

ZYXEL

Your Networking Ally

ZLD4.35

Outline

01

**Gateway
Product
Roadmap**

02

**ATP Security
Service
Enhancements**

03

**Networking
Enhancements**

04

**IPSec VPN
Enhancements**

05

**AP Controller
Enhancements**

06

**Hotspot
Enhancements**

Outline

07

**System
Management
Enhancements**

08

**Usability
Enhancements**

09

**SecuReporter
Enhancements**

Gateway Product Roadmap



2019 ZyWALL Series New Product Roadmap

Q4,2019

Q1,2020

Medium
Biz



VPN1000

V.10.03

Jan,20

SMB Biz



ATP700

ZLD4.35

Feb,20

Small Biz



ATP100

ZLD4.35

Oct,19



ATP100W (11ac dua band)

ZLD4.50

Feb,20

2019 FW Release Plan

■ Available
■ Developing

Jan, 19

June, 19

Oct, 19

ZyWALL USG

USG ZLD4.33

-- Bug fixed

USG ZLD4.35

- APC3.40
- Email to SMS
- Two factor authentication for administrator
- Web console
- Hotspot for USG60(W)
- Easy mode for ZyWALL110 & USG110

ZyWALL ATP

ATP ZLD4.33

- Anti-Malware Enhancement (Cloud Query)
- Bug fixed

ATP ZLD4.33 patch1

- Service Setting on Initial Setup Wizard

ATP ZLD4.35

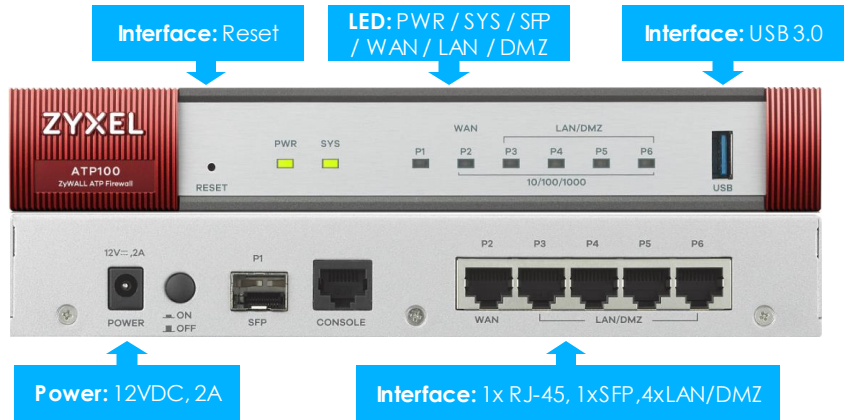
- IP Reputation
- APC3.40
- Email to SMS
- Two factor authentication for administrator
- Sandbox Enhancements
- Security Exception
- Web console

ZyWall ATP100 Next-Gen Firewall for SMBs

- Hardware Spec
 - 1.2GHz Dual Core
 - 8GB storage size
 - 2GB DDR3



ATP100

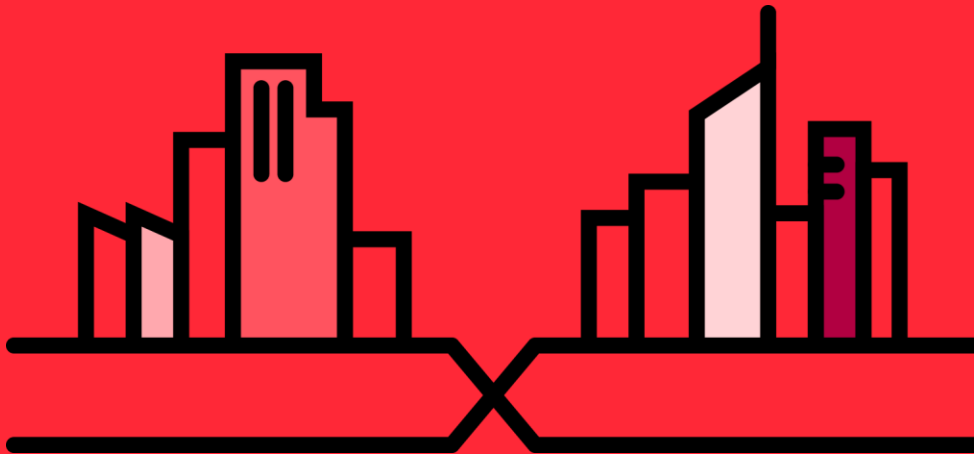


System Capacity and Performance

	ATP100	ATP200	ATP500	ATP800
Firewall throughput	1 G bps	2 Gbps	2.6 Gbps	8 Gbps
IPSec VPN throughput	300 Mbps	500 Mbps	900 Mbps	1.5 Gbps
IDP throughput	600 Mbps	1.2 Gbps	1.7 Gbps	2.7 Gbps
AV throughput	250 Mbps	450 Mbps	700 Mbps	1.2 Gbps
UTM throughput (AV+IDP)	250 Mbps	450 Mbps	700 Mbps	1.2Gbps
Max. TCP concurrent Sessions	300,000	600,000	1,000,000	2,000,000
Max. concurrent IPSec VPN tunnel	40	40	100	200
Max. concurrent SSL VPN user (default/max.)	10	10	50	100
Managed AP Number (default/max.)	2/10	2/18	2/34	2/130

ATP Security Service Enhancements

02



Agenda

01

**ATP Security
Service
License**

02

**Anti-Malware
Enhancements**

03

**Sandbox
Enhancements**

04

**Reputation
Filter**

05

**Security
Exception
Enhancements**

ZyWALL ATP Service License (1/3)

- There is only 1 year security license package for ATP models

License module	Feature	No License	Gold Security Pack (1 year)
Web Security	Content Filter		✓
	Botnet Filter		✓
Application Security	App Patrol		✓
	Email Security		✓
Malware Blocker	Anti-Malware		✓
Reputation Filter	IP Reputation		✓
Intrusion Prevention	IDP		✓
Geo Enforcer	GeoIP		✓
Sandboxing	Sandboxing		✓
Managed AP Service*	Wireless Controller	2 APs	Max. APs
SecuReporter	SecuReporter		✓

Bundled with new device

* : License could be purchased separately

ZyWALL ATP Service License (2/3)

- Silver security pack is no longer available for ATP gateway
- No single security service license is available for purchase.
- When the license of 1 year Gold Security Bundle is expired.
 - Purchase Gold Security Pack for renew
 - 1 or 2 years
- Service License Transfer Capability
 - Gold Security Bundle: **The license can't be transferred.**
 - Gold Security Pack (Renew): The license can be transferred.

ZyWALL ATP Service License (3/3)

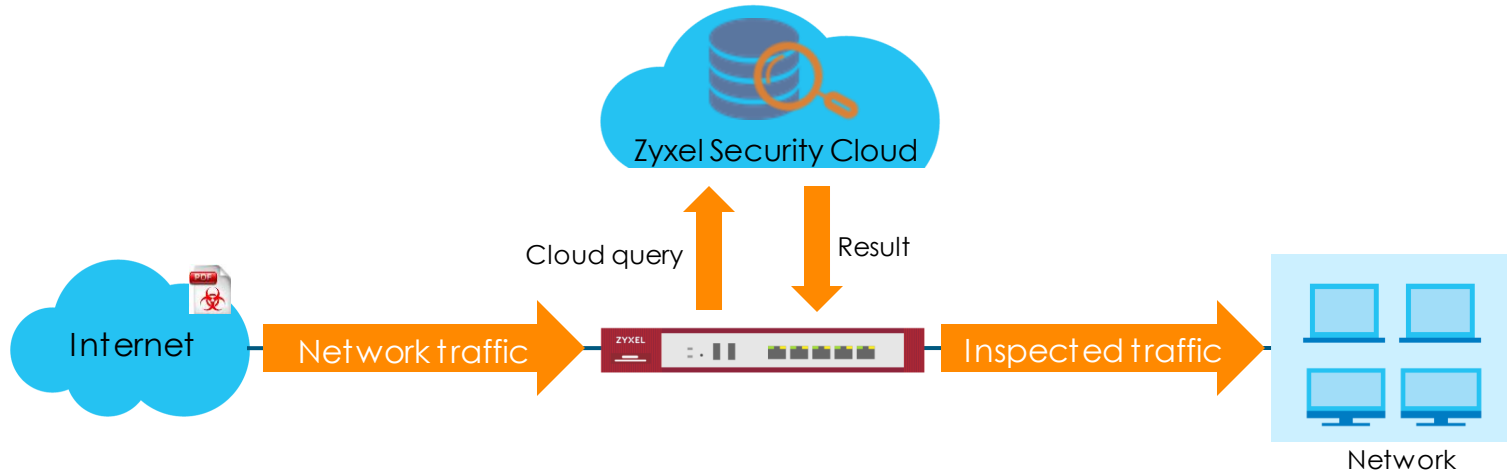
	ATP100	ATP200	ATP500	ATP800
Gold Security Pack	✓	✓	✓	✓
Device HA Pro*			✓	✓
SSL Inspection *	✓	✓	✓	✓

* : Support by default , no license required

Anti-Malware Enhancements

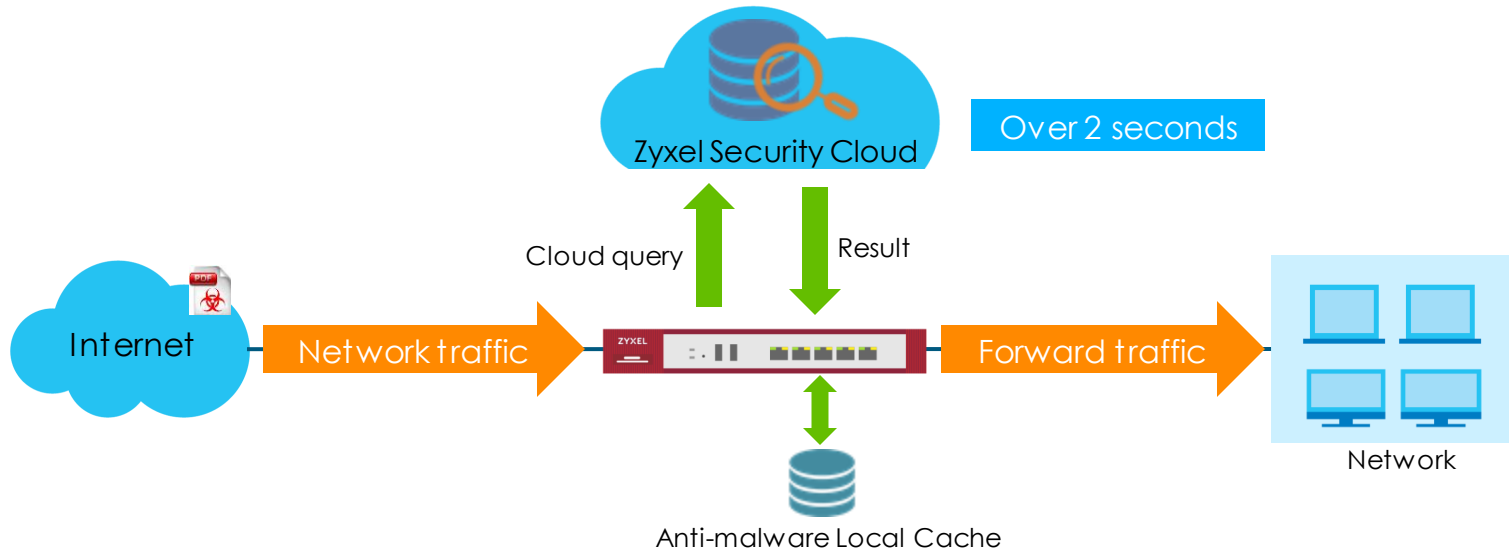
Cloud Query Enhancement (1/2)

- Gateway inspects the file by sending the MD5 hash value to the cloud. The cloud checks its database then replies gateway within 2 seconds
 - Expand the detection coverage by cooperating with a security partner
 - Shorten the time gap between daily signatures update



Cloud Query Enhancement (2/2)

- The gateway forwards the traffic if the Cloud does not respond within 2 second.
 - Late response but not over 60 seconds will be stored in local cache

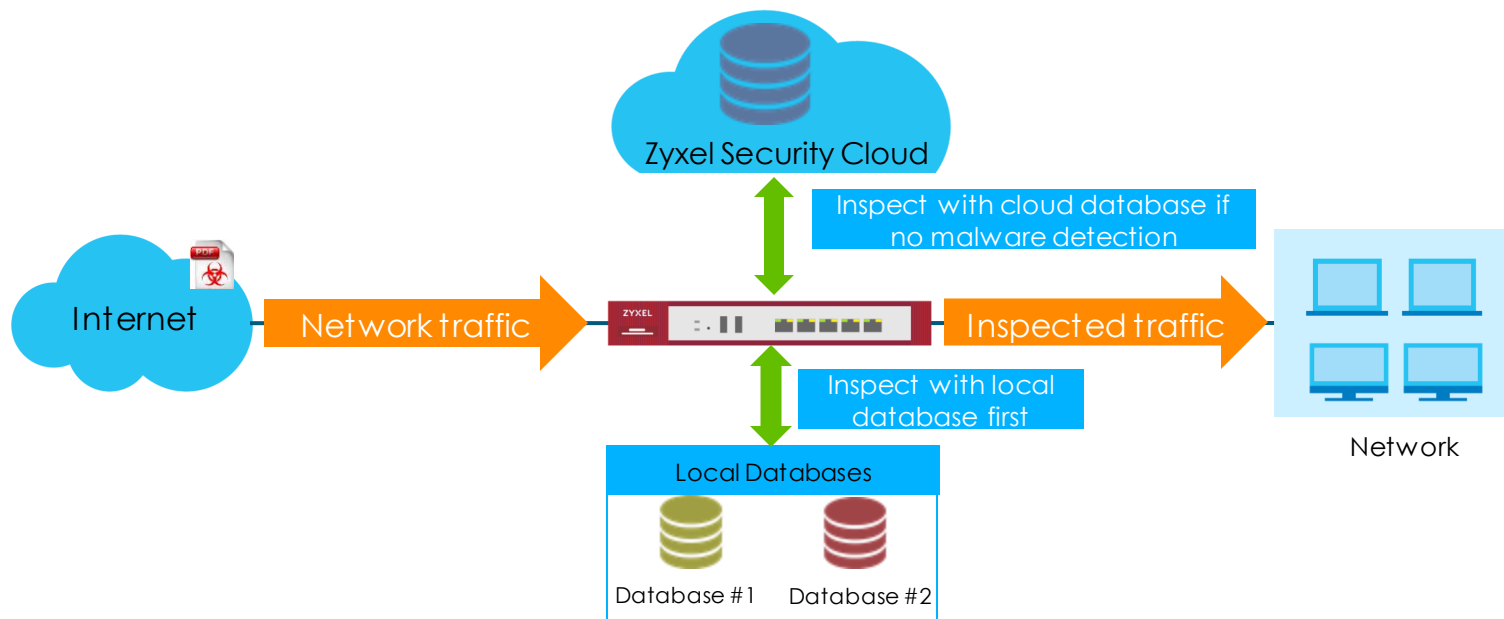


Supported Protocols, File Type and Size

- Protocol support
 - HTTP, HTTPS, FTP, FTPS, POP3, POP3S, SMTP, SMTPS
- File type support
 - Archives: 7Z, RAR, ZIP, BZIP2, GZIP
 - Adobe: PDF, SWF
 - Executables: EXE
 - Microsoft Office: Word, Excel, PowerPoint, Outlook and more
 - Video/Audio/Image: AVI, BMP,GIF, JPG, MOV, MP3, MPG, PNG, RM, TIFF, WAV
- File size
 - No file size limits

Cloud Query Integration

- Integrating cloud query solution into Anti-Malware service for deeper inspection for know malware
 - Gateway only queries cloud if no malware detection by local databases



Anti-Malware Configuration

- Configuration > Security Service > Anti-Malware

Anti-Malware

IP Exception List Black/White List Signature

CONFIGURATION

- + Licensing
- + Wireless
- Network
 - Interface
 - Routing
 - DDNS
 - NAT
 - Redirect Service
 - ALG
 - UPnP
 - IP/MAC Binding
 - Layer 2 Isolation
 - DNS Inbound LB
 - IPnP
- + VPN
- BWM
- Web Authentication
- + Security Policy
- Security Service
 - App Patrol
 - Content Filter
 - **Anti-Malware**
 - Reputation Filter
 - IDP
 - Sandboxing
 - Email Security
 - SSL Inspection

Anti-Malware

General Settings

Enable **Enable Anti-Malware**

Scan and detect EICAR test virus

Cloud Query

Enable Cloud Query **Enable cloud query**

Available File Types

- 7z Archive (7z)
- AVI Video (avi)
- BMP Image (bmp)
- BZ2 Archive (bz2)
- GIF Image (gif)
- GZ Archive (gz)
- JPG Image (jpg)
- MOV Video (mov)
- MP3 Audio (mp3)
- MPG Video (mpg)
- PNG Image (png)
- RAR Archive (rar)
- RM Video (rm)

Applied File Types

- Executables (exe)
- Macromedia Flash Data (swf)
- MS Office Document (doc...)
- PDF Document (pdf)
- RTF Document (rtf)
- ZIP Archive (zip)

Select file types are inspected by cloud

Actions When Matched

Destroy infected file

Log: log

File decompression

Enable file decompression (ZIP and RAR)

Destroy compressed files that could not be decompressed

Anti-Malware Log

- Monitor > Log > View Log

The screenshot displays the 'View Log' interface for Anti-Malware. It features a navigation bar with 'View Log' and 'View AP Log' tabs. Below the navigation bar is a 'Show Filter' button. The main content area is titled 'Logs' and includes a 'Category:' dropdown menu set to 'Anti-Malware'. There are three action buttons: 'Email Log Now', 'Refresh', and 'Clear'. A table of logs is shown with the following columns: '#', 'Time', 'Priority', 'Category', 'Message', 'Source', 'Destination', and 'Note'. Two log entries are visible, with entry 182 highlighted in green. A tooltip is displayed over entry 182, showing the full message: 'Virus infected Rule_id=1 SSI=N Type=Cloud Query Virus=Malicious.Virus File=eicar_com.zip Protocol=HTTP'. At the bottom of the interface, there is a pagination control showing 'Page 1 of 1' and 'Show 50 Items', along with a status indicator 'displaying 1 - 2 of 2'.

#	Time	Priority	Category	Message	Source	Destination	Note
173	2019-05-...	crit	Anti-Mal...	Virus infected Rule_id=1 SSI=N Type=Cloud Quer...	213.211.198...	192.168.2.33:1...	FILE DEST...
182	2019-05-...	crit	Anti-Mal...	Virus infected Rule_id=1 SSI=N Type=Cloud Quer...	213.211.198...	192.168.2.33:1...	FILE DEST...

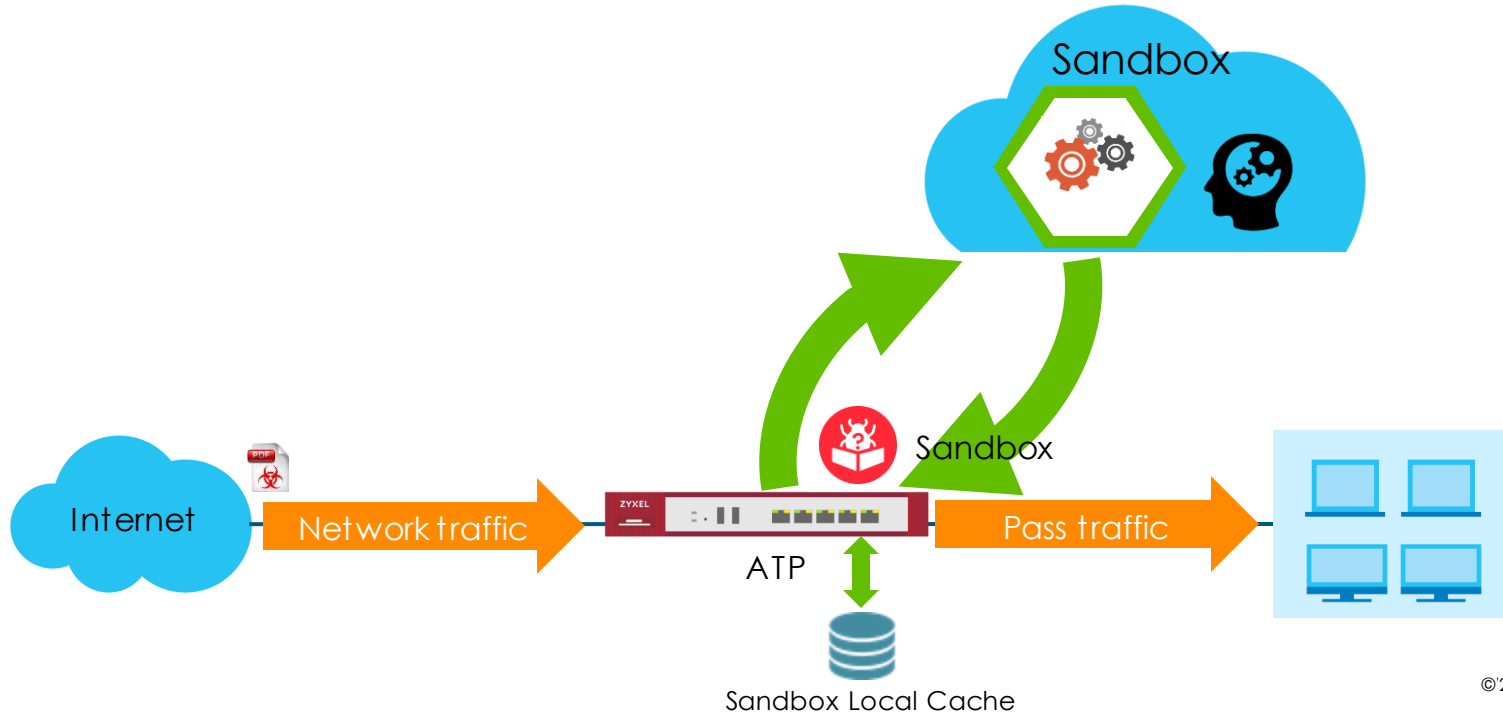
Notice

- Cloud query doesn't decompress archived files
 - Gateway simply generates a MD5 for archived file, not of the files inside

Sandbox Enhancements

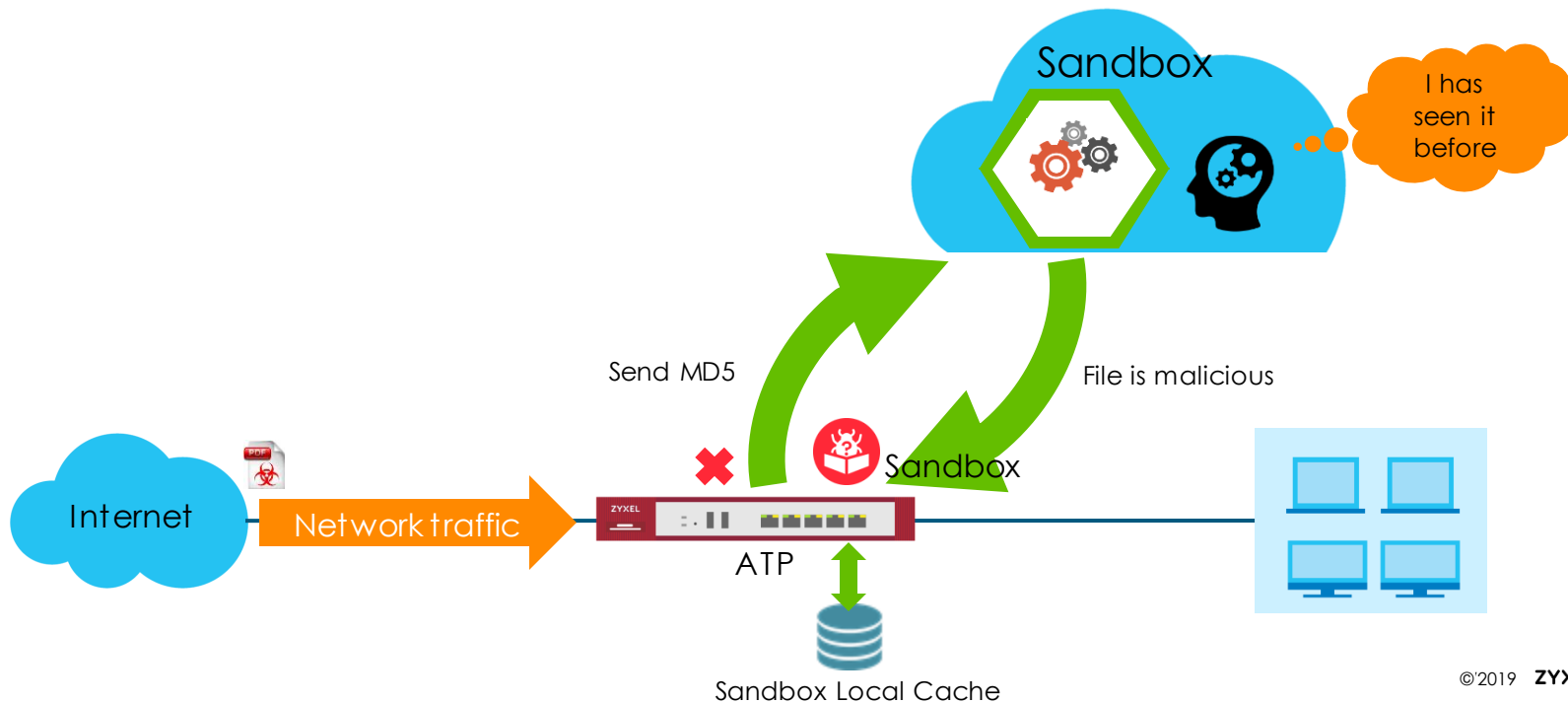
Traditional Sandbox

- ATP gateway with Sandbox service does not destroy the file that has not been seen by gateway



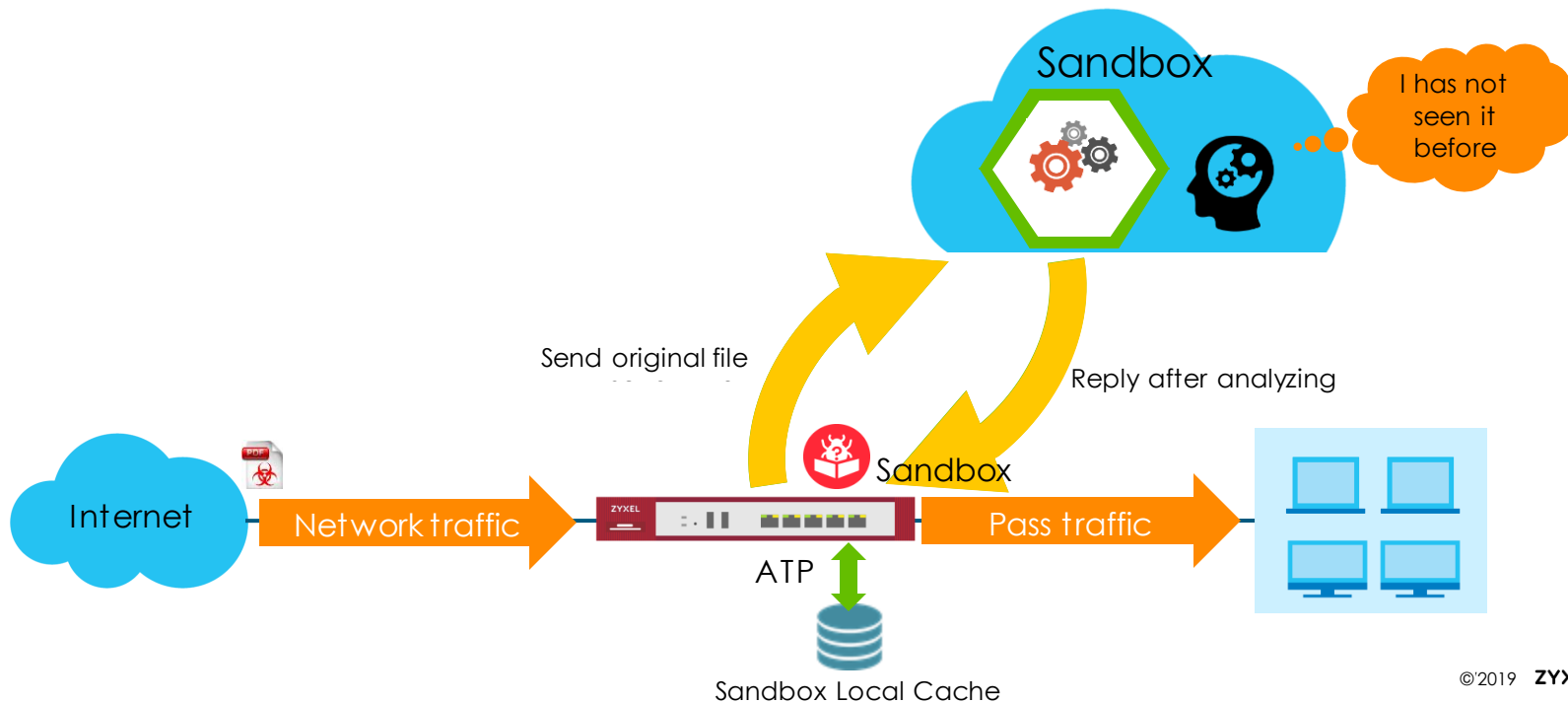
Advanced Inspection for Sandbox (1/2)

- ATP gateway inspects the file by sending the MD5 hash value to the cloud before uploading the original file
 - The malicious file could be destroyed in the first time gateway has seen



Advanced Inspection for Sandbox (2/2)

- Gateway only sends original file to cloud sandbox if the file has not been seen by sandbox before
 - Gateway forwards the file before sending to sandbox



Sandbox Configuration

- Configuration > Security Service > Anti-Malware

Sandboxing

General

Enable Sandboxing **Enable Sandboxing**

Action For Malicious File: destroy

Log For Malicious File: log

Action For Suspicious File: destroy

Log For Suspicious File: log

Advanced Inspection

Inspect Selected Downloaded Files **Enable advanced inspection**

The file types you select will be regarded as a possible threat. This feature inspects the files which are being downloaded from the Internet and have never been inspected before. Safe files will be passed through after inspection.

Note:
Downloads may be interrupted and need to be restarted.

File Submission Options

Archives (.zip)
 Executables
 MS Office Documents
 Macromedia Flash Data
 PDF
 RTF **Select file types are send to cloud sandbox**

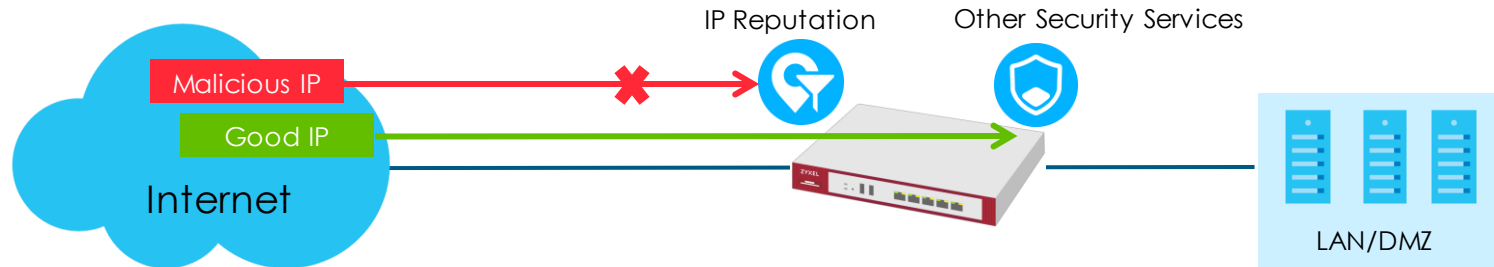
Supported Protocols, File Type and Size

- Protocol support
 - HTTP, FTP, POP3, SMTP, HTTPS, FTPS, POP3S, SMTPS
- File type
 - Archives(.zip)
 - Executable (.exe)
 - MS Office Documents (.xls, .xlsx, .xls, .pptx, .ppt, .pps, .doc,.docx)
 - Macromedia Flash Data (.swf)
 - PDF
 - RTF
- File size
 - $32B \leq \text{File} \leq 10 \text{ MB}$

IP Reputation

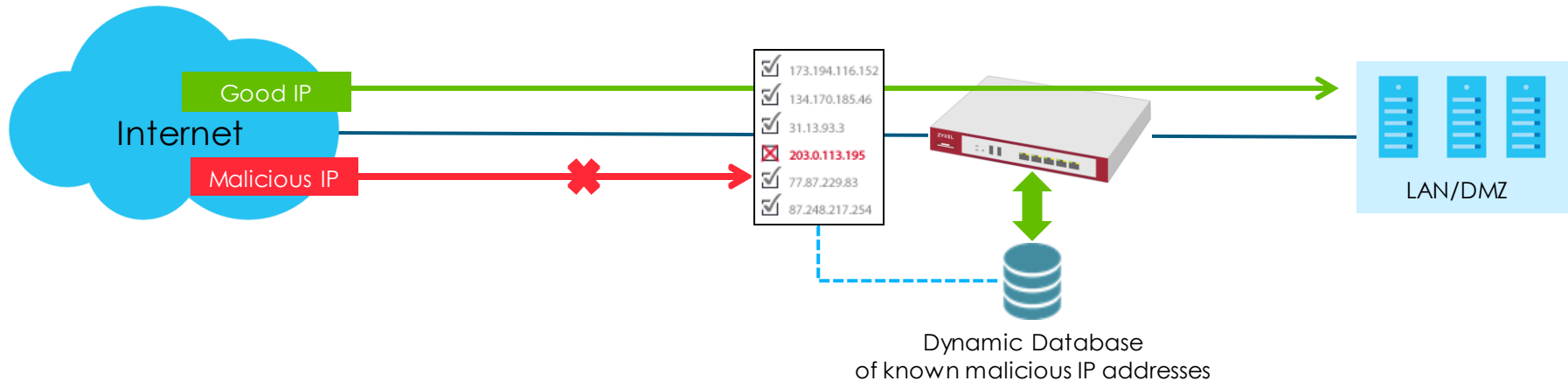
Why Do Need IP Reputation ?

- Blocking traffic to/from known malicious IP addresses is the effective way to improve the network secure and gateway performance
 - Quick filter both unencrypted and encrypted traffic
 - Reduce the packets need to scan by other security service such as IDP, Anti-Malware



IP Reputation

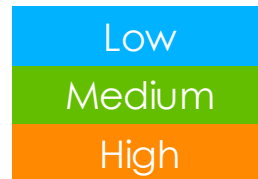
- IP reputation service provides a **database of known malicious public IP addresses** enables gateway can take the action when receives traffic from/to an IP address on the list
 - Database is updated every day



Cyber Threat Types

- Malicious public IP address in the database are classified into 10 threat types, 3 threat levels

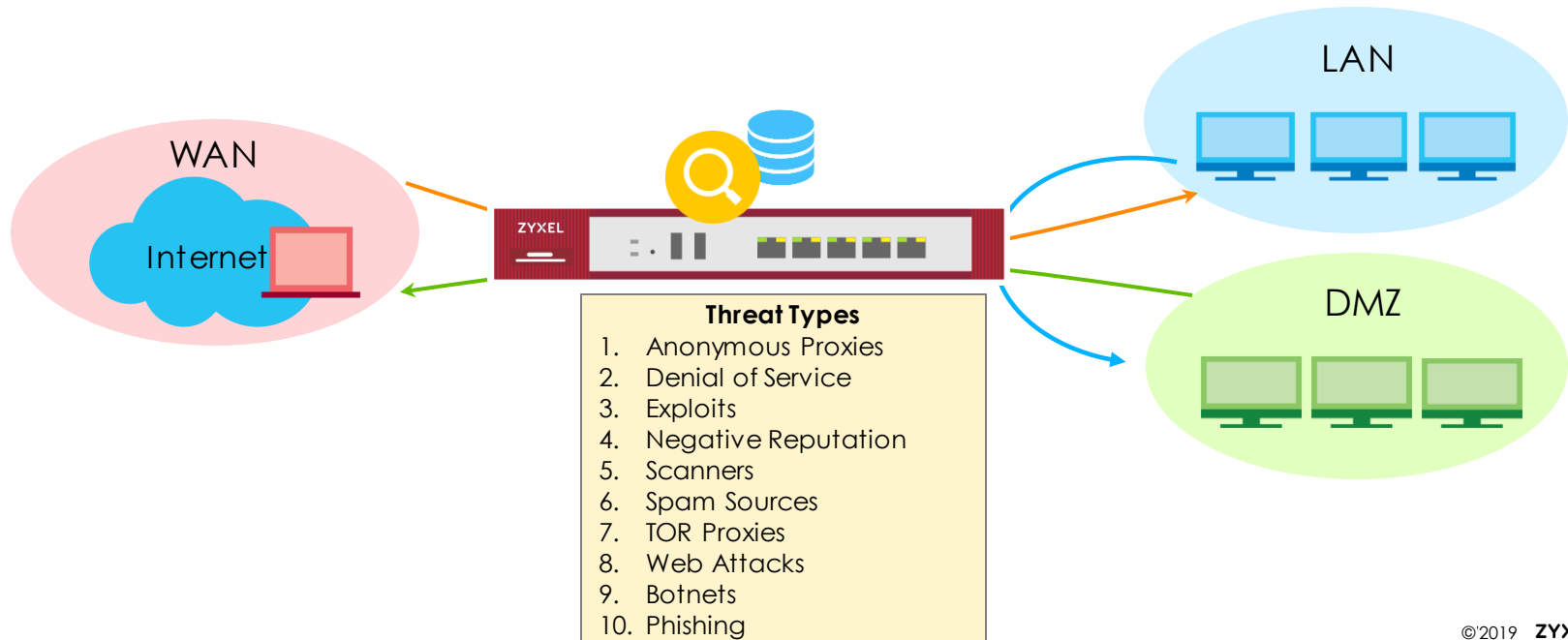
1. Anonymous Proxies
2. Denial of Service
3. Exploits
4. Negative Reputation
5. Scanners
6. Spam Sources
7. TOR Proxies
8. Web Attacks
9. Botnets
10. Phishing



Threat levels

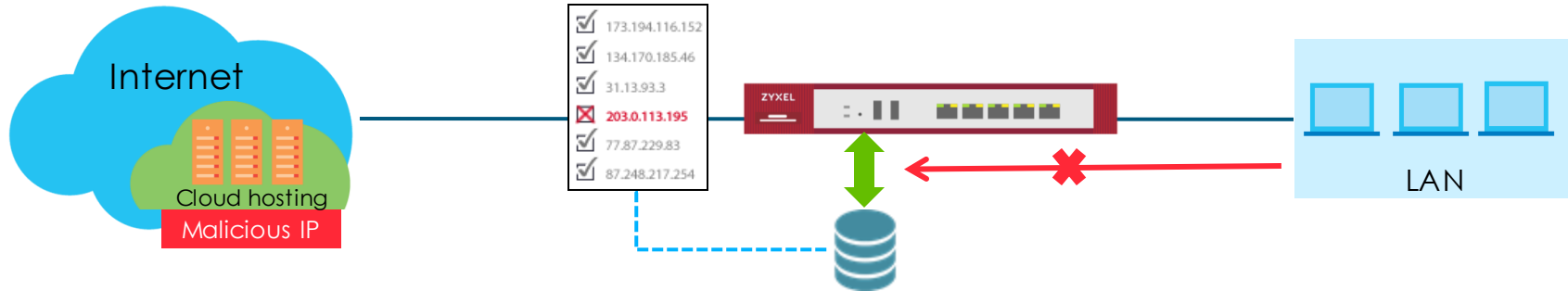
IP Reputation- Traffic Inspection

- Gateway checks the source/destination IP address of all traffic that pass through it. All threat types from the Internet or local network could be blocked



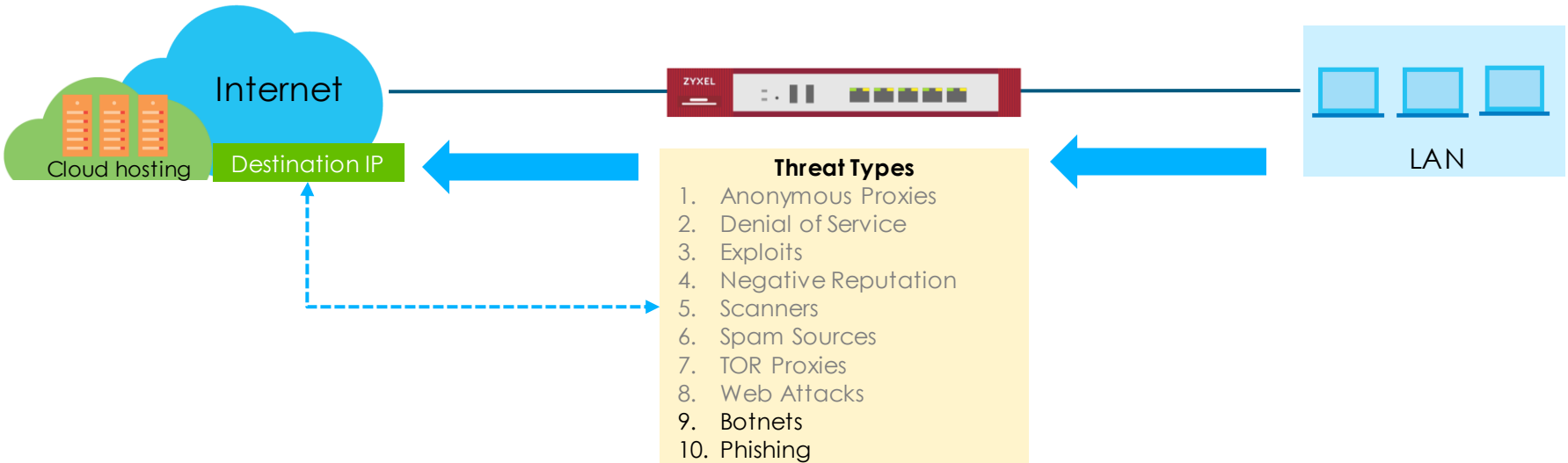
IP Reputation: Cloud Service Challenge

- Nowadays, cloud services such as cloud hosting share public IP address to many tenants, its' public IP address sometimes is listed as malicious
 - Take block action for outgoing traffic causes user can't access the cloud service



Solution

- For outgoing traffic, when the gateway scans the destination IP address, gateway only inspect the Botnets and Phishing – the critical threats



IP Reputation Setting

- Configuration > Security Service > Reputation Filter > IP Reputation

IP Reputation **Boinet Filter**

General White List Black List

IP Blocking

Enable IP Reputation

Action: block

Threat Level Threshold: Low and above

Log: log

Select the action corresponding the threat level

Types of Cyber Threats Coming From The Internet

Anonymous Proxies Denial of Service Exploits

Negative Reputation Scanners Spam Sources

TOR Proxies Web Attacks

Types of Cyber Threats Coming From The Internet And Local Networks

Botnets Phishing

Test IP Threat Category

IP to test: 195.20.42.1 Query

Signature Information

Current Version: 1.0.0.20190122.0

Signature Number: 1460521

Released Date: 2019-01-30 10:51:46

Message

Threat Category: BotNets/Scanners/Phishing/Anonymous Proxies

Threat Level: High

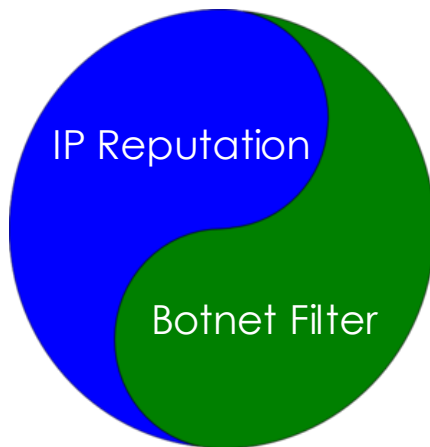
OK

Notice

- IP Reputation only support IPv4 address

Reputation Filter Service

- Reputation Filter is a combination of IP Reputation and Botnet Filter services
 - IP Reputation : Filters traffic base on IP address
 - Botnet Filter : Filter traffic based on URL category



Reputation Filter Service- Web GUI Setting

- Configuration > Security Service > Reputation Filter

The screenshot displays the web management interface for the Reputation Filter service. The left sidebar shows a navigation tree with 'Reputation Filter' selected. The main content area is titled 'Botnet Filter' and includes tabs for 'General', 'White List', and 'Black List'. The 'General' tab is active, showing configuration options for URL Blocking, blocked site messages, managed categories, and signature information.

IP Reputation Botnet Filter

General White List Black List

URL Blocking Botnet Filter

Enable

Action:

Log:

Message to display when a site is blocked

Message to display when a site is blocked

Denied Access Message:

Redirect URL:

Managed Categories

Anonymizers Botnet C&C Compromised

Malware Phishing & Fraud Spam Sites

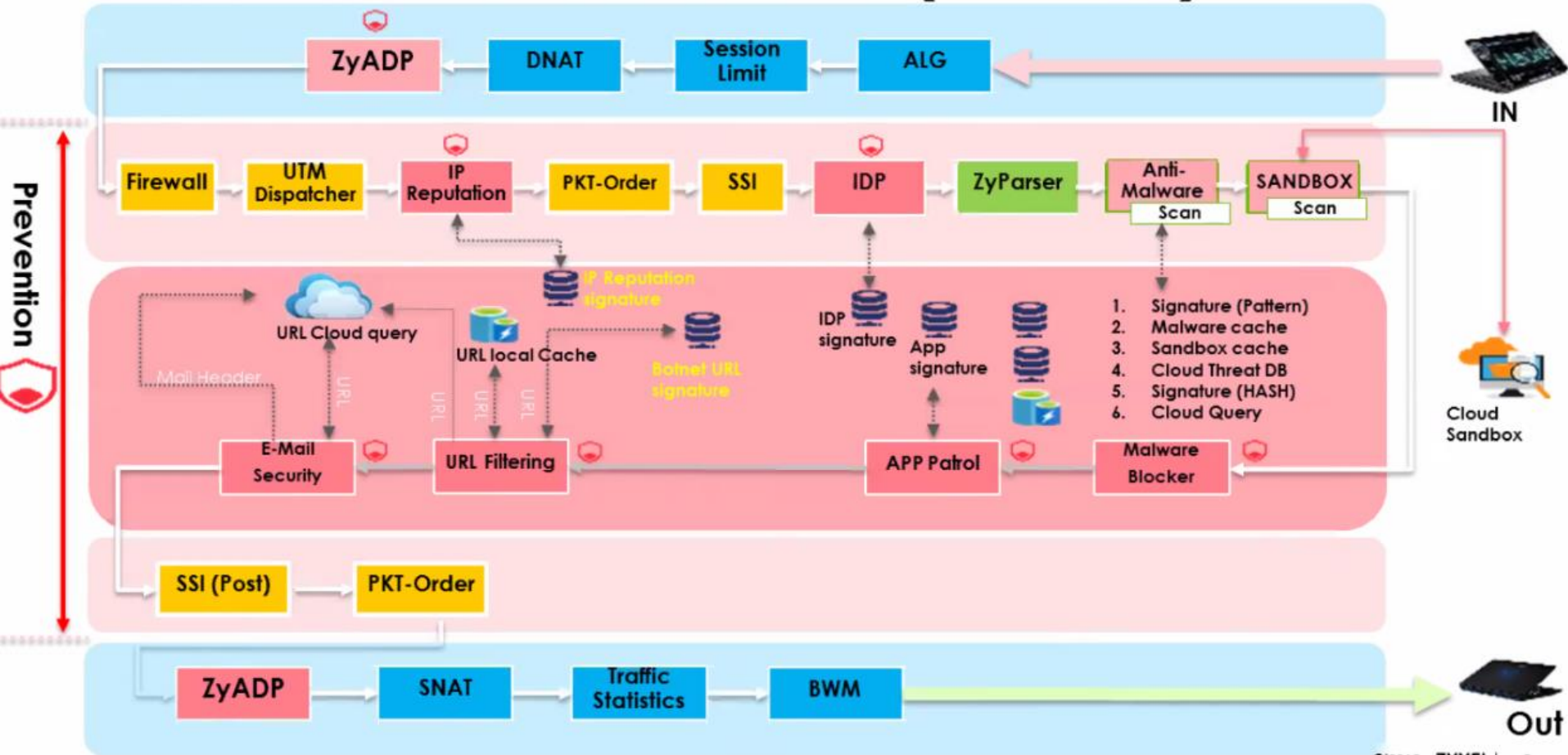
Signature Information

Current Version: 1.0.1.20190814.0

Signature Number: 200000

Released Date: 2019-08-14 10:47:09

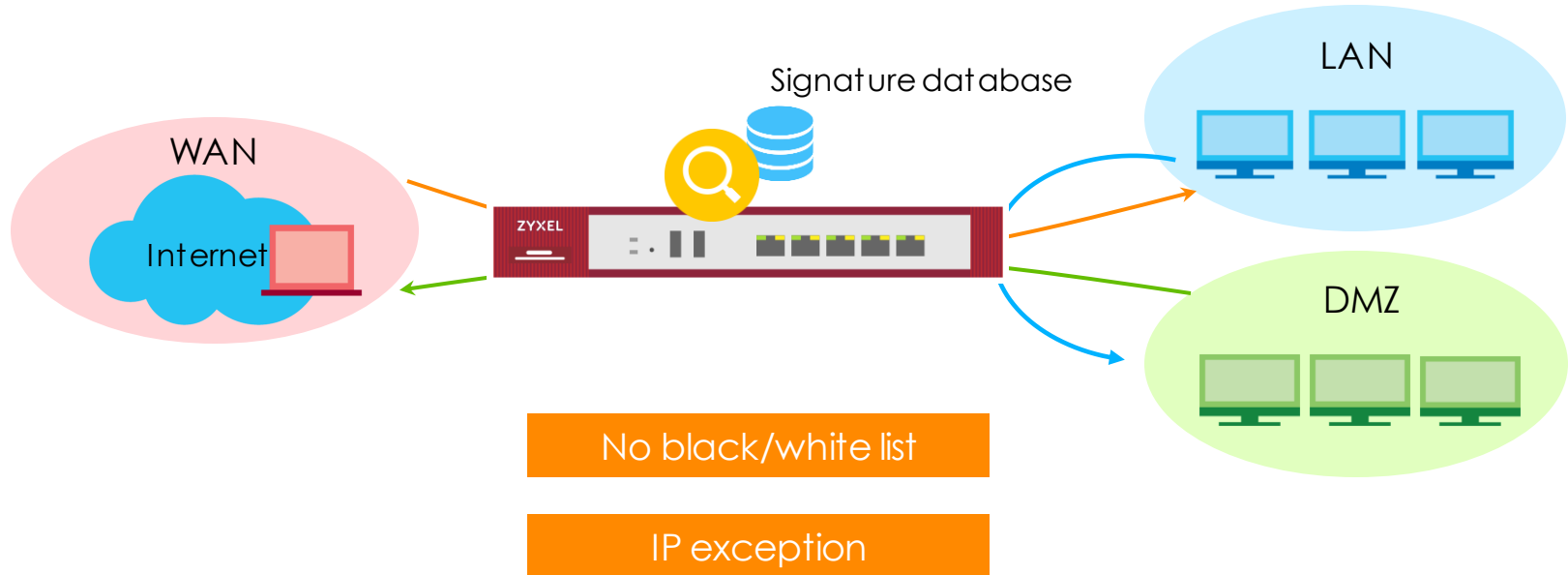
Packet Flow for ATP Series (ZLD 4.35)



Security Exception Enhancements

Security Exception Enhancements (1/2)

- In ZLD4.33, ATP gateway checks all traffic pass the gateway when IDP/Anti-Malware/Reputation Filter is enabled



Security Exception Enhancements (2/2)

- In ZLD4.35, user can configure black/white list, IP exception for security services on ATP gateway

Feature Enhancements	IDP	Anti-Malware	Reputation Filter
Black list	√*	√	√
White list	√	√	√
IP exception	√	√	Not support yet

*: User can create/import custom IDP signature for a new attach, so black list is not necessary

Black/White List Setting (1/2)

- User can manual add specific file to black/white list
 - Example: Configure black list in Anti-Malware

Anti-Malware IP Exception List Black/White List Signature

White List Black List

Check Black List

+ Add ✎ Edit ✖ Remove 💡 Activate 💡 Inactivate

#	Status	Type	Value
1	💡	MD5 Hash	9C7814C65AC689C16FED4C9178E93663
2	💡	File Pattern	*.pdf

Page 1 of 1 Show 50 items

Custom signature using file pattern or MD5 hash

Black/White List Setting (2/2)

- User can quickly add/remove the detected file to white list from security statistics
 - Example: Configure black list in Anti-Malware

MONITOR

- + System Status
- + Wireless
- + VPN Monitor
- Security Statistics**
 - App Patrol
 - Content Filter
 - Anti-Malware**
 - Reputation Filter
 - IDP
 - Sandboxing
 - Email Security
 - SSL Inspection
 - Log

Summary

General Settings

Collect Statistics since 2019-05-08 15:50:22 to 2019-05-13 14:25:39

Refresh **Flush Data**

Summary

Total Viruses Detected: 4

Statistics

Top Entry By: Virus Name

Add to white list **Remove from white list**

#	Virus Name	Hash	Occurrence	White List
1	Malicious Virus(detected by Cloud Threat ...	6CE6F415D8475545BE5BA114F208B0FF	2	<input type="checkbox"/>
2	Malicious.Virus(detected by Cloud Query)	6CE6F415D8475545BE5BA114F208B0FF	2	<input type="checkbox"/>

Page 1 of 1 Show 50 items Displaying 1 - 2 of 2

IP Exception Setting

- User can configure IP exception to allows gateway bypasses scanning for trusted sources/destination
 - **Configuration > Security Service > Anti-Malware > IP Exception List**

The screenshot displays the configuration interface for IP exceptions. On the left is a navigation menu with the following items: CONFIGURATION, VPN, BWM, Web Authentication, Security Policy, Security Service (with sub-items: App Patrol, Content Filter, Anti-Malware, Reputation Filter, IDP, Sandboxing, Email Security, SSL Inspection), IP Exception (highlighted), and Object. The main area shows the 'IP Exception' configuration page, specifically the 'IPv4 Exception List' section. A '+ Add' button is highlighted with a red box. Below it is a table with columns for '#', 'Name', and 'Page'. A modal window titled 'Add Exception IP' is open, showing the following fields: Name (LAN_to_DMZ), Description (empty), Source (LAN_SUBNET_GE4, highlighted with a red box), Destination (DMZ_SUBNET, highlighted with a red box), and Log (Yes). Under the 'Service To Bypass' section, checkboxes for 'Anti-Malware' and 'IDP' are checked and highlighted with a red box. The modal window has 'OK' and 'Cancel' buttons at the bottom.

Limitation

- IP Exception List only support hasn't supported FQDN and Geo IP objects as source/destination
 - Only support IPv4,IPv6 address objects

+ Add Exception IP

Create New Object ▾

Name: LAN_to_DMZ

Description:

Source: LAN_SUBNET_GE4 ▾

Destination: DMZ_SUBNET ▾

Log: Yes ▾

Service To Bypass

Anti-Malware

IDP

OK Cancel

No FQDN/Geo IP object selection

Networking Enhancements

03



Agenda

01

**NAT
Enhancement**

02

**Geo-IP
Enhancement**

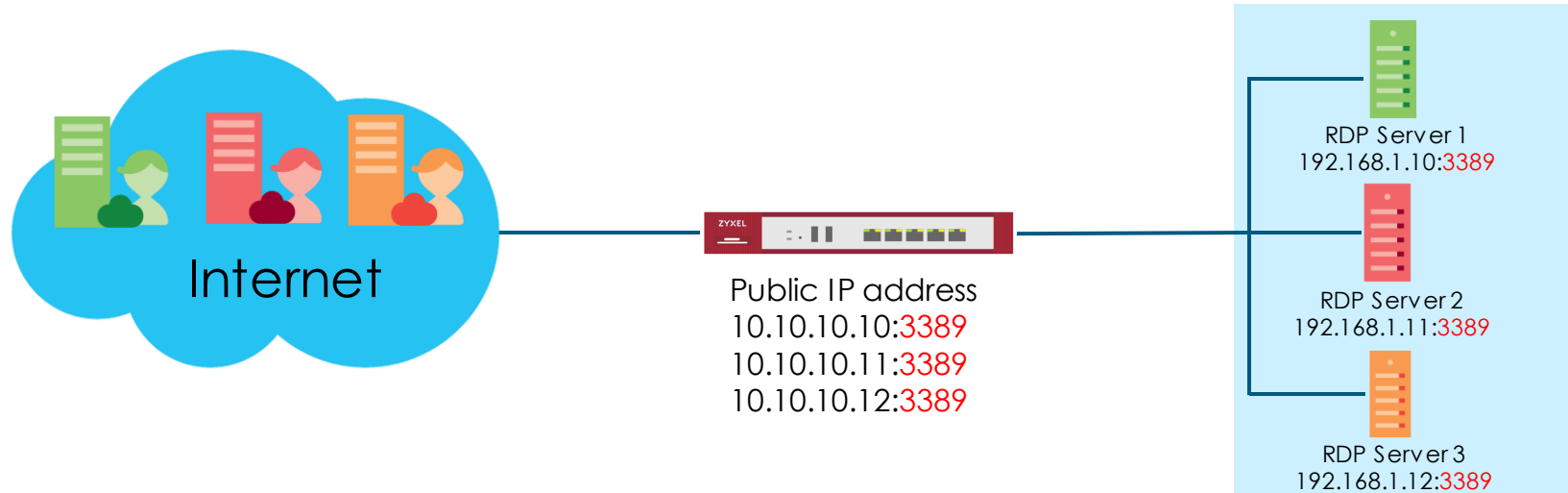
03

**Interface
Connectivity
Check
Enhancement**

NAT Enhancement

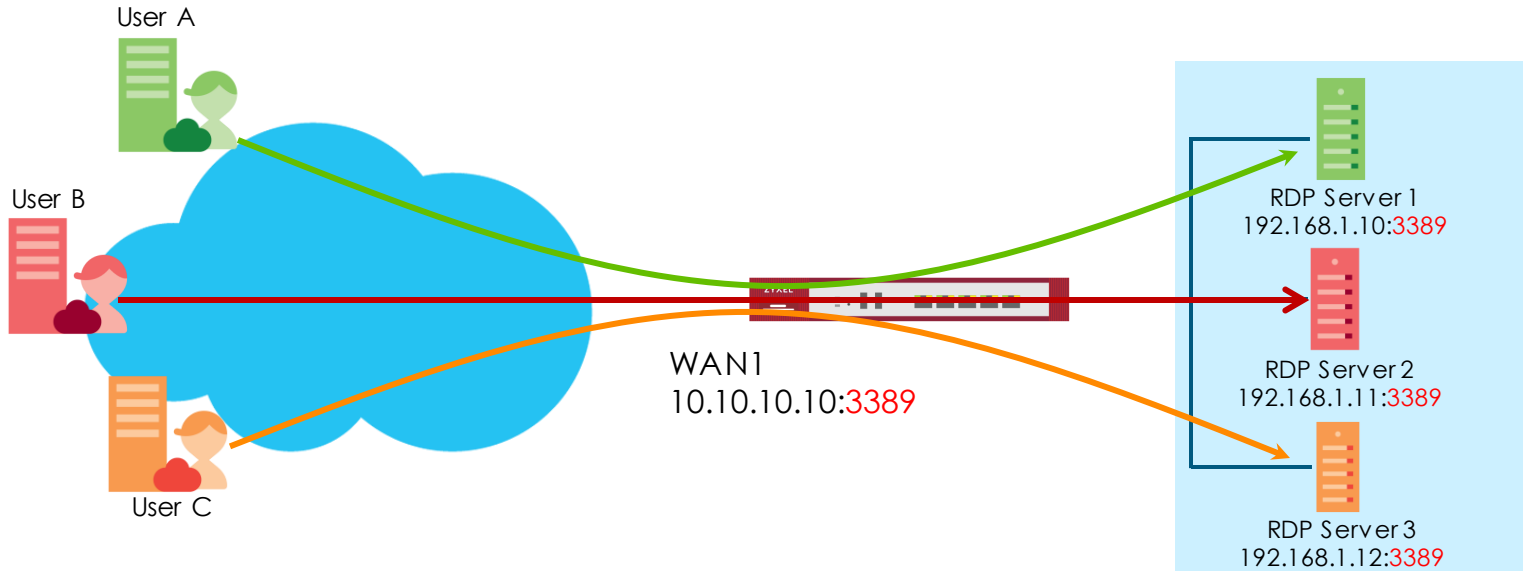
Motivation (1/2)

- In ZLD4.33, 1 public IP address only can map to 1 dedicated server which uses the same port number



Motivation (2/2)

- Server hosting provider wants to set up multiple dedicated servers to different users by using only 1 public IP address
 - All dedicated server uses the same port number



NAT Enhancement

- In ZLD4.35, user can set up NAT mapping to different internal server by source IP address

Add NAT

Create New Object ▼

General Settings

Enable Rule

Rule Name: RDP_Server

Port Mapping Type

Classification: Virtual Server 1:1 NAT Many 1:1 NAT

Mapping Rule

Incoming Interface: wan1

Source IP: user_a HOST, 20.20.20.20

External IP: User Defined

User-Defined External IP: 10.10.10.10 (IP Address)

Internal IP: User Defined

User-Defined Internal IP: 192.168.1.10 (IP Address)

Port Mapping Type: Service

External Service: RDP TCP, 3389

Internal Service: RDP TCP, 3389

OK Cancel

Limitation

- NAT setting does not support FQDN for Source IP

The screenshot shows the 'Add NAT' configuration window with the following settings:

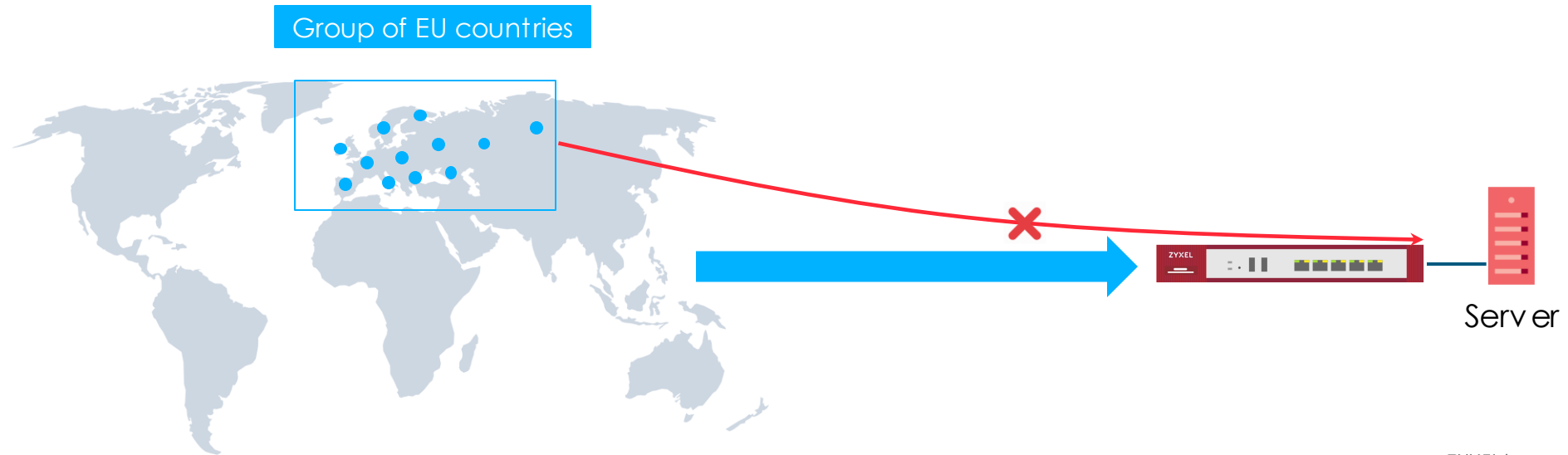
- General Settings:**
 - Enable Rule
 - Rule Name: RDP_Server
- Port Mapping Type:**
 - Classification: Virtual Server 1:1 NAT Many 1:1 NAT
- Mapping Rule:**
 - Incoming Interface: wan1
 - Source IP: user_a (highlighted with a red box)
 - External IP: User Defined
 - User-Defined External IP: 10.10.10.10 (IP Address)
 - Internal IP: User Defined
 - User-Defined Internal IP: 192.168.1.10 (IP Address)
 - Port Mapping Type: Service
 - External Service: RDP TCP, 3389
 - Internal Service: RDP TCP, 3389

A blue callout box points to the 'Source IP' dropdown with the text: "Source IP should be static public IP addresses".

Geo-IP Enhancement

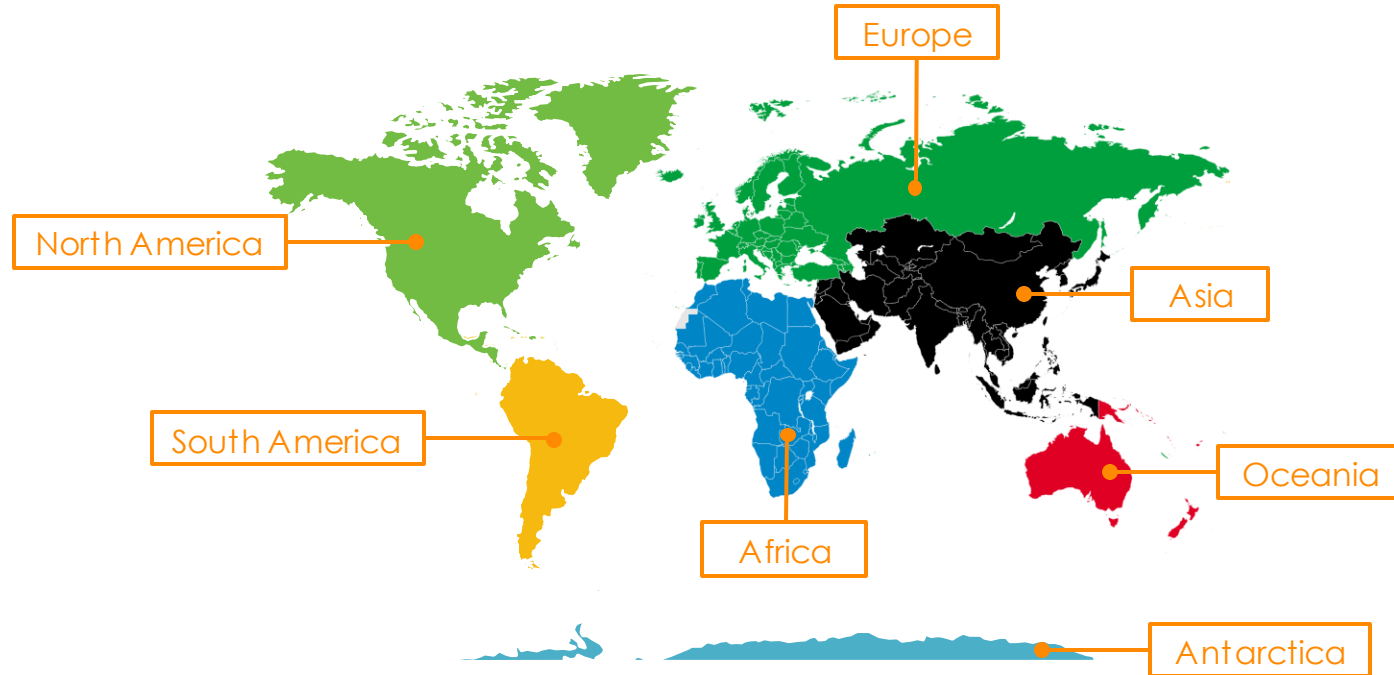
Geo IP Enhancement (1/5)

- In ZLD4.33, user must add countries in a group to block traffic from a continent such as EU, Asia,...



Geo IP Enhancement (2/5)

- Geo IP lists all countries in 7 continents, user can select the specific countries or continents to block



Geo IP Enhancement (3/5)

- Configuration > Object > Address/Geo IP > Address

The screenshot displays the ZyXEL configuration interface for IPv4 Address Configuration. The left sidebar shows the navigation menu with 'CONFIGURATION' expanded to 'Address'. The main area shows a table of existing address rules and a modal window for adding a new 'Address Rule'.

IPv4 Address Configuration Table:

#	Name
1	DMZ
2	DMZ_SUBNET
3	IP6to4-Relay
4	LAN1
5	LAN_SUBNET_GE4
6	LAN_SUBNET_GE5
7	RFC1918_1
8	RFC1918_2
9	RFC1918_3
10	WIZ_VPN_LOCAL
11	WIZ_VPN_REMOTE

Add Address Rule Modal:

- Name: Europe
- Address Type: GEOGRAPHY
- Region: Europe (selected from a dropdown menu)

Region Dropdown List:

- Europe
- Estonia
- Egypt
- Equatorial Guinea
- Eritrea
- Ethiopia
- Eswatini
- El Salvador
- Ecuador

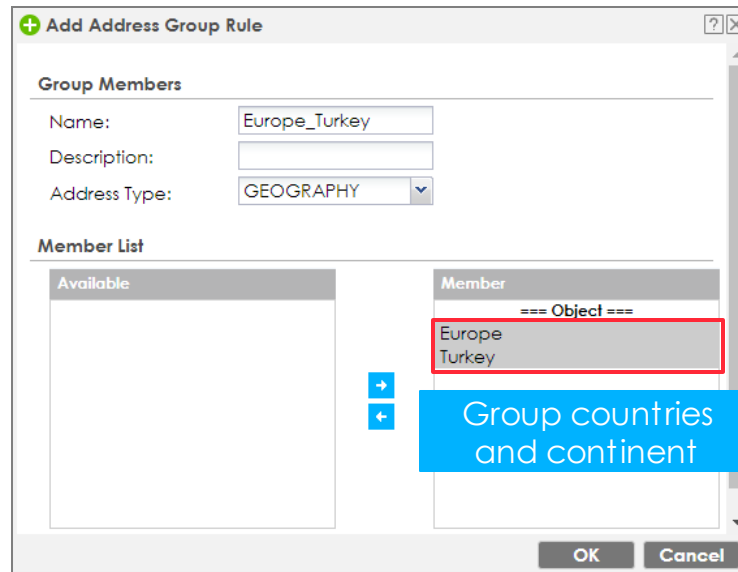
IPv4 Address Table:

IPv4 Address
10.10.10.0-255.255.255.0
ge6-192.168.3.0/24
100.0.0.1
ge5-192.168.2.0/24
10.0.0.0/8
172.16.0.0/12
192.168.0.0/16
192.168.1.0/24
0.0.0.0/24

A blue callout box with the text "Select the country or continent" points to the 'Region' dropdown menu.

Geo IP Enhancement (4/5)

- User can make group countries and continents objects
 - **Configuration > Object > Address/Geo IP > Address Group**



Geo IP Enhancement (5/5)

- User can search which continent the country belong to, the country list of the continent
 - **Configuration > Object > Address/Geo IP > Geo IP**

The screenshot displays a web interface for configuring Geo IP. At the top, there are three tabs: 'Address', 'Address Group', and 'Geo IP'. Below the tabs, the main section is titled 'Region vs. Continent'. It contains two input fields: 'Region:' with a text box containing 'Russia' and a 'Region To Continent' button; and 'Continent:' with a dropdown menu showing 'Europe' and a 'Region List' button. To the right, there is a search box with the text 'Search which continent the country belong to'. Below the search box, a list of countries is displayed, including Aland Islands, Albania, Andorra, Austria, Belarus, Belgium, Bosnia and Herzegovina, and Bulgaria. The search box and the list of countries are highlighted with red boxes.

Search country list of the continent

Interface Connectivity Check Enhancement

Connectivity Check Settings

- Support Interfaces
 - Ethernet, VLAN, Bridge
- **Configuration > Network > Interface**

Edit Bridge br0 [?] [X]

Show Advanced Settings

Connectivity Check

Enable Connectivity Check

Check Method: icmp

Check Period: 20 (5-600 seconds)

Check Timeout: 5 (1-10 seconds)

Check Fail Tolerance: 5 (1-10)

Check Default Gateway 0.0.0.0

Check These Addresses

10.214.48.254

10.214.48.33

Probe Succeeds When: all respond(s)

any one

all

Two domain name or IP addresses for the connectivity check

The check pass when one or both domain name /IP addresses respond

IPSec VPN Enhancement

04



Agenda

01

**Diffie Hellman
Groups 15-18
Support**

Diffie Hellman Groups 15-18 Support

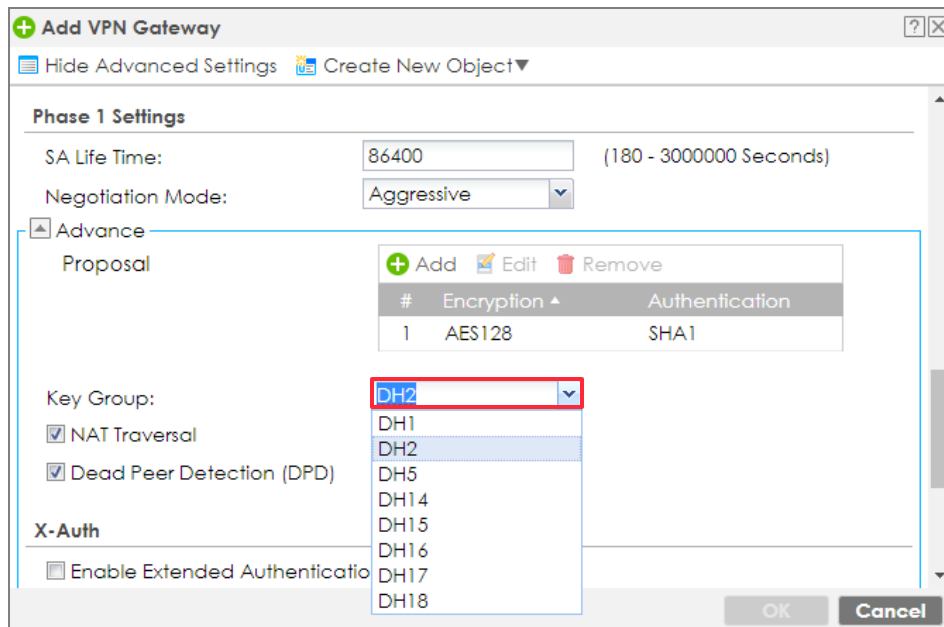
Diffie Hellman Group Support (1/2)

- ZyWALL/USG/ATP supports Diffie Hellman Group 15-18 for IPsec VPN

Diffie Hellman Group	Random number length
DH1	768 bit
DH2	1024 bit
DH5	1536 bit
DH14	2048 bit
DH15	3072 bit
DH16	4096 bit
DH17	6144 bit
DH18	8192 bit

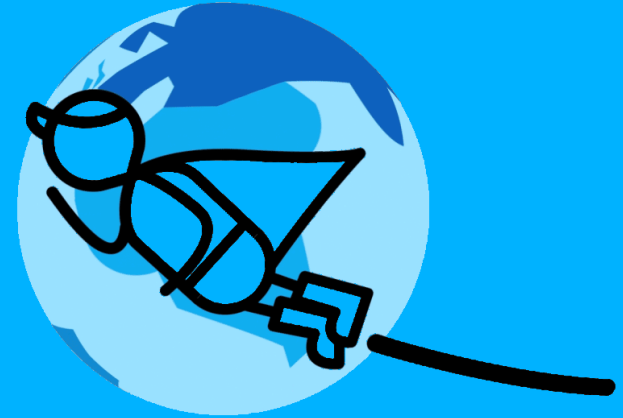
Diffie Hellman Group Support (2/2)

- Configuration > VPN > IPsec VPN



APC 3.40 Enhancements (NXC 5.40)

05



Agenda

01

**New supported
AP**

02

**APC 3.40
Enhancements**

Support AP List

ZLD4.35	Supported Managed AP	
ZyWALL/USG/ATP	NWA3160-N NWA3550-N NWA3560-N NWA5160N NWA5550-N NWA5560-N NWA5121-NI NWA5123-NI NWA5121-N NWA5301-NJ WAC6502D-E	WAC6502D-S WAC6503D-S WAC6553D-E WAC6103D-I NWA5123-AC WAC5302D-S NWA5123-AC HD WAC6303D-S WAC6552D-S WAX650S * WAX510 *

Available
 New Support

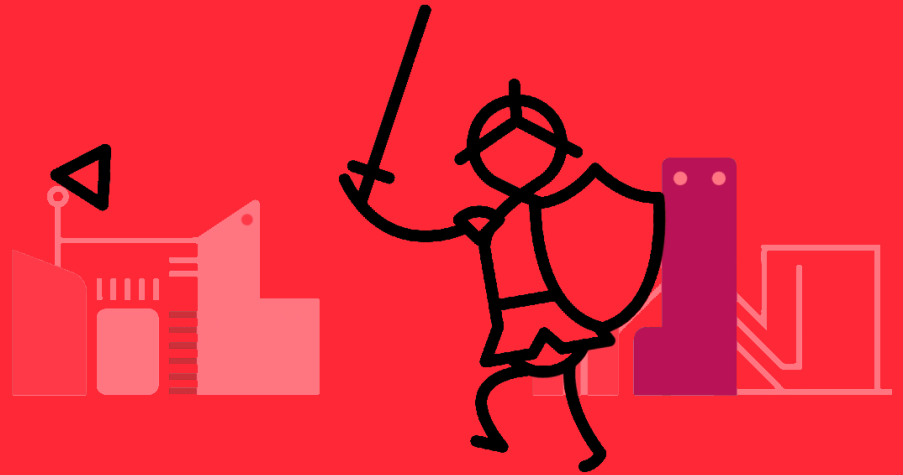
* : Forward Compatible APs

APC 3.40 Enhancements

- AP firmware upgrade by group
- Rogue AP detection in AP mode
- AP cloud firmware upgrade
- ARP Proxy for STA
- 802.11r
- 802.11k/v assisted roaming
- Controller offline policy
- Capture AP packets on controller
- Change AP IP address on controller
- Accounting

Hotspot Enhancement

06



Agenda

01

**Hotspot License
for USG60/60W**

Hotspot Service for USG60(W)

- USG60(W) supports hotspot service in ZLD4.35
 - License is required

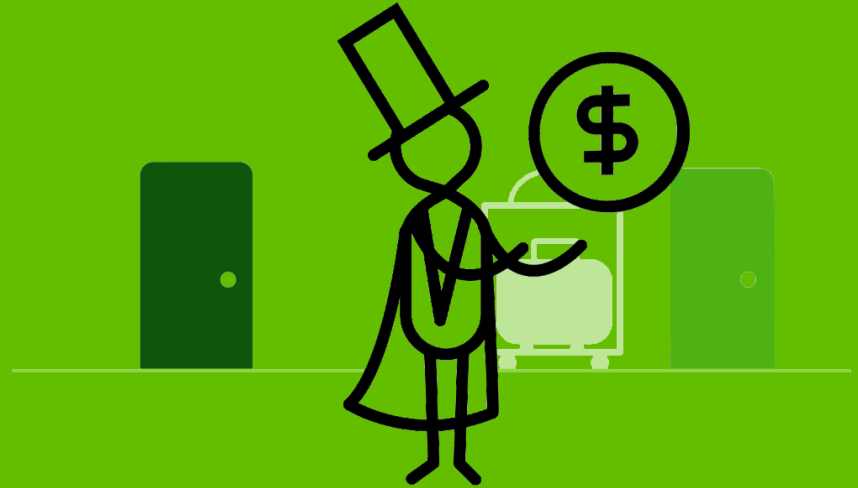
	USG60(W)
Hotspot Service	Yes <i>(ZLD4.35 or later)</i>
Concurrent Login	200 <i>(128 in ZLD4.33)</i>
Max Dynamic Account List	2000
Managed AP number (default/max)	2/18

Supported Models

- Gateway supports hotspot services
 - USG60(W)/110/210/310/1100/1900/2200/2200-VPN
 - ZyWALL 110/310/1100
 - VPN100/300

System Management Enhancements

07



Agenda

01

Web Console

02

**Send Certificate
by Email**

03

**2FA for Admin
Login via
GUI/SSH/Telnet**

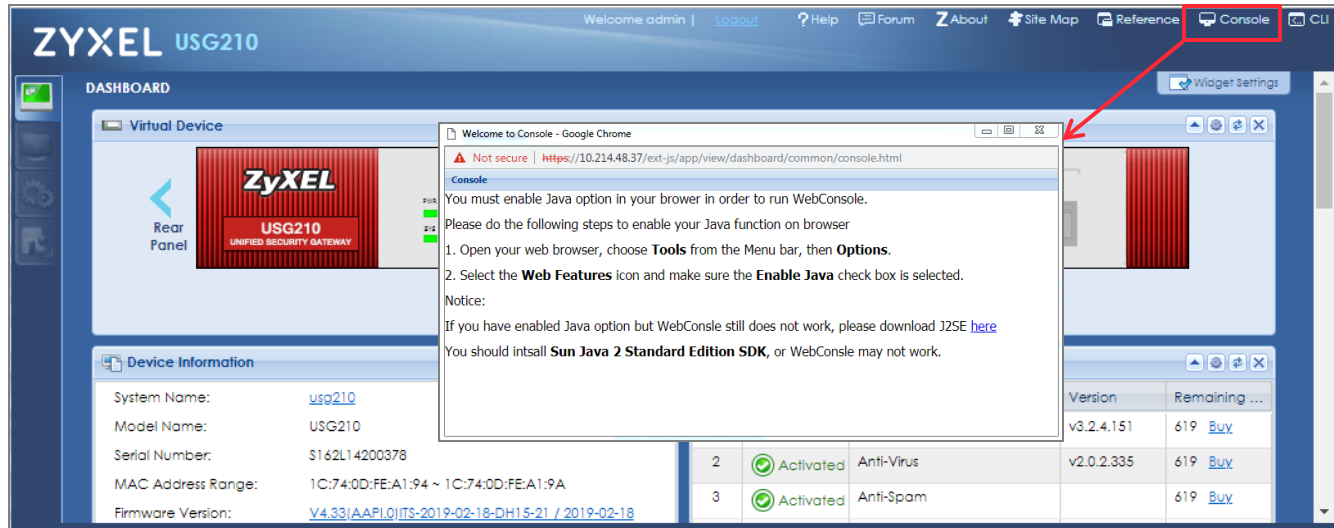
04

**Email to SMS
Support**

Web Console

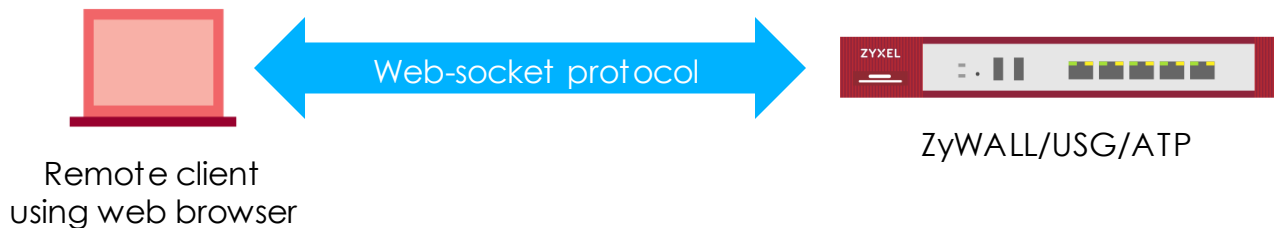
Web Console (1/2)

- Chrome/Firefox/IE/Safari has dropped support Java plug-in, and therefore Web console which uses Java Plugin doesn't work in your web browser



Web Console (2/2)

- Web Console uses WebSocket protocol for communication between a browser and a gateway over HTTPS port 443
 - Ensure secure connection
 - WebSocket protocol is supported by all modern browsers



WebSocket Browser Support List

- Web-Socket fully supported by all modern browsers
 - Chrome 16 + (incl. Chrome for Android)
 - Firefox 11 + (incl. Firefox for Android)
 - Internet Explorer 10+ (incl. Internet Explorer Mobile on Windows Phone 8)
 - Safari 6 +
 - Opera 12.1 + (incl. Opera Mobile)



Open Web Console

- Web console is implemented on ZyWALL/USG/ATP series

ZYXEL ATP500

General | **Advanced Threat Protection**

CPU Usage: 8 %
Memory Usage: 27 %
Flash Usage: 13 %
USB Storage Usage: 0/0 MB
Active Sessions: 78/1000000
DHCP Table: 1 Host(s)

Console

```
web-console-login (atp500) x +
Not secure | https://10.214.48.31/webconsole/
Username: admin
Password:
Router# show interface all
No. Name      Status      IP Address  Mask        IP Assignment
-----
1 ge1         Down        0.0.0.0    0.0.0.0     DHCP client
2 ge2         100M/Full   10.214.48.31 255.255.255.0 DHCP client
3 ge3         Down        0.0.0.0    0.0.0.0     DHCP client
4 ge4         Down        192.168.1.1 255.255.255.0 Static
5 ge5         Down        192.168.2.1 255.255.255.0 Static
6 ge6         Down        192.168.3.1 255.255.255.0 Static
7 ge7         Down        0.0.0.0    0.0.0.0     Static
8 ge8         Down        0.0.0.0    0.0.0.0     Static
Router#
```

bb:ec:a3:b6:b6:0c ~ bb:ec:a3:b6:b6:13 | 2019-04-23 / 10:25:13 UTC+08:00
Firmware Version: [V4.35\(ABFU.0\)b2s1 / 2019-04-18 22:15:00](#)

Notice (1/2)

- Web console only support HTTPs to device GUI
- Multiple web console can be opened concurrently
- Debug messages will not show on web console

Notice (2/2)

- Web console uses port 11080 for terminal emulation. User can't use this port for other service
 - Web GUI setting

The image shows two screenshots from a network device's web console. The left screenshot is titled 'TELNET' and shows the 'General Settings' section. The 'Enable' checkbox is checked, and the 'Server Port' is set to '11080', which is highlighted with a red box. A red arrow points from this box to the right screenshot. The right screenshot is an 'Error Message' dialog box with the following text: 'CLI Number: 0', 'Error Number: -9003', and 'Error Message: 'Change TELNET port has failed. Port has been used for other services.''. There is an 'OK' button at the bottom right of the dialog.

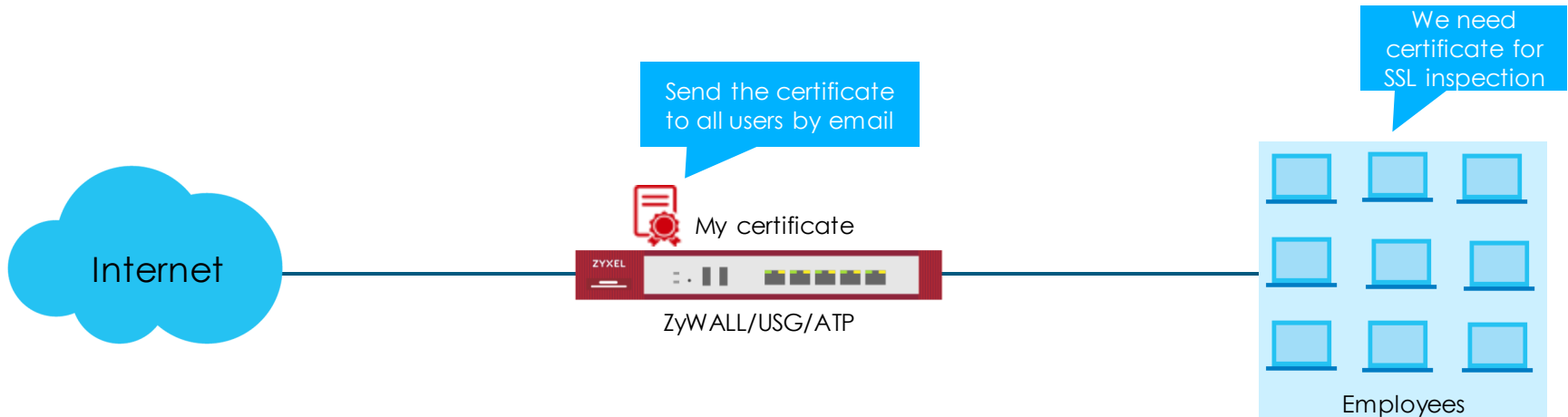
- CLI setting

```
Router(config)# ip telnet server port 11080
% Change TELNET port has failed. Port has been used for other services.
retval = -9003
ERROR: Change TELNET port has failed. Port has been used for other services.
```

Send Certificate by Email

Send Certificate by Email (1/3)

- In ZLD4.35, ZyWALL/USG/ATP can directly send its certificate to specific user by email
 - Quickly distribute to multiple users



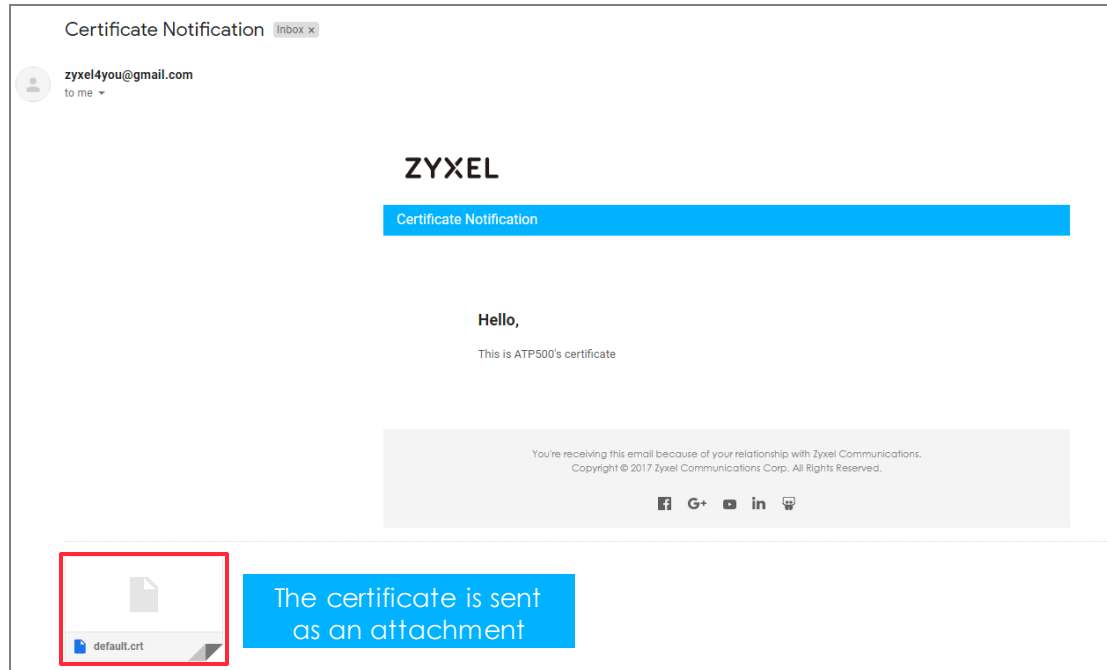
Send Certificate by Email (2/3)

- The certificate is sent to specific user via email. You opt to compress as zip file
 - **Configuration > Object > Certificate > My certificate**

The screenshot displays the ZyXEL configuration interface. On the left, a navigation menu shows 'CONFIGURATION' with sub-items like Anti-Malware, Reputation Filter, IDP, Sandboxing, Email Security, SSL Inspection, IP Exception, Object, Zone, User/Group, AP Profile, MON Profile, ZyMesh Profile, Address/Geo IP, Service, Schedule, AAA Server, and Auth. Method. The 'Certificate' option is highlighted. The main area shows 'My Certificates' with a table containing one entry: '1 default'. A dialog box titled 'Email My Certificate' is open, showing 'Email Settings'. The 'Mail Subject' is 'Certificate Notificatic'. The 'Mail To' field contains 'all_employee@zyxel.' and is highlighted with a red box and a blue callout 'User's email address'. Below it are three empty email address fields. The 'Send Certificate with Private Key' checkbox is checked. The 'Password' field is empty. The 'E-mail Content' field contains 'This is the ATP500's certificate'. The 'Compress as a ZIP file' checkbox is checked and highlighted with a red box and a blue callout 'Compress certificate in ZIP file'. The dialog has 'Send Email' and 'Cancel' buttons at the bottom.

Send Certificate by Email (3/3)

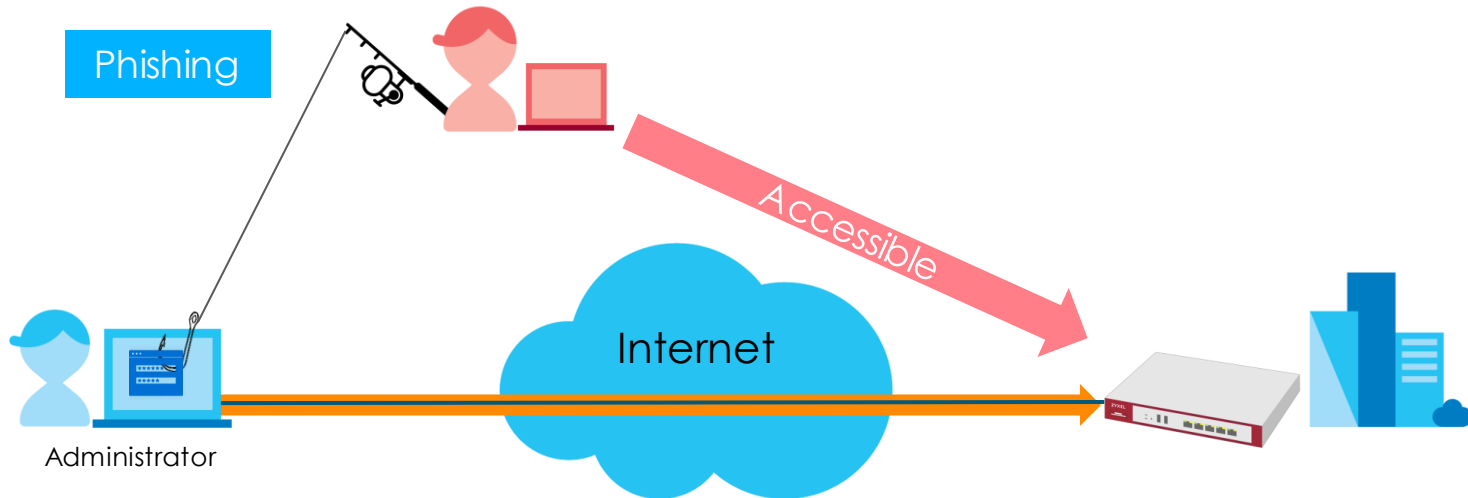
- The gateway's certificate is sent to user via email as an attachment



2 Factor-Authentication for Administrator

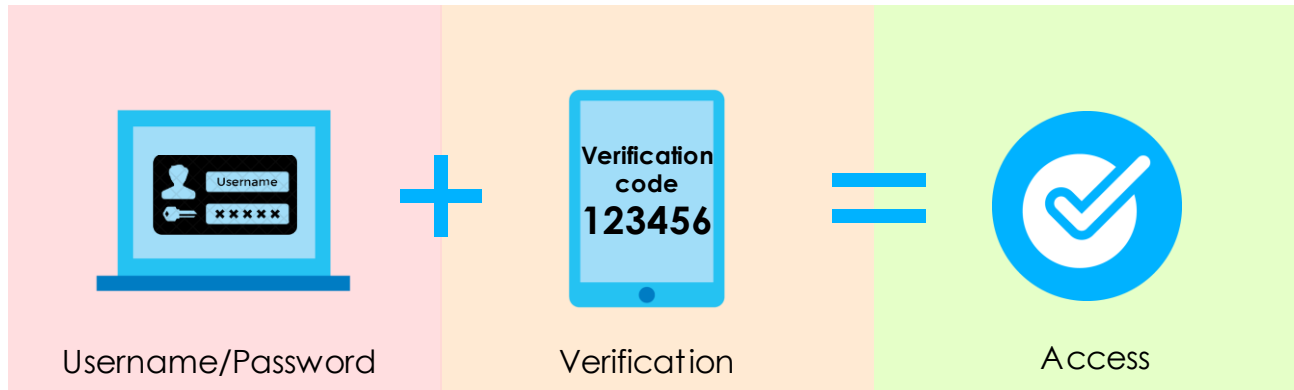
2FA for Administrator (1/4)

- Using only username/password authentication for administrator is not enough to prevent hackers gain access to your enterprise.
 - Username/password could be phished, hacked, or guessed



2FA for Administrator (2/4)

- Two-Factor authentication requires administrator enters a verification code after their user name and password are accepted
 - Gateway sends a verification code to administrator via SMS/Email
 - Administrator must key the verification code before expiration time



2FA for Administrator (3/4)



2FA for Administrator (4/4)

- Supported login services
 - Web
 - SSH
 - Telnet
- Second-step authentication
 - 6-digit verification code
- Verification code delivery methods
 - Email
 - SMS
 - SMS service
 - **Email-to-SMS service**

Configuration Steps

1

Setup Notification Server

Mail Server, SMS services

2

Setup Admin Account

Email address and phone number

3

Enable 2 FA for Admin Access

Valid time, Web/SSH/TELNET services

Setup Notification Server (1/2)

- Setup Mail Server
 - Configuration > System > Notification > Mail Server

Mail Server	SMS
General Settings	
Mail Server:	<input type="text" value="smtp.gmail.com"/> (Outgoing SMTP Server Name or IP Address)
Mail Subject:	<input type="checkbox"/> Append system name <input type="checkbox"/> Append date time
Mail Server Port:	<input type="text" value="587"/> <input checked="" type="checkbox"/> TLS Security <input checked="" type="checkbox"/> STARTTLS <input type="checkbox"/> Authenticate Server
Mail From:	<input type="text" value="zyxel4you@gmail.cor"/> (Email Address)
<input checked="" type="checkbox"/> SMTP Authentication	
User Name :	<input type="text" value="zyxel4you@gmail.cor"/>
Password:	<input type="password" value="....."/>
Retype to Confirm:	<input type="password" value="....."/>
Schedule	
Time For Sending Report:	<input type="text" value="0"/> (hours) <input type="text" value="0"/> (minutes)

Setup Notification Server (2/2)

- Setup SMS service using ViaNett account
 - Need to purchase SMS credit
 - **Configuration > System > Notification > SMS**

Mail Server | **SMS**

General Settings

Enable SMS Enable SMS service

Default country code for phone number: (1-4) digit

SMS Provider: Select ViaNett SMS provider

Purchase SMS Voucher from Zyxel reseller

If you want to activate SMS credits, please go to zyxel.vianett.com.

ViaNett Configuration

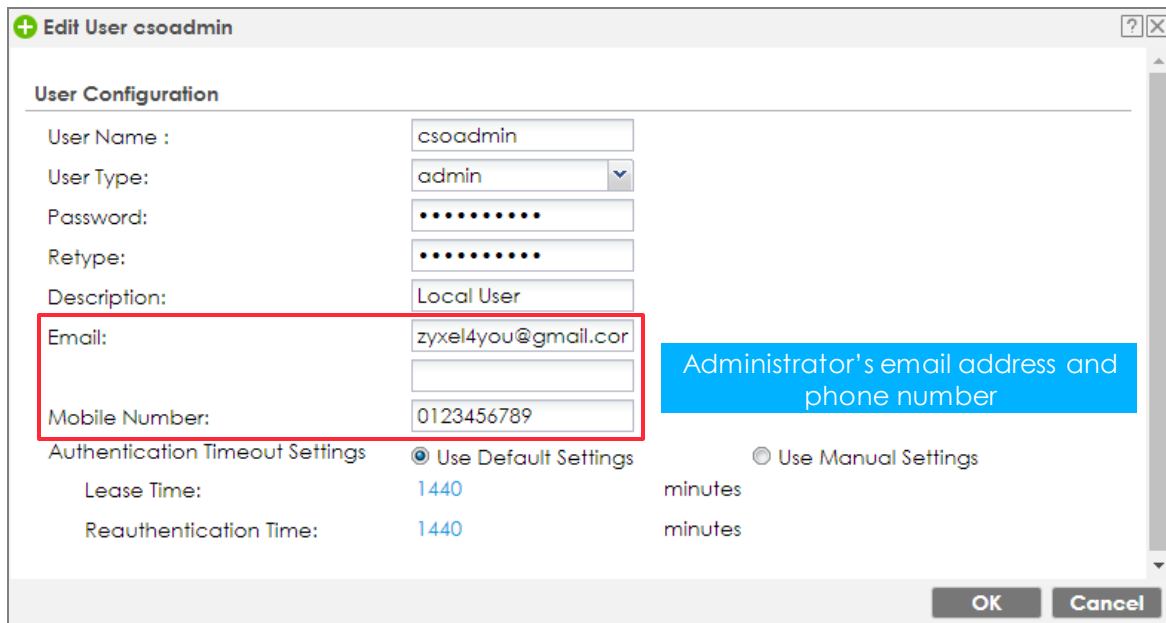
User Name: Enter your ViaNett account

Password:

Retype to Confirm:

Setup Admin Account

- Add phone number or email address for administrator
 - **Configuration > Object > User/Group > User**



The screenshot shows a dialog box titled "Edit User csoadmin" with a "User Configuration" section. The fields are as follows:

User Name :	csoadmin
User Type:	admin
Password:
Retype:
Description:	Local User
Email:	zyxel4you@gmail.com
Mobile Number:	0123456789

Below the fields, there are radio buttons for "Authentication Timeout Settings":

- Use Default Settings
- Use Manual Settings

Under "Use Default Settings", the following values are shown:

Lease Time:	1440	minutes
Reauthentication Time:	1440	minutes

A red box highlights the "Email" and "Mobile Number" fields. A blue callout box points to these fields with the text "Administrator's email address and phone number".

Notice

- User can verify the email address and phone number of root admin to avoid misconfiguration

Edit User admin

User Configuration

User Name : admin

User Type: admin

Password:

Retype:

Description: Administration account

Email: zyxel4you@gmail.com **Send Code**

Mobile Number: 0123456789 **Send Code**

Authentication Timeout Settings

Use Default Settings Use Manual Settings

Lease Time: 0 minutes

Reauthentication Time: 0 minutes

OK **Cancel**

Enter to verify the email address

Verify Root Admin's Information

- User can verify the root admin's email address and phone number by clicking to **Send Code** button

Edit User admin

User Configuration

User Name : admin

User Type: admin

Password:

Retype:

Description: Administration accou

Email: zyxel4you@gmail.com ✓

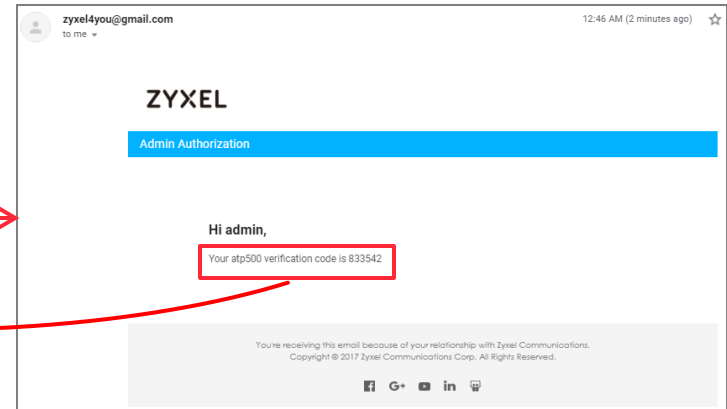
Mobile Number: 0123456789

Authentication Timeout Settings

Use Default Settings Use Manual Settings

Lease Time: 0 minutes

Reauthentication Time: 0 minutes



Enable 2 FA for Admin Access

- Configuration > Object > Auth. Method > Two-factor Authentication

Authentication Method Two-factor Authentication

VPN Access **Admin Access**

General Settings

Enable **Enable two-factor authentication**

Valid Time: (1-5 minutes) **Expiration times of two-factor authentication key**

Two-factor Authentication for Services:

Web SSH TELNET **Login services the 2FA apply for**

User

Selectable User Objects

Selected User Objects

=== Object ===

csoadmin

admin **Select administrator or limited administrator account for two-factor authentication**

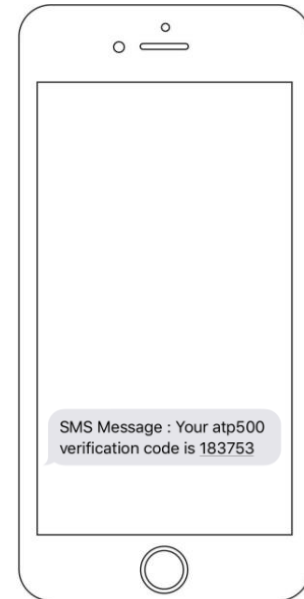
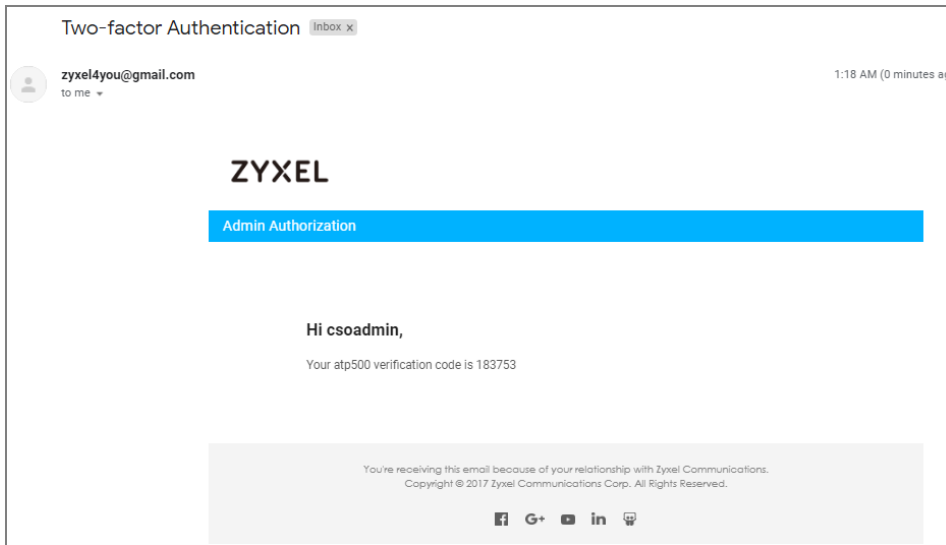
Delivery Settings

Verification Code Delivery Method SMS Email **Select verification code delivery methods**

Apply **Reset**

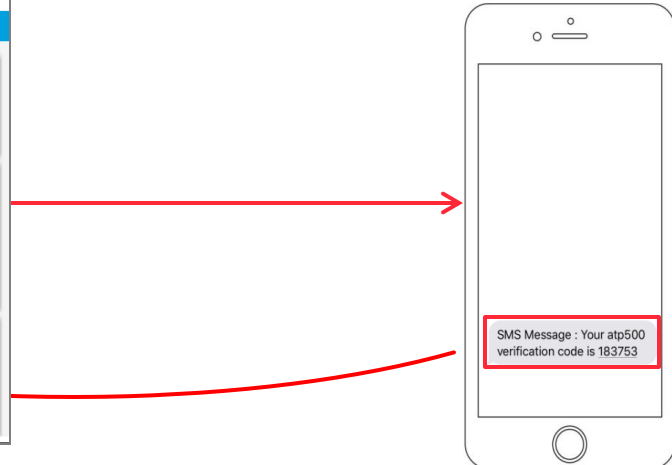
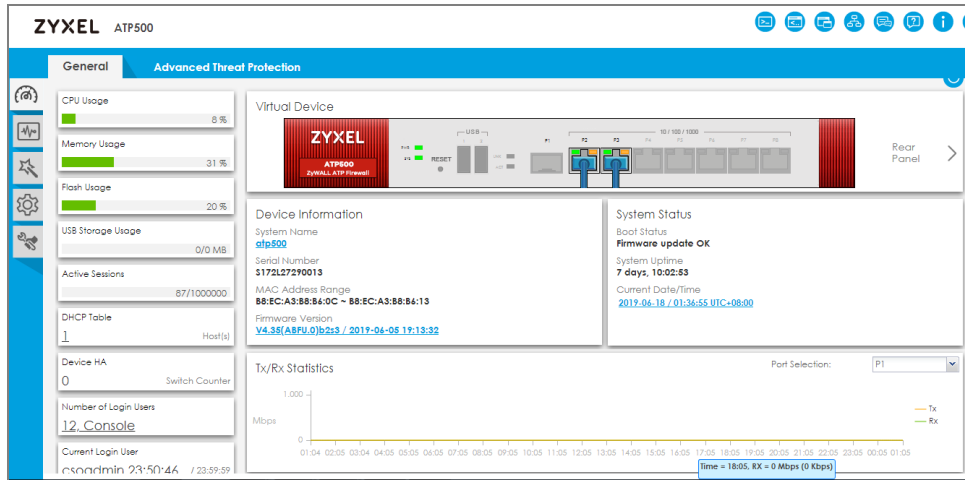
Email/SMS Verification

- When administrator attempts to access the gateway with username/password, the system will send a verification code via email/SMS



SMS/Email Verification

- Administrator must enter the verification code get the access. The access is granted only if:
 - Administrator enters the code by the valid time, and not enter wrong code over 3 times.



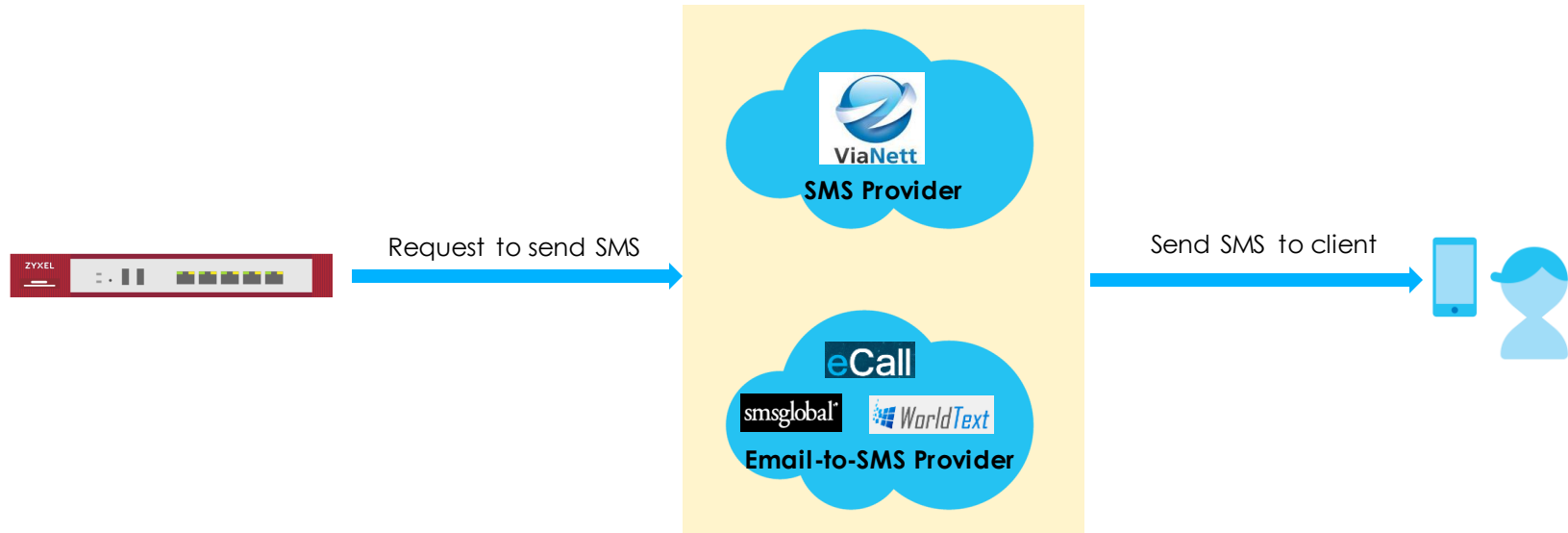
Notice

- Two-factor authentication supports for both limited admin and admin type
 - Local user only
- If both Email and SMS delivery methods are selected, only one verification code is generated and sent via both Email and SMS

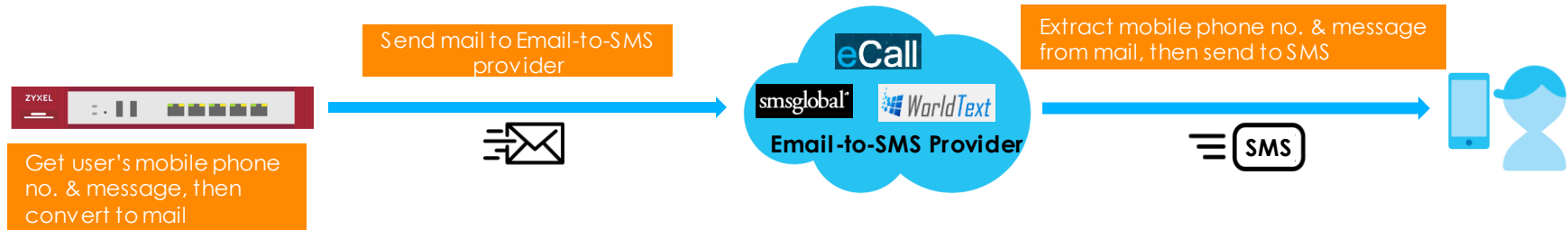
Email to SMS Support

Email to SMS Support

- Support as another option allows gateway sends information to client through SMS

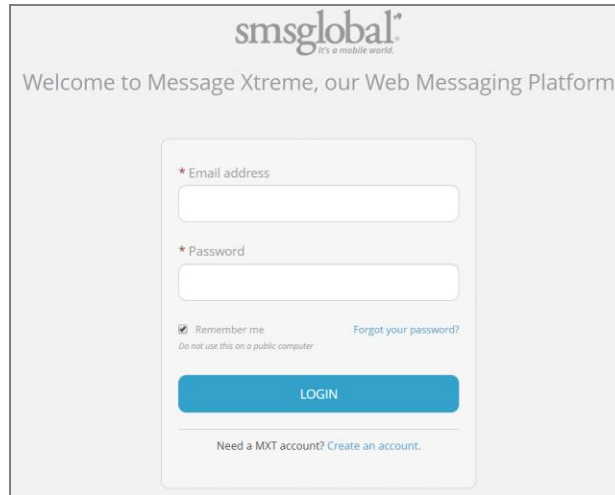


Email to SMS: How Does It Work ?



Subscribe Email to SMS Account

- Sign-up an account of Email to SMS service and purchase credit
 - Check the Email-to-SMS provider available in your country and choose the right SMS gateway provider to meet your needs
 - Reference : <https://email2sms.info/?>
- Example: SMSGlobal



The image shows a login form for SMSGlobal. At the top, the logo 'msglobal' is displayed with the tagline 'It's a mobile world.' Below the logo, the text 'Welcome to Message Xtreme, our Web Messaging Platform' is visible. The login form contains two input fields: '* Email address' and '* Password'. Below the password field, there is a checked checkbox for 'Remember me' and a link for 'Forgot your password?'. A blue 'LOGIN' button is positioned below the form. At the bottom of the form, there is a link that says 'Need a MXT account? Create an account.'

Subscribe Email to SMS Account

- Manage allowed sender
 - Email-to-SMS provider only accepts the request from senders who listed in 'Allowed sender email addresses'.

The screenshot displays the MXT API & Integrations dashboard. The left sidebar contains navigation links: Dashboard, Send Messages, Reports, Purchase, Virtual Numbers, API & Integrations (selected), Sales Enquiry, and Support. The main content area shows the 'API & Integrations' section with a welcome message for 'tongquang126@gmail.com'. The 'Email Settings' menu item is active, leading to the 'Email to SMS/MMS' configuration page. This page features a toggle switch for 'Email to SMS/MMS' which is turned on. Below this, the 'Allowed Sender Email Addresses' section contains a text input field with 'zyxel4you@gmail.com' entered, highlighted by a red border. A blue callout box points to this field with the text 'Enter allowed sender email address'. The 'Email replies to' section has three radio button options: 'Your account email address (tongquang126@gmail.com)' (selected), 'The email address that sent the original message', and 'A custom email address'. A note at the bottom states: 'Please note: Any changes to this setting will also affect the "SMS Replies to Email" settings.'

Setup Notification Server

- Configure mail server on gateway
 - **System > Notification > Mail Server**

Mail Server **SMS**

General Settings

Mail Server: (Outgoing SMTP Server Name or IP Address)

Mail Subject: Append system name Append date time

Mail Server Port: TLS Security STARTTLS Authenticate Server

Mail From: Enter the email address as same as allowed sender email address

SMTP Authentication

User Name :

Password:

Retype to Confirm:

Schedule

Time For Sending Report: (hours) (minutes)

Setup Notification Server

- Configure SMS service on gateway
 - **System > Notification > SMS**

Mail Server **SMS**

General Settings

Enable SMS

Default country code for phone number: (1-4) digit **Enter the country code**

SMS Provider: **Select Email-to-SMS provider**

Provider Domain: **Enter provider domain**

Mail Subject: (Optional)

Mail From: (Optional)

Mail To: @email.msgglobal.com

Note

1. If you select to use an Email-to-SMS provider, configure a mail server before you enable SMS.
2. If you leave the Mail From field blank here, the system automatically uses the mail address configured in the Mail Server screen.
3. "Mail To" default format is "\$mobile_number\$@provider domain" and some Service Providers might require prefix symbol like "+" added before \$mobile_number\$.

Setup User Account (Optional)

- You need to configure user's phone number for two-factor authentication
 - VPN access
 - Administrator access
- **Configuration > Object > User/Group > User**

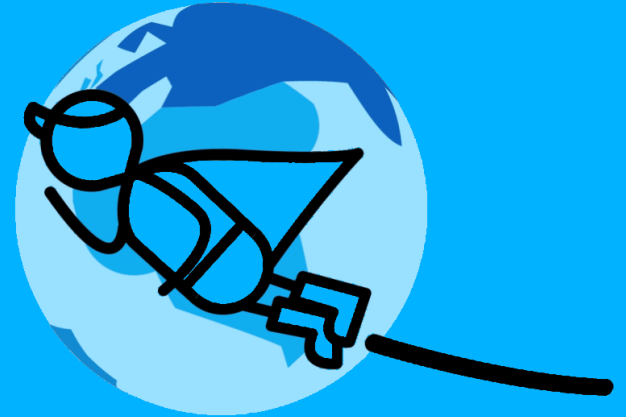
The screenshot shows a dialog box titled "Edit User csoadmin" with the following fields and values:

Field	Value
User Name :	csoadmin
User Type:	admin
Password:	••••••••
Retype:	••••••••
Description:	Local User
Email:	zyxel4you@gmail.com
Mobile Number:	0123456789
Authentication Timeout Settings	<input checked="" type="radio"/> Use Default Settings <input type="radio"/> Use Manual Settings
Lease Time:	1440 minutes
Reauthentication Time:	1440 minutes

At the bottom of the dialog are "OK" and "Cancel" buttons. A blue callout box with the text "Enter administrator's phone number" is positioned over the Mobile Number field.

Usability Enhancements

08



Agenda

01

**EZ Mode for
ZyWALL110/
USG110**

02

**Ethernet Port
Speed Setting
on GUI**

EZ Mode for ZyWALL110/USG110

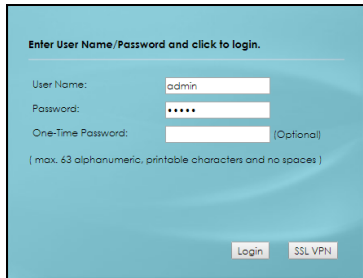
EZ Mode for ZyWALL110/USG110

- Since ZLD4.35, ZyWALL/USG110 supports “easy mode” setting in the GUI for entry-level and SOHO users

Model	Default Mode Setting	Firmware Support
USG20(W)-VPN USG40(W) USG60(W)	Easy Mode	ZLD4.20 +
ZyWALL/USG110	Selectable	ZLD4.35 +

EZ Mode for ZyWALL110/USG110

- For ZyWALL/USG110, when users log in for first time, user can select Easy Mode or Expert Mode to access



Enter User Name/Password and click to login.

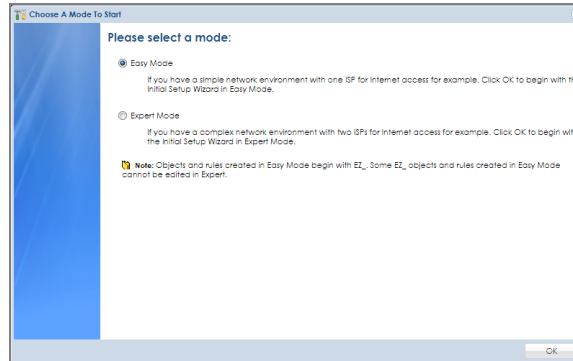
User Name:

Password:

One-Time Password: (Optional)
(max. 63 alphanumeric, printable characters and no spaces)

Login SSL VPN

First-time login



Choose A Mode To Start

Please select a mode:

Easy Mode
If you have a simple network environment with one IP for internet access for example. Click OK to begin with the initial Setup Wizard in Easy Mode.

Expert Mode
If you have a complex network environment with two IPs for internet access for example. Click OK to begin with the initial Setup Wizard in Expert Mode.

Note: Objects and rules created in Easy Mode begin with EZ_ some EZ_ objects and rules created in Easy Mode cannot be edited in Expert.

OK

Easy/Expert Mode Selection



Initial Setup Wizard

Choose your language: English

Welcome to the Zyxel Initial Setup Wizard. To protect your network, this Wizard prompts you to register your Device and activate security service(s) at myZyxel first. Your Device must be able to connect with myZyxel. You can re-run this Wizard to change configurations at anytime.

Basic Setup

- 1 Connect to Internet (WAN)
- 2 Date and Time Setting
- 3 Register Device
- 4 Activate Service
- 5 Wireless LAN
- 6 Remote Management

Optional Features

- Security Service (Content Filter, DP, Anti-Virus)
- Port Forwarding
- Guest LAN (Wired Network)
- VPN

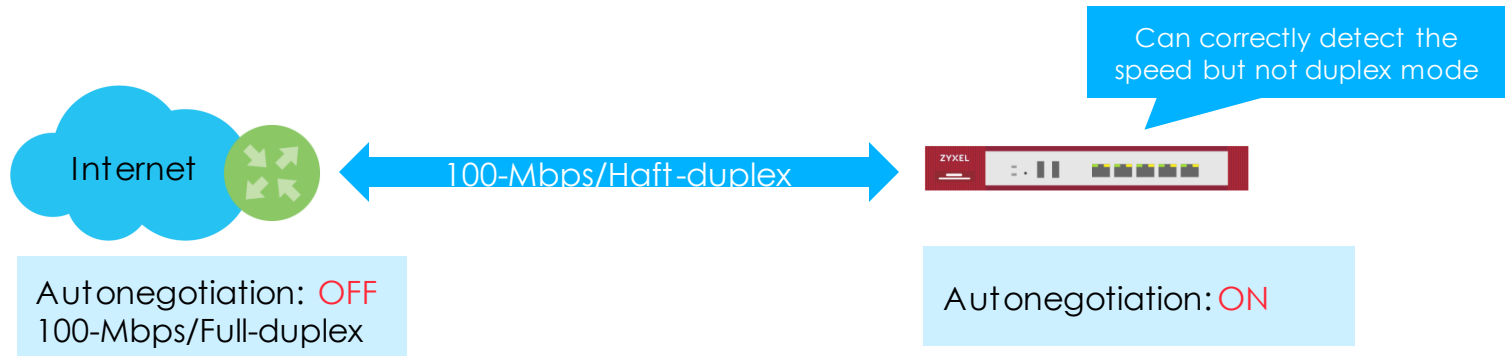
Exit < Back Next >

Initial Setup Wizard in corresponding mode

Ethernet Port Speed Setting on GUI

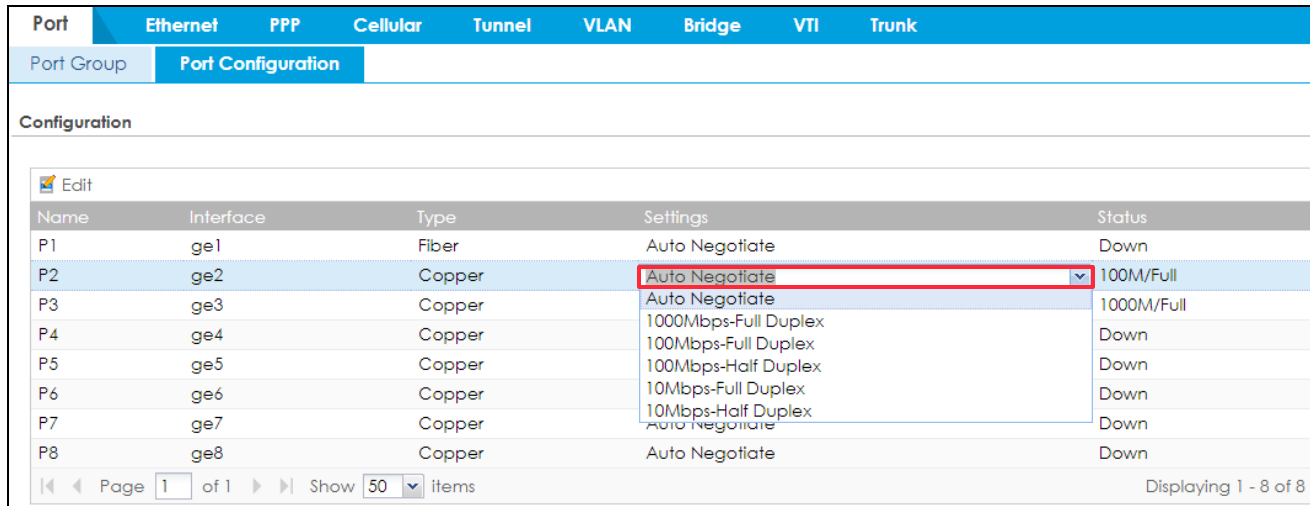
Configure Speed and Duplex


- By default, gateway will auto-negotiate the speed and duplex settings.
 - Autonegotiation failures can lead to a duplex mismatch



Configure Speed and Duplex on GUI

- Since ZLD4.35, user can configure the speed and duplex mode of the Ethernet port on GUI
 - **Configuration > Network > Interface > Port > Port Configuration**

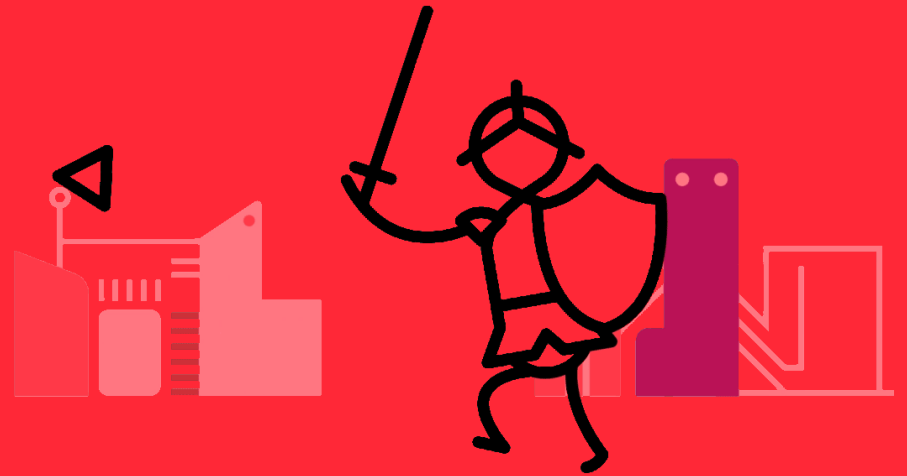


Port	Ethernet	PPP	Cellular	Tunnel	VLAN	Bridge	VTI	Trunk
Port Group	Port Configuration							
Configuration								
 Edit								
Name	Interface	Type	Settings	Status				
P1	ge1	Fiber	Auto Negotiate	Down				
P2	ge2	Copper	Auto Negotiate	100M/Full				
P3	ge3	Copper	Auto Negotiate	1000M/Full				
P4	ge4	Copper	1000Mbps-Full Duplex	Down				
P5	ge5	Copper	100Mbps-Full Duplex	Down				
P6	ge6	Copper	10Mbps-Full Duplex	Down				
P7	ge7	Copper	10Mbps-Half Duplex	Down				
P8	ge8	Copper	Auto Negotiate	Down				
Page 1 of 1 Show 50 items Displaying 1 - 8 of 8								

Note: You can't configure the speed and duplex mode of the fiber port on the USG2200

SecuReporter Enhancements

09



2019 SecuReporter Release Plan

■ Available
■ Developing

June, 19

Oct, 19

Cloud

1.8 Major release

- Daily, Weekly, Monthly Report
- Log Download

2.0 Major release

- Sandboxing analytics
- Botnet filtering analytics
- IP Reputation analytics

Firmware

ATP ZLD4.33 P1

- Service Setting on Initial Setup Wizard

ZyWALL/USG/ATP ZLD4.35

- Log Selection to SecuReporter

SecuReporter Promotion for ZyWALL/USG Series

Aug,2019

Sept,2019

Oct,2019

Nov,2019~

Promotion Program

- To celebrate the 30th anniversary of Zyxel, we offer 13-months default SecuReporter license for all ZyWALL/USG models with ZLD4.32 or ZLD4.33 firmware
- Promotion Period: Aug, 5 to Oct, 31, 2019
- No expiration date for free license activation

Device Bundled

- From Nov, 1, 2019, 13-months default SecuReporter license is bundled into ZyWALL/USG after upgrading to ZLD4.35.
- Excluding ZyWALL/USG got the 13-months default license before

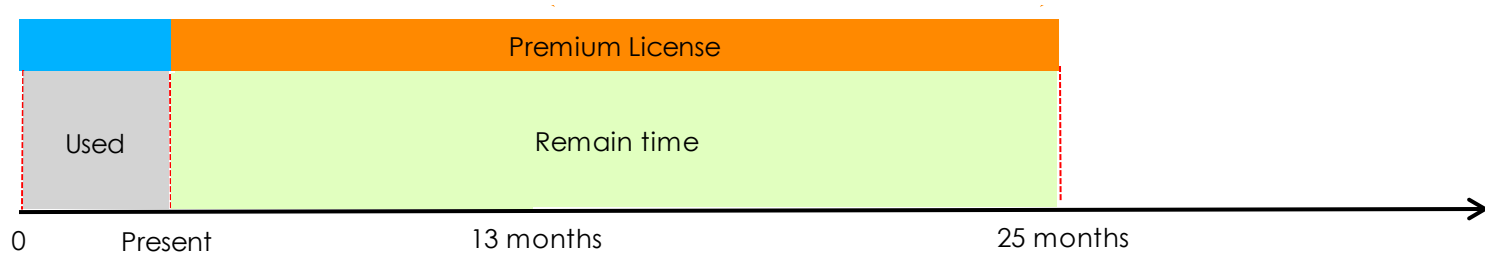
Default and Premium SecuReporter License

	Default License	Premium License
Service Period	13 months (396 days)	12 months (1 year license) 24 months (2 year license)
Grace period	0 day	15 days
Analytics	Last hour Last 24 hours Last 7 days	Last hour Last 24 hours Last 7 days Last 30 days*
Log download	Last 7 days	Last 1 year
Report	Daily report Weekly report	Daily report Weekly report Monthly report
Customized Report	No	Yes

*: The feature will be available in October

Upgrade Default License to Premium License

- Once user purchases and activates the premium license on ZyWALL/USG, the activated default license is automatically upgraded to premium license



ZYXEL

Your Networking Ally