2012

ZyWALL USG ZLD 3.0 Support Notes

[Type the document subtitle]







Scenario 1 - Reserving Highest Bandwidth Management Priority for VoIP Traffic

1.1 Application scenario

In an enterprise network, there are various types of traffic. But most of the company's Internet bandwidth is limited. All traffic will contend for it and 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. A ZyWALL 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 environment, VoIP traffic should usually be awarded the highest priority over all other types of traffic.



Network conditions:

USG:

Data LAN: 192.168.1.0/24

VoIP LAN: 192.168.2.0/24

Goals to achieve:

- 1) The priority of VoIP traffic is the highest and without any bandwidth restriction.
- 2) Restrict FTP download/upload bandwidth to 1000/500 kbps and set priority of FTP traffic to 4 for all users.

USG configuration:

Step 1: Configuration > ALG > check "Enable SIP ALG" function and "Enable SIP transformations".

•	CONFIGURATION	ALG
	₩ Quick Setup ■ Licensing ■ Network ■ Interface ■ Routing	SIP Settings
r.	Zone DDNS NAT HTTP Redirect ALC IP/MAC Binding DNS Inbound LB Auth. Policy Firewall	Image: SIP Enable Configure SIP Inactivity Timeout: 120 (seconds) SIP Signaling Inactivity Timeout: 1800 (seconds) SIP Signaling Port: Image: Add Image:

Step 2: Configuration > BWM > check "Enable BWM" and "Enable Highest Bandwidth priority for SIP Traffic".

10	CONFIGURATION	BWM											
	CONFIGURATION Y Quick Setup Ucensing Network Inferface Rotuting Zone DDNS NAT HTTP Redirect ALG IPMAC Binding ONS HousendLB Auth. Policy	BWM Global Se Configuration Add Configuration Configurati	tting M Highest Bandwi It Poscription It I of 1 }	dth Priority for Activate @ User any H Show 54	SIP Traffic [] Inactivate M Schedule none D v Items	Move Incoming Inte any	Outgoing Inte any	Source any	Destination any	DSCP any	Service Obj:any	BWM In/Pri/Out/Pri no/7/no/7	DSCP Marking preserve/pre Displaying 1 - 1 of 1
	Frewall VPN App Patrol Gwto Constant Device HA Object System Log & Report												

Step 3: Configuration > BWM > Select the "Add"

- (1) Select the "WAN trunk interface" in incoming and outgoing interface
- (2) And service object select the "FTP".

(3) Limit the **inbound** traffic to 1000Kbps and **Outbound** to 500Kbps and set all of the - priority levels to **4**.

7	TVXFI TUWALLUSC 100		Add Policy			🛛 ICE 🖵 Console 🖾 CLI
	YAEL ZYWALL		🔚 Create new Object 🗸			
10	CONFIGURATION	BWM	Criteria			
	ILcensing ILcensing Interface Interface Rotuing 20ne DDNS NAT HTRRedired 4LG IMACDINGING 0NS Inbound LB 4Ath Policy Firmal VPN App Patrol EMA-St Object System Log & Report	BWH Global Setting Chable BVM Enable Highest Bandwidth Priority for Configuration Add 2 Edit Remove Activate @ Status Priority Description User dentity Status Priority Description User any Remove Activate @ Status Priority Description User any Remove Activate @ Status Priority Description User any Remove Activate @ Status Priority Description User Status Priori	User: Schedule: Incoming Interface: Outgoing Interface: Source: Destination: DSCP Code: Service Object: DSCP Marking DSCP Marking Bandwidth Shaping Guaranteed Bandwidth	any v none SYSTEM_DEFAULT_WANL v SYSTEM_DEFAULT_WANL v SYSTEM_DEFAULT_WANL v any v any v Service Object App Patrol Service FTP v Shound Marking: preserve v Dutbound Marking: preserve v Service Object V Maximum 0 kbps Outbound: 500 kbps (0 : Priority: 4 Maximum 0 kbps Outbound: 500 kbps (0 : Priority: 4 disabled) Maximum 0 kbps Outbound: 500 kbps (0 : Priority: 4 disabled) Maximum 0 kbps Outbound: 500 kbps (0 : Priority: 4 disabled) Maximum 0 kbps Outbound: 500 kbps (0 : Priority: 4 disabled) Maximum 0 kbps	E	3P Marking serve/pre paying I - 1 of 1
https	//192.168.1.1/ext-js/web-pages/	index/index.html#				

Scenario 2 - Assign IPv6 to your LAN to access remote IPv6 network

2.1 Application scenario

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



2.2 6to4 IP translation introduction

Network conditions:

USG:

WAN1: 61.222.9.5(Static PPPoE v4)

Or

WAN1:59.124.163.155(Static)

Goal to achieve:

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

USG configuration

	IPv6
CONFIGURATION TY Quick Setup Licensing Network Auth. Policy Firewall VPN App Patrol BWM Anti-X Object System	IPv6 Global Setting IPv6
 Host Name USB Storage Date/Time Console Speed DNS WWW SSH TELNET FTP SNMP Vantage CNM Language 	
• Language • IPv6 ⊡ Log & Report	

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

Step 2: Setting the static IP on WAN1

 Configuration > Interface > Ethernet > Double Click WAN1 interface and configure with static IP address 59.124.163.155.

	CONFIGURATION	Port Ro	le Et	thernet PPP	Cellular Tunr	nel VLAN	Bridge Trunk	
	¶♥ Quick Setup ⊡ Licensing	Config	juration					
Ö.	Network Interface	Z E	Edit 🍵 Re	emove 🧕 Activate	🔞 Inactivate 🖷 Cre	eate Virtual Inter	face 📴 Object Reference	
	→ Routing	#	Status	Name	IP Address		Mask	_
R,	+ Zone	1	9	wan1	STATIC 59.124.1	63.155	255.255.255.224	
	+ DDNS + NAT	2	0	wan2	DHCP 0.0.0.0		0.0.0.0	
	HTTP Redirect	3	9	lan1	STATIC - 192.168.	.1.1	255.255.255.0	
	+ ALG	4	@	lan2	STATIC - 192.168.	2.1	255.255.255.0	
	 IP/MAC Binding DNS Inbound LB 	5	0	dmz	STATIC - 192.168.	3.1	255.255.255.0	
	+ Auth. Policy	14	4 Page	e 🔟 of 1 🕨 🕅	Show 50 👻 it	ems		Displaying 1 - 5 of 5
	+ Firewall							
	VPN App Patrol	IPv6 C	Configura	ation				
	+ BWM	Z E	Edit 💡 A	ctivate 🔞 Inactivat	e ा 🔤 Object Referen	nce		
	Anti-X Object	#	Status	Name		IP Address		
	⊞ Object ⊞ System	1	9	wan1				

Step 3: Setting IPv6 IP address on LAN1

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

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	
Zone:	LAN1	
MAC Address:	50:67:F0:5C:AE:45	
Description:		(Optional)
IPv6 Address Assignment		

(2) Convert WAN1 IP address to hexadecimal

Check Enable Stateless Address Auto-configuration(SLAAC) box and enter 2002:3b7c:a39b::/64 in the prefix table.

(3) Check IPv6 Router Advertisement Setting box and add the prefix in the Advertised Prefix Table.

IPv6 View 🔻 🏢 Show Advanced Sett	ings 🔚 Create new Object
MAC Address:	50:67:F0:5C:AE:45
Description:	(Optional)
month and a	
IPv6 Address Assignment	
Enable Stateless Address Auto-	configuration (SLAAC)
Link-Local Address:	fe80::5267:f0ff:fe5c:ae45/64
IPv6 Address/Prefix Length:	2002:3b7c:a39b::/64 (Optional)
DHCPv6 Setting	
DHCPv6:	N/A 👻
IPv6 Router Advertisement Sett	ing
Enable Router Advertisement	
Router Preference:	Medium 👻
Advertised Prefix Table	🛇 Add 🔀 Edit. 🍵 Remove
	# IPv6 Address/Prefix Length ~
	1 2002:3b7c:a39b::/64
	I Page 1 of 1 Show 50 v items Displaying 1 - 1 of 1

Step 4: Enable 6 to 4 tunnel.

(1) Configuration > Interface > Tunnel > Click Add button

9	CONFIGURATION	Port R	ole	Ethernet	PPP Cellular	Tunnel	N Bridge	Trunk			
	₩ Quick Setup Licensing Network	Confi	guratio	n Edit 🗯 Rem	nve 🙆 Artivate (🖗 Inactivate 🚾 Obio	rt Reference				
	 Interface Routing Zone 	#	Statu	s Name	IP Address	Tun	iel Mode		My Address	Remote Gateway Address	a display
	 DDNS NAT HTTP Redirect 										
	ALG IP/MAC Binding										
	DNS Inbound LB Auth Policy										

- (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

Show Advanced Settings	
eneral Settings	
V Enable	
iteriate Properties	
Interface Name:	tunnel0
Zone:	TUNNEL 🔽
Tunnel Mode:	6to4 👻
v6 Address Assignment	
IPv6 Address/Prefix Length:	(Optional)
Metric:	0 (0-15)
to4 Tunnel Parameter	
6to4 Prefix:	2002::/64
Relay Router:	192.88.99.1 (Optional)

After these configuration steps, connect your computer to the device and check that your computer received an IPv6 IP address from tunnel.

Scenario 3 – DNS Inbound Load Balance

3.1 Application scenario

As an enterprise network gateway, the ZyWALL USG often has more than one WAN connection to share the network traffic. With DNS inbound load balance feature, the ZyWALL USG can reply with its other WAN IP to client according to network administrator's demand. Therefore, clients can visit the server behind ZyWALL USG smoothly via different connections.



- 1. Clients send DNS query for <u>www.zyxel.com.tw</u> to the client DNS server.
- 2. The client DNS server asks the query to DNS server.
- 3. DNS server reply to client DNS server to ask WAN1 IP for www.zyxel.com
- 4. Client DNS server reply to clients to ask WAN1 IP for <u>www.zyel.com</u>
- 5. Clients ask <u>www.zyxel.com.tw</u> to WAN1 IP of USG.
- 6. USG replies with WAN1 or WAN2 IP based on different balancing algorithm.
- 7. Clients access web page to WAN1 or WAN2.

ZyXEL – ZyWALL USG Support Notes

Network condition:

USG:

- WAN1 IP: 59.124.163.150
- WAN2 IP: 59.124.163.135
- WAN1 downstream bandwidth: 50M
- WAN2 downstream bandwidth: 10M

Global DNS server:

- Leave DNS forward record for zyxel.com.tw to WAN1
- Web Server behind USG:
- IP: 192.168.1.33

Goals to achieve:

To balance traffic loading from Internet to WAN interfaces by using DNS inbound load balancing feature based on WRR algorithm.

Step 1: Set up the Authoritative DNS for <u>zyxel.com.tw</u> on DNS Global Server.

- a. Set up the zone file for entry
 - (a) www.zyxel.com.tw NS WAN1
 - (b) www.zyxel.com.tw NS WAN2
- b. Set up the IP address for wan1 and wan2
 - (a) WAN1 A 59.124.163.150
 - (b) WAN2 A 59.124.163.135
- Step 2: Go to **Configuration -> Network -> Interface -> Ethernet**. Configure WAN IP address.

🕜 Edit Ethernet		? ×
Show Advanced Settings		
		<u>^</u>
General Settings		
Enable Interface		
Interface Properties		
Interface Type:	external 💉 🚺	E
Interface Name:	ge3	
Port:	P3	
Zone:	WAN 🗸 👔	
MAC Address:	00:19:CB:11:5C:3C	
Description:	(Optional	0
IP Address Assignment		
Get Automatically	0.0.0.0	
Use Fixed IP Address		
IP Address:	59.124.163.150	
Subnet Mask:	255.255.255.224	
Gateway:	59. 124. 163. 129 (Optional)	
Metric:	0 (0-15)	-
•	m	Þ
	ОК	Cancel
🕜 Edit Ethernet		? ×

III Show Advanced Settings		
General Settings		-
Interface Properties		
Interface Type:	external 🗸 👔	
Interface Name:	ge4	=
Port:	P4	
Zone:	WAN	
MAC Address:	00-10-02-11-50-30	
Description	0.15.05.11.30.30	
Description:	(Optional)	
IP Address Assignment		
Get Automatically		
Use Fixed IP Address		
IP Address:	59.124.163.135	
Subnet Mask:	255.255.255.224	
Gateway:	59. 124. 163. 129 (Ontional)	
Interface Parameters	0 (0-13)	-
	Cancel	

Step 3. Go to Configuration -> Network -> DNS Inbound LB, and add DNS Load Balancing

a. Edit the Query Domain Name that is needed, and choose the Load Balancing Algorithm "Weighted Round Robin".

Edit DNS Load Balancing		? >
Create new Object 🗸		
General Setting		-
✓ Enable		
DNS Settings		
Query Domain Name:	www.zyxel.com.tw	
Time to Live:	0 (0-604800 seconds, 0 is unchanged)	
Query From Settings		
IP Address:	any 🗸	=
Zone:	any 🗸	
Load Balancing Member		
Load Balancing Algorithm:	Weighted Round Robin	

b. Add load DNS Load Balancing member

O Edit Load Balancing Member		? X
Load Balancing Member		
Member:	1	
Monitor Interface:	ge3 Static 59. 124. 163. 150/255. 255. 224	
Weight:	1 (1-10)	
IP Address		
Same as Monitor Interface	59.124.163.150	
Custom	59, 124, 163, 150	
		_
Add Z Edit Remove	OK Cance	2
# IP Address		

Edit Load Balancing Member		? X
Load Balancing Member		
Member:	2	
Monitor Interface:	ge4 Static 59. 124. 163. 135/255. 255. 255. 224	
Weight:	1 (1-10)	
IP Address		
Same as Monitor Interface	59, 124, 163, 135	
Custom	59. 124. 163. 135	
	OK Canc	el
	Monitor Interface Weight	

c. Enable DNS Load Balancing.

	CONFIGURATION	DNS Load Ba	alancing						
	Licensing Licensing Network Interface Routing Zone Donus	Global Setti Enable Configuration	ing DNS Load I on Z Edit 👕	Balancing Remove 🥥 Activate 🎯 Inactivate 🐠 Mov	G Activate @ Inactivate #Move				
	NAT HTTP Redirect ALG PMAC Binding DIS Inbound LB Auth. Policy Frewall	Status	Priority 1 Page 1	Query Domain Name www.zyxel.com.tw of 1 ▶ ▶ Show 50 ∨ items	Query From Address any	Query From Zone any	Load Balancing Member ng <u>e3,nge4</u>	Algorithm Veighted Round Robin Displaying 1 - 1 of 1	

Step 4. Go to Configuration -> Network -> NAT. Configure the Virtual Server to forward the traffic from WAN to DNS Server.

a. Add a NAT rule for WAN1.

🖉 Edit NAT		Welcome admin Lonout	- 🦓 Help - 💆 About - 🤹 Site Map - 🎵	? ×
🔚 Create new Object-				
General Settings				^
Enable Rule				
Rule Name:	NAT_WAN1			
Port Mapping Type				
Classification:	Virtual Server	1:1 NAT	Many 1:1 NAT	
Mapping Rule				=
Incoming Interface:	wan1	*		
Original IP:	User Defined	~		
User-Defined Original IP:	59.124.163.150	(IP Address)		
Mapped IP:	User Defined	~		
User-Defined Mapped IP:	192.168.1.33	(IP Address)		
Port Mapping Type:	Port	~		
Protocol Type:	any	~		
Original Port:	80			
Mapped Port:	80			
				-
			ОК	Cancel

b. Add a NAT rule for WAN2.

🕜 Edit NAT		Welcome admin (Looout	P Help Z About 💲 Site Map (⊇Of	? ×
🔚 Create new Object 🗸				
General Settings				Â
Enable Rule				
Rule Name:	NAT_WAN2			
Port Mapping Type				
Classification:	Virtual Server	1:1 NAT	Many 1:1 NAT	
Mapping Rule				=
Incoming Interface:	wan2	*		
Original IP:	User Defined	~		-
User-Defined Original IP:	59.124.163.135	(IP Address)		
Mapped IP:	User Defined	~		
User-Defined Mapped IP:	192.168.1.33	(IP Address)		
Port Mapping Type:	Port	~		
Protocol Type:	any	~		
Original Port:	80			
Mapped Port:	80			
				-
	Apply	Reset	OK Can	cel

c. Make sure all NAT rules have been added.

	CONFIGURATION	NAT									
	TV Quick Setup	Configur	ration								
	 Network Interface Reuting 	🏹 No If you	ote: want to c	onfigure SNAT, pl	ease go to <u>Policy Ro</u>	ute.					
R.	 Rouning Zone 	🕥 Ad	💿 Add 🖉 Edit. 🁕 Remove 😡 Activate 😡 Inactivate								
	DDNS	#	Status	Name	Mapping Type	Interface	Original IP	Mapped IP	Protocol	Original Port	Mapped Port
	HTTP Redirect	1	0	NAT_WAN1	Virtual Server	■wan1	59.124.163.150	192.168.1.33	any	80	80
	+ ALG	2	0	NAT_WAN2	Virtual Server	■wan2	59.124.163.135	192.168.1.33	any	80	80
	IP/MAC Binding DNS Inbound LB	M <	🛛 Page	1 of 1 D	▶ Show 50	 items 					Displaying 1 - 2 of 2

Scenario 4 – Dialing up L2TP VPN connection to USG by using iOS/Android mobile device

4.1 Application scenario

Smart phones become increasingly popular with consumers. Though it brings us much more convenience, but also brings security concerns. A ZyWALL USG is compatible with iOS/Android mobile devices to establish L2TP VPN connection, provide secure and private mobile data transferring no matter if your mobile devices is behind NAT. In the following diagram, outside employees who need to visit an internal website in Intranet, can just dial up an L2TP VPN to ZyWALL USG and access the needed internal resource.



4.2 Configuration Guide

Network conditions:

USG:

- WAN1 IP: 59.124.163.155
- Local subnet: 192.168.1.0/24
- L2TP pool:192.168.100.0/24
- Intranet website: http://info.zyxel.com

iOS/Android mobile device:

- IP: 118.169.105.67(3G mobile network)
- IP: 192.168.1.33(Behind NAT device)

IPSec VPN conditions:

Phase 1:

- Authentication: 12345678
- Local/Peer IP: WAN1/0.0.0.0
- Negotiation: Main mode
- Encryption algorithm: 3DES/3DES/DES Authentication algorithm:
- Authentication algorithm:

Phase 2:

- Encapsulation Mode: Transport mode
- Active protocol: ESP
- Encryption algorithm: 3DES/3DES/DES

SHA1/MD5/SHA1

- SHA1/MD5/SHA1 Perfect Forward Secrecy: none
- Key group: DH2

Goals to achieve:

Build up an L2TP over IPSec VPN tunnel for mobile users to access Intranet website.

USG configuration

Step 1: Click Configuration > VPN > IPSec VPN > VPN Gateway to visit VPN gateway

	CONFIGURATION	VPN Connection	VPN Gateway	Concentrator	Configurati	on Provisioning	
	₩ Quick Setup Licensing Network	Configuration	The Remove Sector	vate @ Inactivate	🖼 Obiect Re	eference	
Ċ.	 Interface Routing 	# Status N	lame	My Add	ess	Secure Gateway	VPN Connection
	+ Zone	1 @ D	efault_L2TP_VPN_G	W wan1		0.0.0.0, 0.0.0.0	Default_L2TP_VPN_Connect
	DDNS	2 Q 12	tp_gateway	∝wan1		0.0.0.0, 0.0.0.0	
- IVAI - HTTP Redirect - ALG - IP/MAC Binding - DNS Inbound LB - Auth. Policy - Firewali - VPN - IPSSc VPN - SSL VP	II I Page	1 of 1 ▶ ▶	Show 50 💌 iter	ns		Displaying 1 - 2 of 2	

configuration screen

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

Step 3: Fill in the needed \	VPN gateway	/ configuration.
------------------------------	-------------	------------------

Add VPN Gateway	Welcome admin
Hide Advanced Settings	
General Settings	
🗹 Enable	
VPN Gateway Name:	l2tp_gateway
Gateway Settings	
My Address	
Interface	WAN1 Static 59.124.163.155/255.255.254
Domain Name / IP	
Peer Gateway Address Static Address 	Primary 0.0.0.0
	Secondary 0.0.0.0
Fall back to Primary Peer Gate	way when possible
Fall Back Check Interval:	300 (60-86400 seconds)
Oynamic Address	
Authentication	
Pre-Shared Key	12345678
Certificate	default (See <u>My Certificates</u>)
Local ID Type:	Ib
Content:	0.0.0.0
Peer ID Type:	Any 👻
Content:	
Phase 1 Settings	
SA Life Time:	86400 (180 - 3000000 Seconds)
Negotiation Mode:	Main
Proposal	💿 Add 🔜 Edit 🍵 Remove
	# Encryption Authentication
	1 3DES SHA1
	2 3DES MD5
	DES SHAT
Key Group:	DH2 👻
NAT Traversal	
Dead Peer Detection (DPD)	
Extended Authentication	
Enable Extended Authentication	
Server Mode	default 👻
Client Mode	
User Name :	
Password:	

Step 4: Click Configuration > VPN > IPSec VPN > VPN Connection to visit the

configuration screen to set phase 2 rule

9	CONFIGURATION	VPN C	onnection	VPN Gateway	Concentrator	Configuration Provisionin	9	
	¶∦Quick Setup ⊕ Licensing	Globa	Setting					
~	Network	V (Ise Policy Rou	ute to control dynam	ic IPSec rules			
<u>e</u>	Routing	V I	gnore "Don't	Fragment" setting in	IP header 🔢			
R.	+ Zone							
	+ DDNS	Config	juration					
	+ NAT + HTTP Redirect	0	Add 📝 Edit	💼 Remove 💡 Activ	ate 🖗 Inactivate	🗟 Connect 🛞 Disconnect	📴 Object Reference	
	+ ALG	#	Status	Name	VPN Gateway	Encapsula.	. Algorithm	Policy
	IP/MAC Binding	1	88	Default_L2TP_VP	Default_L2TP_	VPN_GW TRANSPO	3DES/SHA1 3DE	«WAN1_IP/
	ONS INDOUND LB Auth. Policy	14	4 Page 1	of1 ▶ ■ S	how 50 👻 iten	ns		Displaying 1 - 1 of 1
	+ Firewall							
	VPN							
	+ IPSec VPN + SSL VPN							
	+ L2TP VPN							

Step 5: Click the "Add" button to add a VPN connection rule.

Step 6: Fill in the needed VPN connection configuration.

Hide Advanced Settings 🔚 Create n	ew Object+		
eneral Settings			
Enable			
Connection Name:	L2TP_VPN		
Nailed-Up			
Enable Replay Detection			
Enable NetBIOS broadcast over J	PSec		
MSS Adjustment			
Custom Size		(200 - 1460 Bytes)	
Auto			
PN Gateway			
Application Scenario			
Site-to-site			
Site-to-site with Dynamic Pee	er		
Remote Access (Server Role)	1		
Remote Access (Client Role)			
VPN Gateway:	l2tp_gateway	WAN1 0.0.0.0 0.0.0.0	
Manual Key			
Manual Key			
My Address:			
Secure Gateway Address:			
SPI:	(256 - 409)	5)	
Encapsulation Mode:		~	
Active Protocol:		~	
For second secon			
Encryption Algorithm:			
Authentication Algorithm:			
Encryption Key:			
Authentication Key:			
olicy			1
Local policy:	WAN1_IP	 INTERFACE IP, 59.124.163.155 	
hase 2 Setting			
SA Life Time:	86400	(180 - 2000000 Seconds)	
A the Parts all	50400	(100 - 5000000 Seconds)	
ACLIVE PROTOCOI:	ESP		
Encapsulation:	Transport	×	
Proposal	💿 Add 🔜 Edit 🍵 F	emove	
	# Encryption	Authentication	
	1 3DES	SHA1	
		110.5	
	2 3DES	MD5	
	2 3DES 3 DES	MD5 SHA1	
Perfect Forward Secrecy (PFS):	2 3DES 3 DES	MD5 SHA1	
Perfect Forward Secrecy (PFS):	2 3DES 3 DES none	MD5 SHA1	
Perfect Forward Secrecy (PFS): elated Settings	2 3DES 3 DES none	MD5 SHA1	
Perfect Forward Secrecy (PFS): elated Settings Zone:	2 3DES 3 DES none IPSec_VPN	MD5 SHA1	
Perfect Forward Secrecy (PFS): elated Settings Zone:	2 3DES 3 DES none IPSec_VPN	MD5 SHA1	
Perfect Forward Secrecy (PFS): elated Settings Zone: onnectivity Check	2 3DES 3 DES none IPSec_VPN	MD5 SHA1	
Perfect Forward Secrecy (PFS): celated Settings Zone: onnectivity Check Enable Connectivity Check []	2 3DES 3 DES none IPSec_VPN	MD5 SHA1	
Perfect Forward Secrecy (PFS): selated Settings Zone: onnectivity Check Enable Connectivity Check 1 Check Method:	2 3DES 3 DES none IPSec_VPN		
Perfect Forward Secrecy (PFS): Related Settings Zone: connectivity Check Enable Connectivity Check 1 Check Method: Check Period:	2 3DES 3 DES none IPSec_VPN 5 (5-30 Seco	MD5 SHA1	
Perfect Forward Secrecy (PFS): elated Settings Zone: connectivity Check Enable Connectivity Check Check Method: Check Period: Check Timeout:	2 3DES 3 DES none IPSec_VPN 5 (5-30 Seco 5 (1-10 Seco	MD5 SHA1	
Perfect Forward Secrecy (PFS): elated Settings Zone: connectivity Check Enable Connectivity Check 1 Check Method: Check Period: Check Timeout: Check Fail Tolerance:	2 3DES 3 DES none IPSec_VPN 5 (5-30 Seco 5 (1-10 Seco (1-10)	MD5 SHA1	
Perfect Forward Secrecy (PFS): elated Settings Zone: onnectivity Check Enable Connectivity Check 1 Check Method: Check Method: Check Timeout: Check Fail Tolerance: Check Fail Tolerance: Check This Address	2 3DES 3 DES none PSec_VPN 5 (5-30 Seco 5 (1-10 Seco 1-10)	MD5 SHA1	
Perfect Forward Secrecy (PFS): kelated Settings Zone: connectivity Check Enable Connectivity Check Check Method: Check Period: Check Fail Tolerance: Check This Address Check the First and Last IP A	2 3DES 3 DES none IPSec_VPN 5 (5-30 Seco 5 (1-10 Seco 1-10) ddress in the Remote P	MD5 SHA1	
Perfect Forward Secrecy (PFS): celated Settings Zone: onnectivity Check Enable Connectivity Check 1 Check Method: Check Period: Check Period: Check Timeout: Check Timeout: Check This Address © Check the First and Last IP A Check The First and Last IP A	2 3DES 3 DES none IPSec_VPN 5 (5-30 Seco 5 (1-10 Seco (1-10) ddress in the Remote P	MD5 SHA1	
Perfect Forward Secrecy (PFS): selated Settings Zone: onnectivity Check Enable Connectivity Check 1 Check Method: Check Period: Check Period: Check Fail Tolerance: Check Fail Tolerance: Check This Address Check the First and Last IP A Log	2 3 DES 3 DES none IPSec_VPN S (5-30 Seco 5 (1-10 Seco (1-10) (1-10) ddress in the Remote P	MD5 SHA1	
Perfect Forward Secrecy (PFS): lelated Settings Zone: connectivity Check Enable Connectivity Check Check Method: Check Method: Check Period: Check Timeout: Check Fail Tolerance: Check This Address Check the First and Last IP A Log bound/Outbound traffic NAT	2 3DES 3 DES none IPSec_VPN 5 (5-30 Seco 5 (1-10 Seco (1-10) ddress in the Remote P	MD5 SHA1	
Perfect Forward Secrecy (PFS): elated Settings Zone: onnectivity Check Enable Connectivity Check [Check Method: Check Period: Check Timeout: Check Timeout: Check Timeout: Check This Address Check the First and Last IP A Check the First and Last IP A Check the First and Last IP A Check IP First and Last IP A	2 3DES 3 DES none PSec_VPN 5 (5-30 Seco 5 (1-10 Seco 5 (1-10) ddress in the Remote P	MD5 SHA1	
Perfect Forward Secrecy (PFS): elated Settings Zone: onnectivity Check Enable Connectivity Check [] Check Method: Check Period: Check Time Address Check This Address Check This Address Check the First and Last IP A Check the First and Last IP A Check The Address Check the First and Last IP A Check The Address Check The	2 3DES 3 DES none IPSec_VPN 5 (5-30 Seco 5 (1-10 Seco 1-10 Seco (1-10) ddress in the Remote P	MD5 SHA1	
Perfect Forward Secrecy (PFS): Related Settings Zone: connectivity Check Enable Connectivity Check Enable Connectivity Check Check Method: Check Period: Check Fail Tolerance: Check This Address Check This Address Check the First and Last IP A Log 1bound/Outbound traffic NAT Outbound Traffic Source NAT Source:	2 3DES 3 DES none IPSec_VPN 5 (5-30 Seco 5 (1-10 Seco 1-10) ddress in the Remote P Please select one	MD5 SHA1	
Perfect Forward Secrecy (PFS): telated Settings Zone: onnectivity Check Enable Connectivity Check [] Check Method: Check Period: Check Period: Check This Address Check This Address Check the First and Last IP A Code Check the First and Last IP A Code Check The First and Last IP A Source: Destination:	2 3DES 3 DES 7 NONE 1PSec_VPN 1PSec_VPN 10 10 10 10 10 10 10 10 10 10 10 10 10	MD5 SHA1	
Perfect Forward Secrecy (PFS): telated Settings Zone: connectivity Check Enable Connectivity Check 1 Check Method: Check Period: Check Period: Check Fail Tolerance: Check Fail Tolerance: Check Timeout: Check Tim	2 3DES 3 DES 1	MD5 SHA1	
Perfect Forward Secrecy (PFS): telated Settings Zone: onnectivity Check Enable Connectivity Check Check Method: Check Period: Check Timeout: Check Fail Tolerance: Check This Address Check This Address Check the First and Last IP A Log bound/Outbound traffic NAT Outbound Traffic Source: Destination: SNAT: Inbound Traffic	2 3DES 3 DES none PSec_VPN 5 (5-30 Seco 5 (1-10 Seco 5 (1-10 Seco 1 (1-10) ddress in the Remote P Please select one Please select one	MD5 SHA1	
Perfect Forward Secrecy (PFS): telated Settings Zone: onnectivity Check Enable Connectivity Check Enable Connectivity Check Check Method: Check Period: Check Fill Tolerance: Check This Address Check Tail Tolerance: Check This Address Check This Address	2 3DES 3 DES none IPSec_VPN 5 (5-30 Seco 5 (1-10 Seco 5 (1-10 Seco 1-10 Seco 4dress in the Remote P Please select one Please select one	MD5 SHA1	
Perfect Forward Secrecy (PFS): telated Settings Zone: connectivity Check Enable Connectivity Check Enable Connectivity Check Check Method: Check Period: Check Time Address Check Time Address Check This Address Che	2 3DES 3 DES 1 1 1 1	MD5 SHA1	
Perfect Forward Secrecy (PFS): telated Settings Zone: connectivity Check Enable Connectivity Check 1 Check Method: Check Period: Check Timeout: Check Fail Tolerance: Check Timeout: Check This Address Check the First and Last IP A Log nbound/Outbound traffic NAT Source: Destination: SNAT: Inbound Traffic Source NAT Source NAT Source: Destination: SNAT: Inbound Traffic Source NAT Source: Destination: Source NAT Source: Destination: Source NAT Source: Destination: Source NAT	2 3DES 3 DES 1	MD5 SHA1 Image: Share of IP Address) Olicy	
Perfect Forward Secrecy (PFS): telated Settings Zone: connectivity Check Enable Connectivity Check 1 Check Method: Check Period: Check Fail Tolerance: Check Timeout: Check Fail Tolerance: Check This Address Check This Address Check This Address Check the First and Last IP A Log nbound/Outbound traffic NAT Outbound Traffic Source: Destination: SNAT: Inbound Traffic Source: Destination: Source: Destination: SNAT:	2 3DES 3 DES 1 none 1 IPSec_VPN 1 IPSec_V	MD5 SHA1 Image: Share of the state o	
Perfect Forward Secrecy (PFS): telated Settings Zone: connectivity Check Enable Connectivity Check [Check Method: Check Period: Check Fall Tolerance: Check Timeout: Check Timeout: Check This Address Check This Address Check the First and Last IP A Log nbound/Outbound traffic NAT Outbound Traffic Source: Destination: SNAT: Inbound Traffic Source: Destination: SNAT: Destination: SNAT: Destination: SNAT:	2 3DES 3 DES 1 none PSec_VPN S (5-30 Seco 5 (1-10 Seco 5 (1-10 Seco 5 (1-10 Seco 1 (1-10) ddress in the Remote P Please select one Please select one Please select one Please select one Please select one Please select one	MD5 SHA1 Image: Share of the second secon	
Perfect Forward Secrecy (PFS): telated Settings Zone: onnectivity Check Check Method: Check Method: Check Period: Check Timeout: Check Fail Tolerance: Check This Address Check	2 3DES 3 DES 3 DES 1 none IPSec_VPN kmp 5 (5-30 Seco 5 (1-10 Seco 5 (1-10 Seco 1 (1-10) ddress in the Remote P Please select one	MD5 SHA1 V Image: Share of IP Address) olicy	

Step 7: Click **Configuration > VPN > L2TP VPN** to visit L2TP VPN configuration screen

Step 8: Create a address object for L2TP users

1	CONFIGURATION	L2TP VPN							
	🎁 Quick Setup	🗊 Show Advanced Settings 🛅 Create new Object 🗸							
		Conoral Cattings							
Ô		Create Address Sec ? X							
R.	 VPN VPN SSL VPN SSL VPN L2TP VPN App Patrol BWM Plant-X 	V IP A Address Type: SUBNET A Network: 192.168.100.0 Kt Netmask: 255.255.0							
		First DNS Server (Optional): Fr@OK Cancel wan2 2nd DNS Server Second DNS Server (Optional): Custom Defined 168.95.1.1 First WINS Server (Optional): Second WINS Server (Optional): Second WINS Server (Optional):							

Step 9: Fill in the needed L2TP VPN connection configuration.

CONFIGURATION	L2TP VPN		
🏋 Quick Setup	🏢 Show Advanced Settings 🔚 Create net	w Object+	
Gock Setup Cock Setup C	General Settings Carbon Rovanced Settings Content of the settings Carbon Settings Content of the settings of the settings Content of the settings C	Default_L2TP_VPN_Conn × L2TP_POOL × default × any × 60 (1-180 seconds) Custom Defined × 192.168.1.1 Custom Defined × 8.8.8.8	

Android mobile client configuration

Step 1: Settings > Wireless & networks > VPN settings > Add VPN



Step 2: Click Add L2TP/IPSec VPN, insert needed L2TP VPN settings and save



Step 3: Connect to the L2TP VPN

	🛜 📊 🕕 14:27
VPN settings	
Add VPN	
VPNs	
ZyWALL_USG Connect to network	

Step 4: Insert L2TP password



Step 5: Device will show connected when dial up is successful.

8-	₹.1	14:28
VPN settings		
Add VPN		
VPNs		
ZyWALL_USG Connected		

Step 6: Visit Intranet web page



iOS mobile client configuration

Step 1: Settings > General > Network > VPN > Add configuration and insert needed L2TP VPN settings



Step 2: Choose the VPN and turn on



Step 3: Insert L2TP password.

ant.中華電信 3G Settings	下午3:52 etwork	VPN	100 % 🛲
Airplane Mode OFF			
WI-FI Off	VPN		ON
VPN Not Connected	Choose a Configur	ation	
Notificat	Interlink	_	0
Cancel	Password	Do	
Password ••••			· · · ·
Cellular			
Brightne			
Picture I			
General			
Mail, Co			
Safari			
iPod			
Wideo Video			
Photos			
• FaceTim			
1 2 3 4 5	6 7	8 9	0 @
QWERT	YU	1 0	P 🛯
ASDF	GHJ	KL	return
	BN	м !	?
.7123	space	.?1	23

Step 4: Visit an Intranet web page.



Scenario 5 - Deploying Content Filtering to Manage Employee Browsing Behavior

During their daily productive work for the company, working crew needs to surf the Internet to search for information to conduct their jobs. Browsing websites that are irrelevant to work is a waste of human resources as well as a waste of company network resources. There're also some unsafe websites which may contain phishing or malicious programs. These unsafe websites should also be avoided. So the network administrator needs to make policies to prevent these undesirable types of browsing.



5.1 Application scenario

During office hours, the employees should dedicate their time to their jobs and be restricted from browsing websites irrelevant to their work. But the manager should be able to access all websites without restriction at all times with the exception of unsafe websites. At other times outside of office hours, the restrictions for employees can be removed. The employees may access all websites except ones that pose a security threat (unsafe).



5.2 Configuration guide

Network conditions:

<u>USG:</u>

- LAN1 subnet: 192.168.1.0/24
- Manager's IP: 192.168.1.33

Goals to achieve:

- 1) The manager can access all websites at any time except security threats (unsafe).
- 2) During office hours, other employees should be restricted from accessing websites that are irrelevant to their work.
- 3) All employees may access any websites outside of office hours except sites that pose a security threat (unsafe).

USG configuration

Step 1: Click Configuration > Object > Address to add an address object for the

CONFIGURATION	Address	Address Group			
₩ Quick Setup Licensing	IPv4 Add	ress Configuration			
Network	🔘 Add	📝 Edit 🍵 Remove 📠	Object Reference		
+ Firewall	# N	ame 🔺	Туре	IPv4 Address	
	1 DI	MZ_SUBNET	INTERFACE SUBNE	f dmz-192.168.3.0/24	
 App Patrol 	2 E)	T_WLAN_SUBNET	INTERFACE SUBNE	F ext-wlan-10.59.0.0/24	
+ BWM	3 IP	6to4-Relay	HOST	192.88.99.1	
H Anti-X Device HA	4 LA	N1_SUBNET	INTERFACE SUBNE	F lan1-192.168.1.0/24	
□ Object	5 L/	N2_SUBNET	INTERFACE SUBNE	F lan2-192.168.2.0/24	
 User/Group 	6 Ma	anager	HOST	192.168.1.50	
+ Address	7 W	LAN-1-1_SUBNET	INTERFACE SUBNE	Г wlan-1-1-10.59.1.0/24	
+ Service	14 4	Page 1 of 1 🕨 🕨	Show 50 🔻 items		Displaying 1 - 7 of 7
 AAA Server Auth. Method 	IPv6 Add	ress Configuration			
Certificate	🔘 Add	📝 Edit 🍵 Remove 📴 (Object Reference		
SSL Application	# N	ame 🔺	Туре	IPv6 Address	
 Endpoint Security 		Page 1 of 1 🕨 🕅	Show 50 v items		No data to display

Step 2: Click **Configuration > Object > Schedule** to add a Recurring schedule for office

CONFIGURATION	Schedule			
📲 Quick Se	tup			
	One Time			
	Add Z Edit 🗮 Romayo 📼	Object Reference		
 Auth. Policy 		Object Reference		
	At Names	Start Day/Time	Stop Day/Time	
→ Firewall	# Name	otarebajriinto	1 1 1	
+ Firewall	# Name	Show 50 vitems		No data to display
 Firewall ⊕ VPN App Patrol 	# Name I I I I	Show 50 vitems		No data to display
 Firewall VPN App Patrol BWM 	# Name I I I Page 1 of 1	Show 50 v items		No data to display
 Firewall VPN App Patrol BWM Anti-X 	# Name I Page 1 of 1 Recurring	Show 50 v items		No data to display
Firewall VPN App Patrol BWM Anti-X Device HA	# Name Id Image Id Image Image Image </th <th>Object Reference</th> <th></th> <th>No data to display</th>	Object Reference		No data to display
Firewall VPN App Patrol BWM Anti-X Device HA Object	# Name I I I I I I I I I I I I I I I I I I I I I I	Object Reference	Ston Time	No data to display
Firewall VPN App Patrol BWM Anti-X Device HA Object User/Group Address	# Name I I I I I I I I I	Object Reference	Stop Time 17:30	No data to display
	# Name I I Page I of 1 I O Add # Name 1 office_hour I Image 1 Page 1 office_hour	Object Reference	Stop Time 17:30	No data to display

Step 3: Click Configuration > Anti-X > Content filter > Filter Profile to add a filtering

pro	ofile.					
	CONFIGURATION YY Quick Setup Ucleansing Network Auth Policy Frewall VPN App Patrol BWM Anti-X Anti-Virus IDP ADP Content Filter - Anti-Sparn Device HA Object System Log & Report	General Profile M Add # F 14 4	Filter Profile anagement	Trusted Web Sites ve ▶ ▶ Show 50 ▼	Forbidden Web Sites	No data to display

Step 4: Choose your licensed content filtering service and start its setup.

Add Hiter Profile			
Commtouch Category Service	BlueCoat Category Service	Custom Service	
General Settings			
License Status:	icensed		
License Type:	Trial		
Name:			
Enable Content Filter Cat	egory Service		
Action for Unsafe Web P	ages: Warn 🗸]	Log
Action for Managed Web	Pages: Block 💌]	Log
Action for Unroted Mich	Dagoost Minas ar	1	· · ·

Step 5: Add a profile which allows users to visit all websites.

Enable Content Filter Category Service.

Set action for Security threat (Unsafe) to "Warn" and check "Log".

Set action for Managed Web Pages to "Pass" and check "Log".

Set action for Unrated Web Pages to "Warn" and check "Log".

Set action When Category Server is Unavailable to "Warn" and check "Log".

Add Filter Profile					e (
Commtouch Category Service	BlueCoat Category Se	rvice Custom S	ervice		
General Settings					
License Status: Lice	nsed				
License Type: Trial					
Name: allov	w_all_category				
Enable Content Filter Catego	ory Service		_		
Action for Unsafe Web Page	warn	*	Log		
Action for Managed Web Pa	ges: Pass	~	🔽 Log		
Action for Unrated Web Pag	yes: Warn	~	🔽 Log		
Action When Category Serve	er Is Unavailable: Warn	*	🔽 Log		
Select Categories					
Select All Categories	Clear All	Categories			
Security Threat (unsafe)					
Phishing	Spyware/1	Malware Sources	📝 Spyware Effe	cts/Privacy Concerns	
Proxy Avoidance					
Managed Categories					

Step 6: Add a profile for employees to surf only allowed websites.

Enable Content Filter Category Service

Set action for Security threat (Unsafe) to "Warn" and check "Log".

Set action for Managed Web Pages to "Block" and check "Log".

Set action for Unrated Web Pages to "Warn" and check "Log".

Set action When Category Server is Unavailable to "Warn" and check "Log".

Add the profile	- Malcomo admini Leonart - 🤉 Uala - Z About - 🏂 Sita Man - 🗔 Object Reference
Add Hiter Profile	
Commtouch Category Service BlueCoat Catego	y service Custom Service
General Settings	
License Status: Licensed	
License Type: Trial	
Name: for_employee	
Enable Content Filter Category Service	
Action for Unsafe Web Pages: V	arn 🔽 Log
Action for Managed Web Pages: B	ock 🔽 🔽 Log
Action for Unrated Web Pages: V	arn 🔽 Log
Action When Category Server Is Unavailable: V	arn 🔽 Log
Select Categories	
	All Otherspice
Select All Categories	r All Categories
Security Threat (unsafe)	
V Prisning V Spyv	are/Malware Sources V Spyware Effects/Privacy Concerns
V Proxy Avoidance	
Managed Categories	
Adult Related	
Adult/Mature Content Alter	native Sexuality/Lifestyles 🛛 📝 Extreme
✓ Intimate Apparel/Swimsuit	y 📝 Pornography
✓ Open/Mixed Content ✓ Sex	iducation
Liability Concerns	Vouestiegshie
Vieles es (Usto /De size	
Violence/Hate/Racism	lons
Security Concerns	
Dotentially Unwanted Software Rem	
File-Transter C Online Storage Peer	to Peer 🛛 Software Downloads
Society/Government	ral/Charitable Organizations
LGBT Milita	v Political/Activist Groups
Religion Socie	tv/Lifestvle
Social Interaction	
✓ Blogs Personal Pages ✓ Gree	ing Cards 🔍 Personals/Dating
Social Networking	_ · •
Multimedia	
V Audio/Video Clips V Medi	
	i Sharing 🛛 🗹 Radio/Audio Streams

Step 7: Switch to **Configuration > Anti-X > Content filter > General** to Enable Content Filter.

	CONFIGURATION	General Filt	er Profile	Trusted Web Sit	es Forbidden	Web Sites			
	📲 Quick Setup	General Setting	gs					*	
	E Licensing Image: Background Stresson Background Stress	Enable Cor	itent Filter						
G 0	+ Auth. Policy	Commt	ouch						
.	Firewall VPN	BlueCoat Second Se							
	+ App Patrol	Enable Cor	ntent Filter I	Report Service 🛛 🧏	eport Server 🔢				
	+ BWM	Content Filter	Category S	ervice Timeout:	10 (1~60 S	econds)			
	 Anti-X Anti-Virus 	Content Filter	Port		🔾 Add 📝 Edit 🏌	Remove			
	+ IDP				# Port 🔺			-	
	ADP Content Filter			1	3128			-	
	 Anti-Spam 			2	80				
	Device HA			3	8080				
		n. Potes							
		Policies							
		Block web access when no policy is applied							
		🔘 Add 📝 Ed	dit 🍵 Remo	ove 🦁 Activate 🖗	Inactivate 📣 Mo	ve			
		# Status	Addres	s S	chedule	User	Filter Profile		
		4 4 Page 1 of 1 ▶ ▶ Show 50 👻 items No data to dis						No data to display	
		Message to dis	play wher	a site is blocked					
		Denied Access	Message:	-	The web access is	restricted. Please of	ontact with administrator.		
		Redirect URL:							
					Apply	Reset			

You can edit the Denied Access Message and Redirect URL if access blocked.

Step 8: Add an access policy for all the staff outside of office hours.

Schedule: none.

Address: LAN1 subnet.

Filter Profile: allow_all_category

O Add Policy		?	×
🔚 Create new Object 🗸			
Enable Policy			
Schedule:	none	~	
Address:	LAN1_SUBNET	~	
Filter Profile :	allow_all_category	~	
User/Group:	any	~	
	Schedule	OK Cancel)

Step 9: Add an access policy for all the employees during office hours.

Schedule: office_hour

Address: select the address object LAN subnet.

Filter Profile: for_employee

Add Policy	Report Serve	? 🗙
🛅 Create new Obj	ect▼	
🔽 Enable Polic	у	
Schedule:	office_hour	~
Address:	LAN1_SUBNET	~
Filter Profile :	for_employee	~
User/Group:	any	*
c		
		OK Cancel

Step 10: Add an access policy for the manager during office hours.

Schedule: none

Address: Manager

Filter Profile: allow_all_category

Add Policy		? ×
🔠 Create new Object 🗸		
Enable Policy		
Schedule:	none	~
Address:	Manager	~
Filter Profile :	allow_all_category	~
User/Group:	any	~
c		
	avate 🖗 Inactivate 🦲	OK Cancel

Check the created policies. The USG will check them one by one, and when the manager tries to access a website, he will trigger the first policy.

olicie	olicies								
B	Block web access when no policy is applied								
O A	dd 📝 Edit	💼 Remove 💡 Activate	🖗 Inactivate 📣 Move						
#	Status	Address	Schedule	User	Filter Profile				
1	@	= Manager	none	any	allow_all_category				
2	@	LAN1_SUBNET	■ office_hour	any	for_employee				
3	@	LAN1_SUBNET	none	any	allow_all_category				
14	🔍 Page 🚺	of 1 🕨 🕅 Show	50 💙 items		Displaying 1 - 3 of 3				

Scenario 6 - Deploying anti-spam to keep spam off your network

With fraudulent, inappropriate and offensive emails being delivered in vast quantities to adults, children and businesses every day, spam protection is an essential component of your network's security strategy. Spam wastes network users' time and network resources, and can be dangerous too. A ZyWALL USG includes an anti-spam feature to keep spam off your network.



6.1 Anti-Spam Check flow introduction

The ZyWALL USG Anti-Spam checks if sender/mail relay IP is in White/Black list when SMTP/POP3 session is established. If it cannot find it in White/Black list, it will ask to Commtouch IP Reputatation server. If the IP Reputation server reports no risk, the USG will start to scan mail's header and content, if the header/content satisfies the conditions defined by the user, Anti-Spam will act according to the user configuration.

Check flow contains the following steps:

- 1. Check if sender or mail relay IP address is in White List.
- 2. Check if sender or mail relay IP address is in Black List.
- 3. Check mail relay IP address on Commtouch IP Reputation server (SMTP only).
- 4. Check if mail's header satisfies other conditions in White list.
- 5. Check if mail's header satisfies other conditions in black list.
- 6. Scan mail content, check Virus Outbreak and check DNSBL

6.2 Configuration guide

Network conditions:

Trusted email address: admin@zyxel.com

Goals to achieve:

Add [Spam] tag on all suspected spam mail except coming from a trusted email address.

USG configuration

Step 1: Click Configuration > Anti-X > Anti Spam > Black/White List

Step 2: Enable White List Checking and add a rule for admin@zyxel.com

	CONFIGURATION	General Mail Scan Black/White List DNSBL
	TY Quick Setup	Black List White List
	 Licensing Registration Signature Update 	General Settings
	Network	Enable White List Checking
R,	 Interface 	White List X-Header: X- : (Optional)
	+ Routing	
	+ DDNS	Rule Summary
	+ NAT	🕲 Add 📝 Edit 📋 Remove 💡 Activate 🖗 Inactivate
	HTTP Redirect	Status # Type
	 IP/MAC Binding 	1 e-mail admin@zyxel.com
	 DNS Inbound LB 	l d Page 1 of 1 ▶ ▶ Show 50 v tems Displaying 1 - 1 of 1
	Auth. Policy Eirowall	
	+ Filewall I VPN	
	 App Patrol 	
	+ BWM	
	Anti-X	
	Anti-virus IDP	
	+ ADP	
	Content Filter	
	Anti-Spam	
	Device HA Device t	
	⊞ Object ⊞ System	
		4 III
		Apply Reset

Step 3: Switch to Configuration > Anti-X > Anti Spam > Mail Scan.

Step 4: Enable Sender Reputation Checking, Mail Content Analysis and Virus Outbreak Detection

	CONFIGURATION	General	Mail Scan	Black/White List	DNSBL							
	7₩ Quick Setup □ Licensing	Sender R	Sender Reputation									
	Registration Signature Update Signature Update											
R	□ Network → Interface	Mail Con	tent Analysis									
	+ Routing + Zone	Enal	ole Mail Content	Analysis	(Ortional)							
	+ DDNS + NAT	Mail Cor Mail Cor	itent Spam Tag itent X-Header:	[Spam] X-	(Optional)	(Optional)						
	HTTP Redirect ALG IP/MAC Binding	Virus Out	tbreak Detecti	on								
	+ DNS Inbound LB	🔽 Enal	ole Virus Outbre	ak Detection			=					
	Auth. Policy Firewall VPN Ann Patrol	Virus Ou Virus Ou	utbreak Tag: utbreak X-Heade	[Virus] r: X-	(Optional)	(Optional)						
	+ BWM	Query Tir	neout Setting	s								
	 Anti-X Anti-Virus IDP 	SMTP:		forward v	vith tag 👻							
	+ ADP	POP3:	+ Vel	forward v	vith tag 👻							
	 Content Filter Anti-Spam 	Timeou	t Value: t Tag:	5 (1	1 (Optional)							
	 Device HA ⊕ Object 	Timeou	t X-Header:	X-	:	(Optional)						
	 Bystem Bystem Bystem 	•			III							
					Apply	set						

Step 5: Switch to Configuration > Anti-X > Anti Spam > General.

Step 6: Add a rule for Anti-Spam and enable it.

O Add rule			? ×
General Settings			•
Enable Policy			
Log:	log	▼ 1	
Email Direction			
From:	any	~	
To:	any	~	
Protocols to Scan			
SMTP 🛛	POP3		
Scan Options			=
🛛 Check White List			
Check Black List			
Check IP Reputation	(SMTP only)		
Check Mail Content			
Check Virus Outbrea	ak		
Check DNSBL			
Actions For Spam Mail	i		
SMTP:	forward with tag	*	
POP3:	forward with tag	*	
			Ŧ
		OK Cance	

1	CONFIGURATION	General	Mail Scan	Black/White List	DNSBL						
	🔐 Quick Setup	III Show Advanced Settings									
	Licensing Registration Signature Update Network Interface Routing Zone Constraints	General Se C Enable Policy Sun C Add	ettings e Anti-Spam nmary 2 Edit. 🗯 Re	move 🥥 Activate 🛙) Inactivate #	-₩ Move	_				
	+ DDNS + NAT	Status	Priority A		rotocol	Scan Ontions					
	HTTP Redirect		1	any any s	mtp, pop3	WL, BL, IP Reputation, Mail Content, Virus Outbreak, DNSBL					
	 ALG IP/MAC Binding DNS Inbound LB Auth. Policy 	Id d I	Page 1 of	1 ▶ ▶ Show	50 🗸 item	is Displaying 1 - 1 of 1					
	+ Firewall	License S	status:	Licensed							
	 VPN App Patrol BWM Anti-X Anti-Virus IDP ADP Content Filter Anti-Spam Device HA Object System Log & Report 	License 3 License 1 Expiration	rype: n Date:	Tral 2012-1-1	8						
						Apply Reset					

Scenario 7 – One click Setup VPN connection to headquarters

In an enterprise, employees often go on business trips around the world. They might need to access resources inside headquarters during these trips, however, this brings security concerns. One of the solutions is to build an IPsec VPN tunnel to achieve the purpose, but it presents a difficulty for non-technical employees and will increase work load for network administrators who need to assist users with setup. A ZyWALL USG provides an EASY VPN solution with a downloadable VPN configuration file for simple import of configuration and building of the VPN connection.



- 1. Login USG via IPSec VPN client software for authentication.
- 2. Retrieve IPSec VPN configuration profile from USG.
- 3. Double click a profile to build up the IPSec VPN tunnel and access internal resources.

7.2 Configuration guide

Network conditions:

USG	:
	_

-	WAN	1	IP:	59.124.163.147
---	-----	---	-----	----------------

- Local subnet: 192.168.1.0/24

IPSec VPN conditions:

Phase 1:

- Authentication: 12345678
- Local/Peer IP: WAN1/0.0.0.0
- Negotiation: Main mode
- Encryption algorithm: DES
- Authentication algorithm: MD5
- Key group: DH1

Outside user:

- IP: 114.16.87.56

Phase 2:

- Encapsulation Mode: Tunnel mode
- Active protocol: ESP
- Encryption algorithm: DES
- Authentication algorithm: SHA1
- Perfect Forward Secrecy: none

Goals to achieve:

Provide an easy way for outside users to build up an IPSec VPN tunnel by using the ZyWALL IPSec VPN Client software for accessing internal resources.

USG configuration



Step 1: Click Configuration > Quick setup >VPN Setup.

Step 2: Select "VPN settings for Configuration Provisioning".

VPN Setup W	ard Role Ethemet PPP Celular Tunnel WLAN VLAN Bridge Auxiliary Truni	×
	VPN Setup Wizard	~
	Wizard Type > VPN Settings > Wizard Completed	
	 Webcome ♥ VPN Settings Wizard Type Wizard Completed Wizard Configuration Provisioning The later steps will guide you to setup the VPN. Wizard Type VPN Settings Wizard Completed 	
	Next >	

Step 3: Select "Express" (or select "Advanced" to define detailed settings manually).

To VPN Setup Wiza	rd rd	×
1	VPN Setup Wizard	~
	Wizard Type > VPN Settings > Wizard Completed	
	Please select the type of VPN policy you wish to setup.	
	Type of VPN policy Express Advanced	
	< Back Next >	

Step 4: Change Rule Name if needed.

To VPN Setup Wiz	ard		Auxiany
11/2	VPN Setup Wizard		**
	Wizard Type > VPN Settings	> Wizard Completed 3	
	Express Settings		
	Scenario		
	Rule Name:	WIZ_VPN_PROVISIONING	
	Application Scenario:	Remote Access (Server Role)	
			< Back Next >

VPN Setup Wizar	rt Role Ethernet PPP Celular Tunnel WLAN VLAN Bridge J	×
128	VPN Setup Wizard	*
	Wizard Type > VPN Settings > Wizard Completed 1 2 3	
	Express Settings	
	Configuration	
	Secure Gateway: Any	
	Pre-Shared Key: 12345678	
	LOCAI POICY (IP/Mask) 192.168.1.0 / 255.255.255.0	
	Remote Policy (IP/Mask): Any	
	< <u>B</u>	ack Next >

Step 5: Fill in Pre-shared key and local policy.

Step 6: Check if IPSec VPN configuration is correct and save the settings.

Ti VPN Setup Wiza	d Role Ethernet PPP				×
	Wizard Type > VPN Settings	> Wizard Completed		*	~
- 1 Strange	1 2	3			
	Express Settings				
	Summary				
	Rule Name:	WIZ_VPN_PROVISIONING			
	Secure Gateway:	Any			
51	Pre-Shared Key:	12345678			
	Local Policy (IP/Mask):	192.168.1.0 / 255.255.255.0			
	Remote Policy (IP/Mask):	Any			
	Configuration for Secure Ga	teway		=	
	## Edit this shell script acco ## the comments before u ## Check the peer-ip interf ## Check the local-ip interf ## Edit the WIZ_VPN_PRO ## Then remove the follow PLEASE REMOVE THIS LINE configure terminal isakmp policy WIZ_VPN_PRC ## If this device's wan1 IP ## consider using DDNS and ## the peer-ip listed here t peer-ip 59.124.163.155 ## Use the correct interfac	rding to sing it in the remote gateway. ace. vISIONING_LOCAL address-object. ing line. VISIONING s dynamic, I changing o a domain name. e name in the		Ţ	
			< Back	Save	

Step 7: Click **Configuration > VPN > IPSec VPN > Configuration Provisioning** and enable Configuration Provisioning

	0						
	CONFIGURATION	VPN Connection	VPN Gateway	Concentrator	Configuration Prov	isioning	
	₩ Quick Setup Licensing Network	General Settings	i	7			
٥	Auth. Policy Firewall	Authentication	guration Provisionin	9			
	 VPN IPSec VPN SSL VPN 	Client Authentic	ation Method:	default	•		
	L2TP VPN App Patrol	Configuration					
	+ BWM	🖸 Add 🛃 Edit	👕 Remove 💡 Ad	tivate 🖗 Inactivat	e 🚽 Move		
	Device HA	Sta Priority	VPN Conn	ection	1	Allowed User	
	⊕ Object ⊕ System	🕅 🖣 Page	1 of 1 ▶ ▶	Show 50 💌 ite	ems		No data to display
	Log & Report						

Step 8: Create a provisioning rule for any user

Config	uration
COIIIIQ	uracion

O Add	💿 Add 🔜 Edit 🍟 Remove 💡 Activate 🥡 Inactivate 📣 Move					
Sta	Priority 🔺	VPN Connection	Allowed User			
@	1	WIZ_VPN_PROVISIONING	any			
14 4	Page 1 of	1 🕨 🕅 Show 50 💌 items	Disp	olaying 1 - 1 of 1		

ZyWALL IPSec VPN Client software configuration

Step 1: Execute ZyWALL IPSec VPN Client

ZyWALL IPSec VPN Client				
Configuration Tools ?				
ZyXEL				
Save Apply	Global Parameters			
VPN Configuration	Global Parameters			
Global Parameters	Lifetime (sec.)			
		Default	Minimal	Maximal
	Authentication (IKE)	86400	180	3000000
	Encryption (IPSec)	86400	180	3000000
	🛛 Dead Peer Detectio	on (DPD) —		
	Check interval	30 se	с.	
	Max. number of retries	5		
	Delay between retries	15 se	с.	
	Miscellaneous			
	Retransmissions	2	IKE Po	rt
	X-Auth timeout	20	NAT Po	rt
		Block non	-ciphered con	nection
VPN Client ready				

Step 2: Click Configuration > Get from Server

ZyWALL IPSec VPN Client		10.00	6	
Configuration Tools ?				
Import				
Export				
Get from Server				
Move to USB Drive	Global Parameters	5		
Wizard	Global Parameters			
Quit	Lifetime (sec.)			
		Default	Minimal	Maximal
	Authentication (IKE)	86400	180	3000000
	Encryption (IPSec)	86400	180	3000000
	🗸 Dead Peer Detectio	on (DPD) —		
	Chadvistanud		_	
	Check Interval	30 se	с.	
	Max. number of retries	5		
	Delay between retries	15 se	с.	
	Miscellaneous			
	Retransmissions	2	IKE Por	rt
	X-Auth timeout	20	NAT Por	rt 🗌
		Block non	-ciphered con	nection
VPN Client ready				

Step 3: Fill in authentication information and click "Next"

VPN Configuration Server Wizard	ł	×				
Step 1: Authentication What are the parameters of the V	PN Server Connection?	ZyXEL				
You are going to download your VPN Configuration from the VPN Configuration Server. Enter below the authentication information required for the connection to the server.						
Gateway Address:	59.124.163.147	Port: 443				
Authentication:	Login + Password	•				
Login:	provision_user					
Password:	1234					
	Next >	Cancel				

Step 4: The VPN profile will be downloaded from USG if authentication is successful.



Step 5: Double left click on the phase 2 profile to dial up IPSec VPN tunnel.

ZyXEL – ZyWALL USG Support Notes

Z ZyWALL IPSec VPN Client	
Configuration Tools ?	
ZyXEL	
Save Apply WIZ_VPN_PROVISIONING: IPSec	
VPN Configuration IPSec Advanced Scripts	
Addresses	
VPN Client address 0 . 0 . 0 . 0	
Address type Subnet address 🔻	
Remote LAN address 192 . 168 . 1 . 0	
Subnet mask 255 , 255 , 0	
FSP	
Made Theat	
PF5	
PFS Group	
VPN Client ready	
	_VPN_PROVISION
	Tunnel opened.
	000000000/

Step 6: Access internal resources.

