

# ZYXEL

Your Networking Ally

# ATP

Smart cloud, defeat the unknown

# Smart Cloud, Defeat the Unknown

**Advanced Threat Protection  
Solution Brief**



# We turn the unknown to the known



# Advanced Threat Protection

We block, learn, and prevent unknown threats

Modern cyber attacks does not only come in multiple volumes, but also in a diverse landscape – Cryptojacking skyrocketed up 8500% in 2017, malware implants has surged, and ransomware variants increased 46% with massive impacted areas.

ZyWALL ATP Firewall is empowered by smart cloud intelligence, giving it seamless protection against all Advanced Persistent Threats, featuring ultimate defense with in-depth prediction of unknown attacks.

---


## Real-time Synchronization

Cloud intelligence constantly provides the most updated top-ranked threat protection from its cloud database into all ATP devices to defend them from a wide range of threats. This daily threat update is way ahead of conventional signature update, useful to defy Zero Day threats.

---

## Global Sharing Synergy

Linked together with real-time cloud-and-device intelligence synchronization, with each threat detected on an individual ATP gateway can ultimately benefit the Cloud Intelligence as well as all other deployed ATP devices, forging a seamless security ecosystem with valuable “one for all, all for one” effect.



ZyWALL ATP Next Generation Firewall

## Timely Defense for Ultimate Protection

# How ATP works

The ZyWALL ATP Firewall Series is an advanced threat protection firewall empowered with cloud intelligence to level up network protection to a higher level especially in tackling unknown threats. Fully compliant with GDPR, the ZyWALL ATP Firewall Series ensures that all your data is private.

Thanks to cloud machine learning, the ZyWALL ATP Firewall Series can safely analyze all unknown file

enquiries, determine if the unknown file enquiries are new threats, and then update the inspection results into the Cloud Threat Database. This self-evolving cloud security intelligence enables growing protection with each new threat detected. The unity of cloud intelligence and all deployed ATP firewalls collectively work together by making a safer online ecosystem to achieve in-depth defense.

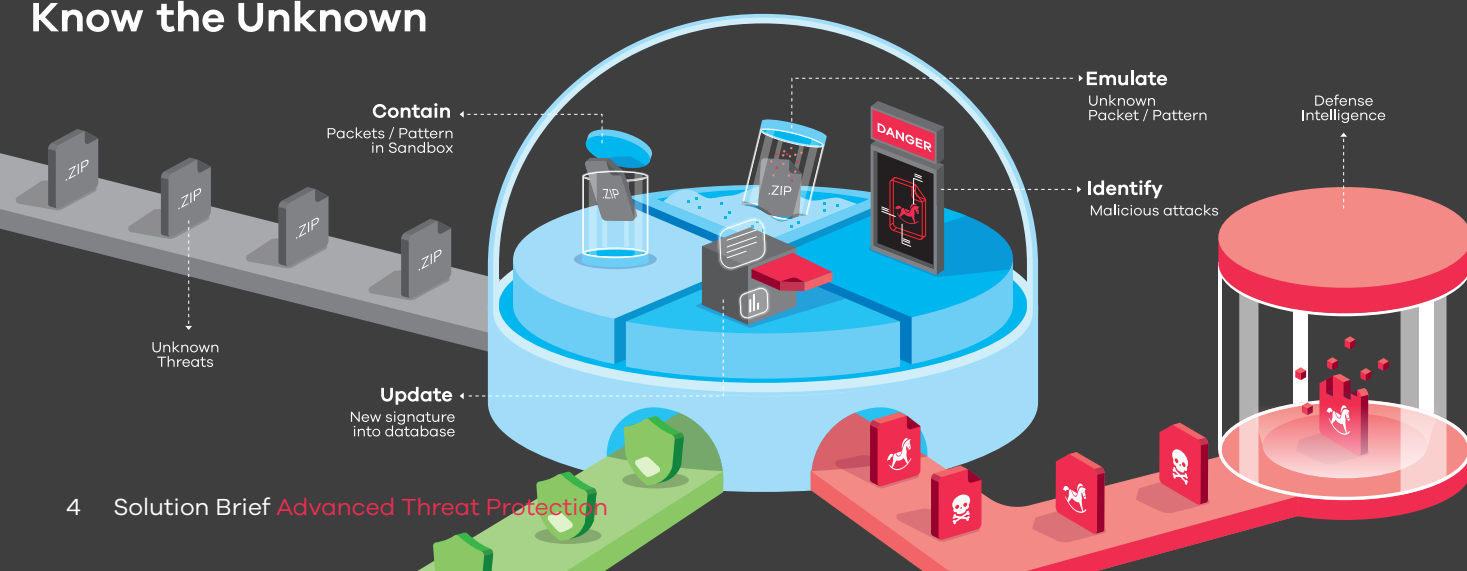
## Self-evolving Cloud Intelligence

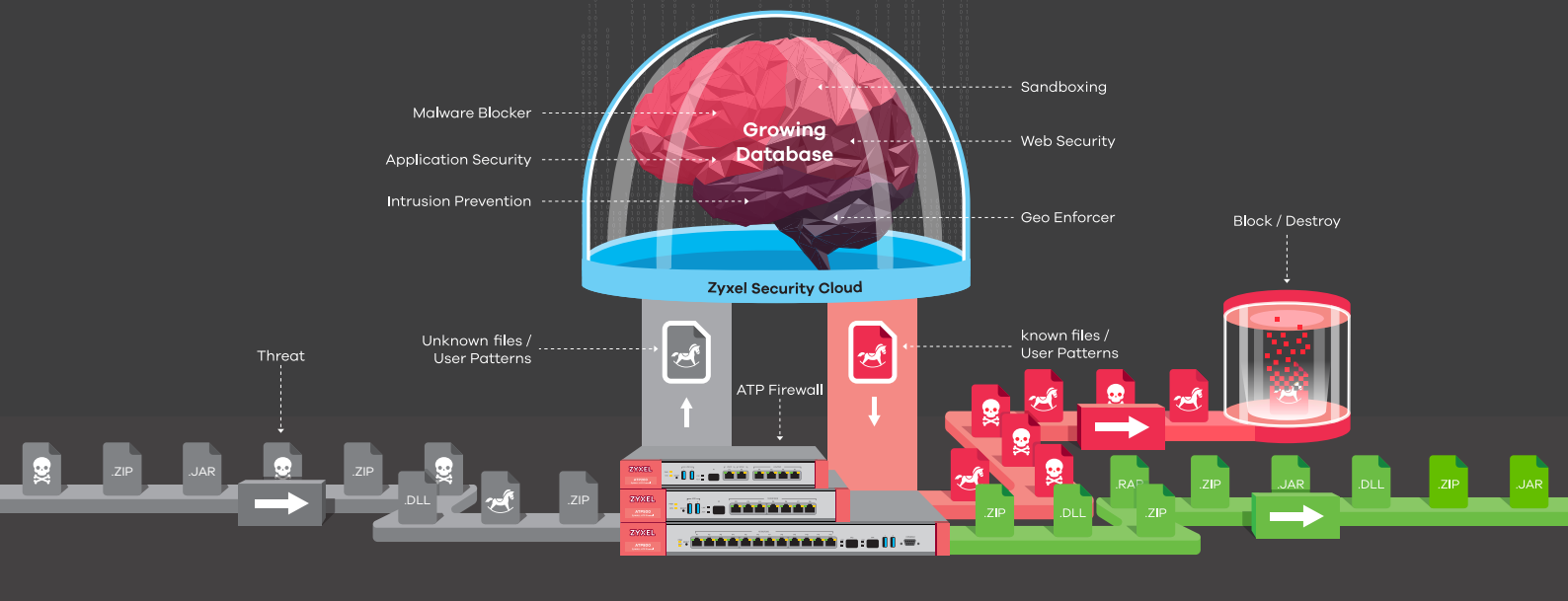
Cloud intelligence receives all unknown files or user patterns from Zyxel ATP firewall's enquiry then identifies and archives inspection results in cloud threat database. It then pushes the most top-ranked threat intelligence into all ATP firewalls so that all ATP devices are all within the seamless 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-Know the Unknown

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.

### Know the Unknown





## Analytical Cloud Report

The Zyxel Cloud CNM SecuReporter is a cloud-based intelligent analytics and report service, providing network administrators with a centralized view of user activities and threats statistics within the entire network.

The Cloud CNM 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.

## User Friendly Interface

The ZyWALL ATP Firewall Series provides a dashboard that conveniently displays since-reboot traffic statistics and seven-day security threat results all on one page for quick insights. Security threat reports hit counts and threat information, covering sandboxing, top IP/URL blocked, top applications blocked etc, with dynamic charts giving a clear and concise visualized view. This user-friendly interface enables ATP users to monitor network security and scanned traffic from a single screen in real-time.



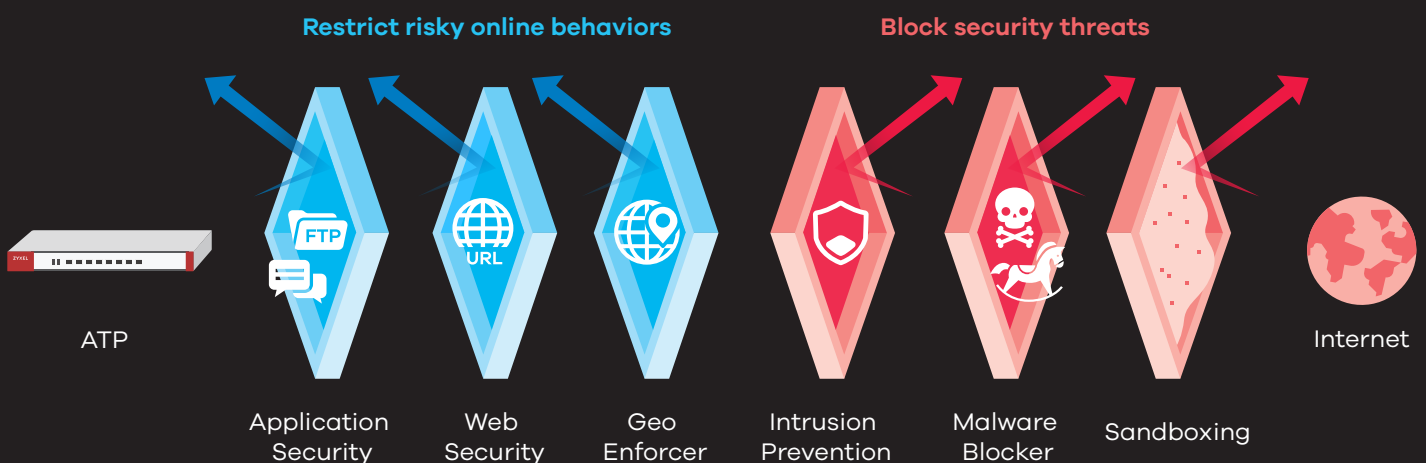


## Cost-effective Protection for SMBs

The ZyWALL ATP Firewall Series is an all-in-one firewall solution that integrates scalable, cloud-based sandboxing with multiple additional layers of security to detect and block known and unknown threats that fly under the radar of conventional security solutions. For those compounding, unknown threats that can't be stopped by conventional security solutions can now be fended off by a cutting-edge and very cost-effective ATP security solution for most of SMBs.

## 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.



# Product at a glance

## ZyWALL ATP Firewall Series



Machine learning cloud intelligence with global sharing synergy



Sandboxing defeats unknown threats



Reporting and analytics on cloud and device



High assurance multi-layered protection



# ATP Licenses & Services

ZyWALL ATP security license is bundled with one-year Gold Security Pack by default. All essential service modules all included. Once the second year starts, you have the option to renew Gold Security Pack or

alternatively Silver Security Pack. Silver Security Pack doesn't include three license modules in Gold Security Pack's offering: Sandboxing, Managed AP Service, and SecuReporter.



## Sandboxing

It can safely run unknown files, determine whether it is malicious or not, and share the results.



## Intrusion Prevention

Scans the network traffic stream in-depth, packet by packet, to find threats (SQL and DoS) by using known exploits and attack vectors.



## Application Security

The module is designed for secured application and email behaviors.



## Geo-Enforcer

Map IP addresses to the sources or destination of attack traffic and restrict Internet access from high risk countries.



## Web Security

Blocks known and unknown malicious URLs, malware, phishing/botnet sites, APTs, and zero-day attacks.



## Managed AP Service

Includes a built-in remote management for AP deployment and monitoring.



## Malware Blocker

Stream-based detection and prevention of malware hidden within compressed files, web contents, or other common file types.



## SecuReporter

Provides network administrators a centralized view of network activities and potential threats within the network. Run report on-demand or on a scheduled basis.

## License Packs

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




<sup>\*1</sup>: All ATP models are bundled with one-year Gold Security Pack by default, and this pack cannot be transferred. ATP800 will be available in Nov. 2018.

<sup>\*2</sup>: 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.

<sup>\*3</sup>: SecuReporter will be available in Oct, 2018.



# Feature matrix

Model	ZyWALL ATP200	ZyWALL ATP500	ZyWALL ATP800*1
Product photo			
<b>Hardware Specifications</b>			
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	-	-
<b>System Capacity &amp; Performance*2</b>			
SPI firewall throughput (Mbps)*3	2,000	2,600	8,000
VPN throughput (Mbps)*4	500	900	1,500
IDP throughput (Mbps)*5	1,200	1,700	2,700
AV throughput (Mbps)*5	450	700	1,200
UTM throughput (AV and IDP)*5	450	700	1,200
Max. TCP concurrent sessions*6	600,000	1,000,000	2,000,000
Max. concurrent IPSec VPN tunnels*6	40	200	1,000
Concurrent SSL VPN users	10	50	100
VLAN interface	16	64	128
<b>WLAN Management</b>			
Managed AP number (1 Year bundled)*7	18	34	130
<b>Security Service</b>			
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
<b>Key Features</b>			
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
<b>Power Requirements</b>			
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

# Feature matrix

Model		ZyWALL ATP200	ZyWALL ATP500	ZyWALL ATP800
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"> <li>• Power adapter</li> <li>• Rack mounting kit (optional, by regions)</li> </ul>	<ul style="list-style-type: none"> <li>• Power adapter</li> <li>• Power cord</li> <li>• Rack mounting kit</li> </ul>	<ul style="list-style-type: none"> <li>• Power cord</li> <li>• Rack mounting kit</li> </ul>
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 ZLD4.32 or later.

\*1: As of July 30th 2018, the following document provides an estimate of ATP800's throughput numbers; this product is still under development and may change as it progresses.

\*2: Actual performance may vary depending on 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: AV and IDP 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: After Gold Pack has expired, it will support only 2 APs.

