ZYXEL NETWORKS

use-IP

ZyWALL ATP100/100W/200/500/700/800

ATP Firewall

Next-Gen Firewall for SMBs

The Zyxel ZyWALL Series is an Advanced Threat Protection Firewall dedicated for small and medium businesses, empowered by cloud intelligence to level up network protection, especially in tackling unknown threats. The ZyWALL ATP Firewall Series not only supports all Zyxel security service such as Web security, Application Security, Malware Blocker, Reputation Filter, etc., but also sandboxing and SecuReporter, and, last but not least, an infographic dashboard, delivering high performance and ensuring comprehensive protection as a self-evolving solution.

- Machine learning threat intelligence with global sync
- Sandboxing defeats unknown threats
- Hybrid scanning leveling up malware blocking
- High assurance multi-layered protection
- Reporting and analytics on cloud and device

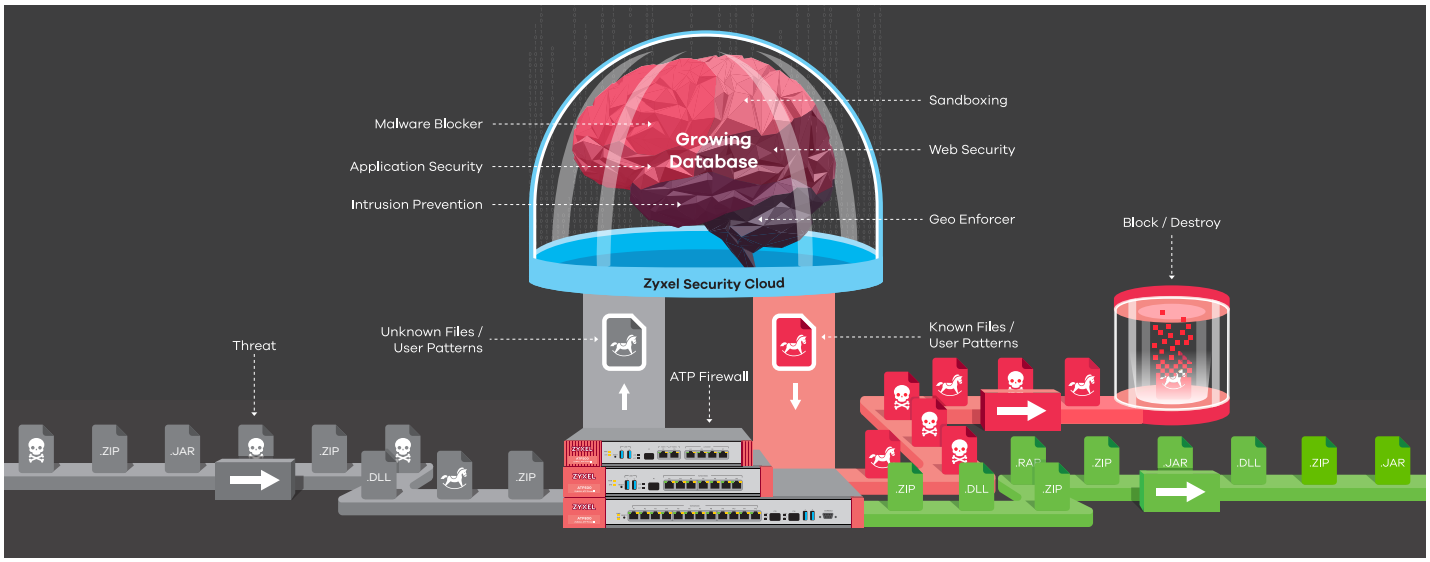
Benefits

Self-evolving cloud intelligence

Cloud intelligence receives all unknown files or user patterns from Zyxel ATP firewall's enquiry then identifies and archives inspection results by Threat Intelligence Machine Learning. It then pushes the most top-ranked threat signature into all ATP firewalls so that all ATP devices are all within the seamless defense shield against new unknown threats. With the real-time cloud-device synchronization, the cloud intelligence becomes a continuously-growing and self-evolving security defense ecosystem, adaptive to external attacks and also more importantly keeping all ATP firewalls in sync at all times.

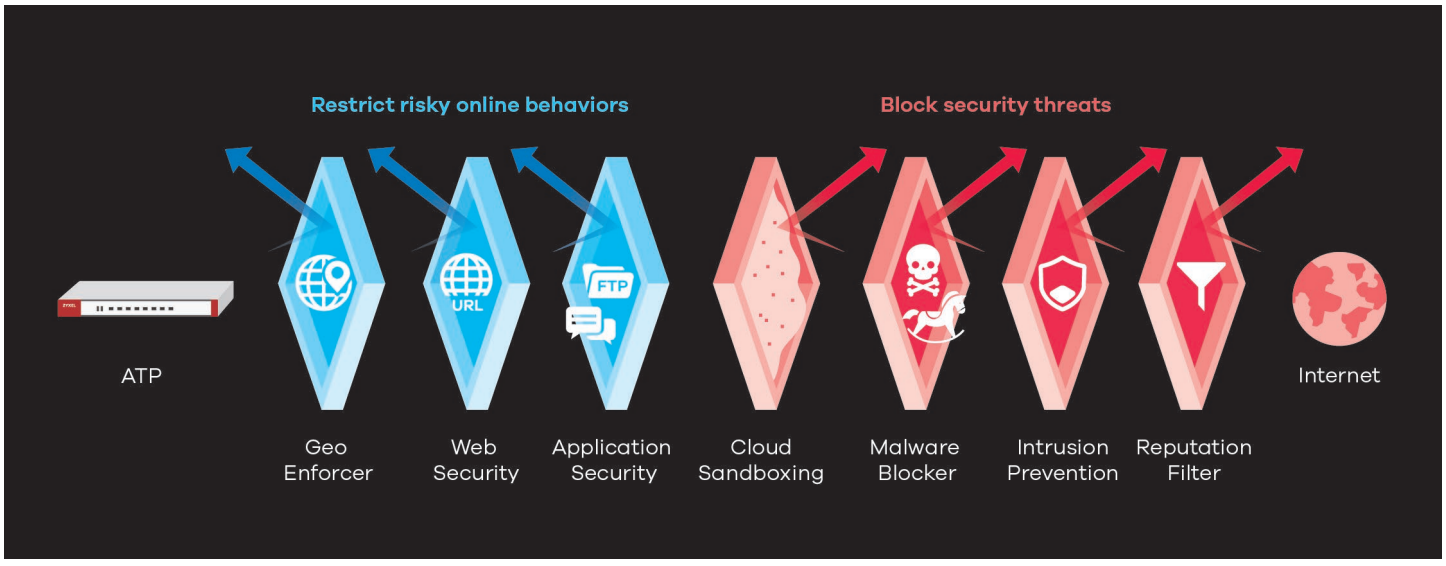
Sandboxing emulates unknown to known

Sandboxing is an isolated cloud environment to contain unknown files that cannot be identified by existing security service on device and to emulate those unknown files to identify whether they are malicious or not. Key values from sandboxing is to inspect packet behavior in isolation so the potential threat does not enter the network at all, and also to identify new malware types which the conventional static security mechanism may not detect. Cloud sandboxing with Zyxel ATP Firewall Series is preventive measure for zero-day attacks of all sorts.



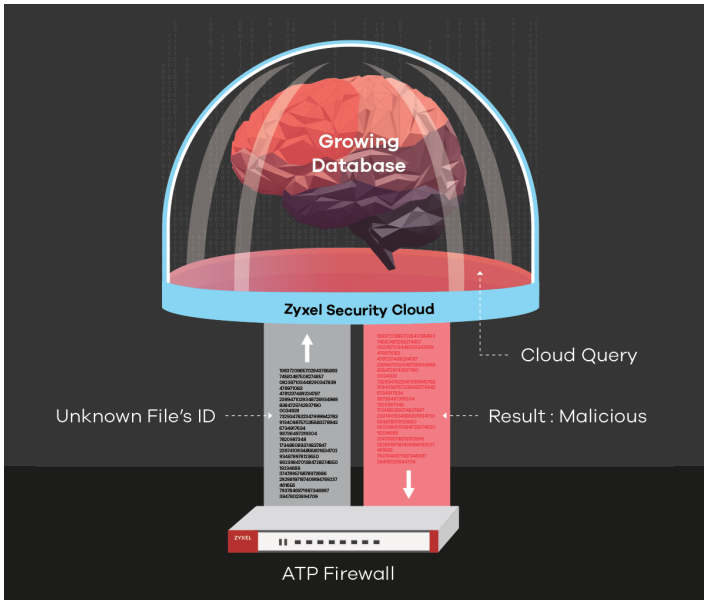
High assurance multi-layered protection

Traditionally a one-to-one solution is designed to stop a specific attack. Malware has evolved and is capable of approaching your networks in every stages of attack. This traditional protection inevitably fails. The ZyWALL ATP Firewall Series is designed with multi-layered protection to guard against threats with multiple vectors from in and out. It contains comprehensive security features like botnet filter, sandboxing, app patrol, content filtering, reputation filter, anti-malware, and IDP. As soon as your devices begin to get up and running, ATP firewalls are a sure way to start safeguarding your network without any unattended openings for attack.



Hybrid scanning leveling up malware blocking

ATP series not only supports a stream-based engine that scans files at the gateway for viruses and other threats but also runs cloud query simultaneously to leverage the multiple-sourced databases from Zyxel security cloud, a machine learning threat intelligence that can adapt to new unknown threats. This hybrid mode protection effectively maximizes malware detection rate without sacrificing throughput.



Reputation Filter preemptive IP/DNS/URL defense

Reputation Filter, consisting of IP Reputation, DNS Filter, and URL threat filter, matches up IP/domain/ URL addresses with the always-up-to-date cloud reputation database and determines if an address is reputable or not. This improves blocking efficiency, restricts access to malicious domain/ URL, and also blocks access from compromised sources, thus providing granular protection against ever-evolving cyber threats.

Web Security with optimized Content Filter

ATP Firewall delivers enhanced web filtering functionality and security through its powerful combination of reputation and category-based filtering. The dynamic content categorization analyzes the content of a previously unknown website and determines if it belongs to an undesirable category including gambling, pornography, games, and many others. CTIRU (Counter-Terrorism Internet Referral Unit) is included to restrict access to terrorism material online.*

Visualize unknown threat analytics and reports

ATP Firewall dashboard gives user-friendly traffic summary and threat statistic visuals. Utilize SecuReporter for a suite of analysis and reporting tools, including network security threats identification/analysis, security services, events, usage of the applications, websites, and traffic. Analyze sandboxing scanning activity details, show the top ranked botnet threat websites, and their types, while listing out which internal hosts are controlled. Provide analytics from reputation services - IP reputation, DNS Filter, and URL Threat Filter - to give full visibility on IP/URL/domain threat events.

*New Content Filter will be available in June 2020

Services and Licenses

The ZyWALL ATP Firewall Series provides a complete feature set to perfectly fit different business requirements as well as to enable the maximum performance and security with an all-in-one appliance. Comprehensive network modularity also empowers IT professionals to customize the system to meet their individual needs.

License Packs

License Service	Feature	ZyWALL ATP100/100W/200/500/700/800* Gold (1 Year/2 Years/4 Years)
Sandboxing	Sandboxing	Yes
Web Security	Content Filter	Yes
Application Security	App Patrol	Yes
	Email Security	Yes
Malware Blocker	Anti-Malware with Hybrid Mode	Yes
	Threat Intelligence Machine Learning	Yes
Intrusion Prevention	IDP	Yes
Reputation Filter	IP Reputation	Yes
	DNS Filter	Yes
	URL Threat Filter	Yes
Geo Enforcer	GeoIP	Yes
Managed AP Service[*1]	Wireless Controller	Unlock to max
SecuReporter	SecuReporter Premium	Yes

*: All ATP models are bundled with one-year Gold Security Pack by default, and this pack cannot be transferred.
*1: Gold Pack gives a year of unlocked managed AP nodes (24 APs for ATP100/100W, 40 APs for ATP200, 72 APs for ATP500, 264 APs for ATP700, 520 APs for ATP800), only 8 APs will be supported if it's no longer renewed.

Specifications

Model	ZyWALL ATP100	ZyWALL ATP100W	ZyWALL ATP200
Product photo			
Hardware Specifications			
10/100/1000 Mbps RJ-45 ports	4 x LAN/DMZ, 1 x WAN, 1 x SFP	4 x LAN/DMZ, 1 x WAN, 1 x SFP	4 x LAN/DMZ, 2 x WAN, 1 x SFP
USB 3.0 ports	1	1	2
Console port	RJ-45	RJ-45	DB9
Rack-mountable	-	-	Yes
Fanless	Yes	Yes	Yes
System Capacity & Performance*1			
SPI firewall throughput (Mbps)*2	1,000	1,000	2,000
VPN throughput (Mbps)*3	300	300	500
VPN IMIX Throughput (Mbps)*3	100	100	160
IDP throughput (Mbps)*4	600	600	1,200
AV throughput (Mbps)*4	380	380	630
UTM throughput (AV and IDP, Mbps)*4	380	380	600
Max. TCP concurrent sessions*5	300,000	300,000	600,000
Max. concurrent IPsec VPN tunnels*6	40	40	100
Concurrent SSL VPN users	30	30	60
VLAN interface	8	8	16
Speedtest Performance			
SPI firewall throughput (Mbps)*10	850	850	900
WLAN Management			
Managed AP number (default/max.)*7	8 / 24	8 / 24	8 / 40
Recommend max. AP in 1 AP Group	10	10	20
Security Services			
Sandboxing*7	Yes	Yes	Yes
Web Security*8	Yes	Yes	Yes
Application Security*7	Yes	Yes	Yes
Malware Blocker*7	Yes	Yes	Yes
Intrusion Prevention (IDP)*7	Yes	Yes	Yes
Geo Enforcer*7	Yes	Yes	Yes
Reputation Filter*7	Yes	Yes	Yes
SecuReporter Premium*7	Yes	Yes	Yes
Key Features			
VPN	IKEv2, IPSec, SSL, L2TP/IPSec	IKEv2, IPSec, SSL, L2TP/IPSec	IKEv2, IPSec, SSL, L2TP/IPSec
SSL (HTTPS) Inspection	Yes	Yes	Yes
2-Factor Authentication	Yes	Yes	Yes
Hotspot Management*7	-	-	-
Ticket printer support*9 / Support Q'ty (max.)	-	-	-
Microsoft Azure	Yes	Yes	Yes
Amazon VPC	Yes	Yes	Yes
Device HA Pro	-	-	-
Link Aggregation (LAG)	-	-	-

Model		ZyWALL ATP100	ZyWALL ATP100W	ZyWALL ATP200
Power Requirements				
Power input		12V DC, 2A max.	12V DC, 2A max.	12V DC, 2.5A max.
Max. power consumption (Watt Max.)		12.5	12.5	13.3
Heat dissipation (BTU/hr)		42.65	42.65	45.38
Physical Specifications				
Item	**Dimensions (WxDxH) (mm/in.)**	216 x 147.3 x 33/ 8.50 x 5.80 x 1.30	216 x 147.3 x 33/ 8.50 x 5.80 x 1.30	272 x 187 x 36/ 10.7 x 7.36 x 1.42
	Weight (kg/lb.)	0.85/1.87	0.85/1.87	1.4/3.09
Packing	**Dimensions (WxDxH) (mm/in.)**	284 x 190 x 100/ 11.18 x 7.48 x 3.94	284 x 190 x 100/ 11.18 x 7.48 x 3.94	427 x 247 x 73/ 16.81 x 9.72 x 2.87
	Weight (kg/lb.)	1.4/3.09	1.4/3.09	2.23 (W/O breacket) 2.42 (W/ breacket)
Included accessories		• Power adapter • RJ-45 - RS-232 cable for console connection	• Power adapter • RJ-45 - RS-232 cable for console connection	• Power adapter • Rack mounting kit
Environmental Specifications				
Operating environment	**Temperature**	0°C to 40°C/ 32°F to 104°F	0°C to 40°C/ 32°F to 104°F	0°C to 40°C/ 32°F to 104°F
	Humidity	10% to 90% (non-condensing)	10% to 90% (non-condensing)	10% to 90% (non-condensing)
Storage environment	**Temperature**	-30°C to 70°C/ -22°F to 158°F	- 30°C to 70°C/ - 22°F to 158°F	-30°C to 70°C/ -22°F to 158°F
	Humidity	10% to 90% (non-condensing)	10% to 90% (non-condensing)	10% to 90% (non-condensing)
MTBF (hr)		989,810.8	989,810.8	529,688.2
Acoustic noise		-	-	-
Certifications				
EMC		FCC Part 15 (Class B), CE EMC (Class B), BSMI	FCC Part 15 (Class B), CE EMC (Class B), BSMI	FCC Part 15 (Class B), CE (Class B), C-Tick (Class B), BSMI
Safety		LVD (EN60950-1), BSMI	LVD (EN60950-1), BSMI	LVD (EN60950-1), BSMI

Model	ZyWALL ATP500	ZyWALL ATP700	ZyWALL ATP800
Product photo			
Hardware Specifications			
10/100/1000 Mbps RJ-45 ports	7(Configurable), 1x SFP	12 (configuratble), 2x SFP (configurable)	12 (configuratble), 2x SFP (configurable)
USB 3.0 ports	2	2	2
Console port	DB9	DB9	DB9
Rack-mountable	Yes	Yes	Yes
Fanless	-	-	-
System Capacity & Performance*1			
SPI firewall throughput (Mbps)*2	2,600	6,000	8,000
VPN throughput (Mbps)*3	900	1,200	1,500
VPN IMIX Throughput (Mbps)*3	240	550	600
IDP throughput (Mbps)*4	1,700	2,200	2,700
AV throughput (Mbps)*4	900	1,600	2,000
UTM throughput (AV and IDP)*4	890	1,500	1,900
Max. TCP concurrent sessions*5	1,000,000	1,600,000	2,000,000
Max. concurrent IPSec VPN tunnels*6	300	1,000	1,000
Concurrent SSL VPN users	150	150	500
VLAN interface	64	128	128
Speedtest Performance			
SPI firewall throughput (Mbps)*10	900	930	930
WLAN Management			
Managed AP number (default/max.)*7	8 / 72	8 / 264	8 / 520
Recommend max. AP in 1 AP Group	60	200	300
Security Services			
Sandboxing*7	Yes	Yes	Yes
Web Security*8	Yes	Yes	Yes
Application Security*7	Yes	Yes	Yes
Malware Blocker*7	Yes	Yes	Yes
Intrusion Prevention (IDP)*7	Yes	Yes	Yes
Reputation Filter*7	Yes	Yes	Yes
Geo Enforcer*7	Yes	Yes	Yes
SecuReporter Premium*7	Yes	Yes	Yes
Key Features			
VPN	IKEv2, IPSec, SSL, L2TP/IPSec	IKEv2, IPSec, SSL, L2TP/IPSec	IKEv2, IPSec, SSL, L2TP/IPSec
SSL (HTTPS) Inspection	Yes	Yes	Yes
2-Factor Authentication	Yes	Yes	Yes
Hotspot Management*7	-	-	-
Ticket printer support*9 / Support Q'ty (max.)	-	-	-
Microsoft Azure	Yes	Yes	Yes
Amazon VPC	Yes	Yes	Yes
Device HA Pro	Yes	Yes	Yes
Link Aggregation (LAG)	Yes	Yes	Yes

Model		ZyWALL ATP500	ZyWALL ATP700	ZyWALL ATP800
Power Requirements				
Power input		12 V DC, 4.17 A	100-240V AC, 50/60Hz, 2.5A max.	100-240 V AC, 50/60 Hz, 2.5 A max.
Max. power consumption (watt)		24.1	46	46
Heat dissipation (BTU/hr)		82.23	120.1	120.1
Physical Specifications				
Item	**Dimensions (WxDxH) (mm/in.)**	300 x 188 x 44/ 11.81 x 7.4 x 1.73	430 x 250 x 44/ 16.93 x 9.84 x 1.73	430 x 250 x 44/ 16.93 x 9.84 x 1.73
	Weight (kg/lb.)	1.65/3.64	3.3/7.28	3.3/7.28
Packing	**Dimensions (WxDxH) (mm/in.)**	351 x 152 x 245/ 13.82 x 5.98 x 9.65	519 x 392 x 163/ 20.43 x 15.43 x 6.42	519 x 392 x 163/ 20.43 x 15.43 x 6.42
	Weight (kg/lb.)	2.83/6.24	4.8/10.58	4.8/10.58
Included accessories		• Power adapter • Power cord • Rack mounting kit	• Power cord • Rack mounting kit	• Power cord • Rack mounting kit
Environmental Specifications				
Operating environment	**Temperature**	0°C to 40°C/ 32°F to 104°F	0°C to 40°C / 32°F to 104°F	0°C to 40°C/ 32°F to 104°F
	Humidity	10% to 90% (non-condensing)	10% to 90% (non-condensing)	10% to 90% (non-condensing)
Storage environment	**Temperature**	-30°C to 70°C/ -22°F to 158°F	- 30°C to 70°C / - 22°F to 158°F	-30°C to 70°C/ -22°F to 158°F
	Humidity	10% to 90% (non-condensing)	10% to 90% (non-condensing)	10% to 90% (non-condensing)
MTBF (hr)		529,688.2	947,736	947,736
Acoustic noise		24.5dBA on <25°C Operating Temperature, 41.5dBA on full FAN speed	25.3dBA on <25°C Operating Temperature 46.2dBA on full FAN speed	25.3dBA on <25°C Operating Temperature 46.2dBA on full FAN speed
Certifications				
EMC		FCC Part 15 (Class A), CE EMC (Class A), C-Tick (Class A), BSMI	FCC Part 15 (Class A), CE EMC (Class A), C-Tick (Class A), BSMI	FCC Part 15 (Class A), CE EMC (Class A), C-Tick (Class A), BSMI
Safety		LVD (EN60950-1), BSMI	LVD (EN60950-1), BSMI	LVD (EN60950-1), BSMI

*: This matrix with firmware ZLD4.60 or later.
*1: Actual performance may vary depending on system configuration, network conditions, and activated applications.
*2: Maximum throughput based on RFC 2544 (1,518-byte UDP packets).
*3: VPN throughput measured based on RFC 2544 (1,424-byte UDP packets); IMIX: UDP throughput based on a combination of 64 byte, 512 byte and 1424 byte packet sizes.
*4: AV (with Express mode) and IDP throughput measured using the industry standard HTTP performance test (1,460-byte HTTP packets). Testing done with multiple flows.
*5: Maximum sessions measured using the industry standard IXIA IxLoad testing tool.
*6: Including Gateway-to-Gateway and Client-to-Gateway.
*7: With Zyxel service license to enable or extend the feature capacity.
*8: SafeSearch function in CF need to enable SSL inspection firstly and not for small business models.
*9: With Hotspot Management license support.
*10: The Speedtest result is conducted with 1Gbps WAN link in real world and it is subject to fluctuate due to quality of the ISP link.

Wireless Specifications

Model		ZyWALL ATP100W
Standard compliance		802.11 a/b/g/n/ac
Wireless frequency		2.4 / 5 GHz
Radio		2
SSID number		8
Maximum transmit power (Max. total channel)	**US (FCC) 2.4 GHz**	25 dBm, 3 antennas
	US (FCC) 5 GHz	25 dBm, 3 antennas
	EU (ETSI) 2.4 GHz	20 dBm(EIRP), 3 antennas
	EU (ETSI) 5 GHz	20 dBm(EIRP), 3 antennas
No. of antenna		3 detachable antennas
Antenna gain		2 dBi @2.4 GHz 3 dBi @ 5 GHz
Data rate		802.11n: up to 450 Mbps 802.11ac: up to 1300 Mbps
Frequency Band	**2.4 GHZ (IEEE 802.11 b/g/n)**	USA (FCC) : 2.412 to 2.462 GHz Europe (ETSI) : 2.412 to 2.472 GHz TWN (NCC) : 2.412 to 2.462 GHz
	5 GHZ (IEEE 802.11 a/n/ac)	USA (FCC) : 5.150 to 5.250 GHz; 5.250 to 5.350 GHz; 5.470 to 5.725 GHz; 5.725 to 5.850 GHz Europe (ETSI) : 5.15 to 5.35 GHz; 5.470 to 5.725 GHz TWN (NCC) :5.15 to 5.25 GHz; 5.25 to 5.35 GHz; 5.470 to 5.725 GHz; 5.725 to 5.850 GHz
Receive sensitivity	**2.4 GHZ**	11 Mbps ≤ -87 dBm 54 Mbps ≤ -77 dBm HT20 ≤ -71 dBm HT40 ≤ -68 dBm
	5 GHZ	54 Mbps ≤ -74 dBm HT40, MCS23 ≤ -68 dBm VHT40, MCS9 ≤ -62 dBm HT20, MCS23 ≤ -71 dBm VHT20, MCS8 ≤ -66 dBm VHT80, MCS9 ≤ -59 dBm

Software Features

Security Service

Firewall

- ICSA-certified corporate firewall
- Routing and transparent (bridge) modes
- Stateful packet inspection
- User-aware policy enforcement
- SIP/H.323 NAT traversal
- ALG support for customized ports
- Protocol anomaly detection and protection
- Traffic anomaly detection and protection
- Flooding detection and protection
- DoS/DDoS protection

Unified Security Policy

- Unified policy management interface
- Support Content Filtering, Application Patrol, firewall (ACL/SSL)
- Policy criteria: zone, source and destination IP address, user, time

Intrusion Detection and Prevention (IDP)

- Routing and transparent (bridge) mode
- Signature-based and behavior based scanning
- Customized signatures supported
- Automatic signature updates

Application Patrol

- Granular control over the most important applications
- Identifies and controls application behavior
- Supports 30+ application categories
- Supports user authentication
- Real-time statistics and reports

Sandboxing

- Cloud-based multi-engine inspection
- Support HTTP/SMTP/POP3/FTP
- Wild range file type examination
- Real-time threat synchronization

Anti-Malware

- Stream-based scan engine (Stream Mode)
- HTTP, FTP, SMTP, and POP3 protocol supported
- No file size limitation
- Automatic signature updates

Hybrid Mode Malware Scanning

- Both stream-based engine and cloud query concurrently in action
- Works with local cache and over 30 billion databases and growing
- HTTP, HTTPS, and FTP protocol supported
- Multiple file types supported

E-mail Security

- Transparent mail interception via SMTP and POP3 protocols
- Spam, Phishing, mail detection
- Blacklist and whitelist support
- Supports DNSBL checking

IP Reputation Filter

- IP-based reputation filter
- Supports 10 Cyber Threat Categories
- Supports external IP blacklist
- Inbound & Outbound traffic filtering
- Blacklist and whitelist support

DNS Filter

- Block clients to access malicious domain
- Effective against any IP protocol

URL Threat Filter

- Botnet C&C websites blocking
- Malicious URL blocking
- Supports External URL blacklist

Content Filtering

- HTTPs domain filtering
- SafeSearch support
- Whitelist websites enforcement
- URL blacklist and whitelist with keyword blocking
- Customizable warning messages and redirect URL
- Customizable Content Filtering block page
- URL categories increased to 111
- CTIRU (Counter-Terrorism Internet Referral Unit) support

Geo Enforcer

- Geo IP blocking
- Geographical visibility on traffics statistics and logs
- IPv6 address support

IP Exception

- Provides granular control for target source and destination IP
- Supports security service scan bypass for Anti-malware (including Sandboxing), IDP, IP Reputation, and URL Threat Filter

VPN

IPSec VPN

- Key management: IKEv1 (x-auth, mode-config), IKEv2 (EAP, configuration payload)
- Encryption: DES, 3DES, AES (256-bit)
- Authentication: MD5, SHA1, SHA2 (512-bit)
- Perfect forward secrecy (DH groups) support 1, 2, 5, 14, 15-18, 20-21
- PSK and PKI (X.509) certificate support
- IPSec NAT traversal (NAT-T)
- Dead Peer Detection (DPD) and relay detection
- VPN concentrator
- Route-based VPN Tunnel Interface (VTI)
- VPN high availability (Failover, LB)
- GRE over IPSec
- NAT over IPSec
- L2TP over IPSec
- Zyxel VPN client provisioning
- Support iOS L2TP/IKE/IKEv2 VPN client provision

SSL VPN

- Supports Windows and Mac OS X
- Supports full tunnel mode
- Supports 2-Factor authentication

Networking

WLAN Management

- Supports AP Controller (APC) version 3.60
- 802.11ax Wi-Fi 6 AP and WPA3 support
- 802.11k/v/r support
- Wireless L2 isolation
- Supports auto AP FW update
- Scheduled WiFi service
- Dynamic Channel Selection (DCS)
- Client steering for 5 GHz priority and sticky client prevention
- Auto healing
- Customizable captive portal page
- WiFi Multimedia (WMM) wireless QoS
- CAPWAP discovery protocol
- Multiple SSID with VLAN
- Supports ZyMesh
- Support AP forward compatibility
- Rogue AP Detection

Mobile Broadband
- WAN connection failover via 3G and 4G* USB modems
- Auto fallback when primary WAN recovers

IPv6 Support
- Dual stack
- IPv4 tunneling (6rd and 6to4 transition tunnel)
- SLAAC, static IP address
- DNS, DHCPv6 server/client
- Static/Policy route
- IPSec (IKEv2 6in6, 4in6, 6in4)

Connection
- Routing mode, bridge mode and hybrid mode
- Ethernet and PPPoE
- NAT and PAT
- NAT Virtual Server Load Balancing
- VLAN tagging (802.1Q)
- Virtual interface (alias interface)
- Policy-based routing (user-aware)
- Policy-based NAT (SNAT)
- GRE
- Dynamic routing (RIPv1/v2 and OSPF, BGP)
- DHCP client/server/relay
- Dynamic DNS support
- WAN trunk for more than 2 ports
- Per host session limit
- Guaranteed bandwidth
- Maximum bandwidth
- Priority-bandwidth utilization
- Bandwidth limit per user
- Bandwidth limit per IP
- Bandwidth management by application
- Link Aggregation support*1

Management

Authentication
- Local user database
- External user database: Microsoft Windows Active Directory, RADIUS, LDAP
- IEEE 802.1x authentication
- Captive portal Web authentication
- XAUTH, IKEv2 with EAP VPN authentication
- IP-MAC address binding
- SSO (Single Sign-On) support
- Supports 2-factor authentication with Google Authenticator as the second factor for administrator account

System Management
- Role-based administration
- Multi-lingual Web GUI (HTTPS and HTTP)
- Command line interface (console, web console, SSH and telnet)
- SNMP v1, v2c, v3
- System configuration rollback
- Configuration auto backup
- Firmware upgrade via FTP, FTP-TLS and Web GUI
- New firmware notify and auto upgrade
- Dual firmware images
- Cloud CNM SecuManager

Logging and Monitoring
- Comprehensive local logging
- Syslog (to up to 4 servers)
- Email alerts (to up to 2 servers)
- Real-time traffic monitoring
- Built-in daily report
- Cloud CNM SecuReporter

*: For specific models supporting the 3G and 4G dongles on the list, please refer to the Zyxel product page at 3G dongle document

*1: Supported models ATP500/700/800

Access Point Compatibility List

Product	Unified AP		Unified Pro AP	
Models	• NWA5301-NJ • NWA5121-NI • NWA5123-AC HD • NWA5123-AC • NWA5123-NI	• WAC5302D-S • WAX510D • WAC5302D-Sv2* • WAC500* • WAC500H*	• WAC6103D-I • WAC6503D-S • WAC6502D-S • WAC6303D-S • WAC6553D-E	• WAC6552D-S • WAC6502D-E • WAX650S • WAX610D*
Functions				
Central management	Yes		Yes	
Auto provisioning	Yes		Yes	
Data forwarding	Local bridge		Local bridge/Data tunnel	
ZyMesh	Yes		Yes	

*: From APC3.0, commercial gateways supporting APC technology are able to recognize APs with FW release higher than APC3.0 as Forward Compatible APs. Resellers can introduce newly-available Zyxel APs with basic features supported without upgrading any new controller firmware.

Accessories

SecuExtender Software

Item	Description	Supported OS
IPSec VPN Client*	IPSec VPN client software for the ZyWALL and USG Series with Easy VPN for zero configuration remote access	• Windows Server 2016 • Windows Server 2019 • Windows 7 (32/64-bit) • Windows 8 (32/64-bit) • Windows 10 (32/64-bit)
SSL VPN Client*	Secured VPN connection between PC/MAC and ZyWALL Firewall	• Windows 7 (32/64-bit) • Windows 8 (32/64-bit) • Windows 10 (32/64-bit) • MacOS 10.14

*: A 30-day trial version of IPSec VPN client and SSL VPN client for MAC OS can be downloaded from official Zyxel website. To continue using the application, please contact your regional sales representatives and purchase a commercial license for the application.

Transceivers (Optional)

Model	Speed	Connector	Wavelength	Max. Distance	Optical Fiber Type	DDMI
SFP10G-SR*	10-Gigabit SFP+	Duplex LC	850 nm	300 m/ 328 yd	Multi Mode	Yes
SFP10G-LR*	10-Gigabit SFP+	Duplex LC	1310 nm	10 km/ 10936 yd	Single Mode	Yes
SFP-1000T	Gigabit	RJ-45	-	100 m/ 109 yd	Multi Mode	-
SFP-LX-10-D	Gigabit	LC	1310 nm	10 km/ 10936 yd	Single Mode	Yes
SFP-SX-D	Gigabit	LC	850 nm	550 m/ 601 yd	Multi Mode	Yes
SFP-BX1310-10-D*[1]	Gigabit	LC	1310 nm(TX) 1490 nm(RX)	10 km/ 10936 yd	Single Mode	Yes
SFP-BX1490-10-D*[1]	Gigabit	LC	1490 nm(TX) 1310 nm(RX)	10 km/ 10936 yd	Single Mode	Yes

*:only USG2200-VPN supports 10-Gigabit SFP+
*1: SFP-BX1310-10-D and SFP-BX1490-10-D are must used in pairs.

For more product information, visit us on the web at www.zyxel.com