

ZyWALL ATP200/500/800 ATP Firewall

Next-Gen Firewall for SMBs

The Zyxel ZyWALL ATP200/500/800 is an Advanced Threat Protection Firewall Series 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, 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 cloud intelligence with global sharing synergy



Sandboxing defeats unknown threats



Reporting and analytics on cloud and device



High assurance multi-layered protection



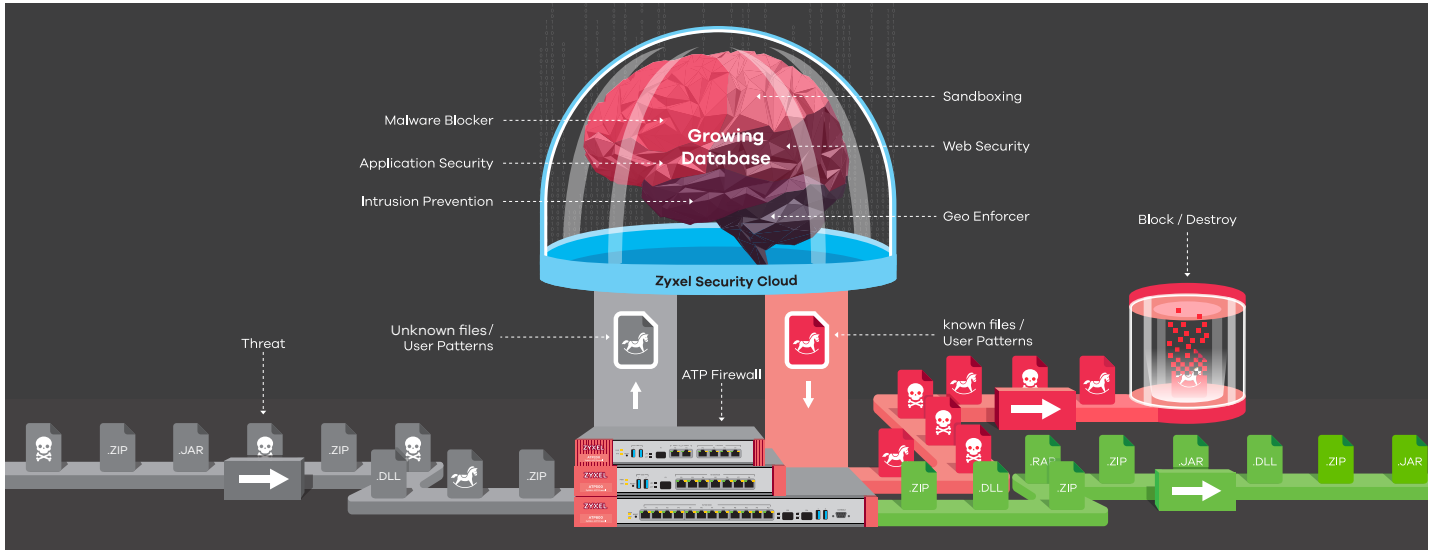
Benefits

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 in cloud threat database. It then pushes the most top-ranked threat intelligence 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

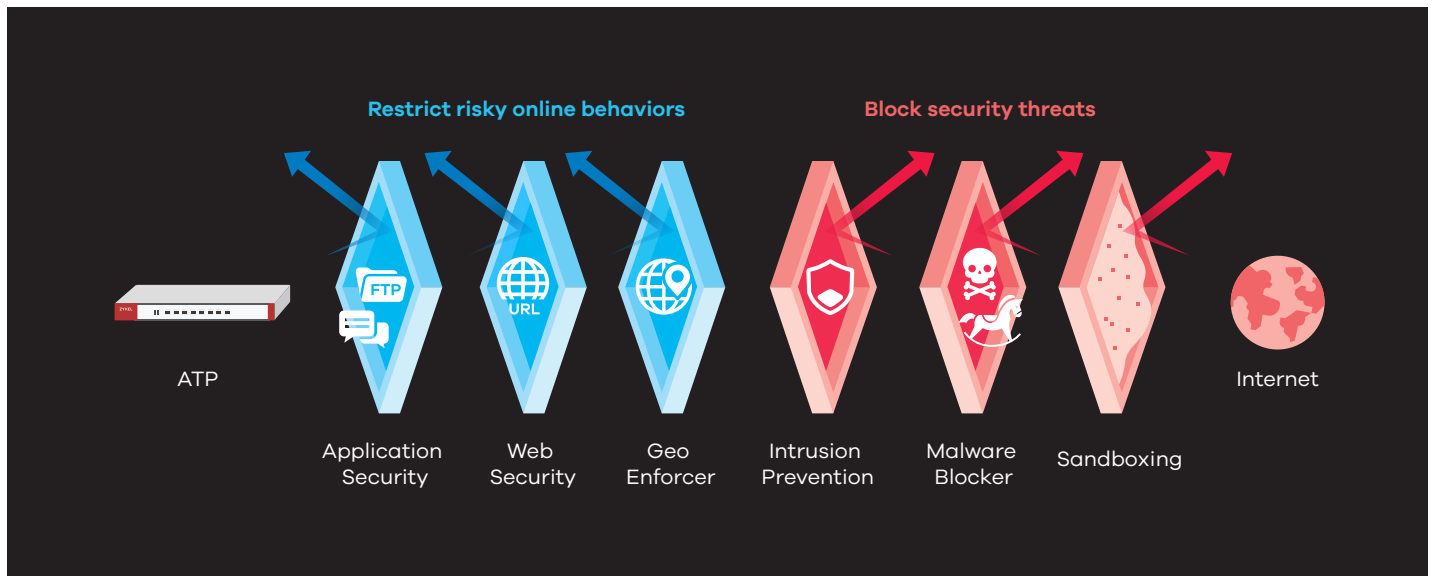
Sandboxing is an isolated cloud environment to contain unknown files that cannot be identified by existing security service on device and to emulate those unknown files to identify whether they are malicious or not. Key values from sandboxing is to inspect packet behavior in isolation so the potential 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

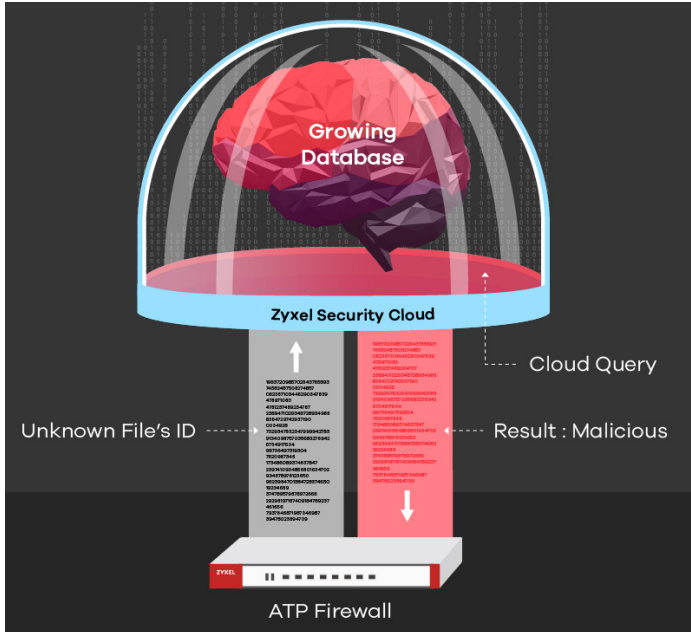
History has proven that a single-focus solution is useful in stopping specific attack; the capabilities of advanced malware are so broad that such protection inevitably fails. The ZyWALL ATP Firewall Series is designed with multi-layered protection guard against multiple types of

threats from in and out. It contains comprehensive security features like botnet filter, sandboxing, app patrol, content filtering, anti-malware, and IDP. ATP firewalls are sure to start safeguarding your network as soon as the device begins up and running without any unattended gaps.



Cloud Query levels up ATP malware defense

When an unknown file appears, Cloud Query quickly checks the file ID in the Cloud Threat Database to check if it's malicious within seconds. This maximizes your network traffic by consuming minimal network resources while maintaining a strong malware coverage with multiple-sourced Cloud Threat Database which has billions of malware data and still growing every minute. Cloud Query also accelerates new malware intelligence that circulates throughout Zyxel Security Cloud, which strengthens every ATP's malware protection capability.



Graphical and analytical cloud report

ATP Firewall dashboard gives user-friendly infographic traffic summary and threat statistics. Users can also utilize SecuReporter for further comprehensive threat analysis. SecuReporter features a suite of analysis and reporting tools, including network security threats identification and analysis, security services, security events, application usage, website usage and traffic usage, VPN status and Device Health status, etc. Users can also run customized report on-demand or on a regular schedule such as daily, weekly, and monthly.



Subscription Service

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.



Sandboxing



Web Security



Application Security



Malware Blocker



Intrusion Prevention



Geo Enforcer



Managed AP Service



SecuReporter

License Packs




License Service	Feature	ZyWALL ATP200/500/800 ^{*1}	
		Gold (1 Year/2 Years)	Silver (1 Year/2 Years)
Sandboxing	Sandboxing	Yes	-
Web Security	Content Filter	Yes	Yes
	Botnet Filter	Yes	Yes
Application Security	App Patrol	Yes	Yes
	Email Security	Yes	Yes
Malware Blocker	Anti-Malware	Yes	Yes
	Cloud Query	Yes	Yes
	Cloud Threat Database	Yes	-
Intrusion Prevention	IDP	Yes	Yes
Geo Enforcer	GeoIP	Yes	Yes
Managed AP Service ^{*2}	Wireless Controller	Unlock to max	2
SecuReporter ^{*3}	SecuReporter	Yes	-

*1: All ATP models are bundled with one-year Gold Security Pack by default, and this pack cannot be transferred.

*2: Gold Pack gives a year of unlocked managed AP nodes (18 APs for ATP200, 34 APs for ATP500, 130 APs for ATP800), only 2 APs will be supported if it's no longer renewed.

*3: The analytic features of Sandbox and Botnet in SecuReporter will be available in October, 2019.

Specifications

Model	ZyWALL ATP200	ZyWALL ATP500	ZyWALL ATP800
Product photo			
Hardware Specifications			
10/100/1000 Mbps RJ-45 ports	4 x LAN/DMZ, 2 x WAN, 1 x SFP	7 (Configurable), 1 x SFP	12 (Configurable), 2 x SFP (Configurable)
USB3.0 ports	2	2	2
Console port	Yes (DB9)	Yes (DB9)	Yes (DB9)
Rack-mountable	Yes	Yes	Yes
Fanless	Yes	-	-
System Capacity & Performance^{*1}			
SPI firewall throughput (Mbps) ^{*2}	2,000	2,600	8,000
VPN throughput (Mbps) ^{*3}	500	900	1,500
IDP throughput (Mbps) ^{*4}	1,200	1,700	2,700
AV throughput (Mbps) ^{*4}	450	700	1,200
UTM throughput (AV and IDP) ^{*4}	450	700	1,200
Max. TCP concurrent sessions ^{*5}	600,000	1,000,000	2,000,000
Max. concurrent IPSec VPN tunnels ^{*5}	40	200	1,000
Concurrent SSL VPN users	10	50	100
VLAN interface	16	64	128
WLAN Management			
Managed AP number (1 Year bundled) ^{*6}	18	34	130

Model	ZyWALL ATP200	ZyWALL ATP500	ZyWALL ATP800	
Security Services				
Anti-Malware	Yes	Yes	Yes	
Intrusion Detection and Prevention (IDP) & Application Patrol	Yes	Yes	Yes	
Email Security	Yes	Yes	Yes	
Application Security	Yes	Yes	Yes	
Sandboxing	Yes	Yes	Yes	
Web Security	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	
Amazon VPC	Yes	Yes	Yes	
Device HA Pro	-	Yes	Yes	
Cloud CNM SecuReporter	Yes	Yes	Yes	
Power Requirements				
Power input	12 V DC, 2.5 A max.	12 V DC, 4.17 A	100-240 V AC, 50/60 Hz, 2.5 A max.	
Max. power consumption (watt)	13.3	24.1	46	
Heat dissipation (BTU/hr)	45.38	82.23	120.1	
Physical Specifications				
Item	Dimensions (WxDxH) (mm/in.)	272 x 187 x 36/ 10.7 x 7.36 x 1.42	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
	Weight (kg/lb.)	1.4/3.09	1.65/3.64	3.3/7.28
Packing	Dimensions (WxDxH) (mm/in.)	427 x 247 x 73/ 16.81 x 9.72 x 2.87	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
	Weight (kg/lb.)	2.23 (W/O bracket) 2.42 (W/ bracket)	2.83/6.24	4.8/10.58
Included accessories	<ul style="list-style-type: none"> Power adapter Rack mounting kit (optional, by regions) 	<ul style="list-style-type: none"> Power adapter Power cord Rack mounting kit 	<ul style="list-style-type: none"> 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	529,688.2	947,736	
Acoustic noise	-	24.5 dBA on < 25°C operating temperature, 41.5 dBA on full FAN speed.	25.3 dBA on < 25°C operating temperature, 46.2 dBA on full FAN speed.	
Certifications				
EMC	FCC Part 15 (Class B), CE EMC (Class B), C-Tick (Class B), 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 ZLD4.33 or later.

*1: Actual performance may vary depending on 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).

*4: AV 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: After Gold Pack has expired, it will support only 2 APs.

Access Point Compatibility List

Product	Unified AP	Unified Pro AP
Models	<ul style="list-style-type: none"> • NWA5121-NI • NWA5123-AC • NWA5123-AC HD* 	<ul style="list-style-type: none"> • NWA5301-NJ • WAC5302D-S
		<ul style="list-style-type: none"> • WAC6103D-I • WAC6303D-S* • WAC6502D-E • WAC6502D-S • WAC6503D-S • WAC6553D-E
Functions		
Central management	Yes	Yes
Auto provisioning	Yes	Yes
Data forwarding	Local bridge	Local bridge/Data tunnel
ZyMesh	Yes	Yes

* Forward Compatible AP: Starting from APC3.0, commercial gateways supporting APC technology are able to recognize APs with APC3.0 firmware version or higher. Resellers can introduce newly-available Zyxel APs with basic features supported without upgrading any new controller firmware.

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
- Application bandwidth management
- 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
- No file size limitation
- HTTP, FTP, SMTP, POP3 protocol support
- Automatic signature updates

Cloud Query

- Cloud-based malware scan engine
- Works with over 30 billion signature database and still growing
- Supports FTP/HTTP/HTTPS-based protocol
- Multiple file types supported

E-mail Security

- Transparent mail interception via SMTP and POP3 protocols
- Sender-based IP reputation filter
- Spam, Phishing, Zero-hour virus mail detection
- Blacklist and whitelist support
- Supports DNSBL checking

Botnet Filter

- Botnet C&C IP blocking
- Malicious URL blocking

Content Filtering

- HTTPs domain filtering
- SafeSearch support
- Whitelist websites enforcement
- URL blacklist and whitelist, keyword blocking support
- Customizable warning messages and redirection URL

Geo Enforcer

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

VPN

IPSec VPN

- Key management: IKEv1 (x-auth, mode-config), IKEv2 (EAP, configuration payload)
- Encryption: DES, 3DES, AES (256-bit)
- Authentication: MD5, SHA1, SHA2 (51-2bit)
- Perfect forward secrecy (DH groups)
- 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

- Support AP Controller (APC) version 3.00
- 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

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
- 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

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

System Management

- Role-based administration
- Multi-lingual Web GUI (HTTPS and HTTP)
- Command line interface (console, SSH and telnet)
- SNMP v1, v2c, v3
- System configuration rollback
- 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.

ZYXEL

Your Networking Ally

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

Copyright © 2019 Zyxel Communications Corp. All rights reserved. Zyxel, Zyxel logo are registered trademarks of Zyxel Communications Corp. All other brands, product names, or trademarks mentioned are the property of their respective owners. All specifications are subject to change without notice.

Datasheet **ZyWALL ATP200/500/800**



5-100-00819002 05/19