG UPnP	Add 🖉 Edit 👕 Remove 🔚 Object Reference		
R	 IP/MAC Binding DNS Inbound LB 	# Name Description ▲ 1 check_SSL_Web	CA Certificate default	Reference 0
	Web Authentication Security Policy Policy Control ADP Session Control	iii 4 Page 1 of 1 >>iii Show 50 whens Image: Show 50 Image: Show 50 Image: Show 50 Image: Show 50 Image: Show 50 Image: Show 50 Image: Show 50 Image: Show 50 Image: Show 50 Image: Show 50 Image: Show 50 Image: Show 50 Image: Show 50 Image: Show 50 Image: Show 50 Image: Show 50 Image: Show 50 Image: Show 50 Image: Show 50 Image: Show 50 Image: Show 50 Image: Show 50 Image: Show 50 Image: Show 50 Image: Show 50 Image: Show 50 Image: Show 50 Image: Show 50 Image: Show 50 Image: Show 50 Image: Show 50 Image: Show 50 Image: Show 50 Image: Show 50 Image: Show 50 Image: Show 50 Image: Show 50 Image: Show 50 Image: Show 50 Image: Show 50 Image: Show 50 Image: Show 50 Image: Show 50 Image: Show 50 Image: Show 50 Image: Show 50 Image: Show 50 Image: Show 50 Image: Show 50 Image: Show 50 Image: Show 50 Image: Show 50 Image: Show 50 Image: Show 50 Image: Show 50 Image: Show 50 Image: Show 50 Image: Show 50 Image: Show 50 Image: Show 50		Displaying 1 - 1 of 1
	VPN VM VUM Profile App Patrol Content Filter IDP Anll-Virus Anll-Spam SistInspan SistInspan Doked	Name: check_SSL_Wel Description: CA Certificate: default Action for connection with SSL v2: block Action for connection with unsupported suit: block	 ✓ ✓ Log: log alert ✓ Log: no 	× ×
	 Zone User/Group AP Profile Application 			OK Cancel

(5) Add the policy control rule to drop Skype and social networks from LAN1 subnet.

Go to **Configuration** > **Security Policy** > **Policy control** > **Policy,** and click on the "**Add**" button to add the rule, and select the objects into this rule.

7	YXEL USG210				O Add	corresponding			Welco	me admin <u>Loqout</u>	? ×	Z About	🕈 Site Map	Got
_	YALL 030210				🛅 Creat	te new Object •								
12	CONFIGURATION	Policy				Enable					_			
	₩ Quick Setup + HTTP Redirect	General	Settings		Nam	ne:	Drop_SKYPE_Social_N	(Optional)						
6		🔽 En	able Policy	Control	Fror	cription: n:	LAN1							
	 IP/MAC Binding DNS Inbound LB 	IPv4 Cor	nfiguration		To:		WAN	~						
	Web Authentication	IIA 📄	ow Asymme	etrical R	Sou	rce:	any	~						
	Security Policy	O Ac	Id 📝 Edit	📋 Rem	Des	tination:	any	~						
	Policy Control ADP	Prior.	Status	Name	Sen	/ice:	any	~					Schedule	
	 Session Control 	1	9	drop_	Use	r:	any	~					none	
	⊕ VPN + BWM	2	@	LAN1	Sch	edule:	none	~					none	
	UTM Profile	3	@	LAN2	Acti	on:	allow	~					none	
	App Patrol	4	9	DMZ_	Log	matched traffic:	no	~					none	
	Content Filter IDP	5	0	IPSec	,								none	
	+ Anti-Virus	6	0	SSL_	UTM F	Profile							none	
	 Anti-Spam 	7	9	TUNN	8	Application Patrol:	Drop_Skype	~	Log:	by profile 💌			none	
	 → SSL Inspection → Device HA 	8	9	LAN1	V	Content Filter:	Social_network	~	Log:	by profile 👻			none	
	 Object 	9	9	LAN2		IDP:	none	~	Log:	by profile 💌			none	
	→ Zone	10	9	DMZ_		Anti-Virus:	none	~	Log:	by profile 💙			none	
	User/Group AP Profile	11	9	WAN_		Anti-Spam:	none	~	Log:	by profile 💌			none	
	+ Application	12	9	IPSec	V			*					none	
	Address	13	9	SSL_	V	SSL Inspection:	check_SSL_Web	•	Log:	by profile 💌			none	
	Service Schedule AAA Server									ОК Са	ncel			
	Auth Mathad													

After configuring these rule, then you can drop Skype and all of the social networks successfully.

Scenario 12 – Block HTTPS Websites by Content Filter

Introduction:

The Content Filter function can distinguish between websites by categories. Since the Content Filter does not know that the traffic has already been encrypted, so the HTTPS websites cannot be detected. But now can we use the "SSL Inspection" function to decrypt the packets, and then to block it.

After enabling the SSL inspection, clients only need to import the certificate generated by the USG, because the USG has become a proxy to help to verify these HTTPS websites, so client only needs to trust the USG.



After using the SSL inspect function, HTTPs traffic can detect it well by the Content Filter function.

12.1 Application Scenario

Block the search engine in the internal website.

12.2 Configuration Guide

(1) Create an object in SSL inspection function.

Go to **Configuration** > **UTM Profile** > **SSL Inspection** > **Profile**, and click on "**Add**" to add an SSL Inspection object.

Profile E	xclude List							
Profile Mana	gement							
🔘 Add 📝	Edit 🏢 Remove 🔚 Object Reference							
# Nam	ne	Description 🔺		CA Certifica	ate		Reference	
	k_Search_Engien			default			1	
4 4 Pa	age 1 of 1 🕨 🕅 Show 50 💌	items						Displaying 1 - 1 of 1
	Zedit Rule Block_Search_Engien						? ×	
	General Settings							
	Name:	[Block_Search_Engien					
	Description:							
	CA Certificate:		default	*				
	Action for connection with SSL v	2:	block	۲ ا	Log:	log	~	
	Action for connection with unsu	oported suit:	pass	۲ ا	Log:	no	~	
						0	K Cancel	
							Cancel	

(2) Create a Content Filter object on the device.

Go to **Configuration** > **UTM Profile** > **Content Filter** > and click on "Add" to create a Content Filter profile.

Edit Filter Profile Search_Eng	ine				? X
Category Service Custom	Service				
General Settings					
License Status: Lice	ensed				
License Type: Sta	indard				
Name: Se	arch_Engine				
Description:		(Optiona	I)		
Enable Content Filter Cate					
Action for Unsafe Web Pag	les:	Warn	~	Log	
Action for Managed Web P	ages:	Block	~	E Log	
Action for Unrated Web Pa	iges:	Warn	~	📄 Log	
Action When Category Ser	ver Is Unavailable:	Warn	~	📄 Log	
Select Categories					
Select All Categories		Clear All Categ	jories		
Security Threat (unsafe)					
Anonymizers	V Bo	otnets		Compromised	
👿 Malware	📝 Ne	etwork Errors		Parked Domains	
Phishino & Fraud	🔍 Sr	am Sites			

In the Managed Categories select "Search Engines/ Portals" to block the search engine.

Edit Filter Profile Search_Engine			? ×
Category Service Custom Service			
Managed Categories			
Advertisements & Pop-Ups	Alcohol/Tobacco	Arts	
Business	Transportation	Chat	
Forums & Newsgroups	Computers & Technology	Criminal Activity	
Dating & Personals	Download Sites	Education	
Entertainment	Finance	Gambling	
Games	Government	Hate & Intolerance	
Health & Medicine	Illegal Drugs	Job Search	
Streaming Media & Downloads	News	Non-profits & NGOs	
Nudity	Personal Sites	Politics	_
Pornography/Sexually Explicit	Real Estate	Religion	
📄 Restaurants & Dining	Search Engines/Portals	Shopping	
Social Networking	Sports	Translators	
Travel	Violence	Weapons	
🔲 Web-based Email	General	Leisure & Recreation	
Cults	Fashion & Beauty	Greeting Cards	
Hacking	Illegal Software	Image Sharing	
Information Security	Instant Messaging	Peer to Peer	
Private IP Addresses	School Cheating	Sex Education	
Tasteless	Child Abuse Images		

(3) After Create SSL Inspection and Content Filter profiles, then go to the **Policy Control** function to setup the rule.

Go to **Configuration** > **Security policy** > **Policy control** and click on the "**Add**" button to add the rule. After you setup a session orientation, then you can setup the UTM profile.

In this example, after you select the profile that you added in this rule, then the end user will not be able to access the search engine any more.

Edit Policy1					? ×
🛅 Create new Object 🔹					
Enable					
Name:	Block_Search_Engine				
Description:		(Optional)		
From:	any	~			
To:	any (Excluding ZyWALL)) 🕶			
Source:	any	~			
Destination:	any	~			
Service:	any	~			
User:	any	~			
Schedule:	none	~			
Action:	allow	~			
Log matched traffic:	no	~			
UTM Profile					
Application Patrol:	none	*	Log:	by profile	~
Content Filter:	Search_Engine	*	Log:	by profile	¥
IDP:	none	*	Log:	by profile	~
Anti-Virus:	none	*	Log:		~
Anti-Spam:	none	*	Log:	by profile	v
SSL Inspection:	Block_Search_Engine	~	Log:	by profile	~
			_		
				ОК	Cancel

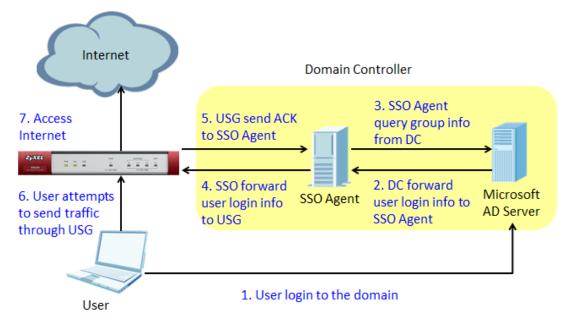
Verification: Access to https:yahoo.com

← ⇒ C fi	😰 https://yahoo.com	☆ =
	Web access is restricted. Please contact the administrator. (Search Engines and Portals)	
	(If you feel this site has been improperly categorized, please visit <u>here</u> to submit a review.)	

Scenario 13: Single Sign-on with USG and Windows Platform

13.1 Application Scenario

When the employee's PC is connected to the company's network, usually he needs to login to the domain first, and then login to the USG with the same username and password again, to pass the web authentication before accessing the Internet and the company's resources. With Single Sign-On agent integrated with Microsoft Active Directory, the SSO Agent sends authentication information to the USG to let users automatically get access to permitted resources. Users just need to login to the domain once and have access to the Internet and company internal resources that they are authorized to access directly without being prompted to login again.



13.2 Configuration Guide

Network conditions

WAN: 59.124.163.151 LAN 1: 192.168.1.0/255.255.255.0 Domain Controller (Windows Server 2008 R2): 192.168.1.34 Client's laptop: 192.168.1.33

Goals to achieve

The user logs into the domain once and is able to access the Internet directly without specifying the username and password in the web browser.

Domain Controller Configuration

1. Go to Active Directory Users and Computers to create a new domain account and add it to the group of "Domain Admins".

Example: ssoadmin

Create some domain users.

Example: Amy

File Action View Help			
🛤 🖄 📅 🗋 🗊 💁 🚺 🖬	5		
Server Manager (WIN-LKBONDKNRKI)	Users 19 objects [Filter Activated	0	
Roles Active Directory Domain Services	Name	Туре	Description
Active Directory Users and Comput	Administrator Allowed RODC Password Repli	User Security Group	Built-in account for admini Members in this group can
Builtin Computers Domain Controllers SorrignSecurityPrincipals Managed Service Accounts Users Active Directory Sites and Services Active Policy and Access Services Features Diagnostics Configuration Storage	Amy Cert Publishers Denied ROOC Password Repl Domain Admins Domain Computers Domain Computers Domain Controllers Domain Guests Domain Users Enterprise Read-only Domain Group Policy Creator Owners RAS and IAS Servers RAS and IAS Servers Read-only Domain Controllers	User Security Group Security Group Security Group Security Group Security Group Security Group Security Group Security Group User Security Group Security Group	Members of this group are Members in this group can Designated administrators All workstations and serve All domain controllers in th All domain guests All domain guests Designated administrators Members of this group can Built-in account for guest Servers in this group can Members of this group can

SSO Agent Installation

- 1. Prepare the package of SSO Agent.
- 2. Install .NET Framework v4.0.30319 or above version.

DotNetFX40	3/24/2014 2:54 PM	File folder
퉬 vcredist_x86	3/24/2014 2:54 PM	File folder
퉬 WindowsInstaller3_1	3/24/2014 2:54 PM	File folder

Double click "dotNetFx40_Full_x86_x64.exe".

🚜 dotNetFx40_Full_x86_x64

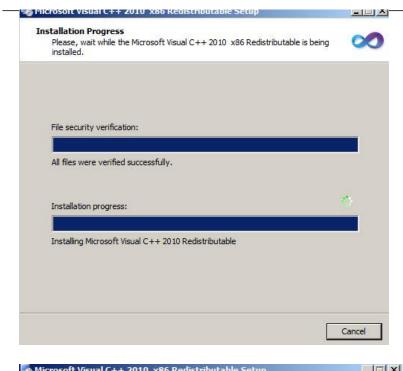
- 10 M	work 4 Setup	
Installation Progress Please wait while th	5 e .NET Framework is being installed.	Microsoft .NET
File security verifica	tion:	
All files were verified	d successfully.	
Installation progress	s:	0
Installing .NET Fram	ework 4 Client Profile	
		Cancel
🌄 Microsoft .NET Framew	ork 4 Setup	
01	Installation Is Complete	
	.NET Framework 4 has been installed.	
Microsoft*	.NET Framework 4 has been installed.	
NET.	Check for more recent versions on Windows Update	rati
Microsoft* .NET		- The
Microsoft* .NET		and the second se

3. Install Visual C++

DotNetFX40	3/24/2014 2:54 PM	File folder
퉬 vcredist_x86	3/24/2014 2:54 PM	File folder
WindowsInstaller3_1	3/24/2014 2:54 PM	File folder

Double-click on the "vcredist_x86.exe".

🚭 vcredist_x86



MICROSOTE VISUALC++ 2010	xoo keuistributable Setup	
Microsoft Visual Studio	Installation Is Complete Microsoft Visual C++ 2010 x86 Redistributable has been installed.	
	You can check for more recent versions of this package on the <u>Microsoft Visual Studio</u> website.	
	Finis	h

4. Double-click on "SSOAgentInstaller.exe" to install SSO Agent.

퉬 DotNetFX40	3/24/2014 2:54 PM	File folder	
퉬 vcredist_x86	3/24/2014 2:54 PM	File folder	
퉬 WindowsInstaller3_1	3/24/2014 2:54 PM	File folder	
📑 Cleaner	3/12/2014 3:32 PM	Application	12 KB
📄 install	3/24/2014 3:17 PM	Text Document	451 KB
🔯 setup	3/21/2014 11:00 AM	Application	418 KB
SSOAgentBoostraper	3/12/2014 2:32 PM	Application	6 KB
🔯 SSOAgentInstaller	3/21/2014 12:03 PM	Application	7,414 KB
😽 SSOAgentSetup	3/21/2014 11:00 AM	Windows Installer P	8,095 KB

Click on "Next" to proceed.

50 Agent Setup					>	-
√elcome to the	SSO Agent Set	up Wiza	ard		5)
ne installer will guide you t	nrough the steps required t	o install SSI) Agent on	your comp	uter.	
	program is protected by co distribution of this program					
	be prosecuted to the max					
	Cance	1	< Back	1	Next>	-
		1000				
					.1 .1 .1	
	r setup with c	lefault	locati	ion an		
	r setup with c	lefault	locati	ion an		on "Ne
550 Agent Setup		lefault	locati	ion an		
550 Agent Setup		lefault	locati	ion an		
550 Agent Setup Telect Installati	on Folder		locati	ion an		
550 Agent Setup Gelect Installati ne installer will install SSC	on Folder Agent to the following fo	lder.				
550 Agent Setup Gelect Installati ne installer will install SSC	on Folder	lder.				
550 Agent Setup Gelect Installati ne installer will install SSC	on Folder Agent to the following fo	lder.				
550 Agent Setup ielect Installati ne installer will install SSC p install in this folder, click	on Folder Agent to the following fo	lder.		below or cli		
SSO Agent Setup Select Installati ne installer will install SSC p install in this folder, click	on Folder Agent to the following fo	lder.		below or cli	ck "Browse	
SSO Agent Setup ielect Installati ne installer will install SSC a install in this folder, clicl Eolder:	ON Folder Agent to the following fo	lder.		below or cli	ck "Browse"	
SSO Agent Setup Select Installati ne installer will install SSC o install in this folder, clich Eolder: C:\Program Files (x86)\	ON Folder Agent to the following fo	lder. fferent fold	er, enter it b	below or cli	ck "Browse"	
SSO Agent Setup Select Installati ne installer will install SSC o install in this folder, clich Eolder: [C:\Program Files (x86)\ Install SSO Agent for you	ON Folder Agent to the following fo "Next". To install to a di ZyXEL\SSOAgent\	lder. fferent fold	er, enter it b	below or cli	ck "Browse"	
SSO Agent Setup Select Installati ne installer will install SSC o install in this folder, clich Eolder: C:\Program Files (x86)\	ON Folder Agent to the following fo "Next". To install to a di ZyXEL\SSOAgent\	lder. fferent fold	er, enter it b	below or cli	ck "Browse"	

In this scenario, SSO Agent is installed on the Domain Controller. Select "DC".

SSO Agent Setup			×
Select Local Machine Installation	e Type of SSO /	Agent	5
Do you want to install SSO Agent o	n?		
© DC			
C WorkStation			
	Cancel	< Back	Next>

Click on "Next" to start the installation.

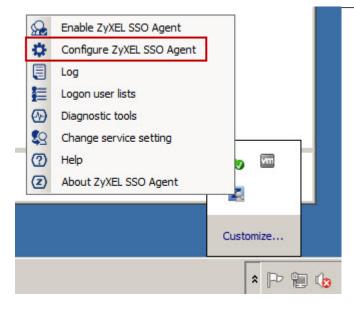
nt on your compute	n.	
3		367
Cancel	K Back	Next >
		nt on your computer.

A dialog box called "Set SSO Agent Service" will pop-up.

Enter the Domain\Username and password of the domain account that was created in **Domain Controller configuration**. Click on "OK" to continue.

550 Agent S	Setup	- 🗆 ×
Installing	SSO Agent	5
	🚰 Set SSO Agent Service	~
SSO Agent is	Please input user account to install service	
	User name format: "DomainName\Username"	
Please wait	User name : CSO\ssoadmin Check Name	
	Password :	
	Confirm Password :	
	Display password as clear text	
_	Cancel OK	
SSO Agent i	Cancel K Back	Next >
🛃 550 Agent :		_ 🗆 🗵
Installatio	on Completed	5
SSO Agent has	: been installed successfully.	
Click "Close" to		
☑ Launch SS	0 Agent after installation completed	
Please use Wir	ndows Update to check for any critical updates to the .NET Framework.	
	Cancel K Back	Close

SSO Agent Installation1. Click on "Configure ZyXEL SSO Agent".



2. Click on "Configure" to configure the LDAP query to get group information of users from the Active Directory.

Agent Listening Port: Logon List Check Interval (minute):						
Config	ure LDAF	P/AD server	Configure			
atewa	y Settin	gs				
Ad	Index	Modify Delete Description	IP	Port	Share Key	

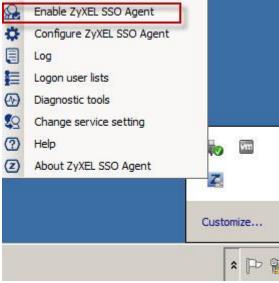
Configure the IP address of the AD server, Base DN, and Bind DN.

LDAP/AD server configuration	
General Settings	
Name	UserGroup
Description	
Server Settings	
Server Address	192.168.1.34
Backup Server Address	
Port	389
Base DN	DC=cso,DC=zyxel,DC=com
Use SSL	
Search time limit	5
Case-sensitive User names	
Server Authentication	
Bind DN	CN=ssoadmin,CN=Users,DC=cso,DC
Bind DN Password	CN=ssoadmin,CN=Users,DC=cso,DC
Password Retype to Confirm	•••••
Password Retype to Confirm User Login Settings	·····
Password Retype to Confirm	•••••
Password Retype to Confirm User Login Settings	·····
Password Retype to Confirm User Login Settings Login Name Attribute	·····
Password Retype to Confirm User Login Settings Login Name Attribute Alternative Login Name Attribute	sAMAccountname
Password Retype to Confirm User Login Settings Login Name Attribute Alternative Login Name Attribute Group Membership Attribute	sAMAccountname memberOf
Password Retype to Confirm User Login Settings Login Name Attribute Alternative Login Name Attribute Group Membership Attribute	sAMAccountname
Password Retype to Confirm User Login Settings Login Name Attribute Alternative Login Name Attribute Group Membership Attribute	sAMAccountname memberOf

Under Gateway Settings, click on "Add" to configure the IP address of the USG and the Pre-Shared Key.

Gateway IP:	192.168.1.1	IPv4 Address
Gateway Port	2158 (1025 - 65535)	
Description	USG40	
PreShareKey		Generate Key
ricondicitoy		denerate hoy
(incondicate)	Check to show PreShareKey as cle	

Enable SSO service.



When the SSO service is started successfully, the icon is enabled.



USG Configuration

1. Go to **CONFIGURATION > Object > AAA server > Active Directory > Edit Active Directory**. Configure the AD server that has the same settings as step 2 of "**SSO Agent Installation**".

Zedit Active Directory			?
General Settings			
Name:	ad		
Description:		(Optional)	
Server Settings			
Server Address:	192.168.1.34	(IP or FQDN)	
Backup Server Address:		(IP or FQDN)(Optional)	
Port:	389	(1-65535)	
Base DN:	DC=cso,DC=zyxel,DC=		
Use SSL			
Search time limit:	5	(1-300 seconds)	
🔲 Case-sensitive User Names	i		
Server Authentication			
Bind DN:	CN=ssoadmin,CN=Use		
Password:	•••••		
Retype to Confirm:	•••••		
User Login Settings			
Login Name Attribute:	sAMAccountName		
Alternative Login Name Attribute:		(Optional)	
Group Membership Attribute:	memberOf		
			OK Cancel

2. Go to **CONFIGURATION > Object > User/Group > User** and add a new ext-group-user. Ex: csosecurity. The domain user "Amy" must belong to this group in the AD.

User Configuration			
	csosecurity		
User Type:	ext-group-user	*	
Group Identifier:	CN=csosecurity,C	N=Users,DC=cso,DC=zyxel,DC=com	
Associated AAA Server Object:	ad	~	
Description:	Local User		
Authentication Timeout Settings	Use De	fault Settings 🛛 💿 Use Manual Settings	
Lease Time:	1440	minutes	
Reauthentication Time:	1440	minutes	
Configuration Validation			
Please enter a user account existe	d in the configured gr	oup to validate above settings.	
User Name :		Test	

3. Go to **CONFIGURATION > Object > Auth. Method** and add "group ad" in the default authentication method.

Edit Authentication Method default	? 🗙
General Settings	
Name: default	
🗿 Add 🛃 Edit 🍵 Remove 🃣 Move	
# Method List	
1 group ad 2 local	
	OK Cancel

4. Go to **CONFIGURATION > Web Authentication > SSO**. Fill-in the Pre-Shared Key which is configured in the **SSO Configuration**.

CONFIGURATION	Web Authentication SSO				
₩ Quick Setup Licensing Wireless	General Settings Listen Port:	2158 (1025-65535)			
 □ Network ◆ Interface ◆ Routing 	Agent PreShareKey: Primary Agent Address:	192.168.1.34			
 DDNS NAT HTTP Redirect 	Primary Agent Port: Secondary Agent Address (Optional):	2158 (1025-65535)			
 ALG IP/MAC Binding 	Secondary Agent Port (Optional):	(1025-65535)			
ONS Inbound LB Web Authentication Security Policy	Note: If you use Re-auth., please enable "Web Authentication" in <u>Web Authentication</u> .				

5. Go to **CONFIGURATION > Web Authentication > Web Authentication Policy Summary** to add a new authentication policy.

Enable the "Single Sign-on" checkbox to be authenticated by the SSO.

eral Settings Enable Policy			
Description:		(Opt	ional)
er Authentication Poli			
Source Address:	LAN1_SUBNET	*	INTERFACE SUBNET, 192.168.1.0/24
Destination Address:	any	*	
Schedule:	none	~	
Authentication:	required	~	
Single Sign-on			
	antina 🕅		
V Force User Authenti	ication 🔢		

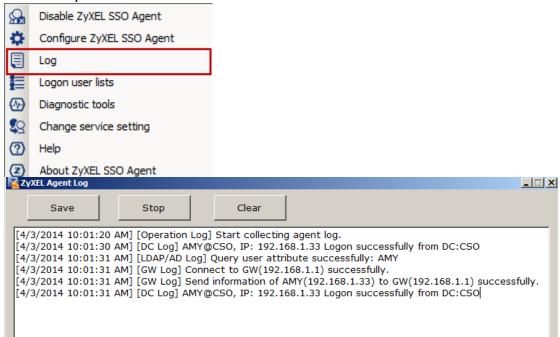
Status	us Priority Source		Destination	Schedule	Authentication
@	1	■LAN1_SUBNET	any	none	SSO/force
	Default	any	any	none	unnecessary
	Page 1	of 1 🕨 🕅 Show 50	▼ items		

Verification

- 1. On the client's laptop, login using the domain account "Amy".
 - Example: CSO\Amy

Open the browser or application on the client's laptop to trigger traffic to pass to the USG. The client "Amy" can surf the Internet directly without extra authentication.

2. Check SSO Agent Log. User login is successful and has sent information to the USG's GW (192.168.1.1) successfully.



3. Check the Logon user lists on the SSO Agent. The user "Amy" is in the logon list.

S.	Disable ZyXE	EL SSO Agent			
Ф	Configure Zy	/XEL SSO Agent			
	Log				
ŧ	Logon user li	ists			
\odot	Diagnostic to	pols			
\$2	Change serv	vice setting			
?	Help				
Z	About ZyXEL	SSO Agent			
🛃 Lo	gon User Lists				_ 🗆 X
Refn	esh Interval(s): 3	0 (5 - 300) App	Ny Refresh Now T	ypes:	Search
S	elect Index	User	IP Address	Logon Time	Logon DC Name
	1	AMY	192.168.1.33	4/3/2014 10:01:30 AM	CSO

4. Go to **MONITOR > System Status > Login Users**.

The client "Amy" is on the current user list with type SSO.

urrent User List								
& F	Force Logout							
#	User ID	Reauth Lease T.	Туре	IP Address	User Info			
1	AMY	23:19:58 / 23:19:58	SSO	192.168.1.33	ext-group-user(csosecurity)			
2	admin	unlimited / 00:30:00	http/https	59.124.163.130	admin(admin)			
14	4 Page 1 of 1 ▶	▶ Show 50 v items			Displaying 1 -			

Scenario 14 – WLAN Controller Function on USG

14.1 Application Scenario

USG with 4.10 firmware supports the AP controller function. You can follow the steps to control your AP device.



14.2 Configuration Guide

Management of external AP device

(1) Add an SSID object on the device

Go to **Configuration > Object > AP Profile > SSID > SSID list**, and click on the "Add" button.

12	CONFIGURATION	Radio	SSID							
		SSID	List	Security List	MAC Filter List					
	Licensing Wireless Network VetAuthenlication Securty Policy VPN UTM Profile Device HA Objed Jone UJSertGroup UsertGroup UsertGroup SertGes Schedule Address Service Schedule Address Service Schedule Address Service Schedule Certificate ISP Account System	SSID S	dd 2 Edi Profile N default SSID	t 📋 Remove 🜆	Object Reference SSID ZyXEL For_test	Add SSID Profile Create new Object Profile Name: SSID: Security Profile: MAC Filtering Profile: QOS: VLAN ID: Hidden SSID Enable Intra-BSS Tr	SSID For_test default default default MIM 1 affic blocking	•	5 X	ofile
								ОК	Cancel	

(2) Go to **Configuration > Object > AP Profile > Radio**, and click on the "Add" button to add 2.4G and 5G radio objects, and set the SSID profile to this object.

lar 1	CONFIGURATION	Radio		
	TY Quick Setup		Add Radio Profile	×
-		Radio Summary	· · · · · · · · · · · · · · · · · · ·	
	Licensing Wretess Wretess WebAuthenheideton Securit Policy VPA WPAUthenheideton VPA UVII Ovice Objed	Radio Summary	General Settings	
	CONFIGURATION Claring and a state of the second state of the seco	Radio SSD Radio Summary Add Zeldt Y Status Profe Net 1 0 2 0 3 0 For_INVA 14 Page 1 of 1 >>1	OK Cancel Add Radio Profile 2 × In Show Advanced Settings If cancel If Show Advanced Settings If cancel If Advate Profile Name: Profile Name: For_INVA_SC Node: 36 Node: 36 MBSSID Settings If SSID Profile If SSID If SSID Profile If SSID If SSID </th <th></th>	

(3) Connect your AP to the LAN interface (this document is using NWA 3560-N to test).

a. The AP must be set as managed mode.

b. After the connection is successful, the NWA will start upgrading the firmware from the USG.

After upgrading the firmware successful, you will see the MAC address and model name in the GUI.

	CONFIGURATION	Mgnt.	AP List								
	₩ Quick Setup Licensing	Mgnt. /	AP List								
2	 Wireless Controller 	📝 E	dit 🍵 Remove 🙋 Reb	poot							
8	AP Management	#	IP Address	MAC Address	Model	R1 Mode / Profile	R2 Mode / Profile	Mgnt. VLAN I	Mgnt. VLAN I	Description 🔺	
	Network	1	192.168.1.33	50:67:F0:37:B9:99	NWA3560-N	AP / default	AP / default2	1	1	AP-5067F037B999	
	Web Authentication	14	4 Page 1 of 1	▶ ▶ Show 50 v item	15					Displaying 1 - 1	1 of
	Security Policy										
	VPN										
	● VPN → BWM										
	VPN BWM UTM Profile										
	VPN BWM UTM Profile Device HA										
	VPN BWM UTM Profile										
	VPN BWM UTM Profile Device HA Object										
	VPN BWM UTM Profile Device HA Sobject System										
	VPN BWM UTM Profile Device HA Sobject System										

	CONFIGURATION	Mgnt. AP List		
	CONFIGURATION TY Quick Setup Ucansing Purcleass - Controller - AP Management Meta-Authentication - Security Policy - Web Authentication - Security Policy - VPN - BWM - Device HA - Device HA - Dopice - Digatem - Digatem	Mgnt. AP List ∭Edt. Remore © Reboot # IP Address MAC Address 102 168.1.33 50.67 F0.37 BP.99 I 4 I 61 J 192 168.1.33 I 9.67 F0.37 BP.99 I 4 I 9.1 > I I 9.1 > I 9.1 > I 9.1 > I I I	Edit AP List ? × Create new Object* ? Configuration	Description AP-5067F037B999 Displaying 1 - 1 of 1
			VLAN Settings VLAN Config Management VLAN ID: 1 (1-4094) As Native VLAN OK Cancel	

(5) Verify the SSID on your network (the SSID is "For_test")

Localbridge_remote	lite.	^
ZyXEL_3DTT		
ZyXEL47614	.all	
ZyXEL_0000		
Speedlink-031		
ZT01680_Spark		
Wireless1	3 41	
ZyXEL	3 41	
Guest	31	
For_test	311	
Alex No1	100	-

Management of Local AP interface (Only for USG40W & USG60W)

(1) Add 2 SSIDs in the SSID list (LAN1 and LAN2 subnet)

Go to **Configuration > Object > AP Profile > SSID > SSID list** and click on the "Add" button to create SSID object. Disable "VLAN support" and select the "LAN1" interface in **Local VAP Settings**.

127	CONFIGURATION	Radio SSID		
	TY Quick Setup	SSID List Security List	Edit SSID Profile For_LAN1 ?	×
			🔚 Create new Object 🕶	
		SSID Summary		
130			Profile Name: For_LAN1	
107 .		🔘 Add 📝 Edit 🃋 Remove 🔚	SSID: For_LAN1	
1 m.		# Profile Name 🔺	Security Profile: default	MAC Filtering Profile VLAN ID
		1 For_LAN1		disable 1
		2 For_LAN2	MAC Filtering Profile:	disable 1
	+ BWM	3 default	QoS: WMM Y	disable 1
		4 4 Page 1 of 1 ▶ ▶	VLAN ID: 1 (1~4094)	Displaying 1 - 3 of 3
			Hidden SSID	
			Enable Intra-BSS Traffic blocking	
	AP Profile	• • • • • • • • • • • • • • • • • • •	Enable marboo maine brooking	
	 Application Address 		Local VAP Setting	
	Address Service			
			VLAN Support: O On Off	
			Outgoing Interface: lan1 💌	
	 Certificate ISP Account 			
	SSL Application			
			OK Cancel	

Disable "VLAN support" and select the "LAN2" interface in Local VAP Setting.

1	CONFIGURATION	Radio SSID				
	📲 Quick Setup	SSID List Security List	Edit SSID Profile For_LAN2	? ×		
			Em Create new Object •			
		SSID Summary				
6	 Controller AP Management 	🔘 Add 📝 Edit 🍟 Remove 📷	Profile Name: For_LAN2			
1			SSID: For_LAN2			
		# Profile Name 🔺	Security Profile: default		MAC Filtering Profile	VLAN ID
		1 For_LAN1	MAC Filtering Profile: disable		disable	1
		2 For_LAN2			disable	1
	BWM	3 default	QoS: WMM		disable	1
		4 4 Page 1 of 1 ▶	VLAN ID: 1 (1~4094)			Displaying 1 - 3 of 3
			Hidden SSID			
	- User/Group		Enable Intra-BSS Traffic blocking			
	- AP Profile		,,,,,,,			
	 Application Address 		Local VAP Setting			
			VLAN Support: O On Off			
			Outgoing Interface: lan2 Y			
	 Auth. Method Certificate 		L			
	ISP Account					
			ОК Са	ancel		
				_		

- (2) Add AP profiles and select these 2 SSID objects in the rule.
- Go to Configuration > Object > AP Profile > RADIO and click on the "Add" button to create the AP profile

2.4G Band			
CONFIGURATION	Radio	Add Radio Profile	
11 Licensing 12 Wirdless 12 Wirdless 13 Bearding 14 UTM Profile 15 UTM Profile 15 UTM Profile 12 UTM Profile 13 Digital 14 Digital 14 Digital 15 Digital <t< td=""><td>Radio Summary</td><td>Show Advanced Settings Create new Object* General Settings Advate Profile Name: Loca_WALN 802.11 Band: 2.46 Mode: b/q/n Channel: 6 MBSSID Settings Keldt For_LAN1 For_LAN1 For_LAN1 For_LAN2 Gable Ga</td><td>Displaying 1 - 2 o</td></t<>	Radio Summary	Show Advanced Settings Create new Object* General Settings Advate Profile Name: Loca_WALN 802.11 Band: 2.46 Mode: b/q/n Channel: 6 MBSSID Settings Keldt For_LAN1 For_LAN1 For_LAN1 For_LAN2 Gable Ga	Displaying 1 - 2 o
5G Band Сонявиатом Шеспяіля У Quick Setup	Radio SSID Radio Summary	8 disable OK Cancel	×
 Wireless Wireless Wireless Web Authentication Security Policy WPN UTM Profile Object Zone Marginal Profile User/Group Arg From Apdress Service Schedule Address Schedule Address Schedule Address Schedule Certificate IS Acount System Log & Report 	Add Z Edk T Rem # Status 1 9 2 9 3 9 4 9 14 4 Page 1 of 1	General Settings	Displaying 1 - 3
		OK Cancel	

(3) Apply AP profiles to the Local AP interface

Go to **Configuration > Wireless > AP Management** and click the local AP (IP address is 172.0.0.1) to edit the rule.

Apply the AP profiles to this rule.

9	CONFIGURATION	Mgnt. AP List							
	U Quick Setup Licensing Wireless - Controller - AP Management	Mgnt. AP List	ot MAC Addre	iss Model	R1 Mode / Profile	R2 Mode / Profile	Mgnt. VLAN I	Mgnt. VLAN I	Description 🔺
R .	Network	1 127.0.0.1	B0:B2:DC:7		/ AP / default	AP / default2	1	n/a	Local-AP
	 Web Authentication Security Policy 	🛛 🗐 🖉 Page 1 🛛 of 1 🛛 🕨	🕅 🛛 Show 🧕	🖉 Edit AP List				? ×	Displayin
	Security Folicy VPN			🛅 Create new Object •					
				Configuration					
				MAC:	B0:B2:DC:70:C1:D6				
				Model:	USG60W				
				Description:	Local-AP				
				Radio 1 OP Mode	AP Mode				
	 Service Schedule 			Radio 1 Profile:	Local_WALN	~			
	AAA Server			Radio 2 OP Mode	AP Mode				
				Radio 2 Profile:	Local_WALN_5G	~			
	Log & Report								
						ſ	OK Cance		
						l			

Verification:

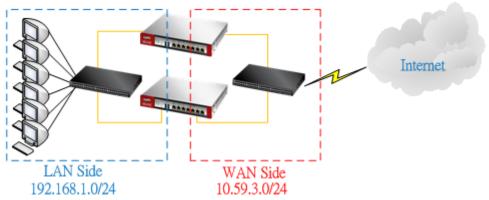
If you have connected to For_LAN1 SSID, then you will get the LAN1 subnet IP address. If you connect to For_LAN2, then you will get the LAN2 subnet IP address.

ZyXEL00036	
VIDEOTRON0048	llee
СНТ6695	llee
For_LAN1	102
Wireless1	<u>.</u>
ZyXEL	3 al 📒
ZyXEL_3DTT	llee
TTNET_ZyXEL_F4YW	llee
Keenetic-5079	lle.
BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB	llee
For_LAN2	- 111

Scenario 15 – Device HA on the USG

15.1 Application Scenario

Setup the Device HA environment.



	Master device	Backup device
WAN interface IP	10.59.3.100/24	10.59.3.100/24
WAN Management IP	10.59.3.101/24	10.59.3.102/24
LAN1 Interface IP	192.168.1.1/24	192.168.1.1/24
LAN1 Management IP	192.168.1.11/24	192.168.1.12/24
Cluster ID	1	1

15.2 Configuration Guide

On Master setting:

(1) Go to Configuration > Network > Interface > Ethernet to check the WAN and LAN interface setting. WAN interface is: 10.59.3.100/24

LAN interface is: 192.168.1.1/24

	uration	.		
		V Activate V Inactivate	Greate Virtual Interface 🔚 Object Reference	
#	Status 🔺	Name	IP Address	Mask
1	<u></u>	wan1	STATIC 10.59.3.100	255.255.255.0
2	@	wan2	DHCP 0.0.0.0	0.0.0.0
3	@	opt	STATIC 0.0.0.0	0.0.0.0
4	@	lan1	STATIC 192.168.1.1	255.255.255.0
5	Q	lan2	STATIC 192.168.2.1	255.255.255.0
6	@	reserved	STATIC 0.0.0.0	0.0.0.0
7	Q	dmz	STATIC 192.168.3.1	255.255.255.0

(2) Go to **Configuration** > **Device HA** > **Activate-Passive Mode** to add the management interface on the master device.

The **Device Role** must be set as "Master". WAN management IP address is: 10.59.3.101 LAN management IP address is: 192.168.1.11

	Activ	e-Passive Mode						
Show	Advanced S	Settings						
enera	al Settings							
Devic	ce Role:	🖲 Master 🛛 🔘 Ba	ckup					
uster	r Settings							
Clust	er ID:	1						
onito	red Interfac	e Summary						
	🔀 Edit. 🧟 Activate 🔞 Inactivate							
📝 E	Edit 💡 Activ	/ate 🗑 Inactivate						
≥ E #	dit 🥥 Activ Status	rate 😡 Inactivate	Virtual Router IP/Netmask	Management IP / Netmask	Link Status			
		-	Virtual Router IP/Netmask 10.59.3.100 / 255.255.255.0	Management IP / Netmask 10.59.3.101 / 255.255.255.0	Link Status Up			
#		Interface 🔺						
	Status	Interface 🔺 wan1			Up			
# 1 2	Status G	Interface 🔺 wan1 wan2			Up Down			
# 1 2 3	Status G	Interface 🔺 wan1 wan2 opt	10.59.3.100 / 255.255.255.0 / /	10.59.3.101/255.255.255.0 / /	Up Down Down			
# 1 2 3 4	Status ତ ତ ତ ତ ତ	Interface wan1 wan2 opt Ian1	10.59.3.100 / 255.255.255.0 / / 192.168.1.1 / 255.255.255.0	10.59.3.101/255.255.255.0 / / 192.168.1.11/255.255.255.0	Up Down Down Up			
# 1 2 3 4 5	Status ତ ତ ତ ତ ତ	Interface wan1 wan2 opt lan1 lan2	10.59.3.100 / 255.255.255.0 / / 192.168.1.1 / 255.255.255.0	10.59.3.101/255.255.255.0 / / 192.168.1.11/255.255.255.0	Up Down Down Up Down			

(3) Go to **Configuration** > **Device HA** > **General** to enable the Device HA function.

After you have enabled the Device HA function, you will see the interface that was monitored above.

ral S	Settings					
Enal	ble Device HA					
_	HA Mode: A	Active-Passive Mode				
wice F						
vice F	HA Mode: P	COVE-Passive Mode				
	d Interface Summary					
tored			Management IP / Netmask	Link Status	HA Status	
tored	d Interface Summary		Management IP / Netmask 10.59.3.101 / 255.255.0	Link Status	HA Status Master / Active	

On Backup setting:

(4) Go to **Configuration** > **Network** > **Interface** > **Ethernet** to check the WAN and LAN interface setting. WAN interface is: 10.59.3.100/24

LAN interface is: 192.168.1.1/24

ort Ro	Etherne	et PPP Cellular	Tunnel VLAN Bridge Trunk	
onfia	uration			
_		💡 Activate 💿 Inactiva	te দ Create Virtual Interface 📴 Object Reference	
#	Status 🔺	Name	IP Address	Mask
1		wan1	STATIC 10.59.3.100	255.255.255.0
2	@	wan2	DHCP 0.0.0.0	0.0.0.0
3	@	opt	STATIC 0.0.0.0	0.0.0.0
4	9	lan1	STATIC 192.168.1.1	255.255.255.0
5	9	lan2	STATIC 192.168.2.1	255.255.255.0
6	@	reserved	STATIC 0.0.0.0	0.0.0.0
7	Q	dmz	STATIC 192.168.3.1	255.255.255.0

(5) Go to Configuration > Device HA > Activate-Passive Mode to add the management interface on the backup device.

The **Device Role** must se as "Backup". WAN management IP address is: 10.59.3.102 LAN management IP address is: 192.168.1.12

Show A	dvanced s	Settings			
eneral s	Settings				
Device	Role:	🔘 Master	Backup		
Prio	ority:	1	(1-254)		
	Enable P	reemption			
uster S	Settings				
Cluster	ID:	1			
onitore	ed Interfac	ce Summary			
		ce Summary vate @ Inactivate			
🖉 Edit			Virtual Router IP/Netmask	Management IP / Netmask	Link Status
📝 Edit	it 💡 Activ	vate 🗑 Inactivate	Virtual Router IP/Netmask 10.59.3.100 / 255.255.255.0	Management IP / Netmask 10.59.3.102 / 255 255 255 0	Link Status Up
2 Edi #	it 💡 Activ	vate @ Inactivate			
2 Edit #	it 💡 Activ Status	vate @ Inactivate Interface wan1			Up
₽ Edit # 1 2 3	it 💡 Activ Status 💡	vate P Inactivate Interface A wan1 wan2			Up Down
✓ Edit # 1 2 3 4	it ୃତ Activ Status ତୃ ଜୁ ଜୁ	vate @ Inactivate Interface _ wan1 wan2 opt	10.59.3.100 / 255.255.255.0 / /	10.59.3.102 / 255.255.255.0 / /	Up Down Down
<pre></pre>	it @ Activ Status @ @ @ @	vate @ Inactivate Interface ~ wan1 wan2 opt Ian1	10.59.3.100 / 255.255.255.0 / / 192.168.1.1 / 255.255.255.0	10.59.3.102 / 255.255.0 / / 192.168.1.12 / 255.255.255.0	Up Down Down Up
🖉 Edit	it @ Activ Status @ @ @ @ @	vate @ Inactivate Interface A wan1 wan2 opt Ian1 Ian2	10.59.3.100 / 255.255.255.0 / / 192.168.1.1 / 255.255.255.0	10.59.3.102 / 255.255.0 / / 192.168.1.12 / 255.255.255.0	Up Down Down Up Down

(6) Go to **Configuration** > **Device HA** > **General** to enable Device HA function.

After you have enabled the Device HA function, you will saw the interface that was monitored above.

ieral	Settings				
il En	able Device HA				
j ena					
	HA Mode: A	ctive-Passive Mode			
evice	- The House -				
evice	, and the second s				
	ed Interface Summary				
nitore	ed Interface Summary				
nitore			Management IP / Netmask	Link Status	HA Status
nitore #	ed Interface Summary		Management IP / Netmask 10.59.3.102 / 255.255.0	Link Status	HA Status Backup / Stand-By

Verification:

You can check the status of the Device HA in the GUI. The status of the master device will be "Master/Activate".

General	Active-Passive Mode				
General	Settings				
Device	able Device HA e HA Mode: Active-Pas ed Interface Summary	sive Mode			
#	Interface 🔺	Virtual Router IP/Netmask	Management IP / Netmask	Link Status	HA Status
1	wan1	10.59.3.100 / 255.255.255.0	10.59.3.101/255.255.255.0	Up	Master / Active
2	lan1	192.168.1.1/255.255.255.0	192.168.1.11/255.255.255.0	Up	Master / Active
14 4	Page 1 of 1 ▶ ▶ S	how 50 👻 items			Displaying 1 - 2 of 2
The s		ackup device will	be "Backup/Stand	l-By"	
General	Active-Passive Mode				

Genera					
Genera	al Settings				
Devi	Enable Device HA ice HA Mode:	Active-Passive Mode			
#	Interface 🔺	Virtual Router IP/Netmask	Management IP / Netmask	Link Status	HA Status
1	wan1	10.59.3.100 / 255.255.255.0	10.59.3.102 / 255.255.255.0	Up	Backup / Stand-By
2	lan1	192.168.1.1 / 255.255.255.0	192.168.1.12/255.255.255.0	Up	Backup / Stand-By
14		▶ ▶ Show 50 v items			Displaying 1 - 2 of 2

Tutorial 1: How to Set Up Your Network

Here are examples of using the Web Configurator to set up your network in the USG.

Note: The tutorials featured here require a basic understanding of connecting to and using the Web Configurator. For field descriptions of individual screens, see the Web Configurator Online Help.

1.1 Wizard Overview

Use the wizards to quickly configure Internet connection and VPN settings as well as activate subscription services.

WIZARD	DESCRIPTION
Installation Setup Wizard	Use this wizard the first time log into the Web Configurator to configure WAN connections and register your USG.
Quick Setup	You can find the following wizards in the CONFIGURATION navigation panel.
WAN Interface	Use these wizard screens to quickly configure a WAN interface's encapsulation and IP address settings.
VPN Setup	Use these wizard screens to quickly configure an IPSec VPN or IPSec VPN configuration provisioning.

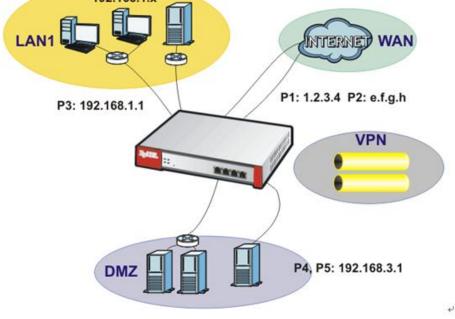
After you complete a wizard, you can go to the **CONFIGURATION** screens to configure advanced settings.

1.2 How to Configure Interfaces, Port Roles, and Zones

This tutorial shows how to configure Ethernet interfaces, port roles, and zones for the following example configuration.

• The **wan1** interface uses a static IP address of 1.2.3.4.

- Add **P5** (lan2) to the DMZ interface (Note: In USG 20/20W, use **P4** (lan2) instead of **P5** in this example). The DMZ interface is used for a protected local network. It uses IP address 192.168.3.1 and serves as a DHCP server by default.
- You want to be able to apply specific security settings for the VPN tunnel created by the Quick Setup - VPN Setup wizard (named WIZ_VPN). So you create a new zone and add WIZ_VPN to it.
- Figure 21 Ethernet Interface, Port Roles, and Zone Configuration Example



1.2.1 Configure a WAN Ethernet Interface

You need to assign the USG's **wan1** interface a static IP address of 1.2.3.4.

Click **Configuration > Network > Interface > Ethernet** and double-click the **wan1** interface's entry in the **Configuration** section. Select **Use Fixed IP Address** and configure the IP address, subnet mask, and default gateway settings and click **OK**.

Pv4 View * 🔝 Show Advanced Setti	ngs 🔠 Create new Object		
Description:			(Optional)
IP Address Assignment			
Get Automatically			
Use Fixed IP Address			
IP Address:	1.2.3.4		
Subnet Mask:	255.255.255.0		
The second se	1.2.3.254	(Option)	
Gateway:			

1.2.2 Configure Port Roles

Here is how to take the **P5** port from the lan2 interface and add it to the dmz interface.

1 Click Configuration > Network > Interface > Port Role.

2 Under **P5** select the **dmz (DMZ)** radio button and click **Apply**.

on					
	000/100/1000			10/100/100	0
1	- FT	57	F7	M	
			(Insurant)		
lan1 (LAN1)		0	0	0	0
		0	0	0	0
lan2 (LAN2)					

1.2.3 Configure Zones

In this example you have created a **WIZ_VPN** tunnel through the **Quick Setup - VPN Setup** wizard. By default, it is assigned to the **IPSec_VPN** zone. Do the following to move **WIZ_VPN** from the **IPSec_VPN** zone to a new zone.

- 1 Click Configuration > Network > Zone and then double-click the IPSec_VPN entry.
- 2 Select **WIZ_VPN** and remove it from the **Member** box and click **OK**.

Edit Zone		7
Group Members		
Name:	IPSec_VPN	
I Block Intra-zone Traffic	0	
Member List		
- Available	Member === VPN Tunnel === Default_LZTP_VPN_Connection VPN_CONN_EXAMPLE WIZ_VPN	
	WIZ_VPN_PROVISIONING	
1		
		ancel

- 3 Back to the **Configuration > Network > Zone** screen and click **Add in the User Configuration** section.
- 4 Enter **VPN** as the new zone's name. Select **WIZ_VPN** and move it to the **Member** box and click **OK**.

iroup Members		
Name:	VPN affic 🚺	
1ember List		
Available	6	Member === VPN Tunnel === WIZ_VPN

Then you can configure firewall rules to apply specific security settings to this **VPN** zone.

1.3 How to Configure a Cellular Interface

Use 3G cards for cellular WAN (Internet) connections. See www.zyxel.com for a supported 3G card. In this example you connect the 3G USB card before you configure the cellular interfaces but is also possible to reverse the sequence.

- 1 Make sure the 3G device's SIM card is installed.
- 2 Connect the 3G device to one of the USG's USB ports.
- 3 Click **Configuration > Network > Interface > Cellular**. Select the 3G device's entry and click **Edit**.

\$	Status	Name	Extension Slot	Connected Device	ISP Settings
1	ନ୍ତ	cellular1	USB 1	Huawei E220	Device Profile 1
14	I Page	1 of 1 >)	Show 50 v items		Displaying 1 - 1

4 Enable the interface and add it to a zone. It is highly recommended that you set the Zone to WAN to apply your WAN zone security settings to this 3G connection. Leaving Zone set to none has the USG not apply any security settings to the 3G connection. Enter the PIN Code provided by the cellular 3G service provider (0000 in this example).

Edit Cellular configuration		?
Hide Advanced Settings		
General Settings		
Enable Interface		
Interface Properties		
Interface Name:	cellular1	
Zone:	WAN Y	
Extension Slot:	USB 1	
Connected Device:	Huawei E220	
Description:	(Optional)	
Connectivity		
V Naled-Up		
Idle timeout:	0 seconds	
SP Settings		
Profile Selection:	Device Custom	
	Profile 1 👻	
APN:	n/a	
Dial String:	n/a	
5IM Card Setting		
PIN Code:		
Retype to Confirm:		
		OK Cancel

- Note: The **Network Selection** is set to **auto** by default. This means that the 3G USB modem may connect to another 3G network when your service provider is not in range or when necessary. Select **Home** to have the 3G device connect only to your home network or local service provider. This prevents you from being charged using the rate of a different ISP.
- **5** Go to the **Dashboard**. The **Interface Status Summary** section should contain a "cellular" entry. When its connection status is **Connected** you can use the 3G connection to access the Internet.

🧕 II	nterface S	tatus Summary			• © ¢ ×
#	Name	Status	Zone	IP Address	Action
1	wan1	Down	WAN	0.0.0.0	n/a
2	wan1_pp	Disconnected	WAN	100000-7	8
3	wan2	Down	WAN	0.0.0.0	Renew
4	lan1	Down	LAN1	192.168.1.1	n/a
5	lan2	100M/Full	LAN2	192.168.2.1	n/a
6	dmz	Down	DMZ	192.168.3.1	n/a
7	cellular1	Connected	n/a	10.000	
14	4 Page	1 of 1 🕨 🕅	Show 50	👻 items Display	/ing 1 - 7 of 7

6 The USG automatically adds the cellular interface to the system default WAN trunk. If the USG is using a user-configured trunk as its default trunk and you want this cellular interface to be part of it, use the **Trunk** screens to add it.

This way the USG can automatically balance the traffic load amongst the available WAN connections to enhance overall network throughput. Plus, if a WAN connection goes down, the USG still sends traffic through the remaining WAN connections. For a simple test, disconnect all of the USG's wired WAN connections. If you can still access the Internet, your cellular interface is properly configured and your cellular device is working.

This tutorial applies only to models that include wireless LAN.

You can configure different interfaces to use on the wireless LAN card. This lets you have different wireless LAN networks using different SSIDs. You can configure the WLAN interfaces before or after you install the wireless LAN card. This example shows how to create a WLAN interface that uses WPA or WPA2 security and the USG's local user database for authentication.

1.4.1 Set Up User Accounts

Besides WPA-PSK, the USG also supports TTLS using PAP so you can use the USG's local user database with WPA or WPA2 instead of needing an external RADIUS server. For each WLAN user, set up a user account containing the user name and password the WLAN user needs to enter to connect to the wireless LAN.

- 1 Click **Configuration > Object > User/Group > User** and the **Add** icon.
- 2 Set the User Name to wlan_user. Enter (and re-enter) the user's password. Click OK.

User Type:	and the second se	
cool ()po.	user	*
Password:	•••••	
Retype:	•••••	
Description:	Local User	
Authentication Timeout Settings	Use Default Setting	gs 🔘 Use Manual Settings
Lease Time:	1440	minutes
Reauthentication Time:	1440	minutes

3 Use the **Add** icon in the **Configuration > Object > User/Group > User** screen to set up the remaining user accounts in similar fashion.

1.4.2 Create the WLAN Interface

- 1 Click **Configuration > Network > Interface > WLAN > Add** to open the **WLAN Add** screen.
- 2 Edit this screen as follows.

A (internal) name for the WLAN interface displays. You can modify it if you want to.

The USG's security settings are configured by zones. Select to which security zone you want the WLAN interface to belong (the WLAN zone in this example). This determines which security settings the USG applies to the WLAN interface.

Configure the **SSID** (ZYXEL_WPA in this example).

If all of your wireless clients support WPA2, select **WPA2-Enterprise** as the **Security Type**, otherwise select **WPA/WPA-2-Enterprise**. Set the **Authentication Type** to **Auth Method**. The

USG can use its default authentication method (the local user database) and its default certificate to authenticate the users.

Add WLAN		8
Show Advanced Settings		
General Settings		
Chable Interface		
Interface Name:	wian-1- 2	
Description:	(Optional)	
Zone:	Please select one	
Virtual Access Point Settings		
SSID:	ZDEL_WPA	
Hide SSID Broadcast		
Block Intra BSS Traffic		
Maximum Associations:	295	
WLAN Security Settings		
Security Type:	WPA2-Enterprise 👻	
Authentication Type:	Auth Method	
Authentication Method:	default v	
TTLS Certificate:	default. V	
IP Address Assignment		
IP Address:	10.1.1.1	
Subnet Mask:	255.255.0.0	
Interface Parameters		
Egress Bandwidth:	1048576 Kbps	
DHCP Setting		
DHCP:	DHCP Server v	
IP Pool Start Address (Optional):	Pool Size:	
First DNS Server (Optional):	Custom Defined v.	
	Accy Access Contraction	Cancel

Configure the interface's IP address and set it to **DHCP Server**. Click **OK**.

2 Turn on the wireless LAN and click **Apply**.

WLAN	Device Settings				
Exte	nsion Slot:		slot1	Y ZYXEL G-17	05
		_			
-	inable WLAN Device		12000		
802.	11 Band:		b+g	~	
Char	nnel:		6	*	
				anna The Advantage	
0	Add 📝 Edit. 🎁 Statu Name 🔺	Constant of the	P Address	Mask	Security
-	Statu Name 🔺	Constant of the	IP Address	La la compañía de la	
-	Statu Name -	SSID	IP Address 10.59.1.1	Mask	Security
# 1 2	Statu Name A wian-1-1 wian-1-2	SSID ZyXEL01 ZYXEL_W	IP Address 10.59.1.1	Mask 255.255.255.0 255.255.0.0	Security

4 Configure your wireless clients to connect to the wireless network.

1.4.2.1 Wireless Clients Import the USG's Certificate

You must import the USG's certificate into the wireless clients if they are to validate the USG's certificate. Use the **Configuration > Object > Certificate > Edit** screen to export the certificate the USG is using for the WLAN interface. Then do the following to import the certificate into each wireless client computer

- 1 In Internet Explorer, click **Tools > Internet Options > Content** and click the **Certificates** button.
- 2 Click Import.
- 3 Use the wizard screens to import the certificate. You may need to change the **Files of Type** setting to **All Files** in order to see the certificate file.
- 4 When you get to the **Certificate Store** screen, select the option to automatically select the certificate store based on the type of certificate.
- 5 If you get a security warning screen, click **Yes** to proceed.
- 6 The Internet Explorer Certificates screen remains open after the import is done. You can see the newly imported certificate listed in the Trusted Root Certification Authorities tab. The values in the Issued To and Issued By fields should match those in the USG's My Certificates screen's Subject and Issuer fields (respectively).

Certificates								?	×
Igtended purpose:	<ai></ai>								<
Trusted Root Certifica	tion Au	thorities	Trusted Publish	ers	Untruster	d Publishers		۲	>
Issued To		Issued B	Y	Ð	piratio	Friendly Na	ame	^	1
Econet Internatio					18/10/02	EUnet Inter	natio		
FESTE, Public No			Pexample.com		12/11/12	FESTE, Pub	lic No.		
FESTE, Verified (FESTE, Verified Certs			2020/01/02 FESTE, Verifie			-	
First Data Digital	First Data Digital C		First Data Digital Certi		19/07/04	First Data Digital			
FNMT Clase 2 CA	FNMT Clase 2 CA		FNMT Clase 2 CA		2019/03/18 Fabric		ional		
Gatekeeper Rool	t CA	Gatekeeper Root CA		20	14/05/24	eSign Australia:			
GeoTrust Global	CA	GeoTrust Global CA		20	22/05/21	GeoTrust Global CA			
GeoTrust Global	CA 2	GeoTrust	Global CA 2	20	19/03/04	GeoTrust G	lobal	~	
Import Export Remove Advanced Certificate intended purposes									
<ai></ai>						C	⊻jew	_)
							Glos	e	

The **My Certificates** screen indicates what type of information is being displayed, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C).

y Cert	tificates	Trusted Cert	tificates		Sector Sector	
KI Sto	orage Space	in Use				
				0.869% used		
u Corl	tificates Set	ting				
0	Add 📝 Edit	TRemove	B Cobject Reference			
#	Name 🔺	Type	Subject	issuer	Valid From	Valid To
1 <	example	SELF	CN=example@example	CN=example@example	2009-11-13 05:39:05 GM	2012-11-12 05:39:05 GM
2	test	SELF	CN-test@example.com	CN-test@example.com	2009-11 13 05:45:24 Ot	2012-11-12 05:45:24 GM
14	4 Page 1	of 1 >	Now 50 ▼ item	×		Displaying 1 - 2 of 2

Repeat the steps to import the certificate into each wireless client computer that is to validate the USG's certificate when using the WLAN interface.

1.4.2.2 Wireless Clients Use the WLAN Interface

Wireless clients enter their username and password when they connect to the wireless network.

1.5 How to Configure Ethernet, PPP, VLAN, Bridge and Policy Routing

The following table describes when to configure the Ethernet, PPP, VLAN, Bridge screens under **Configuration > Network > Interface** and the **Configuration > Network > Routing > Policy Routing** screen.

SCREEN	DESCRIPTION
Ethernet	Configure this if any interface on the USG is connecting to an Ethernet network. Ethernet interfaces are the foundation for defining other interfaces and network policies.
PPP	Configure this if you need your service provider to provide an IP address through PPPoE or PPTP in order to access the Internet or another network.
VLAN	Configure this if you want to divide your physical networks into multiple VLANs, or your service provider or an aggregated network needs the USG to recognize the VLAN tags in the packets flowing through the USG.
Bridge	Configure this if you want the USG to combine two or multiple network segments into one single network. Although the USG is "transparent" in this mode, you can still apply security checking on packets flowing through the USG.
Policy Routing	Configure this if you want to override the USG's default routing behavior in order to send packets through the appropriate interface or VPN tunnel.

 Table 10
 Ethernet, PPP, VLAN, Bridge and Policy Routing Screen Relationships

Since firmware version 3.00, the USG supports IPv6 configuration in these **Ethernet**, **PPP**, **VLAN**, **Bridge** and **Policy Route** screens under **Configuration** > **Network** > **Interface** and **Configuration** > **Network** > **Routing**. Basically, these are the same as the ones for IPv4 networks except the following differences:

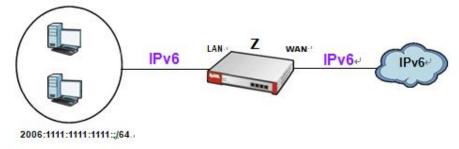
- You have to enable IPv6 globally in the CONFIGURATION > System > IPv6 screen to make the IPv6 settings work.
- An **Enable IPv6** setting Select this in the screens listed above to enable the USG to be able to send and receive IPv6 packets through the interface. Otherwise, the USG discards IPv6 packets flowing through the interface.
- **IPv6 Address Assignment** This section allows you to enable auto-configuration and configure prefix delegation.
- **DHCPv6 Setting** This section allows you to configure the DHCPv6 role and the corresponding settings for the interface.

1.6 How to Set Up IPv6 Interfaces For Pure IPv6 Routing

This example shows how to configure your USG **Z**'s WAN and LAN interfaces which connects two IPv6 networks. USG **Z** periodically advertises a network prefix of 2006:1111:1111:1111:/64 to the LAN through router advertisements.

Note: Instead of using router advertisement, you can use DHCPv6 to pass the network settings to the computers on the LAN.

Figure 22 Pure IPv6 Network Example



1.6.1 Setting Up the WAN IPv6 Interface

- 1 In the **CONFIGURATION** > **Network** > **Interface** > **Ethernet** screen's **IPv6 Configuration** section, double-click the **wan1**.
- 2 The Edit Ethernet screen appears. Select Enable Interface and Enable IPv6. Select Enable Auto-Configuration. Click OK.

Note: Your ISP or uplink router should enable router advertisement.

Edit Ethernet				7
IPv6 View 🔹 🋄 Show Advanced Setting	s 🛅 Create new Object			
General Settings Image: Constraint of the setting General IPv6 Setting Image: Constraint of the setting Image: Constraint of the setting				
Interface Properties Interface Type:	external			
Interface Name: Port:	P1			
Zone:	WAN			
MAC Address:	00:00:AA:79:73:	79		
Description:			(Optional)	
IPv6 Address Assignment				
Enable Auto-configuration Link-Local Address:	n/a			
IPv6 Address/Prefix Length:	1.04	(Optional)		

1.6.2 Setting Up the LAN Interface

- 1 In the CONFIGURATION > Network > Interface > Ethernet screen, double-click the lan1 in the IPv6 Configuration section.
- 2 The Edit Ethernet screen appears. Select Enable Interface and Enable IPv6.

Select **Enable Router Advertisement** and click **Add** and configure a network prefix for the LAN1 (2006:1111:1111:1111::/64 in this example). Click **OK**.

	? ×
sate new Object	
	<u>^</u>
internal	
lan1	
P3, P4	
LAN1	
00:00:AA:79:73:75	
	(Optional)
n/a	
(Optional)	
N/A 👻	
Medum	
Add Edit TRemove	
Pv6 Address/Prefix Length +	
1 2006:1111:1111:111:064	
[4 4 Page 1 of 1 ▷ ▷] Show 50 ♥ to	ems No data to display
	Ian1 P3, P4 LAN1 00:00:AA:79:73:75

You have completed the settings on the USG. But if you want to request a network address prefix from your ISP for your computers on the LAN, you can configure prefix delegation $\,$.

1.6.3 Prefix Delegation and Router Advertisement Settings

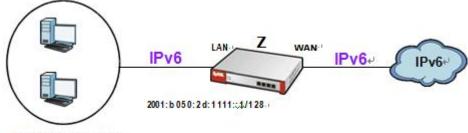
This example shows how to configure prefix delegation on the USG's WAN and router advertisement on the LAN.

1.6.3.1 Apply a Network Prefix From Your ISP

First of all, you have to apply a network prefix from your ISP or the uplink router's administrator. The WAN port's DUID is required when you apply the prefix. You can check the DUID information in the **WAN IPv6 Interface Edit** screen.

This example assumes that you were given a network prefix of 2001:b050:2d::/48 and you decide to divide it and give 2001:b050:2d:1111::/64 to the LAN network. LAN1's IP address is 2001:b050:2d:1111::1/128.

Figure 23 Pure IPv6 Network Example Using Prefix Delegation



2002:b050:2d:1111::/64

1.6.3.2 Setting Up the WAN IPv6 Interface

- 1 In the Configuration > Network > Interface > Ethernet screen's IPv6 Configuration section, double-click the wan1.
- 2 The Edit Ethernet screen appears. Select Enable Interface and Enable IPv6.

Click **Create new Object** to add a **DHCPv6 Request** object with the **Prefix Delegation** type. Select **Enable Auto-Configuration**.

Select **Client** in the **DHCPv6** field. (WAN1's DUID appears.)

Click **Add** in the **DHCPv6 Request Options** table and select the DHCPv6 request object you just created. You cannot see the prefix your ISP gave you in the **Value** field until you click **OK** and then come back to this screen again. It is 2001:b050:2d::/48 in this example.

Note: Your ISP or a DHCPv6 server in the same network as the WAN should assign an IPv6 IP address for the WAN interface.

Edit Ethernet		?
Pv6 View • III Show Advanced Setting	Create new Object	
General Settings	🔕 Add Request Object	
Enable Interface General IPv6 Setting	Name: Request_WAN1_PD Request Type: Prefix Delegation	
Enable IPv6	Request Type: Prefix Delegation	
Interface Properties		
Interface Type:	external	
Interface Name:	wan1	
Port:	P1	
Zone:	WAN	
MAC Address:	00:00:AA:79:73:69	
Description:	(Optional)	
IPv6 Address Assignment IPv6 Address Auto-configuration Unk-Local Address: IPv6 Address/Prefix Length: DHCPv6 Setting	fe80::200:aafl;fe79:7369/64 (Optional)	
DHCPv6:	Client v	
DUID:	00:03:00:01:00:00:AA:79:73:69	
Request Address		
DHCPv6 Request Options	Add Remove To Object Reference	
	# Name - Type Value	
	1 Request_WAN1_PD prefix-delegation n/a	
	[4] 4 Page 1 of 1 ▷ 3 Show 50 v items Displaying 1	- 1 of 1

1.6.3.3 Setting Up the LAN Interface

- 1 In the **Configuration** > **Network** > **Interface** > **Ethernet** screen, double-click the **lan1** in the **IPv6 Configuration** section.
- 2 The **Edit Ethernet** screen appears. Click **Show Advanced Settings** to display more settings on this screen.

Select Enable Interface and Enable IPv6.

In the **Address from DHCPv6 Prefix Delegation** table, click **Add** and select the DHCPv6 request object from the drop-down list, type ::1111:0:0:0:1/128 in the **Suffix Address** field. (The combined address 2001:b050:2d:1111::1/128 will display as LAN1's IPv6 address after you click **OK** and come back to this screen again).

Note: You can configure the IPv6 Address/Prefix Length field instead if the delegated prefix is never changed.

Select Enable Router Advertisement.

In the **Advertised Prefix from DHCPv6 Prefix Delegation** table, click **Add** and select the DHCPv6 request object from the drop-down list, type ::1111/64 in the **Suffix Address** field. (The combined prefix 2001:b050:2d:1111::/64 will display for the LAN1's network prefix after you click **OK** and come back to this screen again).

sea al Settings	
Enable Interface	
E Date Dut	
torface Properties	
Interface Type:	attend
Interlace Name	bel
Rut:	17.14
Interi	LANE
HINC Allarma:	00.00 AA 29 72 75
Gescription	(Optime)
vis Address Assignment	
🗇 Enable Stabilitis Address Auto-configur	ation (0.444)
Unik-Local Address:	4/4
INs Address/Invefix Length:	(Optional)
Gatterian):	(Optimal)
Hetric:	0-01
Address from DHONG Prefix Delegation	(Q AAI) (2 M Themas
	A Detraded Public Suffy Address Address
	(1 Repert, WAY, PD 11115511118 **
	30 C Page 1 (of 1 3 3) Show 70 (so her No data to shutter
The Letter	
	NA (w)
	N/A (<u>m</u>)
	N/A (m)
MP46	NA (m)
i Routor Advertisement Setting	
6 Router Advertisement Setting 7 Enable Router Advertisement 3 Advertised tradit Get Network Configu	nation from DHCIVE
6 Router Advertisement Setting (Enable Inster Advertisement 3 Advertised trads Get Network Configurat 3 Advertised trads Get Other Configurat	nation from DHCPv9 Inn From DHCPv9
A Rooter Advertisement Setting Finalis Invire Advertisement Advertised tools Get Network Cardiga Advertised Tools Get Other Cardigant Isolar Preference:	nation From DHCPV6 Ion From DHCPV6 Medium
Cirul Setting SHCPuts 46 Rowbor Advertisement Setting 27 Enable Inster Advertisement 28 Advertised Hode Get Other Certigant Inster Preference: Hits: tax Linkt	nation Anum DHCIV6 Ine Front DHCIV6 Medium 3990 (1.380-1500, 0 is divadient)
StCPut: 6 Router Advertisement Setting 7 Index Roder Advertisement 9 Advertised Hode Cardigat 1 Advertised Hod	nation from DHCDV6 Ine From DHCDV6 Heddum 1980 (L380-1500, 0 is disabled) 01 (0-255, 0 is disabled)
Router Advertisement Setting Ender Index Advertisement Advertise Index Advertisement Advertised Holds Get Network Configurat Advertised Holds Get Other Configurat advertised Holds Records Tax age Land:	Add and an
StOve: 6 Rowton Advertisement Setting 7 India India Advertisement 9 Advertised Hindu Get Other Gerligand India Professore Higs	nation from DHCDV6 Ine From DHCDV6 Heddum 1980 (L380-1500, 0 is disabled) 01 (0-255, 0 is disabled)
Router Advertisement Setting Ender Inder Advertisement Advertise Fields Cardigat Advertised Fields Cardigat Advertised Fields Cardigat Advertised Fields Cardigat Inder Preference: Tip: Tip:	Add and an
NCPuE 6 Rowles Advertisement Sutting (Enable Rowler Advertisement) 3 Advertised Holls Git Ober Configurat ander Profesence Tip: top Linet: doortised Profes Table	nation from DHDHs Ine From DHDHs Hedum 1990 (J.380-1500, 0 is disabled) M (J.380-1500, 0 is dis disabled) M (J.380-1500, 0 is disabled) M (J.380-1500, 0 is
6 Router Advertisement Setting 6 Router Advertisement Setting 7 Advertised Hode Advertisement 9 Advertised Hode Get Ober Gerligant sader Helevence Hits: tag Land:	nitian Franc DHCIV4 Ine Franc DHCIV4 Medium 1980 (J.180-1500, 0 s disetiled) 64 (J.180-255, 0 s disetiled) 65 (J.180-255, 0 s disetiled) 66 (J.180-255, 0 s disetiled) 67 (J.180-255, 0 s disetiled) 68 (J.180-255, 0 s

1.6.4 Test

1 Connect a computer to the USG's LAN1.

2 Enable IPv6 support on you computer.

In Windows XP, you need to use the IPv6 install command in a Command Prompt.

In Windows 7, IPv6 is supported by default. You can enable IPv6 in the **Control Panel** > **Network** and **Sharing Center** > **Local Area Connection** screen.

- **3** Your computer should get an IPv6 IP address (starting with 2001:b050:2d:1111: for this example) from the USG.
- 4 Open a web browser and type http://www.kame.net. If your IPv6 settings are correct, you can see a dancing turtle in the website.

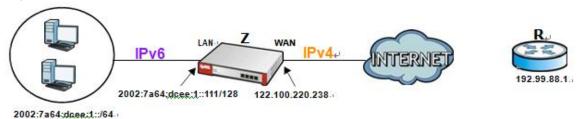
1.6.5 What Can Go Wrong?

- 1 If you forgot to enable **Auto-Configuration** on the WAN1 IPv6 interface, you will not have any default route to forward the LAN's IPv6 packets.
- 2 To use prefix delegation, you must set the WAN interface to a DHCPv6 client, enable router advertisements on the LAN interface as well as configure the Advertised Prefix from DHCPv6 Prefix Delegation table.
- 3 If the **Value** field in the WAN1's **DHCPv6 Request Options** table displays **n/a**, contact your ISP for further support.
- 4 In Windows, some IPv6 related tunnels may be enabled by default such as Teredo and 6to4 tunnels. It may cause your computer to handle IPv6 packets in an unexpected way. It is recommended to disable those tunnels on your computer.

1.7 How to Set Up an IPv6 6to4 Tunnel

This example shows how to use the interface configuration screens to create the following 6to4 tunnel.

Figure 24 6to4 Tunnel Example



In this example, the USG (**Z**) acts as a 6to4 router which connects the IPv4 Internet (through WAN1 with an IP address of 122.100.220.238) and an IPv6 intranet network. In the 6to4 tunnel application, you must configure the LAN1 with an IP address starting with 2002:7a64:dcee::/48 if you decide to use the WAN1 IP address to forward 6to4 packets to the IPv4 network. The second and third sets of 16-bit IP address from the left must be converted from 122.100.220.238. It becomes 7a64:dcee in hexadecimal. You are free to use the fourth set of 16-bit IP address from the left in order to allocate different network addresses (prefixes) to IPv6 interfaces. In this example,

the LAN1 network address is assigned to use 2002:7a64:dcee:1::/64 and the LAN1 IP address is set to 2002:7a64:dcee:1::111/128.

A relay router **R** (192.99.88.1) is used in this example in order to forward 6to4 packets to any unknown IPv6 addresses.

1.7.1 Configuration Concept

After the 6to4 tunnel settings are complete, IPv4 and IPv6 packets transmitted between WAN1 and LAN1 will be handled by the USG through the following flow.

Figure 256to4 Tunnel Configuration Concept



1.7.2 Setting Up the LAN IPv6 Interface

- 1 In the **CONFIGURATION** > **Network** > **Interface** > **Ethernet** screen's **IPv6 Configuration** section, double-click the **lan1**.
- 2 The Edit Ethernet screen appears. Select Enable Interface and Enable IPv6.

Type **2002:7a64:dcee:1::111/128** in the **IPv6 Address/Prefix Length** field for the LAN1's IP address.

Enable **Router Advertisement**. Then click **Add** in the **Advertised Prefix Table** to add **2002:7a64:dcee:1::/64**. The LAN1 hosts will get the network prefix through the router advertisement messages sent by the LAN1 IPv6 interface periodically. Click **OK**.

General Settings	
Enable Interface	
General IPv6 Setting	
Enable IPv6	
Interface Properties	
Interface Type:	internal
Interface Name:	lan1
Port:	P2, P3
Zone:	LANI
MAC Address:	00:00:AA:79:73:6A
Description:	(Optional)
IPv6 Address Assignment	
Enable Stateless Address Auto-configurati Link-Local Address:	on (SLAAC) fe80::200:aaff:fe79:736a/64
IPv6 Address/Prefix Length:	2002:7a64:dcee:1::111 Optional)
DHCPv6 Setting	
DHCPv6:	N/A 👻
IPv6 Router Advertisement Setting	
Enable Router Advertisement	
Router Preference:	Medum 🛩
Advertised Prefix Table	Add ZEdt. TRemove
	# IPv6 Address/Prefix Length
	1 2002:7a64:dcee:1::/64
	4 4 Page 1 of 1 ▶ ▶ Show 50 v items Displaying 1 - 1 of 1

1.7.3 Setting Up the 6to4 Tunnel

- 1 Click Add in the CONFIGURATION > Network > Interface > Tunnel screen.
- 2 The Add Tunnel screen appears. Select Enable.

Enter tunnel0 as the Interface Name and select 6to4 as the Tunnel Mode.

In the **6to4 Tunnel Parameter** section, this example just simply uses the default **6to4 Prefix**, 2002:://16. Enter your relay router's IP address (192.88.99.1 in this example).

Select wan1 as the gateway. Click OK.

Add Tunnel	Farry States	
Show Advanced Settings		
General Settings		
Enable		
Interface Properties		
Interface Name:	(tunnel0	
Zone:	TUNNEL 📉 🚺	
Tunnel Mode:	(6to4	
IPv6 Address Assignment		
IPv6 Address/Prefix Length:		10.000
		(Optional)
Metric:	0 (0-15)	
6to4 Tunnel Parameter		
6to4 Prefix:	2002::/16	
	100.00.00.1	
Relay Router:	192.88.99.1	(Optional)
		(Optional)
	192.88.99.1	(Optional)
NOTE: traffic destinated to the r		(Optional)
		(Optional)
NOTE: traffic destinated to the r	on-6to4 prefix domain tunnels to the relay router	- 122.100.220.238/255.255.255.0
NOTE: traffic destinated to the r Gateway Settings My Address	on-6to4 prefix domain tunnels to the relay router	

1.7.4 Testing the 6to4 Tunnel

- 1 Connect a computer to the USG's LAN1.
- 2 Enable IPv6 support on you computer.

In Windows XP, you need to use the IPv6 install command in a Command Prompt.

In Windows 7, IPv6 is supported by default. You can enable IPv6 in the **Control Panel** > **Network** and **Sharing Center** > **Local Area Connection** screen.

- **3** You should get an IPv6 IP address starting with 2002:7a64:dcee:1:.
- **4** Type ping -6 ipv6.google.com in a Command Prompt to test. You should get a response.

1.7.5 What Can Go Wrong?

1 Do not enable Auto-Configuration for the LAN1 IPv6 interface. Enabling it will cause two default routes, however, the USG only needs a default route generated by your relay router setting.

In 6to4, the USG doesn't need a policy route to determine where to forward a 6to4 packet (starting with 2002 in the IPv6 IP address). The next gateway information of where to forward a 6to4 packet can be retrieved from the packet's destination IP address. The USG only forwards a 6to4 packet to the relay router using the default route if the packet's destination is not an IP address starting with 2002.

2 You don't need to activate the WAN1 IPv6 interface but make sure you enable the WAN1 IPv4 interface. In 6to4, the USG uses the WAN1 IPv4 interface to forward your 6to4 packets over the IPv4 network.

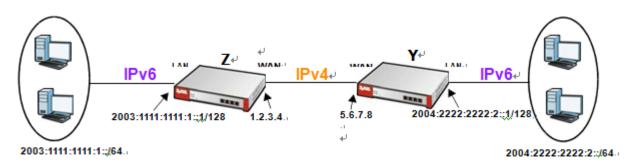
Note: For 6to4, you do not need to enable IPv6 in the wan1 since the IPv6 packets will be redirected into the 6to4 tunnel.

3 In Windows, some IPv6 related tunnels may be enabled by default such as Teredo and 6to4 tunnels. It may cause your computer to handle IPv6 packets in an unexpected way. It is recommended to disable those tunnels on your computer.

1.8 How to Set Up an IPv6-in-IPv4 Tunnel

This example shows how to use the interface and policy route configuration screens to create an IPv6-in-IPv4 tunnel.

Figure 26 IPv6-in-IPv4 Tunnel Example



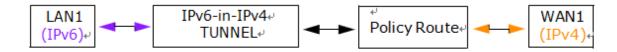
In this example, the USGs (**Z** and **Y**) act as IPv6-in-IPv4 routers which connect the IPv4 Internet and an individual IPv6 network. This configuration example only shows the settings on USG **Z**. You can use similar settings to configure USG **Y**.

Note: In the IPv6-in-IPv4 tunnel application, you must configure the peer gateway's WAN IPv4 address as the remote gateway IP.

1.8.1 Configuration Concept

After the IPv6-in-IPv4 tunnel settings are complete, IPv4 and IPv6 packets transmitted between WAN1 and LAN1 will be handled by the USG through the following flow.

Figure 27 IPv6-in-IPv4 Tunnel Configuration Concept



1.8.2 Setting Up the IPv6-in-IPv4 Tunnel

1 Click Add in the CONFIGURATION > Network > Interface > Tunnel screen.

2 The Edit Tunnel screen appears. Select Enable.

Enter tunnel0 as the Interface Name and select IPv6-in-IPv4 as the Tunnel Mode. Select wan1 in the Interface field in the Gateway Settings section.

Enter 5.6.7.8 as the remot	e gateway's IP	address.	Click OK .
-----------------------------------	----------------	----------	-------------------

Edit Tunnel		7
Show Advanced Settings		
General Settings		
Enable		
Interface Properties		
Interface Name:	tunnel0	
Zone:	TUNNEL 👻 🔳	
Tunnel Mode:	IPv6-in-IPv4	
IPv6 Address Assignment		
IPv6 Address/Prefix Length:		(Optional)
IPv6 Address/Prefix Length: Metric:	0 (0-15)	(Optional)
Metric:	0 (0-15)	(Optional)
Metric:	0 (0-15)	(Optional)
Metric: Gateway Settings		(Optional)
Metric: Gateway Settings My Address		

1.8.3 Setting Up the LAN IPv6 Interface

- 1 Select lan1 in the IPv6 Configuration section in the CONFIGURATION > Network > Interface > Ethernet screen and click Edit.
- 2 The Edit Ethernet screen appears. Select Enable Interface and Enable IPv6.

Type **2003:1111:1111:1::1/128** in the **IPv6 Address/Prefix Length** field for the LAN1's IP address.

Enable **Router Advertisement**. Then click **Add** in the **Advertised Prefix Table** to add **2003:1111:1111:1::/64**. The LAN1 hosts will get the network prefix through router advertisements sent by the LAN1 IPv6 interface periodically. Click **OK**.

Edit Ethernet		7
IPv6 View * 🔝 Show Advanced Settings	Em Create new Object	
General Settings General IPv6 Setting IPv6 Setting Ipv6 Setting		_
Interface Properties		
Interface Type:	internal	
Interface Name:	lan1	
Ports	P2, P3	
Zone:	LANI	
MAC Address:	00:00:AA:79:73:6A	
Description:	(Optional)	
IPv6 Address Assignment Enable Stateless Address Auto-co Link-Local Address:	nfguration (SLAAC) fe80:::200:aaff:fe79::736a;64	-
IPv6 Address/Prefix Length:	2003:1111:1111:1::1/1 Optional)	
DHCPv6 Setting		
DHOPv6:	NjA 🛩	
IPv6 Router Advertisement Settin	9	- 1
Router Preference:	Medum 🛩	
Advertised Prefix Table	Add WEdt TRemove	
	Pv6 Address/Prefix Length	
	1 2003:1111:1111:1::64	
	4 4 Page 1 of 1 > > Show 50 ♥ items Displaying 1-1 of 1	

1.8.4 Setting Up the Policy Route

- 1 Go to the **CONFIGURATION** > **Network** > **Routing** screen and click **Add** in the **IPv6 Configuration** table.
- 2 The Add Policy Route screen appears. Click Create New Object to create an IPv6 address object with the address prefix of 2003:1111:111:1::/64. Select Enable.

Select the address object you just created in the **Source Address** field.

Select any in the Destination Address field.

Select **Interface** as the next-hop type and then **tunnel0** as the interface. Click **OK**.

Configuration Enable Description:	(Op	Name: Object Type: IPv6 Address Prefix:	LANI_SUBNET SUBNET × 2003:1111:1111:1::/64
Criteria			
User:	any	•	
Incoming:	any (Excluding ZyWALL)	•	
Source Address:	LAN1_SUBNET		
Destination Address:	any	2	
DSCP Code:	any		
Schedule:	none	· ·	
Service:	any		
Source Port:	any	•	
Next-Hop			
Type:	Interface		
Interface:	tunnel0	5)	

1.8.5 Testing the IPv6-in-IPv4 Tunnel

- 1 Connect a computer to the USG's LAN1.
- 2 Enable IPv6 support on you computer.

In Windows XP, you need to use the IPv6 install command in a Command Prompt.

In Windows 7, IPv6 is supported by default. You can enable IPv6 in the **Control Panel** > **Network** and **Sharing Center** > **Local Area Connection** screen.

- **3** You should get an IPv6 IP address starting with 2003:1111:1111:1000:.
- 4 Use the ping -6 [IPv6 IP address] command in a Command Prompt to test whether you can ping a computer behind USG **Y**. You should get a response.

1.8.6 What Can Go Wrong?

- 1 You don't need to activate the WAN1 IPv6 interface but make sure you enable the WAN1 IPv4 interface. In IPv6-in-IPv4, the USG uses the WAN1 IPv4 interface to forward your 6to4 packets to the IPv4 network.
- 2 In Windows, some IPv6 related tunnels may be enabled by default such as Teredo and 6to4 tunnels. It may cause your computer to handle IPv6 packets in an unexpected way. It is recommended to disable those tunnels on your computer.

Tutorial 2: Protecting Your Network

These sections cover configuring the USG to protect your network.

2.1 Firewall

The firewall controls the travel of traffic between or within zones for services using static port numbers. Use application patrol to control services using flexible/dynamic port numbers. The firewall can also control traffic for NAT (DNAT) and policy routes (SNAT). Firewall rules can use schedule, user, user groups, address, address group, service, and service group objects. To-USG firewall rules control access to the USG itself including management access. By default the firewall allows various types of management from the LAN, HTTPS from the WAN and no management from the DMZ. The firewall also limits the number of user sessions.

This example shows the USG's default firewall behavior for WAN to LAN traffic and how stateful inspection works. A LAN user can initiate a Telnet session from within the LAN zone and the firewall allows the response. However, the firewall blocks Telnet traffic initiated from the WAN zone and destined for the LAN zone. The firewall allows VPN traffic between any of the networks.

Figure 28 Default Firewall Action



2.1.1 What Can Go Wrong

- The USG checks the firewall rules in order and applies the first firewall rule the traffic matches. If traffic is unexpectedly blocked or allowed, make sure the firewall rule you want to apply to the traffic comes before any other rules that the traffic would also match.
- Even if you have configured the firewall to allow access for a management service such as HTTP, you must also enable the service in the service control rules.
- The USG is not applying your firewall rules for certain interfaces. The USG only apply's a zone's rules to the interfaces that belong to the zone. Make sure you assign the interfaces to the appropriate zones. When you create an interface, there is no security applied on it until you assign it to a zone.

2.2 User-aware Access Control

You can configure many policies and security settings for specific users or groups of users. Users can be authenticated locally by the USG or by an external (AD, RADIUS, or LDAP) authentication server. Here is how to have the USG use a RADIUS server to authenticate users before giving them access.

- 1 Set up user accounts in the RADIUS server.
- 2 Set up user accounts and groups on the USG (**Configuration > Object > User/Group**).
- 3 Configure an object for the RADIUS server. Click **Configuration > Object > AAA Server > RADIUS** and double-click the **radius** entry.
- 4 Then, set up the authentication method, Click **Configuration > Object > Auth. Method**. Doubleclick the **default** entry. Click the **Add** icon.
- **5** Configure the USG's security settings. The USG can use the authentication method in authenticating wireless clients, HTTP and HTTPS clients, IPSec gateways (extended authentication), L2TP VPN, and authentication policy.

2.2.1 What Can Go Wrong

- The USG always authenticates the default **admin** account locally, regardless of the authentication method setting. You cannot have the RADIUS server authenticate the USG's default admin account.
- The authentication attempt will always fail if the USG tries to use the local database to authenticate an **ext-user**. An external server such as AD, LDAP or RADIUS must authenticate the ext-user accounts.
- Attempts to add the admin users to a user group with access users will fail. You cannot put

access users and admin users in the same user group.

• Attempts to add the default admin account to a user group will fail. You cannot put the default **admin** account into any user group.

2.3 Device and Service Registration

This tutorial shows you how to create a myZyXEL.com account and register the USG. You can then activate your service subscription.

1 You can directly create a myZyXEL.com account and register the USG on the **Registration** screen. Click **Configuration > Licensing > Registration** to open the following screen. Select **new myZyXEL.com account**. Fill in the fields marked in red in this screen. Click **Apply** to create your account and register the device.

tegistration Service	
Seneral Settings	
	d to myZyXEL.com. Please enter information below to register your device. .com account, please select "new myZyXEL.com account" below. If you have
a myZyXEL.com account, b	ut you forget your User Name or Password, please go to <u>www.myZvXEL.com</u> for help.
new myZyXEL.com acco	int) © existing myZyXEL.com account
User Name:	you can click to check if username exists
User Name: Password:	you can click to check if username exists
Spectrum 25	you can click to check if username exists
Password:	you can click to check if username exists

2 Click the **Service** tab. To activate or extend a standard service subscription enter your iCard's license key in the **License Key** field. The license key can be found on the reverse side of the iCard.

1 Anti-Virus Signature Service Not Licensed N/A 2 IDPIAppPatrol Signature Service Not Licensed N/A 3 Anti-Spam Service Not Licensed N/A 4 Commtouch Content Filter Service Not Licensed N/A	
3 Anti-Spam Service Not Licensed N/A 4 Commtouch Content Filter Service Not Licensed N/A	
4 Commtouch Content Filter Service Not Licensed N/A	
5 BlueCost Content Filter Service Not Licensed N/A	
6 SSL VPN Service Not Licensed 2	
4 4 Page 1 of 1 ≥ ≥ Show 50 v items Di	playing 1 - 6 of



2.4 Anti-Virus Policy Configuration

This tutorial shows you how to configure an Anti-Virus policy.

Note: You need to first activate your Anti-Virus service license or trial. See

1 Click Configuration > Anti-X > Anti-Virus to display the Anti-Virus General screen. In the Policies section click Add to display the Add Rule screen. Select Enable. In the Direction section, you can select the From and To zones for traffic to scan for viruses. You can also select traffic types to scan for viruses under Protocols to Scan. Click OK.

Add Rule				1
Configuration				
Enable	2			
Direction				
From:	WAN	~		
To:	LAN1	~		
Protocols to	Scan			
И нттр	📝 FTP	SMTP	POP3	IMAP4
Log:	log log Black List Checking	~		
V Check W				
Check Bl				
File decompr	ession			
Enable fi	e decompression (ZIP an	d RAR)		
Dest	troy compressed files that	t could not be decompre	issed	
			(OK Cancel

2 The policy configured in the previous step will display in the **Policies** section. Select **Enable Anti-Virus and Anti-Spyware** and click **Apply**.

General Black/White List	Signature	
Show Advanced Settings		
General Settings		
Enable Anti-Virus and Anti-	Spyware	
Policies		
Policies		
	😡 Activate 😡 Inactivate 🚽	Move
	<table-cell> Activate 🖓 Inactivate 😅</table-cell>	Protocol
Add ZEdt: Pr From	To	and the second se
Add ZEdit TRemove	To R LAN1	Protocol HTTP FTP SMTP POP3 MAP4

2.4.1 What Can Go Wrong

- The USG does not scan the following file/traffic types:
 - Simultaneous downloads of a file using multiple connections. For example, when you use FlashGet to download sections of a file simultaneously.
 - Encrypted traffic. This could be password-protected files or VPN traffic where the USG is not the endpoint (pass-through VPN traffic).
 - Traffic through custom (non-standard) ports. The only exception is FTP traffic. The USG scans whatever port number is specified for FTP in the ALG screen.
 - ZIP file(s) within a ZIP file.

2.5 IDP Profile Configuration

IDP (Intrusion, Detection and Prevention) detects malicious or suspicious packets and protects against network-based intrusions.

Note: You need to first activate your IDP service license or trial.

You may want to create a new profile if not all signatures in a base profile are applicable to your network. In this case you should disable non-applicable signatures so as to improve USG IDP processing efficiency.

You may also find that certain signatures are triggering too many false positives or false negatives. A false positive is when valid traffic is flagged as an attack. A false negative is when invalid traffic is wrongly allowed to pass through the USG. As each network is different, false positives and false negatives are common on initial IDP deployment.

You could create a new 'monitor profile' that creates logs but all actions are disabled. Observe the logs over time and try to eliminate the causes of the false alarms. When you're satisfied that they have been reduced to an acceptable level, you could then create an 'inline profile' whereby you configure appropriate actions to be taken when a packet matches a signature.

2.5.1 Procedure To Create a New Profile

To create a new profile:

1 Click **Configuration > Anti-X > IDP > Profile** and in the **Profile Management** section of this screen, click the **Add** icon. A pop-up screen will appear allowing you to choose a base profile. Select a base profile to go to the profile details screen.

O Base Profile	? ×
Please select one IDP Base Profile.	
Base Profile	~
none	
al	
wan	
lan	
dmz	
	-
	-

Note: If Internet Explorer opens a warning screen about a script making Internet Explorer run slowly and the computer maybe becoming unresponsive, just click **No** to continue.

2 Type a new profile **Name**. Enable or disable individual signatures by selecting a row and clicking **Activate** or **Inactivate**. Click **OK**.

ame: SPF4146	Switch to query view]			
ature Group					
💡 Activate 💡 Inactivate 📄 Log 🗸 🌐 Action 🗸 💦					
Status Service Message	SID	Severity	Policy Type	Log	Action
Service: DATABASE (106 Items)					
Service: DHCP (6 Items)					
Service: DNS (22 Items)					
Service: DOS (172 Items)					
Service: EXPLOIT (700 Items)					
Service: FILEFORMAT (101 Items)					
Service: FTP (57 Items)					
Service: IMAP (32 Items)					
Service: MISC (198 Items)					

3 Edit the default log options and actions.

2.6 ADP Profile Configuration

ADP (Anomaly Detection and Prevention) protects against anomalies based on violations of protocol standards (RFCs – Requests for Comments) and abnormal traffic flows such as port scans.

You may want to create a new profile if not all traffic or protocol rules in a base profile are applicable to your network. In this case you should disable non-applicable rules so as to improve USG ADP processing efficiency.

You may also find that certain rules are triggering too many false positives or false negatives. A false positive is when valid traffic is flagged as an attack. A false negative is when invalid traffic is wrongly allowed to pass through the USG. As each network is different, false positives and false negatives are common on initial ADP deployment.

You could create a new 'monitor profile' that creates logs but all actions are disabled. Observe the logs over time and try to eliminate the causes of the false alarms. When you're satisfied that they have been reduced to an acceptable level, you could then create an 'inline profile' whereby you configure appropriate actions to be taken when a packet matches a detection.

2.6.1 Procedure To Create a New ADP Profile

To create a new profile:

1 Click Configuration > Anti-X > ADP > Profile and in the Profile Management section of this screen, click the Add icon. A pop-up screen will appear allowing you to choose a base profile. Select a base profile to go to the profile details screen.



Note: If Internet Explorer opens a warning screen about a script making Internet Explorer run slowly and the computer maybe becoming unresponsive, just click **No** to continue.

2 The Traffic Anomaly screen will display. Type a new profile Name. Enable or disable individual scan or flood types by selecting a row and clicking Activate or Inactivate. Selecting different levels in the Sensitivity drop-down menu adjusts levels for scan thresholds and sample times. Edit the default log options and actions by selecting a row and making a selection in the Log or Action drop-down menus. Click OK.

affic	Anomaly	Protocol Anomaly			
ner	al				
Name	e:	APF9600			
an [Detection				
Sens	itivity:	medum 💙			
9	Activate <table-cell> 🖓 Ind</table-cell>	activate 📄 Log 🗸 🎯 Action 🔹			
	Status	Name 🔺		Log	Action
1	9	(portscan) TCP Portscan		log	none
2	9	(portscan) TCP Portscan Fin		log	none
3	9	(portscan) TCP Portscan Syn		log	none
4	9	(portscan) UDP Portscan		log	none
5	9	(sweep) TCP Port Sweep		log	none
14	Page 1	of 1 🕨 🕅 Show 50 🔽 items			Displaying 1 - 5 of 5
bod	Detection				
2	Edit 🍚 Activat	e 🞯 Inactivate 🛅 Log 🗸 🥮 Action 🗸			
	Status	Name -	Log	Action	Threshold(pkt/sec)
1	0	(flood) ICMP Flood	log	none	1000

3 Click the **Protocol Anomaly** tab. Type a new profile **Name**. Enable or disable individual rules by selecting a row and clicking **Activate** or **Inactivate**. Edit the default log options and actions by selecting a row and making a selection in the **Log** or **Action** drop-down menus. Click **OK**.

ner	ral			
lam	e: Aj	PF9600		
	ecoder			
	SAME A			
W.	The second second second second	diviste 🕒 Log + 🛞 Action +)	1.00	bergerer (11)
1	Status	Name A (tcp_decoder) bad-tcp-flag ATTACK	Log	Action
	0	(tcp_decoder) bad-tcp-I4-size ATTACK	log	none
	0	(tcp_decoder) tcp-land ATTACK	log	none
			Ny	
19	1 Page [1	of 1 🕨 🕅 Show 50 🛩 items		Displaying 1 - 3 of 3
PD	ecoder			
	Activate 🌘 Ina	ctivate 🛅 Log 🔹 🍪 Action 🖌		
	Status	Name -	Log	Action
	0	(udp_decoder) bad-udp-I4-size ATTACK	log	none
	0	(udp_decoder) udp-land ATTACK	log	none
	9	(udp_decoder) udp-smurf ATTACK	log	none
	Page 1	of 1 🕨 🕅 Show 50 🛩 items		Displaying 1 - 3 of 3
14				
14.				
14.	Decoder			
14 1P		ctivate 🛅 Log 🖌 🍪 Action 🖌		
14 1P		divate 📄 Log + 🚳 Action +	Log	Action
14 1P	Activate 👰 Ine		Log log	Action

2.7 Content Filter Profile Configuration

Content filter allows you to control access to specific web sites or filter web content by checking against an external database. This tutorial shows you how to configure a Content Filter profile.

- Note: You need to first activate your Content Filter service license or trial to use Commtouch or BlueCoat content filtering service.
- 1 You will first configure a content filter profile. Click Configuration > Anti-X > Content Filter > Filter Profile > Add to open the following screen. Enter a profile Name and select Enable Content Filter Category Service and select desired actions for the different web page categories. Then select the categories to include in the profile or select Select All Categories. Click Apply.

ense Status:	Licensed			
ense Type:	Trial			
me:	BlueCoat			
Enable Content Filter C	ategory Service			
Action for Unsafe Web	Pages:	Warn	~	C Log
Action for Managed W	eb Pages:	Block	~	E Log
Action for Unrated We	b Pages:	Warn	*	E Log
Action When Category	Server Is Unavailable:	Warn	~	🕅 Log
ct Categories				

2 Click the **General** tab and in the **Policies** section click **Add**. In the **Add Policy** screen that appears, select the **Filter Profile** you created in the previous step. Click **OK**.

Add Policy			?
Create new Object 🗸			
Enable Policy			
Schedule:	none	*	
Address:	any	~	
Filter Profile :	BlueCoat	~)
User/Group:	any	~	
		ОК	Cancel

3 In the **General** screen, the configured policy will appear in the **Policies** section. Select **Enable Content Filter** and select **BlueCoat**. Then select **Enable Content Filter Report Service** to collect content filtering statistics for reports. Click **Apply**.

eneral Set	tings Content Filter				
O Co	mmtouch				
Blue	eCoat				
🔽 Enable	Content Filter Report Servio	ce <u>Report Serv</u>	er 🔳		
Content Filt	er Category Service Timeou	ut: 10	(1~60 Seconds)		
Content Filt	er Port	🙆 Add 🗧	Edit TRemove		
		# Por	t		
		1 80			
olicies					
Block w	eb access when no policy is	applied			
🕜 Add [🚰 Edit 👕 Remove 🛛 😡 Ac	tivate 😡 Inactivate 🚽	Move		
# Sta	tus Address	Schedule	User	Filter Profile	
1 0	any	none	any	BlueCoat	

2.8 Viewing Content Filter Reports

Content filtering reports are generated statistics and charts of access attempts to web sites belonging to the categories you selected in your device content filter screen. You need to register your iCard before you can view content filtering reports. Alternatively, you can also view content filtering reports during the free trial (up to 30 days).

1 Go to http://www.myZyXEL.com. Fill in your myZyXEL.com account information and click Login.

	ZyXEL
LOGIN CONTACT US	
Spotlights	WELCOME
Spollights	 New Account Language Registered? FAQ Support Note

2 A welcome screen displays. Click your USG's model name and/or MAC address under **Registered ZyXEL Products** (the USG 20W is shown as an example here). You can change the descriptive name for your USG using the **Rename** button in the **Service Management** screen.

TY ZyXEL			
Welcome My Account	My Product Bownload Center	sm	MAP CONTACT US LOGOUT
WELCOME	Welcome/ Welcome! Customer. You have logged in myZyXEL.com for 4 times. Last Viewed * 19: 203.160.254.59 * Viewed Date: 2011-09-16 * Viewed time: 17:36:44(GMT-8:00)Beijing		Spollights
	Registered ZyXEL Products To register product. <mark>Click here</mark>		^{my} Security _{zone}
		n Code / MAC	
	27WALL USG 20W- 0000AA797369 20W AAAA797369 0000AA	\$797369	

3 In the Service Management screen click Content Filter (BlueCoat) or Content Filter (Commtouch) in the Service Name column to open the content filter reports screens.

My Products / Service Activation							
Service Management							
Product Information							
ZYWALL USC 20W-0000AA797369							
CT 1111LE 0.54 2011 0000000197307			Edit Reseller Information				
Serial Number:	AAAA797369		Reseller Business Name:				
Products:	Products: ZVWALL USG 20W		Reseller Email:				
Authentication Code / MAC Address:	Authentication Code / MAC Address: 0000AA797369		Reseller Phone Numberi				
Activation Keyi	Activation Keys N/A		VAT Numberi				
Manage Product							
Manage this product's registration by clicki	no on the appropriate buttons bel	5w					
> ZYWALL USG 20W-0000AA797369	R	ename Transfer					
Available Service List							
To enable your service(s), please click "Ac	tivate" shown below to enter your	license key(s).					
Service	Vame	Service Activation	Service Type	Status	Expiration Date	Remark	
1 Content Filter(Blu	eCoat)(Applied	Upgrade	Trial	Installed	2011-09-30 extends to 2012-09-30		
2 Content Filter(Commtouch)	Upgrade	Trial	Installed	2011-09-30 extends to 2012-09-30		

4

In the Web Filter Home screen, click Commtouch Report or BlueCoat Report.

ZyXEL	comptouch Real Security. In Real Time.	Blue Coat	Technical Support
Web Filter Home			
You're protected by Web Filtering. Web Filtering provides you the ability to control what web sites can be accessed on your home or business PC. Web Filter allows you to modify blocked categories and view reports of Internet activity. REPORTS:			
Track Internet activity by viewing user reports, including site violations. Click links below to enter Commouch / BlueCoat report:			
Commtouch Report BlueCoat Report			

5

Select items under **Global Reports** to view the corresponding reports.

ZyXE	L	comptouch Real Security to Real Time.	Blue®Coat	Technical Support
Commtouch Reports	l Global Repo	rts.)		
Report H	lome			
Global reports provide You Global Reports	with an overview of all you	ur Internet use.	- 2	
Allowed/Blocked				
Categories				
URLs				

6 Select a time period in the **Date Range** field, either **Allowed** or **Blocked** in the **Action Taken** field and a category (or enter the user name if you want to view single user reports) and click **Run Report**.

The screens vary according to the report type you selected in the **Report Home** screen.

A chart and/or list of requested web site categories display in the lower half of the screen.

🔕 BlueCoat Reports		
Report Home	Global Reports	
0	•	
Global Reports	- Categories	
This report shows the total numbers of	allowed or blocked requests for each ca	tegory.
Select a report type and a date range f category to view a report of the URLs r		Ify this report. Click on a
	Date Range:	Last 24 Hours
	Action taken:	Allowed 💌
		Run Report
Categories where the request was:	Alowed	
Email	-	18% Email
Search Engines/Portals		
Web Advertisement Computers/Internet	-	
NewsMedia		
Social Networking	H 🔺	
Reference		
Proxy Avoidance		
Blogs/Newsgroups		
Business/Economy		
Political/Activist Groups		
Travel		
 Unrated 	-	
Category		Number of Requests
Email Search Engines/Portals		15190
Web Advertisement		10219
Computers/Internet		7518

7

8 You can click a category in the **Categories** report or click **URLs** in the **Report Home** screen to see the URLs that were requested.

Zy	XEL	Real Security. In Real Time.	Blue <br< th=""><th>Technical Suppor</th></br<>	Technical Suppor
	port Home I Global Rep	ports		
6	Global Reports - URLs			
This repo	ort displays allowed or blocked URLs requeste Date Range:	Last 24 Hours		
	Action taken:	Allowed •		
	Category:	Email	•	
		Run Report	•	
URLs Red	quested for category: Email			
ltem #	URL		Number of Requests	Open Web Page
1	www.mail.yahoo.com/		10	8
2	mail.yahoo.com/		10	8
3	mail.google.com/a/stam.com.my/		10	2
4	mail.google.com/mail/		9	2
5	mail.google.com/mail/?ui=28view=bsp8ver	=1gygpcgurkovy	9	8

2.9 Anti-Spam Policy Configuration

This tutorial shows you how to configure an Anti-Spam policy with Mail Scan functions and DNS Black List (DNSBL).

- Note: You need to first activate your Anti-Spam service license or trial to use the Mail Scan functions (Sender Reputation, Mail Content Analysis and Virus Outbreak Detection).
- 1 To use the Mail Scan functions (Sender Reputation, Mail Content Analysis and Virus Outbreak Detection) you need to enable them in the Mail Scan screen. Click Configuration > Anti-X > Anti-Spam > Mail Scan to open this screen. Enable the desired Mail Scan functions. Click Apply.

Enable Sender Reputation Chi	ecking (SMTP only)		
ail Content Analysis			
Enable Mail Content Analysis Mail Content Spam Tag:) [Spam]	(Optional)	
Mail Content X-Header:	X-		(Optional)
Mail Content X-Header:	1.0000		(Options
us Outbreak Detection			

2 To configure DNS Black List (DNSBL), click the DNSBL tab. Select Enable DNS Black List (DNSBL) Checking. In the DNSBL Domain section click Add. Enter the DNSBL Domain for a DNSBL service. In this example, zen.spamhaus.org is used. Click Apply.

Enable DNS Black List (DN			
DNSBL Spam Tag:	[Spam] (Op	ional)	
DNSBL X-Header:	X-	: (Optional)
SMTP:	forward with tag		
SMTD:	forward with here	1	
POP3:		1	
Timeout Value:	5 (1-10 Seconds)		
Timeout Tag:	[Timeout] (Op	ional)	
Timeout X-Header:	X-	: (Optional)
		·	
NSBL Domain List			

3 Click the **General** tab. In the **Policy Summary** section, click **Add** to display the **Add rule** screen. Select from the list of available **Scan Options** and click **OK** to return to the **General** screen.

Enable Policy			
Log:	log	¥ 🚺	
mail Direction			
From:	any	~	
To:	any	*	
Protocols to Scan	POP3		
SMTP Can Options Check White List		$\overline{}$	
SMTP			
SMTP Can Options Check White Lis Check Black List	tion (SMTP only)		
SMTP SMTP Check White List Check Black List Check Black List Check IP Reputz	t ation (SMTP only) ent		
SMTP Check White Lis Check Black List Check Black List Check Black List Check Mail Cont	t ation (SMTP only) ent break		
SMTP Check White Lis Check White Lis Check Black List Check Black List Check Mail Cont Check Mail Cont Check Vrus Out Check Vrus Out Check NSBL	t ation (SMTP only) ent break		

4 In the **General** screen, the policy configured in the previous step will display in the **Policy Summary** section. Select **Enable Anti-Spam** and click **Apply**.

General Mail Scan Bi	lack/White List DNSBL		
Show Advanced Settings			
General Settings			
Enable Anti-Spam			
V chable who-spain			
Policy Summary			
Policy Summary			
	e 🧛 Activate 👰 Inactivate 🪙	Move	
	e 💡 Activate 🧔 Inactivate 🚙 Te	Move Protocol	Scan Options
Add PEdt Premove			Scan Options WL, BL, IP Reputation, Mail Content, Virus Outbre

Tutorial 3: Create Secure Connections Across

the Internet

These sections cover using VPN to create secure connections across the Internet.

3.1 IPSec VPN

Besides using the VPN quick setup wizard to configure settings for an IPSec VPN tunnel, you can use the **Configuration > VPN > IPSec VPN** screens to configure and activate or deactivate VPN gateway and IPSec VPN connection policies. You can also connect or disconnect IPSec VPN connections.

- Use the **VPN Gateway** screens to manage the USG's VPN gateways. A VPN gateway specifies the IPSec routers at either end of a VPN tunnel and the IKE SA settings (phase 1 settings). You can also activate or deactivate each VPN gateway.
- Use the **VPN Connection** screens to specify which IPSec VPN gateway an IPSec VPN connection policy uses, which devices behind the IPSec routers can use the VPN tunnel, and the IPSec SA settings (phase 2 settings). You can also activate or deactivate and connect or disconnect each VPN connection (each IPSec SA).

3.1.1 Test the VPN Connection

After you configure the VPN gateway and VPN connection settings, set up the VPN settings on the peer IPSec router and try to establish the VPN tunnel. To trigger the VPN, either try to connect to a device on the peer IPSec router's LAN or click **Configuration > VPN > IPSec VPN > VPN Connection** and use the VPN connection screen's **Connect** icon.

3.1.2 Configure Security Policies for the VPN Tunnel

You configure security policies based on zones. The new VPN connection was assigned to the IPSec_VPN zone. By default, there are no security restrictions on the IPSec_VPN zone, so, next, you should set up security policies that apply to the IPSec_VPN zone.

3.1.3 What Can Go Wrong

If the IPSec tunnel does not build properly, the problem is likely a configuration error at one of the IPSec routers. Log into both IPSec routers and check the settings in each field methodically and slowly. Make sure both the USG and remote IPSec router have the same security settings for the VPN tunnel. It may help to display the settings for both routers side-by-side.

Here are some general suggestions.

- The system log can often help to identify a configuration problem.
- If you enable NAT traversal, the remote IPSec device must also have NAT traversal enabled.
- Both routers must use the same authentication method to establish the IKE SA.
- Both routers must use the same negotiation mode, encryption algorithm, authentication algorithm, and DH key group.
- When using manual keys, both routers must use the same encryption key and authentication key.
- When using pre-shared keys, both routers must use the same pre-shared key.
- The USG's local and peer ID type and content must match the remote IPSec router's peer and local ID type and content, respectively.
- Both routers must use the same active protocol, encapsulation, and SPI.
- If the sites are/were previously connected using a leased line or ISDN router, physically disconnect these devices from the network before testing your new VPN connection. The old route may have been learnt by RIP and would take priority over the new VPN connection.
- To test whether or not a tunnel is working, ping from a computer at one site to a computer at the other.

Before doing so, ensure that both computers have Internet access (via the IPSec routers).

• It is also helpful to have a way to look at the packets that are being sent and received by the USG and remote IPSec router (for example, by using a packet analyzer such as Wireshark). Check

the configuration for the following USG features.

- Make sure the To-USG firewall rules allow IPSec VPN traffic to the USG. IKE uses UDP port 500, AH uses IP protocol 51, and ESP uses IP protocol 50.
- The USG supports UDP port 500 and UDP port 4500 for NAT traversal. If you enable this, make sure the To-USG firewall rules allow UDP port 4500 too.
- Make sure regular firewall rules allow traffic between the VPN tunnel and the rest of the network. Regular firewall rules check packets the USG sends before the USG encrypts them and check packets the USG receives after the USG decrypts them. This depends on the zone to which you assign the VPN tunnel and the zone from which and to which traffic may be routed.
- If you set up a VPN tunnel across the Internet, make sure your ISP supports AH or ESP (whichever you are using).
- If you have the USG and remote IPSec router use certificates to authenticate each other, You must set up the certificates for the USG and remote IPSec router first and make sure they trust each other's certificates. If the USG's certificate is self-signed, import it into the remote IPsec router. If it is signed by a CA, make sure the remote IPsec router trusts that CA. The USG uses one of its **Trusted Certificates** to authenticate the remote IPSec router's certificate. The trusted certificate can be the remote IPSec router's self-signed certificate or that of a trusted CA that signed the

remote IPSec router's certificate.

• Multiple SAs connecting through a secure gateway must have the same negotiation mode.

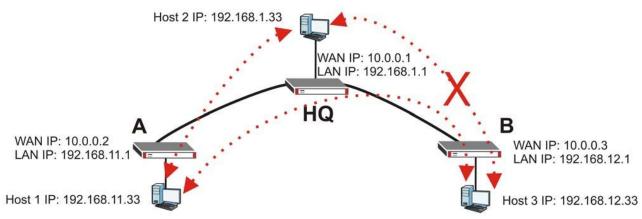
If you have the **Configuration > VPN > IPSec VPN > VPN Connection** screen's **Use Policy Route to control dynamic IPSec rules option** enabled and the VPN connection is up but VPN traffic cannot be transmitted through the VPN tunnel, check the routing policies to see if they are sending traffic elsewhere instead of through the VPN tunnels.

3.2 VPN Concentrator Example

A VPN concentrator uses hub-and-spoke VPN topology to combine multiple IPSec VPN connections into one secure network. The hub routes VPN traffic between the spoke routers and itself. This reduces the number of VPN connections to set up and maintain. Here a VPN concentrator connects ZLD-based USGs at headquarters (HQ) and branch offices A and B in one secure network.

- Branch A's USG uses one VPN rule to access both the headquarters (HQ) network and branch B's network.
- Branch B's USG uses one VPN rule to access branch A's network only. Branch B is not permitted to access the headquarters network.

Figure 29 IPSec VPN Concentrator Example



This IPSec VPN concentrator example uses the following settings.

Branch Office A

VPN Gateway (VPN Tunnel 1):

- My Address: 10.0.0.2
- Peer Gateway Address: 10.0.0.1

VPN Connection (VPN Tunnel 1):

- Local Policy: 192.168.11.0/255.255.255.0
- Remote Policy: 192.168.1.0/255.255.255.0
- Disable Policy Enforcement

Policy Route

• Source: 192.168.11.0

- Destination: 192.168.12.0
- Next Hop: VPN Tunnel 1

Headquarters

VPN Gateway (VPN Tunnel 1):

- My Address: 10.0.0.1
- Peer Gateway Address: 10.0.0.2

VPN Connection (VPN Tunnel 1):

- Local Policy: 192.168.1.0/255.255.255.0
- Remote Policy: 192.168.11.0/255.255.255.0
- Disable Policy Enforcement

VPN Gateway (VPN Tunnel 2):

- My Address: 10.0.0.1
- Peer Gateway Address: 10.0.0.3

VPN Connection (VPN Tunnel 2):

- Local Policy: 192.168.1.0/255.255.255.0
- Remote Policy: 192.168.12.0/255.255.255.0
- Disable Policy Enforcement

Concentrator

• Add VPN tunnel 1 and VPN tunnel 2 to an IPSec VPN concentrator.

Firewall

• Block traffic from VPN tunnel 2 from accessing the LAN.

Branch Office B

VPN Gateway (VPN Tunnel 2):

- My Address: 10.0.0.3
- Peer Gateway Address: 10.0.0.1

VPN Connection (VPN Tunnel 2):

- Local Policy: 192.168.12.0/255.255.255.0
- Remote Policy: 192.168.1.0/255.255.255.0
- Disable Policy Enforcement

Policy Route

- Source: 192.168.12.0
- Destination: 192.168.11.0
- Next Hop: VPN Tunnel 2

3.2.1 What Can Go Wrong

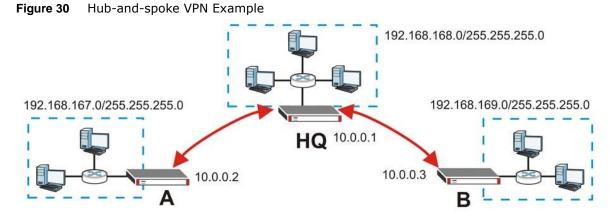
Consider the following when using the VPN concentrator.

- The local IP addresses configured in the VPN rules should not overlap.
- The concentrator must have at least one separate VPN rule for each spoke. In the local policy, specify the IP addresses of the networks with which the spoke is to be able to have a VPN tunnel. This may require you to use more than one VPN rule for each spoke.
- To have all Internet access from the spoke routers go through the VPN tunnel, set the VPN rules in the spoke routers to use 0.0.0.0 (any) as the remote IP address.
- Your firewall rules can still block VPN packets.
- If on a USG USG or USG 1050 the concentrator's VPN tunnels are members of a single zone, make sure it is not set to block intra-zone traffic.

3.3 Hub-and-spoke IPSec VPN Without VPN Concentrator

Here is an example of a hub-and-spoke VPN that does not use the USG's VPN concentrator feature. Here branch office A has a ZyNOS-based USG and headquarters (HQ) and branch office B have ZLD-based USGs.

- Branch A's USG uses one VPN rule to access both the headquarters (HQ) network and branch B's network.
- Branch B's USG uses one VPN rule to access both the headquarters and branch A's networks.



This hub-and-spoke VPN example uses the following settings.

Branch Office A (ZyNOS-based USG):

Gateway Policy (Phase 1):

- My Address: 10.0.0.2
- Primary Remote Gateway: 10.0.0.1

Network Policy (Phase 2): Local Network: 192.168.167.0/255.255.255.0; Remote Network: 192.168.168.0~192.168.169.255

Headquarters (ZLD-based USG):

VPN Gateway (VPN Tunnel 1):

- My Address: 10.0.0.1
- Peer Gateway Address: 10.0.0.2

VPN Connection (VPN Tunnel 1):

- Local Policy: 192.168.168.0~192.168.169.255
- Remote Policy: 192.168.167.0/255.255.255.0
- Disable Policy Enforcement

VPN Gateway (VPN Tunnel 2):

- My Address: 10.0.0.1
- Peer Gateway Address: 10.0.0.3

VPN Connection (VPN Tunnel 2):

- Local Policy: 192.168.167.0~192.168.168.255
- Remote Policy: 192.168.169.0/255.255.255.0
- Disable Policy Enforcement

Branch Office B (ZLD-based USG):

VPN Gateway:

- My Address: 10.0.0.3
- Peer Gateway Address: 10.0.0.1

VPN Connection:

- Local Policy: 192.168.169.0/255.255.255.0
- Remote Policy: 192.168.167.0~192.168.168.255
- Disable Policy Enforcement

3.3.1 What Can Go Wrong

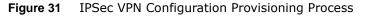
Consider the following when implementing a hub-and-spoke VPN.

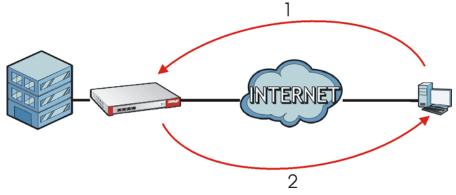
- This example uses a wide range for the ZyNOS-based USG's remote network, to use a narrower range.
- The local IP addresses configured in the VPN rules should not overlap.
- The hub router must have at least one separate VPN rule for each spoke. In the local policy, specify the IP addresses of the hub-and-spoke networks with which the spoke is to be able to have a VPN tunnel. This may require you to use more than one VPN rule.
- To have all Internet access from the spoke routers to go through the VPN tunnel, set the VPN rules in the spoke routers to use 0.0.00 (any) as the remote IP address.
- Your firewall rules can still block VPN packets.
- If the ZLD-based USGs' VPN tunnels are members of a single zone, make sure it is not set to block intra-zone traffic.
- The ZyNOS based USGs don't have user-configured policy routes so the only way to get traffic destined for another spoke router to go through the ZyNOS USG's VPN tunnel is to make the remote policy cover both tunnels.
- Since the ZLD-based USGs automatically handle the routing for VPN tunnels, if a ZLD-based USG USG is a hub router and the local policy covers both tunnels, the automatic routing takes care of it without needing a VPN concentrator.

• If a ZyNOS-based USG's remote network setting overlaps with its local network settings, set <code>ipsec swSkipOverlapIp</code> to on to send traffic destined to A's local network to A's local network instead of through the VPN tunnel.

3.4 USG IPSec VPN Client Configuration Provisioning

VPN configuration provisioning gives USG IPSec VPN Client users VPN rule settings automatically.





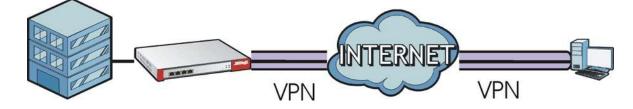
- 1 User Charlotte with the USG IPSec VPN Client sends her user name and password to the USG.
- 2 The USG sends the settings for the matching VPN rule.

3.4.1 Overview of What to Do

- 1 Create a VPN rule on the USG using the VPN Configuration Provisioning wizard.
- 2 Configure a username and password for the rule on the USG.
- 3 On a computer, use the USG IPSec VPN Client to get the VPN rule configuration.

Now user Charlotte can access the network behind the USG through the VPN tunnel.

Figure 32 USG IPSec VPN Client with VPN Tunnel Connected



3.4.2 Configuration Steps

1 In the USG **Quick Setup** wizard, use the **VPN Settings for Configuration Provisioning** wizard to create a VPN rule that can be used with the USG IPSec VPN Client.

- 2 Click **Configuration > Object > User/Group** and create a user account for the USG IPSec VPN Client user.
- 3 Then, enable Configuration Provisioning in Configuration > VPN > IPSec VPN > Configuration Provisioning and configure it to allow the newly created user to retrieve this rule's settings using the USG IPSec VPN Client.
- 4 On the USG IPSec VPN Client, select **Configuration > Get From Server.**

ZyWALL IPSec VPN Client	
Configuration Tools ?	
Import Export	
Get from Server Move to USB Drive Wizard Quit	'N Configuration N Configuration
	VPN Configuration Written by VpnConf 3.00 Last modification: 09-27-2011

5 Enter the WAN IP address or URL for the USG. If you changed the default HTTPS port on the USG, then enter the new one here. Enter the user name (**Login**) and and password exactly as configured on the USG or external authentication server. Click **Next**.

itep 1: Authentication		చ	P
What are the parameters of the	VPN Server Connection?	00	
You are going to download your Enter below the authentication in			
	myconfserv.dyndns.org	Port:	443
Gateway Address:			
Gateway Address: Authentication:	Login + Password		

6 Click **OK**. The rule settings are now imported from the USG into the USG IPSec VPN Client.

3.4.3 What Can Go Wrong

• VPN rule settings violate the the USG IPSec VPN Client restrictions:

Check that the rule does not contain $\bf AH$ active protocol, $\bf NULL$ encryption, $\bf SHA512$ authentication, or a subnet/range remote policy.

The USG IPSec VPN Client can also indicate rule violations. Check its warning screen.

Although the rule settings may be valid, whether the tunnel actually works depends on the network environment. For example, a remote policy IP address for a server may be valid, but the server may be down or have an actual different IP address.

• There is a login problem:

Reenter the user name (**Login**) and password in the USG IPSec VPN Client exactly as configured on the USG or the external authentication server.

Check that the client authentication method selected on the USG is where the user name and password are configured . For example, if the user name and password are configured on the USG, then the configured authentication method should be **Local**.

• There's a network connectivity problem between the USG and the USG IPSec VPN Client:

Check that the correct USG IP address and $\ensuremath{\mathsf{HTTPS}}$ port (if the default port was changed) was entered.

Ping the USG from the computer on which the USG IPSec VPN Client is installed. If there is no reply, check that the computer has Internet access.

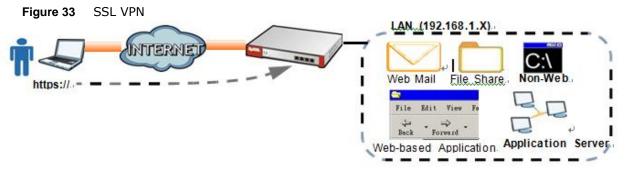
If the computer has Internet access, contact the USG administrator.

• The entry is not activated:

Make sure that both **Enable Configuration Provisioning** in **Configuration > VPN > IPSec VPN > Configuration Provisioning** is selected and that the entry has a yellow **Status** icon.

3.5 SSL VPN

SSL VPN uses remote users' web browsers to provide the easiest-to-use of the USG's VPN solutions. A user just types the USG's web address and enters his user name and password to securely access the USG's network. Here a user uses his browser to securely connect to network resources in the same way as if he were part of the internal network.



• Click **Configuration > Object > SSL Application** and configure an SSL application object to specify the type of application and the address of the local computer, server, or web site SSL users are to be able to access.

- Click Configuration > VPN > SSL VPN > Access Privilege to configure SSL access policies.
- Use the Configuration > VPN > SSL VPN > Global Setting screen to set the IP address of the USG (or a gateway device) on your network for full tunnel mode access, enter access messages or upload a custom logo to be displayed on the remote user screen.

Remote users can access resources on the local network using one of the following methods:

Using a supported web browser

Once you have successfully logged in through the USG, you can access intranet sites, web- based applications, or web-based e-mails using one of the supported web browsers.

• Using the USG SecuExtender client

Once you have successfully logged into the USG, if the SSL VPN access policy has network extension enabled the USG automatically loads the USG SecuExtender client program to your computer. With the USG SecuExtender, you can access network resources, remote desktops and manage files as if you were on the local network.

3.5.1 What Can Go Wrong

• If you uploaded a logo to show in the SSL VPN user screens but it does not display properly, check that the logo graphic is in GIF, JPG, or PNG format. The graphic should use a resolution of

103 x 29 pixels to avoid distortion when displayed. The USG automatically resizes a graphic of a different resolution to 103 x 29 pixels. The file size must be 100 kilobytes or less. Transparent background is recommended.

- If users can log into the SSL VPN but cannot see some of the resource links check the SSL application object's configuration.
- If the user account is not included in an SSL VPN access policy, the USG redirects the user to the user aware screen.
- Operating system and browser requirements for the remote user's computer:
 - Windows 7 (32 or 64-bit), Vista (32 or 64-bit), 2003 (32-bit), XP (32-bit), or 2000 (32-bit)
 - Internet Explorer 7 and above or Firefox 1.5 and above
 - Using RDP requires Internet Explorer
 - Sun's Runtime Environment (JRE) version 1.6 or later installed and enabled.
- Changing the HTTP/HTTPS configuration disconnects SSL VPN network extension sessions. Users need to re-connect if this happens.

3.6 L2TP VPN with Android, iOS, and Windows

L2TP VPN uses the L2TP and IPSec client software included in remote users' Android, iOS, or Windows operating systems for secure connections to the network behind the USG.

- 1 L2TP VPN uses one of the USG's IPSec VPN connections. Edit **Default_L2TP_VPN_GW** as follows:
 - Set My Address to the WAN interface domain name or IP address you want to use.
 - Replace the default Pre-Shared Key.
- 2 Create a host-type address object containing the **My Address** IP address configured in the **Default_L2TP_VPN_GW** and set the **Default_L2TP_VPN_Connection**'s **Local Policy** to use it.
- 3 In **Configuration > VPN > L2TP VPN** enable the connection and set the VPN connection L2TP VPN uses, the L2TP client IP address pool, the authentication method, and the allowed users.
- 4 Configure a policy route to let remote users access resources on the network behind the USG.
 - Set the policy route's **Source Address** to the address object that you want to allow the remote users to access (**LAN1_SUBNET** in the following example).
 - Set the **Destination Address** to the IP address pool that the USG assigns to the remote users (L2TP_POOL in the following example).
 - Set the next hop to be the VPN tunnel you are using for L2TP.

3.6.1 L2TP VPN Example

Here a sales representative uses a laptop to securely connect to the USG's network.

Figure 34 L2TP VPN Example



- The USG has a WAN interface with a static IP address of 172.16.1.2.
- The remote user has a dynamic public IP address and connects through the Internet.
- You configure an IP address pool object named **L2TP_POOL** to assign the remote users IP addresses from 192.168.10.10 to 192.168.10.20 for use in the L2TP VPN tunnel.
- The VPN rule allows the remote user to access the LAN1_SUBNET (the 192.168.1.x subnet). Do

the following to configure the L2TP VPN example:

1 Click Configuration > VPN > IPSec VPN > VPN Gateway and double-click the Default_L2TP_VPN_GW entry.

Select Enable.

Set **My Address**. This example uses a WAN interface with static IP address 172.16.1.2. Set **Authentication** to **Pre-Shared Key** and configure a password. This example uses **top-secret**. Click **OK**.

Edit VPN Gateway Default_L2TP_V	PN_GW	WISIONING wwant	0000.000	? ×
Show Advanced Settings				
General Settings				
C Enable				1
VPN Gateway Name:	Default_L21	TP_VPN_GV		
Gateway Settings				
My Address				
Interface	wan1	✓ Static -	172.16.1.2	
O Domain Name / IP				1
Peer Gateway Address				
Static Address	Primary	0.0.0		
	Secondary	0.0.0.0		
Fall back to Primary Peer Gat	eway when possib	ale		
Fall Back Check Interval:	300	(60-86400 sec	onds)	
Oynamic Address				
Authentication				
Pre-Shared Key	top-secret			-
			(OK Cancel

2 Click the VPN Connection tab and double-click the Default_L2TP_VPN_Connection entry.

Click **Create New Object > Address** and create a host type address object that contains the **My Address** IP address you configured in the **Default_L2TP_VPN_GW**. The address object in this example uses the WAN interface's IP address (172.16.1.2) and is named **L2TP_IFACE**.

Select **Enable**, set **Application Scenario** to **Remote Acces** and **Local Policy** to **L2TP_IFACE**, and click **OK**.

	Object -			Create Address		
Enable Connection Name: VPN Gateway	Default_L2TP_VPN_Conne	ection		Name: Address Type:	L2TP_IFACE	
Application Scenario				IP Address:	172.16.1.2	
 Site-to-site with Dynamic Peer Remote Access (Server Role) Remote Access (Client Role) 						
VPN Gateway:	Default_L2TP_VPN_GW	~	wan10.0.0.00.0	.0.0		
Policy	and the second se	1.0	HOST, 172.16.1.3	2		
Policy Local policy:	L2TP_JFACE	×	110013 272.20.20	•		

3 Click Configuration > VPN > L2TP VPN and then Create New Object > Address to create an IP address pool for the L2TP VPN clients. This example uses L2TP_POOL with a range of 192.168.10.10 to 192.168.10.20. Click Create New Object > User/Group to create a user object for the users allowed to use the tunnel. This example uses a user object named L2TP-test.

Enable the connection.

Set VPN Connection to Default_L2TP_VPN_Connection.

Set IP Address Pool to L2TP_POOL.

Select the authentication method (default in this example), and select the users that can use the tunnel (**L2TP-test** in this example).

L2TP VPN			Create Address			
🔟 Show Advanced Settings 🛅 Create	e new Object •					
General Settings			Name:	L2TP_POOL		
Enable L2TP Over IPSec			Address Type:	RANGE	~	
VPN Connection:	Default_L2TP_VPN_Co	nnex 👻	Starting IP Address:	192.168.10.10		
IP Address Pool:	L2TP_POOL	*	End IP Address:	192.168.10.20		-
Authentication Method:	default	*	🔾 Add User			
Allowed User:	L2TP-test	*	User Configuratio	on		
			User Name :		L2TP-test	
	Apply	Reset	User Type:		user	*
			Password:		••••	
			Retype:			

3.6.2 Configuring Policy Routing

You must also configure a policy route to let remote users access resources on the network behind the USG.

- Set the policy route's **Source Address** to the address object that you want to allow the remote users to access (**LAN_1SUBNET** in this example).
- Set the **Destination Address** to the IP address pool that the USG assigns to the remote users (L2TP_POOL in this example)).
- Set the next hop to be the VPN tunnel that you are using for L2TP VPN.

Add Policy Route			2 ×
🛚 Show Advanced Settings 🔡 Create	e new Object 🔹		
Configuration			
💟 Enable			-
Description:	L2TP_VPN	(Optional)	
Criteria			
User:	any	~	
Incoming:	any (Excluding ZyWALL)	~	
Source Address:	LAN1_SUBNET	~	
Destination Address:	L2TP_POOL	~	
DSCP Code:	any	~	
Schedule:	none	~	
Service:	any	~	
Next-Hop			
Type:	VPN Tunnel	*	
VPN Tunnel:	Default_L2TP_VPN_Conn	er 🛩	

USG's return traffic back through the L2TP VPN tunnel.

- Set **Incoming** to **USG**.
- Set **Destination Address** to the L2TP address pool.
- Set the next hop to be the VPN tunnel that you are using for L2TP.

Add Policy Route	LVP. A LOTP_POOL ANY	алу	307	any	? >
III Show Advanced Settings 🛅 Create	e new Object 🔹				
Configuration					
Enable					
Description:	Remote Management (0	(ptional)			
Criteria					
User:	admin	*			
Incoming:	ZyWALL	~			
Source Address:	any	~			
Destination Address:	L2TP_POOL	*			
DSCP Code:	any	*			
Schedule:	none	*			
Service:	any	*			
Next-Hop					
Type:	VPN Tunnel	~			
VPN Tunnel:	Default_L2TP_VPN_Conner	*			

If some of the traffic from the L2TP clients needs to go to the Internet, create a policy route to send traffic from the L2TP tunnels out through a WAN trunk.

- Set **Incoming** to **Tunnel** and select your L2TP VPN connection.
- Set the **Source Address** to the L2TP address pool.
- Set the **Next-Hop Type** to **Trunk** and select the appropriate WAN trunk.

Edit Policy Route			? ×
🔝 Show Advanced Settings 🛅 Create n	ew Object •		
Configuration			
C Enable			
Description:	L2TP VPN to Internet ((Optional)	
Criteria			_
User:	L2TP-test	~	
Incoming:	Tunnel	×	E
Please select one member:	Default_L2TP_VPN_Conne	n v	
Source Address:	L2TP_POOL	*	
Destination Address:	any	×	
DSCP Code:	any	¥	
Schedule:	none	×	
Service:	any	v	
Next-Hop			
Туре:	Trunk	~	
Trunk:	SYSTEM_DEFAULT_WAN_		

3.6.3

To configure L2TP VPN in an Android device, go to **Menu > Settings > Wireless & networks > VPN settings > Add VPN > Add L2TP/IPSec PSK VPN** and configure as follows..

- **VPN name** is for the user to identify the VPN configuration.
- Set VPN server is the USG's WAN IP address.
- Set IPSec pre-shared key is the pre-shared key of the IPSec VPN gateway the USG uses for L2TP VPN over IPSec (top-secret in this example).
- Enable L2TP secret turn this off.
- DNS search domain leave this on.
- When dialing the L2TP VPN, the user will have to enter his account and password.

3.6.4 Configuring L2TP VPN in iOS

To configure L2TP VPN in an iOS device, go to **Settings > VPN > Add VPN Configuration > L2TP** and configure as follows.

- **Description** is for the user to identify the VPN configuration.
- Server is the USG's WAN IP address.
- Account is the user's account for using the L2TP VPN (L2TP-test in this example).
- **RSA SecurID** leave this off.
- **Password** is the password for the user's account.
- **Secret** is the pre-shared key of the IPSec VPN gateway the USG uses for L2TP VPN over IPSec (top-secret in this example).
- Send All Traffic leave this on.
- Proxy leave this off.

3.6.5 Configuring L2TP VPN in Windows

The following sections cover how to configure L2TP in remote user computers using Windows 7, Vista, or XP.

3.6.5.1 Configuring L2TP in Windows 7 or Windows Vista

Do the following to establish an L2TP VPN connection.

Create a Connection Object

1 Open the **Network and Sharing Center** screen.

Windows 7: click Start > Control Panel > View network status and tasks > Set up a new connection or network.

Windows Vista: click **Start > Network > Network and Sharing Center > Set up a connection or network**).

- 2 Select Connect to a workplace and click Next.
- 3 Select Use my Internet connection (VPN).
- 4 For the **Internet address** enter the **My Address** domain name or WAN IP address of the VPN gateway the USG is using for L2TP VPN (172.16.1.2 in this example).
 - **4a** For the **Destination name**, specify a name to identify this VPN (L2TP to USG for example).
 - 4b Select Don't connect now, just set it up so I can connect later and click Next.

Type the Internet a	ddress to connect to
Your network administra	tor can give you this address.
Internet address:	172.16.1.2
Destination name:	L2TP to ZyWALL
This option allow	ble to use this connection is anyone with access to this computer to use this connection. bw; just set it up so I can connect later
	Next Cancel

4 Enter your USG user name and password and click **Create**.

Type your user nar	me and password	
User name:	L2TP-test	
Password:	•••••	
	Show characters	
	Remember this password	
Domain (optional):		
		Create Cancel

6 Click Close.

Configure the Connection Object

1 In the **Network and Sharing Center** screen, click **Connect to a network**. Right-click the L2TP VPN connection and select **Properties**.

Dial-up and VPN	^	
L2TP to ZyWALL	Connect	1
	Properties	L

2 In Windows 7, click Security and set the Type of VPN to Layer 2 Tunneling Protocol with IPsec (L2TP/IPSec). Then click Advanced settings.

In Windows Vista, click **Networking**. Set the **Type of VPN** to **L2TP IPSec VPN** and click **IPSec Settings**.

Windows 7	Windows Vista+
VPN Connection Properties	L2TP to ZyWALL Properties
General Options Security Networking Sharing	General Options Security Networking Sharing
Type of VPN:	Type of VPN:
Layer 2 Tunneling Protocol with IPsec (L2TP/IPSec)	L2TP IPsec VPN
Advanced settings	IPsec Settings
Require encryption (disconnect if server declines)	Internet Protocol Venion 6 (TCP/IPv6)
Use Extensible Authentication Protocol (EAP) Properties Allow these protocols	File and Printer Sharing for Microsoft Networks Trend Micro NDIS 6.0 Filter Driver Client for Microsoft Networks Install Install Properties
Challenge Handshake Authentication Protocol (CHAP) Challenge Handshake Authentication Protocol (CHAP) Microsoft CHAP Version 2 (MS-CHAP v2) Automatically use my Windows logon name and	Description TCP/IP version 6. The latest version of the internet protocol that provides communication across diverse interconnected networks.
password (and domain, if any)	OK Cancel

2 Select **Use preshared key for authentication** and enter the pre-shared key of the VPN gateway entry the USG is using for L2TP VPN (top-secret in this example). Click **OK** to save your changes and close the **Advanced Properties** screen. Then click **OK** again to close the **Properties** window.

L2TP	
🔘 Use p	reshared key for authentication
Key:	top-secret
🔘 Use c	ertificate for authentication
DIV	erify the Name and Usage attributes of the server's certificate

4 If a warning screen about data encryption not occurring if PAP or CHAP is negotiated, click **Yes**. When you use L2TP VPN to connect to the USG, the USG establishes an encrypted IPSec VPN tunnel first and then builds an L2TP tunnel inside it. The L2TP tunnel itself does not need encryption since it is inside the encrypted IPSec VPN tunnel.

A	The protocols you have selected include PAP and/or CHAP. If one of
	these is negotiated, data encryption will not occur. Do you want to keep these settings?

Connect Using L2TP VPN

1 In the Network and Sharing Center screen, click Connect to a network, select the L2TP VPN connection and click Connect to display a login screen. Enter the user name and password of your USG user account and click Connect.

User name:	L2TP-test		
Password:	••••		
Domain:			
Save this u		word for the following	users:
	who uses ans comp		

2 A window appears while the user name and password are verified. The **Connect to a network** screen shows **Connected** after the L2TP over IPSec VPN tunnel is built.

Dial-up and VPN		^
L2TP to USG.	Connected	

- **3** After the connection is up a connection icon displays in your system tray. Click it and then the L2TP connection to open a status screen.
- 4 Click the L2TP connection's **View status** link to open a status screen.

Network and Sha	ring Center	View full map
(This c	1477-VISTA Multiple networks	Internet
ZyXEL.com (Dom Access	ain network) Local and Internet	Customize
		100000000
Connection	Broadcom NetXtreme	View status
L2TP to ZyWALL	(Public network)	Customize
Access	Local only	\frown
Connection	L2TP to ZyWALL	View status
		Disconnect

5 Click **Details** to see the address that you received is from the L2TP range you specified on the USG (192.168.10.10-192.168.10.20 in the example).

etwork Connection Details	1	
Property	Value	
Connection-specific DN		
Description	L2TP to ZyWALL	
Physical Address		
DHCP Enabled	No	
IPv4 IP Address	192.168.10.12	
IPv4 Subnet Mask	255.255.255.255	
IPv4 Default Gateway		
IPv4 DNS Server		
IPv4 WINS Server		
NetBIOS over Topip En	Yes	

6 Access a server or other network resource behind the USG to make sure your access works.

3.6.5.2 Configuring L2TP in Windows XP

In Windows XP, first issue the following command from the Windows command prompt (including the quotes) to make sure the computer is running the Microsoft IPSec service.

net start "ipsec services".

Then do the following to establish an L2TP VPN connection.

- 1 Click Start > Control Panel > Network Connections > New Connection Wizard.
- 2 Click Next in the Welcome screen.
- 3 Select Connect to the network at my workplace and click Next.

What do you want to do?	S.
O Connect to the Interne	
Connect to the Internet so	you can browse the Web and read email.
Connect to the network	k at my workplace
Connect to a business net a field office, or another loc	work (using dial-up or VPN) so you can work from home, cation.
O Set up a home or small	office network
Connect to an existing hom	e or small office network or set up a new one.
O Set up an advanced c	onnection
	r computer using your serial, parallel, or infrared port, or it other computers can connect to it.

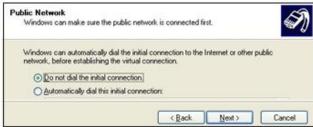
4 Select Virtual Private Network connection and click Next.



5 Type L2TP to USG as the Company Name.

Connection Name Specify a name for this connect	ion to your workplace.
Type a name for this connection Company Ngme	in the following box.
L2TP to ZyWALL	
For example, you could type the will connect to.	name of your workplace or the name of a server you
	<back next=""> Cancel</back>

6 Select Do not dial the initial connection and click Next.



7 Enter the domain name or WAN IP address configured as the **My Address** in the VPN gateway configuration that the USG is using for L2TP VPN (172.16.1.2 in this example).

/PN Server Selection What is the name or address of	of the VPN server?
Type the host name or Internet connecting.	t Protocol (IP) address of the computer to which you are
	sxample, microsoft.com or 157.54.0.1 }
These regions on the degreess from e	

- 8 Click Finish.
- 9 The Connect L2TP to USG screen appears. Click Properties > Security.



10 Click Security, select Advanced (custom settings) and click Settings.



11 Select Optional encryption (connect even if no encryption) and the Allow these protocols

radio button. Select **Unencrypted password (PAP)** and clear all of the other check boxes. Click **OK**.



12 Click IPSec Settings.



13 Select the **Use pre-shared key for authentication** check box and enter the pre-shared key used in the VPN gateway configuration that the USG is using for L2TP VPN. Click **OK**.



14 Click Networking. Select L2TP IPSec VPN as the Type of VPN. Click OK.



15 Enter the user name and password of your USG account. Click **Connect**.

	(1997)
6	~
User name:	
Password	
Save this us	ser name and password for the following users:

- 16 A window appears while the user name and password are verified.
- 17 A USG-L2TP icon displays in your system tray. Double-click it to open a status screen.
- 18 Click **Details** to see the address that you received from the L2TP range you specified on the USG (192.168.10.10-192.168.10.20).

eneral Details		
Property	Value	
Device Name	WAN Miniport (L2TP)	
Device Type	vpn	
Server type	PPP	
Transports	TCP/IP	
Authentication	PAP	
IPSEC Encryption	IPSec, ESP 3DES	
Compression	(none)	
PPP multiink framing	Off	
Server IP address	0.0.0.0	
Client IP address	192.168.10.12	

19 Access a server or other network resource behind the USG to make sure your access works.

3.6.6 What Can Go Wrong

The IPSec VPN connection must:

- Be enabled
- Use transport mode
- Not be a manual key VPN connection

- Use Pre-Shared Key authentication
- Use a VPN gateway with the **Secure Gateway** set to **0.0.0.0** if you need to allow L2TP VPN clients to connect from more than one IP address.

Disconnect any existing L2TP VPN sessions before modifying L2TP VPN settings. The remote users must make any needed matching configuration changes and re-establish the sessions using the new settings.

Tutorial 4: Managing Traffic

These sections cover controlling the traffic going through the USG.

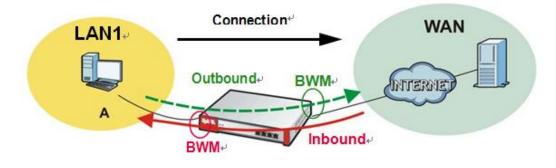
4.1 How to Configure Bandwidth Management

Bandwidth management is very useful when applications are competing for limited bandwidth.

Connection and Packet Directions

Bandwidth management looks at the connection's direction from the interface it was initiated on to the interface it goes out. The connection initiator sends outbound traffic and receives inbound traffic. The USG controls each flow's bandwidth as it goes out through an interface or VPN tunnel. For example, a LAN1 to WAN connection is initiated from LAN1 and goes to the WAN.





- Outbound traffic goes from a LAN1 device to the WAN. The USG applies bandwidth management before sending the packets out a WAN interface.
- Inbound traffic comes back from the WAN to the LAN1 device. The USG applies bandwidth management before sending the traffic out a LAN1 interface.

You can set outbound and inbound guaranteed and maximum bandwidths for an application.

4.1.1 Bandwidth Allocation Example

Say a 10-person office has WAN1 connected to a 50 Mbps downstream and 5 Mbps upstream VDSL line and you want to allocate bandwidth for the following:

- SIP: Up to 10 simultaneous 100 Kbps calls guaranteed
- Video conferencing: Up to 10 simultaneous 128 Kbps Skype video calls guaranteed
- Video streaming: up to 10 simultaneous 256 Kbps sessions
- HTTP: Internet access including downloading files for 10 users
- SMTP: 10 users sending email
- POP3: 10 users receiving email
- FTP: 10 users uploading and downloading files

Here is an example of allocating the any to WAN connection's inbound and outbound packet flows. Enable Maximize Bandwidth Usage (Max B.U.) on a packet flow to set no limit on it and let it use any available bandwidth on the out-going interface.

DDI	ORITY AND APPLICATION	GUARANTEED K / MAXIMUM K OR MAX B.U		
FNI	ORITI AND AFFEICATION	INBOUND	OUTBOUND	
1	SIP	1000/2000	1000/2000	
2	Video conferencing	1280/3840	1280/3840	
3	Video streaming	2560/3584	*	
4	HTTP	10240/46080	*	
4	SMTP	*	2048/Max B.U.	
4	POP3	10240/Max B.U.	*	
5	FTP	10240/46080	792/3072	
Tota	guaranteed bandwidth:	35560 Kbps	5120 Kbps	

 Table 11
 50 Mbps / 5 Mbps Connection Any to WAN Bandwidth Allocation Example

* This application does not usually generate enough traffic in this direction to require management.

4.1.2 Setting the Interface's Bandwidth

Use the **Configuration** > **Interface** screens to set the WAN1 interface's upstream (egress) bandwidth to be equal to (or slightly less than) what the connected device can support. This example uses 5120 Kbps.

4.1.3 SIP Bandwidth Management

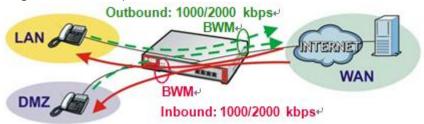
The most effective way to ensure the quality of SIP calls is to go to the **Configuration** > **BWM** screen and enable BWM and select **Enable Highest Bandwidth Priority for SIP Traffic**. See the following section if you prefer to configure specific bandwidth management rules for SIP instead.

4.1.4 SIP Any-to-WAN and WAN-to-Any Bandwidth Management Example

• Manage SIP traffic going to WAN1 from users on the LAN or DMZ.

• Inbound and outbound traffic are both guaranteed 1000 kbps and limited to 2000 kbps.

Figure 37 SIP Any-to-WAN Guaranteed / Maximum Bandwidths Example



- 1 In the **Configuration** > **BWM** screen, click **Add**.
- 2 In the Add Policy screen, select **Enable** and type **SIP Any-to-WAN** as the policy's name.

Leave the incoming interface to **any** and select **wan1** as the outgoing interface.

Select **App Patrol Service** and **sip** as the service type.

Set the inbound and outbound guaranteed bandwidth to **1000** (kbps) and maximum bandwidth to **2000** kbps and priority **1**. Click **OK**.

Note: Use **App Patrol Service** for the services classified by the USG's IDP packet inspection signatures. Use **Service Object** for pre-defined services.

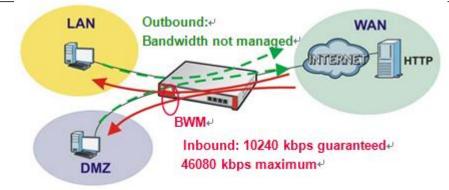
2 Repeat the steps above to create another policy named SIP WAN-to-Any for calls coming in from the SIP server on the WAN. It is the same as the SIP Any-to-WAN policy, but with the directions reversed (WAN-to-Any instead of Any-to-WAN).

Create new Object *			Add Policy	
Configuration			E Create new Object •	
V Enable			Configuration	
Description:	SIP Any-to-WAN	(Optional)	C Enable	
Criteria			Description:	SIP WAN-to-Any (Optional)
User:	any	~	Criteria	
Schedule:	none	~	User:	any
Incoming Interface:	any	~	Schedule:	none
Outgoing Interface:	wan1	~	Incoming Interface:	wan1
Source:	any	~	Outgoing Interface:	any
Destination:	any	~	Source:	any 👻
DSCP Code:	any	~	Destination:	anv
Service Type:	Service Object	· App Patrols	DSCP Code:	\sim

4.1.5 HTTP Any-to-WAN Bandwidth Management Example

- Set inbound guaranteed and maximum rates as the local users on the LAN and DMZ will probably download more than they upload to the Internet.
- Set fourth highest priority (4) for the HTTP traffic in both directions.

Figure 38 HTTP Any-to-WAN Bandwidth Management Example



- 1 In the **Configuration** > **BWM** screen, click **Add**.
- 2 In the Add Policy screen, select **Enable** and type **HTTP Any-to-WAN** as the policy's name.

Leave the incoming interface to **any** and select **wan1** as the outgoing interface.

Select **App Patrol Service** and **http** as the service type.

Set the guaranteed inbound bandwidth to **10240** (kbps) and set priority **4**. Set the maximum to **46080** (kbps). Set the outbound priority to **4**. Click **OK**.

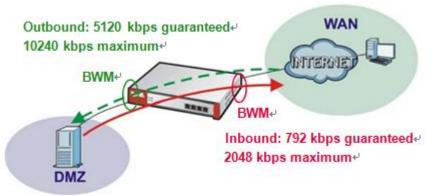
				ł
Create new Object 🔻				
onfiguration				
I Enable				
Description:	HTTP Any-to-WAN (Optional)			
riteria				
User:	any 👻			
Schedule:	none 👻			
Incoming Interface:	any			
Outgoing Interface:	wan1			
Source:	any 👻			
Destination:	any 👻			
DSCP Code:	any 🎽			
	Control of account of the second of	62567 101		
Service Type:	Service Object App Patro	Service		
Service Type: App Patrol Service:	Service Object App Patro	Service		
App Patrol Service:		Service		
App Patrol Service: SCP Marking	http v	Service		
App Patrol Service:	Inbound Marking: preserve	I Service		
App Patrol Service: SCP Marking	http v	I Service		
App Patrol Service: ISCP Marking DSCP Marking	Inbound Marking: preserve	I Service		
App Patrol Service: ISCP Marking DSCP Marking	Inbound Marking: preserve	Priority:	4	
App Patrol Service: SCP Marking DSCP Marking andwidth Shaping	http Inbound Marking: preserve Outbound Marking: preserve			kt
App Patrol Service: SCP Marking DSCP Marking andwidth Shaping	Inbound Marking: preserve V Outbound Marking: preserve V Inbound: 10240 kbps (0 : disabled)	Priority:		kt
App Patrol Service: DSCP Marking DSCP Marking	Inbound Marking: preserve V Outbound Marking: preserve V Inbound: 10240 kbps (0 : disabled)	Priority:		kt

4.1.6 FTP WAN-to-DMZ Bandwidth Management Example

Suppose the office has an FTP server on the DMZ. Here is how to limit WAN1 to DMZ FTP traffic so it does not interfere with SIP and HTTP traffic.

- Allow remote users only 2048 kbps inbound for downloading from the DMZ FTP server but up to 10240 kbps outbound for uploading to the DMZ FTP server.
- Set the fifth highest priority (5) for the FTP traffic.

Figure 39 FTP WAN-to-DMZ Bandwidth Management Example



- 1 In the **Configuration** > **BWM** screen, click **Add**.
- In the Add Policy screen, select Enable and type FTP WAN-to-DMZ as the policy's name.
 Select wan1 as the incoming interface and dmz as the outgoing interface.

Select App Patrol Service and ftp as the service type.

Set inbound guaranteed bandwidth to **792** kbps, priority **5**, and maximum **2048** kbps.

Set outbound guaranteed bandwidth to **5120** kbps, priority **5**, and maximum **10240** kbps. Click **OK**.

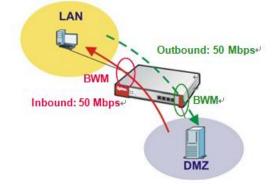
Create new Object *				
Configuration				
V Enable				
Description:	(PTP WAN-to-DMZ (Optional)			
Criteria				
User:	any			
Schedule:	none			
Incoming Interface:	wan1 👻			
Outgoing Interface:	dmz			
Source:	any			
Destination:	any			
DSCP Code:	any 🛩			
Service Type:	Service Object	Service		
App Patrol Service:	ftp v	14.0		
DSCP Marking				
DSCP Marking	Inbound Marking: preserve 👻			
	Outbound Marking: preserve 💙			
Bandwidth Shaping				-
Guaranteed Bandwidth	Inbound: 792 kbps (0 : disabled)	Priority:	5	
	Maximize Bandwidth Usage	Maximum:	2048	kbps
	Outbound: 5120 kbps (0 : disabled)	Priority:	5	1
	Maximize Bandwidth Usage	Maximum:	10240	kbps
Related Setting				
Relation second	in the second			
Log	no 👻			
	ine initiality			

4.1.7 FTP LAN-to-DMZ Bandwidth Management Example

FTP traffic from the LAN1 to the DMZ can use more bandwidth since the interfaces support up to 1 Gbps connections, but give it lower priority and limit it to avoid interference with other traffic.

- Limit both outbound and inbound traffic to 50 Mbps.
- Set fifth highest priority (5) for the FTP traffic.

Figure 40 FTP LAN-to-DMZ Bandwidth Management Example



- 1 In the **Configuration** > **BWM** screen, click **Add**.
- 2 In the Add Policy screen, select Enable and type FTP LAN-to-DMZ as the policy's name.

Select **lan1** as the incoming interface and **dmz** as the outgoing interface.

Select **App Patrol Service** and **ftp** as the service type.

Type **10240** (kbps) with priority **5** for both the inbound and outbound guaranteed bandwidth. Do not select the **Maximize Bandwidth Usage**. Set the maximum to **51200** (kbps). Click **OK**.

Add Policy			? ×
Create new Object •			
Configuration			
V Enable			
Description:	(Optional)		
Criteria			
User:	any		
Schedule:	pone Y		
Incoming Interface:	lan1		
Outgoing Interface:	dmz ~		
Source:	any 👻		
Destination:	any 👻		
DSCP Code:	any 👻		
Service Type:	Service Object App Patrol Service	æ	
App Patrol Service:	ftp	_	
DSCP Marking			
DSCP Marking	Inbound Marking: preserve Y		
	Outbound Marking: preserve		
Bandwidth Shaping			
Guaranteed Bandwidth	Inbound: 10240 kbps (0 : disabled) Prio	rity: 5	
	Maximize Bandwidth Usage Max	imum: 51200	kbps
	Outbound: 10240 kbps (0 : disabled) Prio	rity: S	1
	Maximize Bandwidth Usage Max	imum: 51200	kbps

Finally, in the BWM screen, select Enable BWM. Click Apply.

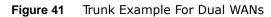
Enabi	Snable Hig) phest Bandwidth Prior	ity for SIP T	raffic 🚺								
Q Add	2 24	t 📋 Remover 💡	Actuate 5	tractivate	of Hour							
Status	Priority	Description	User	Schedule	Incoming I	Outgoing L_	Source	Destina	DSC	Service	BWM INPNIO	DSCP M_
9	1	FTP LAN-to-DMZ	any	none	miant	n dmz	влу	any	any	Appre ftp	10240/5/102	preserv
9	2	FTP WAN-to-DMZ	any	none	n want	n dmz	any	any	any	App: to	792/5/5120/5	preserv
9	3	HTTP Any-to-WAN	any	none	any	e waot	any	any	any	Appra.h	10240/4/no/4	preserv
0	4	SIP Any-to-WAN	any	none	any	s want	any	any	any	App:sip	1000/1/1000/1	preserv
0	5	SIP WAN-to-Any	any	none	swant	any	any	any	any	App:sip	1000/1/1000/1	preserv
0	6	FTP LAN-to-DMZ	any	none	s lan1	n druz	апу	any	any	Objany	10000/5/100	preserv
	defaut		any	none	any	any	any	any	any	Objany	no/7/no/7	preserv
14.4	Page	l of 1 > >	Show 50	✓ items							Disp	laying 1 - 7 of

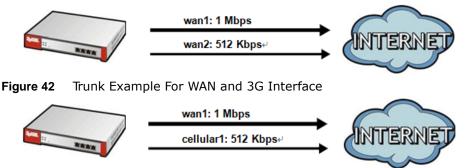
4.1.8 What Can Go Wrong?

- The "outbound" in the guaranteed bandwidth settings apply to traffic going from the connection initiator to the outgoing interface. The "inbound" refers to the reverse direction.
- Make sure you have registered the IDP/App.Patrol service on the USG to use **App Patrol Service** as the service type in the bandwidth management rules. The application patrol service uses the

4.2 How to Configure a Trunk for WAN Load Balancing

These examples show how to configure a trunk for two WAN connections to the Internet. The available bandwidth for the connections is 1 Mbps (**wan1**) and 512 Kbps (**wan2 or cellular1**) respectively. As these connections have different bandwidth, use the **Weighted Round Robin** algorithm to send traffic to wan1 and wan2 (or cellular1) in a 2:1 ratio.





You do not have to change many of the USG's settings from the defaults to set up this trunk. You only have to set up the outgoing bandwidth on each of the WAN interfaces and configure the WAN_TRUNK trunk's load balancing settings.

4.2.1 Set Up Available Bandwidth on Ethernet Interfaces

Here is how to set a limit on how much traffic the USG tries to send out through each WAN interface.

1 Click **Configuration > Network > Interface > Ethernet** and double-click the **wan1** entry. Enter the available bandwidth (1000 kbps) in the **Egress Bandwidth** field. Click **OK**.

	ttings 🔚 Create new Object	
ieneral Settings		
Enable Interface		
nterface Properties		
Interface Type:	external	
Interface Name:	wani	
Ports	P1	
Zone:	WAN	
MAC Address:	00:00:AA:79:73:79	
Description:	(0)	ptional)
P Address Assignment		
Get Automatically		
Use Fixed IP Address		
IP Address:	1.2.3.4	
Subnet Mask:	255.255.255.0	
State ick midden	1.2.3.254 (Optional)	
Gateway:	1.2.3.254 (Optional)	
	(Optional) 0 (0-15)	
Gateway: Metric:	fahrenalt	
Gateway: Metric:	fahrenalt	
Gateway: Metric: nterface Parameters Egress Bandwidth:	0 (0-15)	
Gateway: Metric: Interface Parameters Egress Bandwidth:	0 (0-15)	
Gateway: Metric: Interface Parameters	0 (0-15)	

- 2 Repeat the process to set the egress bandwidth for **wan2** to 512 Kbps.
- **3** For 3G interface settings, go to **Configuration > Network > Interface > Cellular**. Double-click the **cellular1** entry and set the egress bandwidth for **cellular1** to 512 Kbps.

4.2.2 Configure the WAN Trunk

- 1 Click **Configuration > Network > Interface > Trunk**. Click the **Add** icon.
- 2 Name the trunk and set the Load Balancing Algorithm field to Weighted Round Robin.Add wan1 and enter 2 in the Weight column.

Add wan2 (or cellular1) and enter 1 in the Weight column.

Click OK.

	runk			
Name:		example		
Load	Balancing Algorithm:	Weighted Ro	nd Robin 💌	
	Add 🔡 Edit 🎁 Ri	CHINTE OF THETE		
	Member	Mode	Weight	100
100	Member Wan1	Mode Active	Weight 2	
100			Weight 2	

Name:	example		
.oad Balancing Algorithm:	Weighted Round R	bin 💌	
🔘 Add 🔜 Edit 🍟 F	Remove 🔐 Move		
🔾 Add 🔜 Edit 🍍 F	Remove Move	Weight	
Add Bdd Bdd Bdd Bdd Bdd Bdd Bdd		Weight	

2 Select the trunk as the default trunk and click **Apply**.

Port Role Ether	net PPP	Celular	Tunnel VL/	N Bric	ige Trur	nk and a later
Show Advanced Se	ttings					
Configuration						
Enable Link St	icking 🚺					
Timeout:		300	(30-600 seconds) 🔳		
Passive Conn	ection Disconnect	t 🚺				
Default WAN True	ik					
Default Trunk Sel	ection					
SYSTEM_	DEFAULT_WAN_	TRUNK				
User Cont	figured Trunk	example		~		

4.3 How to Use Multiple Static Public WAN IP Addresses for

LAN-to-WAN Traffic

If your ISP gave you a range of static public IP addresses, this example shows how to configure a policy route to have the USG use them for traffic it sends out from the LAN.

4.3.1 Create the Public IP Address Range Object

Click **Configuration > Object > Address > Add** (in **IPv4 Address Configuration**) to create the address object that represents the range of static public IP addresses. In this example you name it **Public-IPs** and it goes from 1.1.1.10 to 1.1.1.17.

Name:	Public-IPs	
Address Type:	RANGE	~
Starting IP Address:	1.1.1.10	
End IP Address:	1.1.1.17	

4.3.2 Configure the Policy Route

Now you need to configure a policy route that has the USG use the range of public IP addresses as the source address for WAN to LAN traffic.

Click Configuration > Network > Routing > Policy Route > Add (in IPv4 Configuration). It

is recommended to add a description. This example uses **LAN-to-WAN-Range**.

Specifying a Source Address is also recommended. This example uses LAN1_SUBNET.

Set the Source Network Address Translation to Public-IPs and click OK.

Add Policy Route			?
Show Advanced Settings 🔠 Create new Obj	ect+		
Configuration			
V Enable			
Description:	LAN-to-WAN-Range	(Optional)	
Criteria			
User:	any	~	
Incoming:	any (Excluding ZyWAL	L) 👻	
Source Address:	LAN1_SUBNET	~	
Destination Address:	any	~	
DSCP Code:	any	*	
Schedule:	none	*	
Service:	any	*	
Next-Hop			
Type:	Auto	~	
DSCP Marking			
DSCP Marking:	preserve	*	
Address Translation			
Source Network Address Translation:	Public-IPs	~	

4.4 How to Use Device HA to Backup Your USG

Use device high availability (HA) to set up an additional USG as a backup gateway to ensure the default gateway is always available for the network.

Active-Passive Mode and Legacy Mode

Active-passive mode has a backup USG take over if the master USG fails and is recommended for general device failover deployments. Use legacy mode if you need a more complex relationship between the master and backup USGs, such as having both USGs active or using different USGs as the master for individual interfaces. The USGs must all use the same device HA mode (either

Management Access IP Addresses

For each interface you can configure an IP address in the same subnet as the interface IP address to use to manage the USG whether it is the master or the backup.

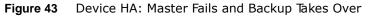
Synchronization

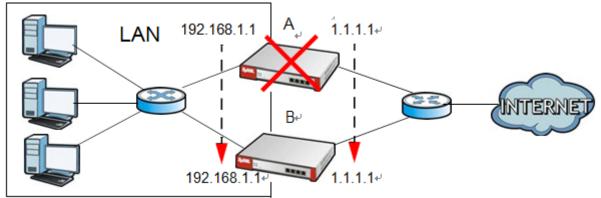
Synchronize USGs of the same model and firmware version to copy the master USG's configuration, signatures (anti-virus, IDP/application patrol, and system protect), and certificates to the backup USG so you do not need to do it manually.

4.4.1 Active-Passive Mode Device HA Example

Here active-passive mode device HA has backup USG B automatically takes over all of master USG A's functions if A fails or loses its LAN or WAN connection.

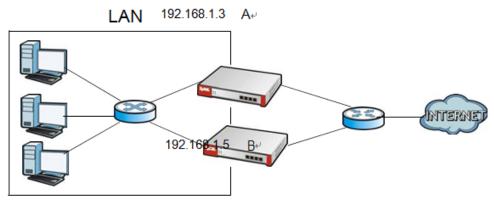
An Ethernet switch connects both USGs' LAN interfaces to the LAN. Whichever USG is functioning as the master uses the default gateway IP address of the LAN computers (192.168.1.1) for its LAN interface and the static public IP address (1.1.1.1) for its WAN interface. If USG A recovers (has both its LAN and WAN interfaces connected), it resumes its role as the master and takes over all of its functions again.





Each USG's LAN interface also has a separate management IP address that stays the same whether the USG functions as the master or a backup. USG A's management IP address is 192.168.1.3 and USG B's is 192.168.1.5.





4.4.2 Before You Start

USG A should already be configured. You will use device HA to copy USG A's settings to B later. To

avoid an IP address conflict, do not connect USG **B** to the LAN subnet until after you configure its device HA settings and the instructions tell you to deploy it.

4.4.3 Configure Device HA on the Master USG

- 1 Log into USG A (the master) and click Configuration > Device HA > Active-Passive Mode. Double-click the LAN interface's entry.
- 2 Configure 192.168.1.3 as the Manage IP and 255.255.255.0 as the Manage IP Subnet Mask. Click OK.

Enable Monitored Interface		
Interface Name:	lan1	
Virtual Router IP(VRIP)/Subnet Mask:	192.168.1.1/255.255.255.0	
Manage IP:	192.168.1.3	
Manage IP Subnet Mask:	255.255.255.0	

3 Set the Device Role to Master. This example focuses on the connection from the LAN to the Internet through the WAN interface, so select the LAN and WAN interfaces and click Activate. Enter a Synchronization Password ("mySyncPassword" in this example). Retype the password and click Apply.

uster Setting				
Cluster ID:	1			
	erface Summary			
Edk 💡	Activate @ Inact	Virtual Router IP/Netmask	Management IP/Netmask	Link Status
	want	1.2.3.4/255.255.0.0	/255.255.0.0	Down
2 0	wan2	1	1	Up
3 0	opt	192.168.4.1 / 255.255.255.0	/ 255 255 255.0	Down
()	lan1	192.168.1.1 / 255.255.255.0	192.168.1.3 / 255.255.255.0	Down
5 @	lan2	192.168.2.1 / 255.255.255.0	/ 255.255.255.0	Down
6 @	ext-wian	10.59.0.1 / 255.255.255.0	/ 255.255.255.0	Down
7 @	dimz	192.168.3.1 / 255.255.255.0	/ 255 255 255 0	Down
14 4 Pa	pe 1 of 1) ≽	E Show 50 V Rems		Displaying 1 - 7 of 7
nchronizati	an			
Server Addres	8: 1.3	2.3.4, 172.16.1.34, 192.168.4.1, 192.1	68.1.1, 192.168.2.1, 10.59.0.1, 1	92.1
Server Port:	21	(Configure)		
Password:	\frown	>		

4 Click the **General** tab, enable device HA, and click **Apply**.

General	Active-Passive Mode	Legacy Mode	
General Se	ttings		
Enable	e Device HA		
Device HA	Mode: Activ	ve-Passive Mode	(Switch to Legacy Mode page)

4.4.4 Configure the Backup USG

- 1 Connect a computer to USG B's LAN interface and log into its Web Configurator. Connect USG B to the Internet and subscribe it to the same subscription services (like content filtering and anti-virus) to which USG A is subscribed. See the **Registration** screens for more on the subscription services.
- 2 In USG B click Configuration > Device HA > Active-Passive Mode and the LAN interface Edit icon.
- **3** Configure 192.168.1.5 as the **Manage IP** and 255.255.255.0 as the **Subnet Mask**. Click **OK**.

Enable Monitored Interface	
Interface Name:	lan1.
Virtual Router IP(VRIP)/Subnet Mask:	192.168.1.1/255.255.255.0
Manage IP:	192.168.1.5
Manage IP Subnet Mask:	255.255.255.0

4 Set the Device Role to Backup. Activate monitoring for the LAN and WAN interfaces. Set the Synchronization Server Address to 192.168.1.1, the Port to 21, and the Password to "mySyncPassword". Retype the password, select Auto Synchronize, and set the Interval to 60. Click Apply.

Show	Advanced Settings			
Genera	l Settings			
Devio	e Role:	Master Backup		
P	niority:	1 (1-254)		
	Enable Preemption	- Landard Control of C		
Juster	Settings			
Cluste	w ID:	1		
	red Interface Summ			
sonico	red incertace sum	nary		
33	ide 😨 Activista 🥳	Inactivata		100000000000000000000000000000000000000
*	Status Interface +	Virtual Router IP/Netmask	Management P/Netmask	Link Status
1 (g want	1.2.3.4 / 255.255.0.0	/ 255 255.0.0	Down
2	@ wan2	1	1	Up
3	g opt	192.168.4.1 / 255.255.255.0	/255.255.255.0	Down
4 (lant	192.168.1.1 / 255.255.255.0	192.168.1.5 / 255.255.255.0	Down
5	@ lan2	192.168.2.1 / 255.255.255.0	/ 255.255.255.0	Down
6	💮 ext-wian	10.59.0.1 / 255.255.255.0	/255.255.255.0	Down
7	💮 dimz	192.168.3.1 / 255.255.255.0	/255.255.255.0	Down
14	Page 1 of 1	>>> Show 50 - Rems		Displaying 1 - 7 of 7
-	and the second second			
ynchr	onization			
Server Address: 192.168.1		192.168.1.1 (IP or FQDN)		
Server Port: 21				
P	assword:	•••••		
VA	uto Synchronize			
	0.0			

5 In the General tab enable device HA and click Apply.

General	Active-Passive Mode	Legacy Mode
General S	iettings	
Really	Device HA	
Device HA		ctive-Passive Mode (Switch to Legacy Mode page)

4.4.5 Deploy the Backup USG

Connect USG **B**'s LAN interface to the LAN network. Connect USG **B**'s WAN interface to the same router that USG **A**'s WAN interface uses for Internet access. USG **B** copies **A**'s configuration (and re-synchronizes with **A** every hour). If USG **A** fails or loses its LAN or WAN connection, USG **B** functions as the master.

4.4.6 Check Your Device HA Setup

- 1 To make sure USG B copied USG A's settings, you can log into USG B's management IP address (192.168.1.5) and check the configuration. You can use the Maintenance > File Manager > Configuration File screen to save copies of the USGs' configuration files that you can compare.
- **2** To test your device HA configuration, disconnect USG **A**'s LAN or WAN interface. Computers on LAN should still be able to access the Internet. If they cannot, check your connections and device HA configuration.

Congratulations! Now that you have configured device HA for LAN, you can use the same process for any of the USG's other local networks. For example, enable device HA monitoring on the DMZ interfaces and use an Ethernet switch to connect both USGs' DMZ interfaces to your publicly available servers.

4.5 How to Configure DNS Inbound Load Balancing

This example shows you how to configure the USG to respond to DNS query messages with the least loaded interface's IP address. The DNS query senders will then transmit packets to that interface instead of an interface that has a heavy load.

This example assumes that your company's domain name is www.example.com. You want your USG's WAN1 (202.1.2.3) and WAN2 (202.5.6.7) to use DNS inbound load balancing to balance traffic loading coming from the Internet.

1 In the CONFIGURATION > Network > Inbound LB screen, select Enable DNS Load Balancing. Click Apply.

DNS Load Balancing	
Global Setting	
Enable DNS Load Balancing	

2 Click **Add** in the **Configuration** table. The following screen appears.

Select Enable, enter *.example.com as the Query Domain Name.

Enter 300 in the Time to Live field to have DNS query senders keep the resolved DNS entries on

their computers for 5 minutes.

Select **any** in the **IP Address** field and **WAN** in the **Zone** field to apply this rule for all DNS query messages the WAN zone receives.

Select Least Load - Total as the load balancing algorithm.

Click **Add** to add WAN1 and WAN2 as the member interfaces. Click **OK**.

Add DNS Load Balancing			7 ×	
Create new Object +				
General Settings			<u>^</u>	
Enable				
DNS Setting				
Query Domain Name:	.example.com	1		
Time to Live:		-)	4.00.000	
THE WORKS	200	214/48364/ \$800	nds, 0 is unchanged)	
Query From Setting				
IP Address:	any	~	Load Balancing Member	
Zone:	WAN	N Menber:		1
			Monitor Interface:	wan1
oad Balancing Member			IP Address	
Load Balancing Algorithm:	Least Load - Total	~)	Same as Monitor Interface	202.1.2.3
Fallover IP Address:	0.0.0.0	(Optional)	Custon	0.0.0.0
Add Zick Themewe			Load Balancing Member	
AND STOR STORE				
# P Address	Monitor In	terface	Menbert	2
	Monitor In wan1	terface	Member: Monitor Interface:	2 wan2
# IP Address		terface	Monitor Interface: IP Address	wand
 P Address 1 202 1 2 3 2 202 5 6.7 	want	terface	Monitor Interface:	

Continue to go to the **Configuration > Firewall** and **Configuration > Network > NAT** screens to configure the corresponding firewall rules and NAT virtual server for the inbound service access.

4.5.1 What Can Go Wrong?

- Using a greater TTL value makes DNS inbound load balancing become ineffective, although it can reduce the USG's loading as the DNS request senders does not need to send new queries to the USG that often.
- If you choose **Custom** in the **Load Balancing Member** screen and enter another IP address for a member interface, make sure the entered IP address is configured in the corresponding firewall and NAT virtual server rules.

4.6 How to Allow Public Access to a Web Server

This is an example of making an HTTP (web) server in the DMZ zone accessible from the Internet (the WAN zone). In this example you have public IP address 1.1.1.1 that you will use on the WAN interface and map to the HTTP server's private IP address of 192.168.3.7.



4.6.1 Configure NAT

Create a NAT rule to send HTTP traffic coming to WAN IP address 1.1.1.1 to the HTTP server's private IP address of 192.168.3.7.

- 1 Click Configuration > Network > NAT > Add > Create New Object > Address and create an IPv4 host address object named DMZ_HTTP for the HTTP server's private IP address of 192.168.3.7. Repeat to create a host address object named Public_HTTP_Server_IP for the public WAN IP address 1.1.1.1.
- 2 Configure the NAT rule.

For the **Incoming Interface** select the WAN interface.

Set the **Original IP** to the **Public_HTTP_Server_IP** object and the **Mapped IP** to the **DMZ_HTTP** object.

HTTP traffic and the HTTP server in this example both use TCP port 80. So you set the **Port Mapping Type** to **Port**, the **Protocol Type** to **TCP**, and the original and mapped ports to 80.

Keep **Enable NAT Loopback** selected to allow users connected to other interfaces to access the HTTP server.

Add NAT	Contration	🔾 Add A	ddress Rule	P1 Show 50	? ×	
Create new Object		Nam	9:	DMZ_HTTP	Add Address Rule	Show 50 V Rene
General Settings		Addr	ess Type:	HOST	Name:	Public_HTTP_Server_IP
V Enable Rule		IP Ad	idress:	192.168.3.7	Address Type:	HOST
Rule Name:	DMZ_HTTP				IP Address:	1.1.1.1
Port Mapping Type						
Classification:	Virtual Service	ver	1:1 NAT	Mar	ny 1:1 NAT	
Mapping Rule						
Incoming Interface:	wan1		~			
Original IP:	Public_HTTP_Se	erver_IP	~			
Mapped IP:	DMZ_HTTP		~			
Port Mapping Type:	Port		*			
Protocol Type:	TCP		*			
Original Port:	80					
Mapped Port:	80					
Related Settings						
Enable NAT Loopback 1						
Configure Firewall						
				_		
				_	OK Cancel	

4.6.2 Set Up a Firewall Rule

Create a firewall rule to allow the public to send HTTP traffic to IP address 1.1.1.1 in order to access the HTTP server. If a domain name is registered for IP address 1.1.1.1, users can just go to the domain name to access the web server.

Click **Configuration > Firewall > Add**. Set the **From** field as **WAN** and the **To** field as **DMZ**. Set the **Destination** to the HTTP server's DMZ IP address object (**DMZ_HTTP**). **DMZ_HTTP** is the destination because the USG applies NAT to traffic before applying the firewall rule. Set the **Access** field to **allow** and the **Service** to **HTTP**, and click **OK**.

Add Firewall Rule		? ×
🛅 Create new Object 🔹		
Enable		
From:	wan 👻	
To:	DMZ 👻	
Description:	(Optional)	
Schedule:	none 👻	
User:	any 👻	
Source:	any 👻	
Destination:	DMZ_HTTP V	
Service:	нттр	
Access:	alow	
Log:	no 👻	
Page 1 of 1 >>	Show 50 🗠 items 🛛 🔿 🔿	Cancel

4.6.3 What Can Go Wrong

- The USG checks the firewall rules in order and applies the first firewall rule the traffic matches. If traffic matches a rule that comes earlier in the list, it may be unexpectedly blocked.
- The USG does not apply the firewall rule. The USG only apply's a zone's rules to the interfaces that belong to the zone. Make sure the WAN interface is assigned to WAN zone.

4.7 How to Manage Voice Traffic

Here are examples of allowing H.323 and SIP traffic through the USG.

4.7.1 How to Allow Incoming H.323 Peer-to-peer Calls

Suppose you have a H.323 device on the LAN for VoIP calls and you want it to be able to receive peer-to-peer calls from the WAN. Here is an example of how to configure NAT and the firewall to have the USG forward H.323 traffic destined for WAN IP address 10.0.0.8 to a H.323 device located on the LAN and using IP address 192.168.1.56.

Figure 46 WAN to LAN H.323 Peer-to-peer Calls Example



4.7.1.1 Turn On the ALG

Click Configuration > Network > ALG. Select Enable H.323 ALG and Enable H.323 transformations and click Apply.

Figure 47 Configuration	> Network > ALG
-------------------------	-----------------

Settings		
Enable SIP ALG		
C Enable SIP Transformations		
2 Enable Configure SIP Inactivity Timeout		
SIP Media Inactivity Timeout :	120	(seconds)
SIP Signaling Inactivity Timeout :	1800	(seconds)
SIP Signaling Port :	🔘 Ad	d 🔡 Edit 🍟 Remove
		Port =
	1	5060
23 Settings		
Enable H.323 ALG		
Enable H.323 Transformations	(1)(2)(1)	-
H.323 Signaling Port :	1720	(1025-65535)
Additional H.323 Signaling Port for Transformations :		(1025-65535) (Optional)

4.7.1.2 Set Up a NAT Policy For H.323

In this example, you need a NAT policy to forward H.323 (TCP port 1720) traffic received on the

USG's 10.0.0.8 WAN IP address to LAN IP address 192.168.1.56.

1 Click Configuration > Network > NAT > Add > Create New Object > Address and create an IPv4 host address object for the public WAN IP address (called WAN_IP-for-H323 here). Repeat to create an address object for the H.323 device's private LAN IP address (called LAN_H323 here).

Configure a name for the rule (WAN-LAN_H323 here).

You want the LAN H.323 device to receive peer-to-peer calls from the WAN and also be able to initiate calls to the WAN so you set the **Classification** to **NAT 1:1**.

Set the **Incoming Interface** to the WAN interface.

Set the **Original IP** to the WAN address object (**WAN_IP-for-H323**).

Set the Mapped IP to the H.323 device's LAN IP address object (LAN_H323).

Set the **Port Mapping Type** to **Port**, the **Protocol Type** to **TCP** and the original and mapped ports to 1720.

Click OK.

Add NAT		Create Address				
General Settings		Name: Address Type:	WAN_IP-fo	r-H323	SUCHELT HOST	
Rule Name:	WAN-LAN_H323	IP Address:	10.0.0.8	Name:	LAN_H323	
Port Mapping Type Classification: Mapping Rule	Virtual Server	I:1 NAT	C Many 1:1 NAT	Address Type: IP Address:	HOST 192.168.1.56	-
Incoming Interface: Original IP:	wan1 WAN_IP-for-H323	* *				
Mapped IP:	LAN_H323	~				
Port Mapping Type:	Port	~				
Protocol Type:	TCP	~				
Original Port: Mapped Port:	1720					
Related Settings						
Enable NAT Loopback Enable NAT Loopback Configure Pressal						
			ОК	Cancel		

4.7.1.3 Set Up a Firewall Rule For H.323

Configure a firewall rule to allow H.323 (TCP port 1720) traffic received on the WAN_IP-for-H323 IP address to go to LAN IP address 192.168.1.56.

1 Click Configuration > Firewall > Add.

In the **From** field select WAN.

In the **To** field select LAN1.

Configure a name for the rule (WAN-to-LAN_H323 here).

Set the **Destination** to the H.323 device's LAN1 IP address object (**LAN_H323**). **LAN_H323** is the destination because the USG applies NAT to traffic before applying the firewall rule.

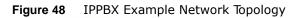
Set the Service to H.323.

Click OK.

Add Firewall Rule	mmary		? X
🛅 Create new Object 🔻			
🗹 Enable			
From:	WAN	*	
To:	LAN1	*	
Description:	WAN-to-LAN_H323	(Optional)	
Schedule:	none	~	
User:	any	~	
Source:	any	~	
Destination:	LAN_H323	~	
Service:	H323	~	
Access:	allow	~	
Log:	no	~	
I Rept		OK C	ancel
			and _

4.7.2 How to Use an IPPBX on the DMZ

This is an example of making an IPPBX x6004 using SIP in the DMZ zone accessible from the Internet (the WAN zone). In this example you have public IP address 1.1.1.2 that you will use on the WAN interface and map to the IPPBX's private IP address of 192.168.3.9. The local SIP clients are on the LAN.





4.7.2.1 Turn On the ALG

Click Configuration > Network > ALG. Select Enable SIP ALG and Enable SIP Transformations and click Apply.

Figure 49	Configuration > Network > ALG
ALG	
SIP Settings	
SIP Seconds	
Enable SI	PALG
🔽 Enab	ole SIP Transformations
🔽 Enab	ole Configure SIP Inactivity Timeout

4.7.2.2 Set Up a NAT Policy for the IPPBX

Click **Configuration > Network > NAT > Add > Create New Object > Address** and create an IPv4 host address object for the IPPBX's private DMZ IP address of 192.168.3.9. Repeat to create a host address object named IPPBX-Public for the public WAN IP address 1.1.1.2.

- Configure a name for the rule (WAN-DMZ_IPPBX here).
- You want the IPPBX to receive calls from the WAN and also be able to send calls to the WAN so you set the **Classification** to **NAT 1:1**.

- Set the **Incoming Interface** to use the WAN interface.
- Set the **Original IP** to the WAN address object (**IPPBX-Public**). If a domain name is registered for IP address 1.1.1.2, users can use it to connect to for making SIP calls.
- Set the Mapped IP to the IPPBX's DMZ IP address object (IPPBX-DMZ).
- Set the **Port Mapping Type** to **Port**, the **Protocol Type** to **UDP** and the original and mapped ports to 5060.
- Keep Enable NAT Loopback selected to allow the LAN users to use the IPPBX.
- Click OK.

Figure 50 Configuration > Network > NAT > Add

Add NAT		0	Add Address Rule	e				
Create new Object +			Name:	104	EXC-DMZ			
General Settings			Address Type:	HO		~		
Enable Rule			IP Address:	196	2.168.3.	9		
Rule Name:	WAN-DMZ_IPPBX					O Add Address Rule	HOST	
Port Mapping Type						Name:	IPP8X-Public	
Classification:	O Virtual Server	۲	1:1 NAT	Many 1	:1 NAT	Address Type:	HOST	~
Mapping Rule						IP Address:	1.1.1.2	
Incoming Interface:	wan1	~				1		
Original IP:	IPPEX-Public	~						
Mapped IP:	IPPEX-DMZ	*						
Port Mapping Type:	Port	~						
Protocol Type:	UDP	~						
Original Port:	5060]						
Mapped Port:	5060							
Related Settings								
Enable NAT Loopback []						~		
					ОК	Cancel		

4.7.2.3 Set Up a WAN to DMZ Firewall Rule for SIP

The firewall blocks traffic from the WAN zone to the DMZ zone by default so you need to create a firewall rule to allow the public to send SIP traffic to the IPPBX. If a domain name is registered for IP address 1.1.1.2, users can use it to connect to for making SIP calls.

Click **Configuration > Firewall > Add**. Set the **From** field as **WAN** and the **To** field as **DMZ**. Set the **Destination** to the IPPBX's DMZ IP address object (**DMZ_SIP**). **IPPBX_DMZ** is the destination because the USG applies NAT to traffic before applying the firewall rule. Set the **Access** field to **allow** and click **OK**.

Add Firewall Rule	hirewall sess	? ×
🔚 Create new Object 🔹		
Enable		
From:	WAN	~
To:	DMZ	~
Description:		(Optional)
Schedule:	none	*
User:	any	*
Source:	any	*
Destination:	IPPEX-DMZ	×
Service:	any	×
Access:	alow	~
Log:	no	~
 Service 	W /	OK Cancel
 Schedule 	9 8	Carca

4.7.2.4 Set Up a DMZ to LAN Firewall Rule for SIP

The firewall blocks traffic from the DMZ zone to the LAN1 zone by default so you need to create a firewall rule to allow the IPPBX to send SIP traffic to the SIP clients on the LAN.

1 Click Configuration > Firewall > Add. Set the From field as DMZ and the To field as LAN1. Set the Destination to the IPPBX'S DMZ IP address object (DMZ_SIP). Set the Source to IPPBX_DMZ. Leave the Access field to allow and click OK.

Create new Object +		
V Enable		
From:	DMZ	~
To:	LAN1	~
Description:		(Optional)
Schedule:	none	~
User:	ATV.	~
Source:	IPPBX-DMZ	v)
Destination:	апу	*
Service:	any	~
Access:	allow	~
Log:	no	~

4.7.3 What Can Go Wrong

- The USG checks the firewall rules in order and applies the first firewall rule the traffic matches. If traffic matches a rule that comes earlier in the list, it may be unexpectedly blocked.
- The USG does not apply the firewall rule. The USG only apply's a zone's rules to the interfaces that belong to the zone. Make sure the WAN interface is assigned to WAN zone.

4.8 How to Limit Web Surfing and MSN to Specific People

The following is an example of using application patrol (AppPatrol) to enforce web surfing and MSN

4.8.1 Set Up Web Surfing Policies

Before you configure any policies, you must have already subscribed for the application patrol service. You can subscribe using the **Configuration > Licensing > Registration** screens or using one of the wizards.

1 Click **Configuration > AppPatrol**. If application patrol is not enabled, enable it, and click **Apply**.



2 Click **Configuration > AppPatrol > Query**. In the first drop down menu select **By Category** and in the second drop down menu select **Web**, then click **Search**. Double-click the **http** entry to edit it.

eard	h:	C	By Category V Web V Search
ry	Result		
20	dit 💡 A	ctivate 🗑 Inactivate	
•	Status	Service +	Defaut Access
	9	ActiveX	forward
	9	Adobe-com	forward
	0	Apple-Safari	forward
	9	Dynamicintranet	forward
	9	Editgrid	forward
	9	Evernote	forward
	9	Glide	forward
	9	Google	forward
	9	Google-Books	forward
0	9	Google-Chrome	forward
1	0	Google-Finance	forward
2	9	Google-Picasa	forward
3	9	Google-Translate	forward
4	9	Google-calendar	forward
5	0	Google-docs	forward
6	9	Google-earth	forward
7	9	HTTP	forward

3 Double-click the **Default** policy.

Enabl	e Service									
rvice Id	entificatio	on								
lame:			TTP							
lassifical	tion:	A	auto							
licy										
	🕑 Edt 🍵	Remove 🂡	Activate 🌚 I	nactivate 📣 M	ove					
	-	Remove 💡	Activate <table-cell> 🖗 I User</table-cell>	nactivate _{sp} ill M	ove To	Source	Destination	Access	Log	
🔾 Add	-					Source any	Destination	Access	Log	
Add Status	# ^ default	Schedule	User any	From any	То			forward		
Add Status	# ^ default	Schedule	User any	From any	То			forward	no	D

4 Change the access to **Drop** because you do not want anyone except authorized user groups to browse the web. Click **OK**.

Edit Policy default				? ×
Create new Object -				
	G			
Access:	dro	p	*	
Log	no		*	

5 Click the Add icon in the policy list. In the new policy, select Sales as the user group allowed to browse the web. (The user group should be set in the Configuration > Object > User/Group > Group > Add screen.) Click OK.

Add Policy			
Create new Object+			
Enable Policy			
Port:	0 (0:a	ny)	
Scheduler	none	*	
Useri	Sales		
From:	any	*	
To:	any	~	
Sources	any	~	
Destinations	any	*	
Access	forward	~	
Log	no	~	

4.8.2 Set Up MSN Policies

In this part of the tutorial, you can set up a recurring schedule and apply it to the MSN application patrol rule so that only the sales department is allowed to use MSN during work hours on weekdays.

1 Click **Configuration > AppPatrol > Query**, and in the second dropdown menu, select **Instant**

Messager, and click Search. Then, double-click the msn entry to edit it.

10	v		ret mére	
19	0	ISPQ	forward	
20	0	ini	forward	
21	0	instan-t	forward	
22	0	Jotrans	forward	
23		Kbx	forward	
24	0	Kubao	forward	
25		Levelave	forward	
26	0	MSN	drop	
27		Message-Send-Protocol	forward	
28	0	MissLee	forward	
29	9	MySpaceM	forward	
30		NateOn	forward	
31	0	Netcal	forward	
32	9	POPO	forward	
33	9	PatakScene	forward	
34	0	PM	forward	
1				120

2 Double-click the **Default** policy.

iervice								
Enable Service								
iervice Identification								
Name:	MSN							
Classification:	Auto							
olicy								
	move 🤪 Activate 🥥 I	Inactivate 📣 Mc	2410					
GAdd ZEdt TR	move 🤪 Activate 🎯 : chedule User	Inactivate MMC	Te	Source	Destination	Access	Log	
Add Edit TR				Source	Destination	Access forward	Log	
Status # S default n	chedule User	From	To			forward		D lof 1
Add Edit TRA	chedule User	From	To			forward	no	D lof 1
Add Edit TRA	chedule User	From	To			forward	no	D Lof 1
Add Edit TRA	chedule User	From	To			forward	no	D lof 1

3 Change the access to **Drop** because you do not want anyone except the authorized user group

(sales) to use MSN. Click **OK**.

Create new Object+					
Access	drop	×)			
Action Block	E Login	Menage	Audo	Video	E File-Transfer
Log	no	~			

4 Now you will need to set up a recurring schedule object first. Click Configuration > Object > Schedule. Click the Add icon for recurring schedules.

5 Give the schedule a descriptive name such as **WorkHours**. Set up the days (Monday through

Friday) and the times (08:00 - 17:30) when the sales group is allowed to use MSN. Click ${\bf OK}.$

	E construction of the second s			
Name:	WorkHours			
ay Time				
Start Time:	06:00	0		
Stop Time:		9		
feekdy				
Week Days:	Monday	V Tuesday	Wednesday	\
	Thursday	Friday	Saturday)

6 Click **Configuration > AppPatrol > Query**, and in the second dropdown menu, select **Instant**

Messager, and click Search. Then, double-click the msn entry to edit it.

forward	6 ISPQ	
	A pera	19
forward	💡 kmi	20
forward	🤪 Instan-t	21
forward	Jotrans	22
forward	G KEx	23
forward	G Kubao	24
ferward	· Lave Lave	26
drop	MSN	26
forward	Message-Send-Protocol	27
forward	💡 MasLee	28
forward	WySpacelM	29
forward	NateOn	30
forward	Netcall	31
forward	POPO	32
forward	PatakScene	33
forward	PMI	34
forward forward forward forward	NateOn Netcal POPO PatakScene	29 30 31 32 33 34

7 Click the Add icon in the policy list. In the new policy, select WorkHours as the schedule and Sales as the user group that is allowed to use MSN at the appointed schedule. Then select forward in the Access field. Click OK to finish the setup.

Edit Policy 1				7 3
Create new Object+				
Enable Policy				
Porti	0 (0 : any)			
Schedule:	WorkHours 👻			
User:	Sales)		
From	any 👻			
To:	any 💌			
Sources	any 👻			
Destination:	any 👻	_		
Access:	forward 👻			
Action Block	🖾 Login 📃 Messa	pe Audio	Video	File-Transfer
Log	no 💌			
				OK Cancel

Now only the sales group may use MSN during work hours on week days.

4.8.3 What Can Go Wrong

If you have not already subscribed for the application patrol service, you will not be able to configure any policies. You can do so by using the **Configuration > Licensing > Registration** screens or using one of the wizards.