ZYXEL
NETWORKS

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

ATP Firewall

Next-Gen Firewall for SMBs

The Zyxel ZyWALL ATP series is an Advanced Threat Protection Firewall dedicated to small and medium businesses, empowered by cloud intelligence leveling up network protection, especially in tackling unknown threats. The series does not only support all Zyxel security services such as Web Filtering, Application Patrol, Anti-Malware, Reputation Filter, etc. but also Sandboxing and SecuReporter. An infographic dashboard is also included, delivering high performance and ensuring comprehensive protection as a self-evolving solution.

Nebula Together

With the newest addition to the Nebula cloud management family, ATP firewalls strongly empower the full-blown Zyxel security matrix in Nebula, further optimize Nebula with holistic security and protection for SMB business networks. Zyxel provides a centralized provisioning security policy to the remote workforce from Nebula and traffic shaping eliminates the network bottleneck to fuel the best business productivity.

- Sandboxing defeats unknown threats
- Flexible to adapt to On Premises or Nebula cloud
- High assurance multi-layered protection
- Device Insight provides better visibility and control
- CDR contains threats at the network edge
- Secure WiFi guarantees remote work security
- Analytics report and enhanced insights

ATP
Uncompromising and Unifying Network Protection

2022 Computing Security Awards
FINALIST

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

ATP Firewall is designed with multi-layer protection against multiple types of threats from inside and out. Sandboxing, Anti-Malware, Reputation Filter, and Intrusion Prevention block external attacks while Application Patrol and Web Filtering empower you to restrict users' inappropriate application usage or web access. Together, they safeguard your network without any unattended gaps. By boarding the Nebula cloud, the provisioning profiles and settings can be quickly configured to managed devices as required. The firewall policies will be provisioned and synchronized in minutes across multiple sites.

Deep insight into all your device

Device insight gives you more visibility of your networks including wired, wireless, BYOD, and IoT devices. You can create access policy with device contextual such as OS version or device category to enforce network segmentation. This reduces the attack surface and prevents threats from spreading. It also helps SMB(s) reduce time spent on investigation. Continuing with our goal of providing our customers with increased visibility, Zyxel SecuReporter gives your organization comprehensive endpoint inventory dashboard.

Comprehensive Web Filtering service

ATP Firewall delivers enhanced web filtering functionality and security through its powerful combination of both reputation and category-based filtering. The dynamic content categorization analyzes the content of a previously unknown website and domain and determines if it belongs to an undesirable category including gambling, pornography, games, and many others. A newly added DNS Content Filter offers a better approach to inspect web access, particularly when the website is deploying ESNI (Encrypted Server Name Indication) where the traditional URL filtering failed to identify the destination domain.

Preemptive IP/DNS/URL defense

Reputation Filter, consisting of IP Reputation, DNS Threat 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 IP/domain/URL, and blocks access from compromised sources, thus providing granular protection against ever-evolving cyber threats. The ATP series now supports monitoring or blocking the use of DoH/DoT for better managing internet activities.

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.

Secure WiFi guarantees remote work security

Businesses striking a balance on productivity and security protection becomes a priority with growing number of devices. Whether it is a wired, wireless, or a IoT device, the Secure WiFi service is used to build a secure L2 tunnel for Work-From-Home user to extend the working experience easily and securely, as if you were in the office with the safety of both two-factor authentication and secure tunnel, which boosts up productivity and eases IT support. The Secure WiFi service also unlocks the number of managed APs to maximum for the ATP firewall.

Stay Ahead of the Threats with CDR

Collaborative Detection & Response (CDR) is used to identify threats and risks posed in the more complex organization workforce, workload, and workplace. ATP firewalls to Nebula provides network admins with a rule-based security policy. The firewalls detect a threat on any of the connected clients and will sync with the Nebula control center, then automatically respond to cyber threats and contain the device(s) at the edge (Wireless Access Point) of your network. It is a perfect fit for IT to address the requirements of a decentralized network infrastructure and provide automatic protection.

Analytics report and enhanced insights

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 Threat Filter, and URL Threat Filter - to give full visibility on IP/URL/domain threat events.

Services and Licenses

ATP Firewall series are bundled with a one-year Gold Security Pack license by default. For the second year, you can choose either a monthly or yearly automatic renewal subscription, which provides continuous protection for your networks without interruption and no need to manually extend your subscription.

Licensed Service	Feature	ZyWALL ATP100/100W/200/500/700/800*
		Gold Security Pack (1 Year/2 Years/4 Years)
Web Filtering	Content Filter	Yes
App Patrol	Application visibility and control	Yes
Email Security*1	Anti-Spam	Yes
Anti-Malware	Anti-Malware with Hybrid Mode	Yes
	Threat Intelligence Maching Learing	Yes
IPS	Intrusion Detection & Prevention	Yes
Reputation Filter	IP Reputation	Yes
	DNS Threat Filter	Yes
	URL Threat Filter	Yes
Sandboxing	Sandboxing	Yes
SecuReporter	SecuReporter	Yes
Secure WiFi	Secure Tunnel for Remote AP	Yes
	Managed AP Service*1	Unlock to Max
CDR	Collaborative Detection & Response	Yes
Network Premium	Single Sign-On	Yes
Security Profile Sync*1	Sync up security profiles across networks	Yes
Nebula Professional Pack*1	Cloud Networking Management	Yes

* All ATP models are bundled with one-year Gold Security Pack by default, and this pack can be renewed.
*1: Gold Pack gives a year of unlocked managed AP nodes (24 APs for ATP100/100W, 40 APs for ATP200, 264 APs for ATP500, 264 APs for ATP700, 520 APs for ATP800). only 8 APs will be supported if it's no longer renewed.
*2: Only supported in Nebula cloud mode.
*3: Only supported in On-Premise mode.

Specifications

Model		ZyWALL ATP100**	ZyWALL ATP100W	ZyWALL ATP200
Product photo				
Hardware Specifications				
Interface		3 x LAN/DMZ, 1 x WAN, 1x OPT	3 x LAN/DMZ, 1 x WAN, 1 x SFP, 1x OPT	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
IPS throughput (Mbps)*4		600	600	1,200
Anti-malware 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		50	50	100
Recommended gateway-to-gateway IPsec VPN tunnels		20	20	50
Concurrent SSL VPN users		30	30	60
VLAN interface		8	8	16
Speedtest Performance				
SPI firewall throughput (Mbps)*7		850	850	900
Key Features				
Security Service	Sandboxing*8	Yes	Yes	Yes
	Web Filtering*8	Yes	Yes	Yes
	Application Patrol*8	Yes	Yes	Yes
	Anti-Malware*8	Yes	Yes	Yes
	IPS*8	Yes	Yes	Yes
	Reputation Filter*8	Yes	Yes	Yes
	Geo Enforcer	Yes	Yes	Yes
	SecuReporter*9	Yes	Yes	Yes
	Collaborative Detection & Response*8	Yes	Yes	Yes
	Device Insight	Yes	Yes	Yes
	Security Profile Sync*9	Yes	Yes	Yes
	SSL (HTTPS) Inspection	Yes	Yes	Yes
	2-Factor Authentication	Yes	Yes	Yes
VPN Features	VPN	IKEv2, IPSec, SSL, L2TP/IPSec	IKEv2, IPSec, SSL, L2TP/IPSec	IKEv2, IPSec, SSL, L2TP/IPSec
	Microsoft Azure	Yes	Yes	Yes
	Amazon VPC	Yes	Yes	Yes

Model		ZyWALL ATP100	ZyWALL ATP100W	ZyWALL ATP200
Key Features				
WLAN Management	Default number of managed AP	8	8	8
	Recommend max. AP in 1 AP Group	10	10	20
	Secure WiFi Service*1	Yes	Yes	Yes
	Maximum Number of Tunnel-Mode AP	6	6	10
	Maximum Number of Managed AP	24	24	40
Management & Connectivity	Nebula Cloud Mode	Yes	Yes	Yes
	Nebula Cloud Monitoring Mode	Yes	Yes	Yes
	Device HA Pro	-	-	-
	Link Aggregation (LAG)	-	-	-
	Concurrent devices logins (max.)	64	64	200
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	2.42/5.34
Included accessories		• Power adapter • RJ-45 cable • RS-232 cable	• Power adapter • RJ-45 cable • RS-232 cable	• 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	989,810	529,688
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				
Interface		7 (configurable), 1x SFP	12 (configurable), 3.1.3 2x SFP (configurable)	12 (configurable), 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 3.1.2	8,000
VPN throughput (Mbps)*3		900	1,200	1,500
IPS throughput (Mbps)*4		1,700	2,200	2,700
Anti-malware throughput (Mbps)*5		900	1,600	2,000
UTM throughput (AV and IDP, Mbps)*6		890	1,500	1,900
Max. TCP concurrent sessions*7		1,000,000	1,600,000	2,000,000
Max. concurrent IPsec VPN tunnels*8		300	500	1,000
Recommended gateway-to-gateway IPsec VPN tunnels		150	300	500
Concurrent SSL VPN users		150	150	500
VLAN Interface		64	128	128
Speedtest Performance				
SPI firewall throughput (Mbps)*9		900	930	930
Key Features				
Security Service	Sandboxing*10	Yes	Yes	Yes
	Web Filtering*10	Yes	Yes	Yes
	Application Patrol*10	Yes	Yes	Yes
	Anti-Malware*10	Yes	Yes	Yes
	IPS*10	Yes	Yes	Yes
	Reputation Filter*10	Yes	Yes	Yes
	Geo Enforcer	Yes	Yes	Yes
	SecuReporter*11	Yes	Yes	Yes
	Collaborative Detection & Response*10	Yes	Yes	Yes
	Device Insight	Yes	Yes	Yes
	Security Profile Sync*10	Yes	Yes	Yes
	SSL (HTTPS) Inspection	Yes	Yes	Yes
	2-Factor Authentication	Yes	Yes	Yes
VPN Features	VPN	IKEv2, IPSec, SSL, L2TP/IPSec	IKEv2, IPSec, SSL, L2TP/IPSec	IKEv2, IPSec, SSL, L2TP/IPSec
	Microsoft Azure	Yes	Yes	Yes
	Amazon VPC	Yes	Yes	Yes
WLAN Management	Default number of managed AP	8	8	8
	Recommend max. AP in 1 AP Group	60	200	300

บริษัท เจเนซิส ไฮเทค จำกัด
GENESIS HI-TECH CO.,LTD.

Model		ZyWALL ATP500	ZyWALL ATP700	ZyWALL ATP800
Key Features				
WLAN Management	Secure WiFi Service*5	Yes	Yes	Yes
	Maximum Number of Tunnel-Mode AP	18	66	130
	Maximum Number of Managed AP	72	264	520
Management & Connectivity	Nebula Cloud Mode	Yes	Yes	Yes
	Nebula Cloud Monitoring Mode	Yes	Yes	Yes
	Device HA Pro	Yes	Yes 3.1.10	Yes
	Link Aggregation (LAG)	Yes	Yes	Yes
	Concurrent devices logins (max.)	300	1500	1500
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	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

*1: This matrix with firmware ZLD5.37 or later.
*2: Actual performance may vary depending on system configuration, network conditions, and activated applications.
*3: Maximum throughput based on RFC 2544 (1,518-byte UDP packets).
*4: VPN throughput measured based on RFC 2544 (1,424-byte UDP packets).
*5: Anti-malware (with Express mode) and IPS throughput measured using the industry standard HTTP performance test (1,460-byte HTTP packets). Testing done with multiple flows.
*6: Maximum sessions measured using the industry standard IXIA IxLoad testing tool.
*7: Including Gateway-to-Gateway and Client-to-Gateway.
*8: 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.
*9: Enable or extend feature capacity with Zyxel service license.
*10: ATP100 rev1 is adopting new hardware design equipped with 4 x LAN/DMZ, 1 x WAN.

Wireless Specifications

Model		ZyWALL ATP100W
Standard compliance		802.11 a/b/g/n/ac
Wireless frequency		2.4 / 5 GHz
Radio		2
SSID number		4
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		2.4 GHz: up to 300 Mbps 5 GHz: up to 866 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

- Routing and transparent (bridge) modes
- Stateful packet inspection
- SIP NAT traversal
- H.323 NAT traversal*1
- 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)
- Firewall: SSL inspection*2
- Policy criteria: source and destination IP address, user group, time
- Policy criteria: zone, user*1

Intrusion Prevention System (IPS)

- Support both intrusion detection and prevention
- Support allowlist (whitelist) to deal with false positives involving known benign activity*3
- Support rate-based IPS signatures to protect networks against application-based DoS and brute force attacks*3
- Signature-based and behavior-based scanning
- Support exploit-based and vulnerability-based protection
- Support Web attacks like XSS and SQL injection
- Stream-based engine
- Support SSL inspection*2
- Inspection on various protocols: HTTP, FTP, SMTP, POP3, and IMAP
- Inspection on various protocols: HTTPs, FTPs, SMTPs, POP3s, and IMAPs*3
- Customizable signature & protection profile*3
- Automatic new signature update mechanism support

Application Patrol

- Smart single-pass scanning engine
- Identifies and control thousands of applications and their behaviors
- Identify, categorize and control over 3,000 apps and behaviors
- Granular control over the most popular applications

- Prioritize and throttle application bandwidth usage
- Real-time application statistics and reports
- Identify and control the use of DOH (DNS over HTTPS)

Sandboxing
- Cloud-based multi-engine inspection
- Support HTTP/SMTP/POP3/FTP
- Wild range file type examination
- Real-time threat synchronization
- SSL Inspection support*7

Anti-Malware
- High performance query-based scan engine (Express Mode)
- Works with over 30 billion of known malicious file identifiers and still growing
- Multiple file types supported
- Stream-based scan engine (Stream Mode)
- No file size limitation
- HTTP, FTP, SMTP, and POP3 protocol supported
- SSL inspection support*7
- Automatic signature update

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*7
- Transparent mail interception via SMTP and POP3 protocols
- Spam, Phishing, mail detection
- Black and Allow List support
- Supports DNSBL checking

IP Reputation Filter
- IP-based reputation filter
- Supports 10 Cyber Threat Categories
- Supports external IP blacklist
- Inbound & Outbound traffic filtering
- Block and Allow List support

DNS Threat Filter
- Block clients to access malicious domain
- Effective against any IP protocol
- Monitoring or blocking the use of DoH/DoT

URL Threat Filter
- Botnet C&C websites blocking
- Malicious URL blocking
- Supports External URL blocklist

Web Filtering
- HTTPs domain filtering
- SafeSearch support: Google, YouTube, and Microsoft Bing*7
- Allow List websites enforcement
- URL Block and Allow List 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
- Support DNS base filtering (domain filtering)

Geo Enforcer
- Geo IP blocking
- Geographical visibility on traffics statistics and logs
- IPv6 address support*7

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

Device Insight
- Agentless Scanning for discovery and classification of devicess
- View all devices on the network, including wired, wireless, BYOD, IoT, and SecuExtender (remote endpoint) on SecuReporter
- Visibility of network devices (switches, wireless access points, firewalls) from Zyxel or 3rd party vendors

Collaborative Detection & Response
- Support Alert/Block/Quarantine containment actions
- Prevent malicious wireless clients network access with blocking feature
- Customizable warning messages and redirect URL
- Bypass by IP or MAC address with exempt list

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*7
- NAT over IPSec
- L2TP over IPSec
- SecuExtender Zero Trust VPN Client provisioning
- Support native Windows, iOS/macOS and Android (StrongSwan) client provision*7
- Support 2FA Email/SMS*7
- Support 2FA Google Authenticator

SSL VPN*7
- Supports Windows and macOS
- Supports full tunnel mode
- Supports 2-Factor authentication

Networking

Secure WiFi
- Secure Tunnel for Remote AP
- L2 access between home office and HQ (Secured Tunnel)
- GRE Tunnel for Campus AP
- Enforcing 2FA with Google Authenticator
- WPA2 Enterprise (802.1x) supported
- Wireless Storm Control
- Applicable regardless of the On Premises/Nebula-managed mode

WLAN Management*7
- Supports AP Controller (APC) version 4.00
- 802.11ax Wi-Fi 6 AP and WPA3 support
- 802.11k/v/r support
- 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

Multi-WAN
- Multi-WAN support on ATP200 and above
- Dual-WAN support on ATP100/100W (with OPT port)

Mobile Broadband*1
- WAN connection failover via 3G and 4G* USB modems
- Auto fallback when primary WAN recovers

IPv6 Support*2
- Dual stack
- IPv4 tunneling (6rd and 6to4 transition tunnel) 3.1.9
- SLAAC, static IP address
- DNS, DHCPv6 server/client
- Static/Policy route
- IPSec IKEv2 6in6, 4in6, 6in4)

Connection
- Routing mode
- Bridge mode and hybrid mode*2
- Ethernet and PPPoE
- NAT and PAT 3.1.5
- NAT Virtual Server Load Balancing
- VLAN tagging (802.1Q)
- Virtual interface (alias interface)
- Policy-based routing (user-aware)*3
- Policy-based NAT (SNAT)
- GRE* 3.1.6
- Dynamic routing (RIPv1/v2 and OSPF, BGP)*2
- 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*3
- Bandwidth limit per IP
- Bandwidth management by application
- Link Aggregation support*1*2

Management

Nebula Cloud Mode
- Unlimited Registration & Central Management (Configuration, Monitoring, Dashboard, Location Map & Floor Plan Visual) of Nebula Devices
- Zero Touch Auto-Deployment of Hardware/Configuration from Cloud
- Over-the-air Firmware Management
- Central Device and Client Monitoring (Log and Statistics Information) and Reporting
- Security Profile Sync

Nebula Cloud Monitoring Mode
- Monitor device on/off status
- Firmware upgrade operation
- Manage firewall licenses
- Access remote GUI (requires Nebula Pro Pack)
- Backup and restore firewall configurations (requires Nebula Pro Pack)

Authentication
- Local user database
- Cloud user database*3
- 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*2
- Supports 2-factor authentication (Google Authenticator, SMS/Email)

System Management
- Role-based administration
- Multi-lingual Web GUI (HTTPS and HTTP) 3.1.7
- Command line interface (console, web console, SSH and telnet)*2
- SNMP v1, v2c, v3
- System configuration rollback*2
- Configuration auto backup*2
- Firmware upgrade via FTP, FTP-TLS and web GUI*2
- New firmware notify and auto upgrade
- Dual firmware images
- Cloud CNM SecuManager*3

Logging and Monitoring 3.1.8
- 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 ZyWall product page or 3G dongle document
*1: Supported models: ATP500/700/800
*2: Only supported in On Premises Mode
*3: Only supported in Nebula Cloud Mode

Access Point Compatibility List

Secure Tunnel for Remote AP

Product	Remote AP	Number of Tunnel Mode AP	Supported Remote AP
ATP	ATP100(W)	6	• WAX655E • WAX650S • WAX640S-6E • WAX630S • WAX620D-6E • WAX610D • WAX510D • WAC500 • WAC500H
	ATP200	10	
	ATP500	18	
	ATP700	66	
	ATP800	130	
USG FLEX	USG FLEX 100(AX/W)	6	
	USG FLEX 200	10	
	USG FLEX 500	18	
	USG FLEX 700	130	
VPN	VPN50	10	
	VPN100	18	
	VPN300	130	
	VPN1000	258	

Managed AP Service

Product	Unified AP		Unified Pro AP	
Models	• NWA5123-AC • NWA5123-AC HD*1 • WAC5302D-S • WAC5302D-Sv2	• WAX510D* • WAC500* • WAC500H* • WAX300H	• WAC6103D-I • WAC6503D-S • WAC6502D-S • WAC6303D-S • WAC6553D-E • WAC6552D-S • WAC6502D-E	• WAX655S • WAX630S • WAX610D • WAX640S-6E • WAX620D-6E • WAX655E
Functions				
Central management	Yes		Yes	
Auto provisioning	Yes		Yes	
Data forwarding	Local bridge		Local bridge / Data tunnel	
ZyMesh	Yes		Yes	

* Support both local bridge and data tunnel for data forwarding

Accessories

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	Single LC	1310 nm	10 km/ 10936 yd	Single Mode	Yes
SFP-SX-D	Gigabit	Single LC	850 nm	500 m/ 601 yd	Multi Mode	Yes
SFP-BX1310-10-D*1	Gigabit	Single LC	1310 nm(TX) 1490 nm(RX)	10 km/ 10936 yd	Single Mode	Yes
SFP-BX1490-10-D*1	Gigabit	Single LC	1490 nm(TX) 1310 nm(RX)	10 km/ 10936 yd	Single Mode	Yes

*only USG2200 Series supports 10-Gigabit SFP+
*1: SFP-BX1310-10-D & SFP-BX1490-10-D, SFP-BX1310-E & SFP-BX1550-E must be used in pairs

ZYXEL

Zyxel Security Gateway (Firewall) Attack Protection

Support Model: USG FLEX 100 / USG FLEX 200 / USG FLEX 500 / USG FLEX 700
ATP100 / ATP100W / ATP200 / ATP500 / ATP700 / ATP800

Firmware Version: ZLD 5.10 or above

Zyxel Security Gateway (Firewall) can support below attack type.

- ✓ Syn flood
- ✓ UDP flood
- ✓ ICMP flood
- ✓ IP Address Spoof
- ✓ IP Address Sweep 3.1.4
- ✓ Port Scan
- ✓ Dos or DDos
- ✓ Teardrop Attack
- ✓ Land Attack
- ✓ TCP Fragment
- ✓ ICMP Fragment

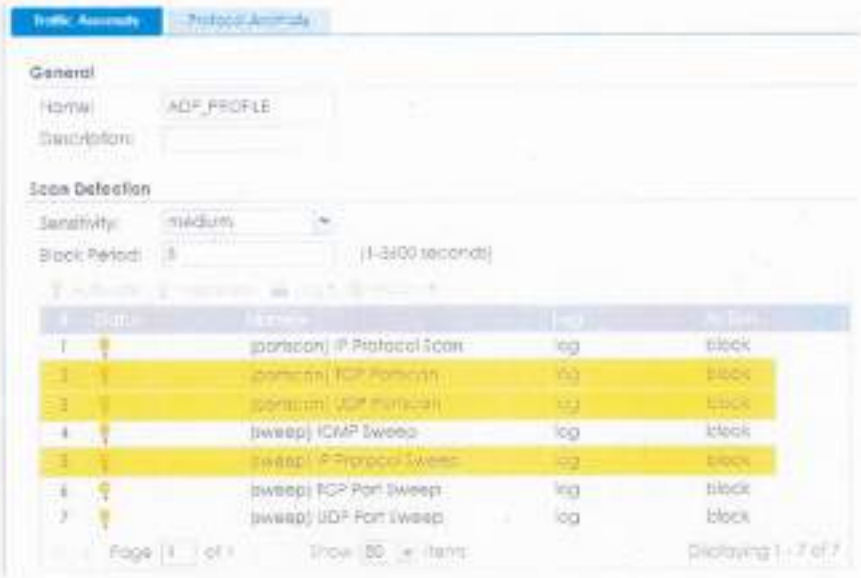
Security Policy >> ADP >> Traffic Anomaly

Flood Detection

- Syn flood or TCP flood
- UDP flood
- ICMP flood

Scan Detection

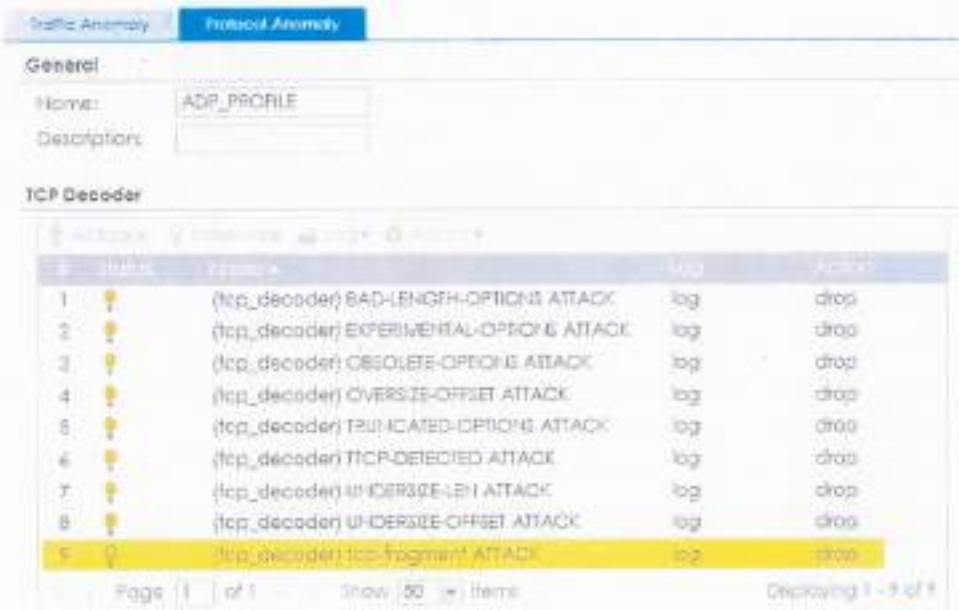
- IP Address Sweep
- Port Scan



Security Policy >> ADP >> Protocol Anomaly

TCP Decoder

- TCP Fragment

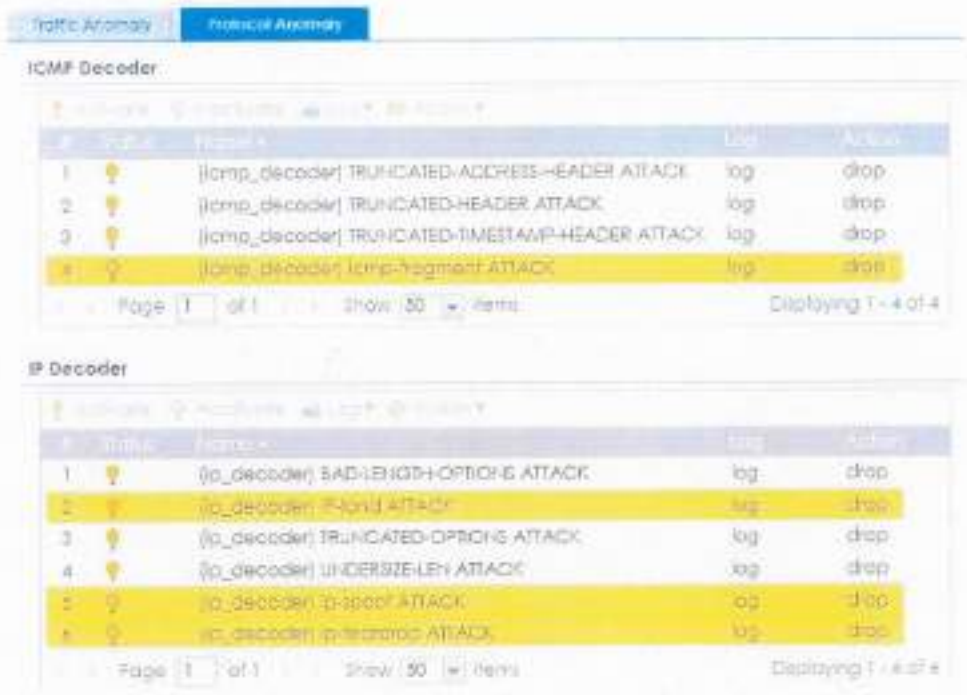


ICMP Decoder

- ICMP Fragment

IP Decoder

- IP Address Spoof
- Teardrop Attack
- Land Attack



[illegible] (Next Generation Firewall) [illegible] 1 [illegible]
User Service and Support ZyWALL ATP700 Enterprise Pack for all License and services [illegible] 1 [illegible]

[illegible]

No.		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
3		[illegible]				
3.1		[illegible] (Next Generation Firewall) [illegible] (License) [illegible]				
	3.1.1	[illegible] Firewall [illegible] Next Generation Firewall [illegible] Appliance	[illegible] Firewall [illegible] Next Generation Firewall [illegible] Appliance	[illegible]	DS_ZyWALL_ATP700_P.1	
	3.1.2	[illegible] Firewall Throughput [illegible] 3 Gbps	[illegible] Firewall Throughput [illegible] Gbps	[illegible]	DS_ZyWALL_ATP700_P.8	
	3.1.3	[illegible] (Network Interface) [illegible] 10/100/1000 Base-T [illegible]	[illegible] (Network Interface) [illegible] 10/100/1000 Base-T [illegible]	[illegible]	DS_ZyWALL_ATP700_P.8	[illegible] 1000Mb/s [illegible]
	3.1.4	[illegible] Syn Flood, UDP Flood, ICMP Flood, IP Address Spoofing, Port Scan, DoS or DDoS, Teardrop Attack, Land Attack, IP Fragment, ICMP Fragment [illegible]	[illegible] Syn Flood, UDP Flood, ICMP Flood, IP Address Spoofing, Port Scan, DoS or DDoS, Teardrop Attack, Land Attack, IP Fragment, ICMP Fragment [illegible]	[illegible]	DS_ZyWALL_ATP700_P.14	
	3.1.5	[illegible] IP Address [illegible] Service Port [illegible] Network Address Translation (NAT) [illegible] Port Address Translation (PAT) [illegible]	[illegible] IP Address [illegible] Service Port [illegible] Network Address Translation (NAT) [illegible] Port Address Translation (PAT) [illegible]	[illegible]	DS_ZyWALL_ATP700_P.12	
	3.1.6	[illegible] Routing [illegible] Static, Dynamic Routing [illegible]	[illegible] Routing [illegible] Static, Dynamic Routing [illegible]	[illegible]	DS_ZyWALL_ATP700_P.12	
	3.1.7	[illegible] HTTPS [illegible] SSH [illegible]	[illegible] HTTPS [illegible] SSH [illegible]	[illegible]	DS_ZyWALL_ATP700_P.12	
	3.1.8	[illegible] (Logging/Monitoring) [illegible] Syslog [illegible]	[illegible] (Logging/Monitoring) [illegible] Syslog [illegible]	[illegible]	DS_ZyWALL_ATP700_P.12	
	3.1.9	[illegible] IPv6 [illegible] Protocol [illegible]	[illegible] IPv6 [illegible]	[illegible]	DS_ZyWALL_ATP700_P.12	
	3.1.10	[illegible] High Availability [illegible] HA [illegible] (Next Generation Firewall) [illegible] ZyWALL ATP700 [illegible]	[illegible] High Availability [illegible] HA [illegible] (Next Generation Firewall) [illegible] ZyWALL ATP700 [illegible]	[illegible]	DS_ZyWALL_ATP700_P.5	
	3.1.11	[illegible]	[illegible]	[illegible]	[illegible]	
3.2		[illegible] (License) [illegible] ZyWALL ATP700 Enterprise Pack for all License and services [illegible] (Next Generation Firewall) [illegible] 1 [illegible]	[illegible] (License) [illegible] ZyWALL ATP700 Enterprise Pack for all License and services [illegible] (Next Generation Firewall) [illegible] 1 [illegible]	[illegible]		

บริษัท เจเนซิส ไฮเทค จำกัด
GENESIS HI-TECH CO.,LTD.

บริษัท เจเนซิส ไฮเทค จำกัด
GENESIS HI-TECH CO.,LTD.

[illegible] (Next Generation Firewall) [illegible] 1 [illegible]
และ Service and Support ZyWALL ATP700 Enterprise Pack for all License and services จำนวน 1 ระบบ

[illegible]

No.		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
4		[illegible]				
	4.1	[illegible] (License) [illegible] 3.1 [illegible]	[illegible] (License) [illegible] 3.1 [illegible]	[illegible]		
	4.2	[illegible] (License) [illegible] 3.2 [illegible]	[illegible] (License) [illegible] 3.2 [illegible]	[illegible]		
	4.3	[illegible] 3.1 [illegible] 3.2 [illegible] High Availability หรือ HA	[illegible] 3.1 [illegible] 3.2 [illegible] High Availability หรือ HA	[illegible]		
	4.4	[illegible] 4.1 [illegible] 4.2 [illegible] 4.3 [illegible] 60 [illegible]	[illegible] 4.1 [illegible] 4.2 [illegible] 4.3 [illegible] 60 [illegible]	[illegible]		
	4.5	[illegible] 1 [illegible] 4.4 [illegible]		[illegible]		
5		[illegible]				
	5.1	[illegible] 3.1 [illegible] 3 [illegible]	[illegible] 3.1 [illegible] 3 [illegible]	[illegible]		
	5.2	[illegible] (License) ของ ZyWALL ATP700 Enterprise Pack for all License and services [illegible] (Next Generation Firewall) [illegible] 3.2 [illegible] 1 [illegible]	[illegible] (License) ของ ZyWALL ATP700 Enterprise Pack for all License and services [illegible] (Next Generation Firewall) [illegible] 3.2 [illegible] 1 [illegible]	[illegible]		
6		[illegible]				
	6.1	[illegible]		[illegible]		
7		[illegible]				
	7.1	[illegible] 60 [illegible]	60 [illegible]	[illegible]		

บริษัท เจเนซิส ไฮเทค จำกัด
GENESIS HI-TECH CO.,LTD.

บริษัท เจเนซิส ไฮเทค จำกัด
GENESIS HI-TECH CO.,LTD.