

ZYXEL



ZyWALL ATP100/200/500/800 ATP Firewall

Next-Gen Firewall for SMBs

The ZyXel ZyWALL ATP100/200/500/800 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, 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 cloud intelligence with global sharing synergy



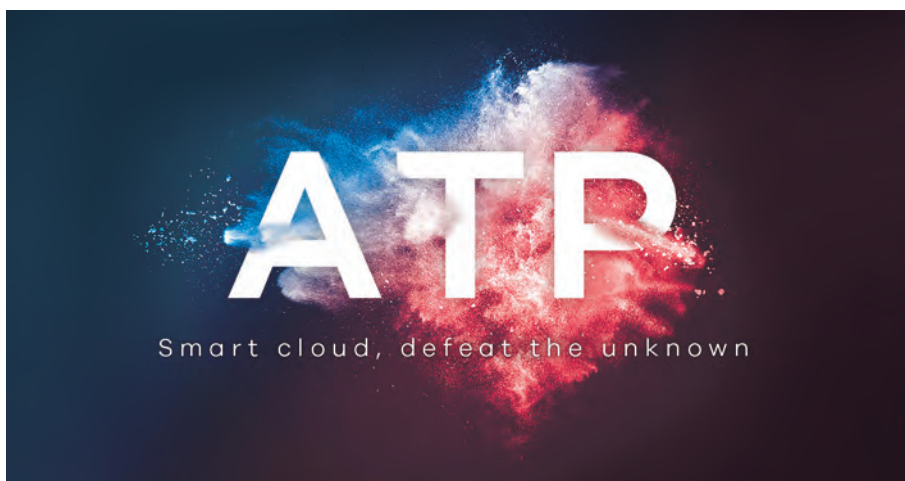
Sandboxing defeats unknown threats



Reporting and analytics on cloud and device



High assurance multi-layered protection



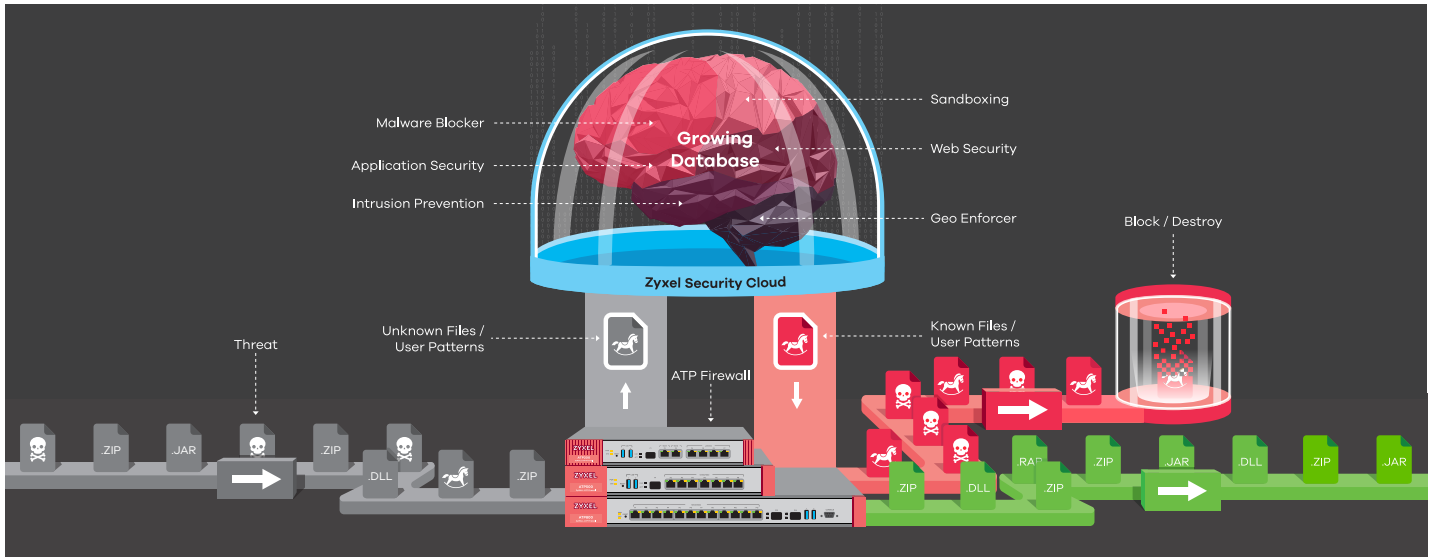
Benefits

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 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

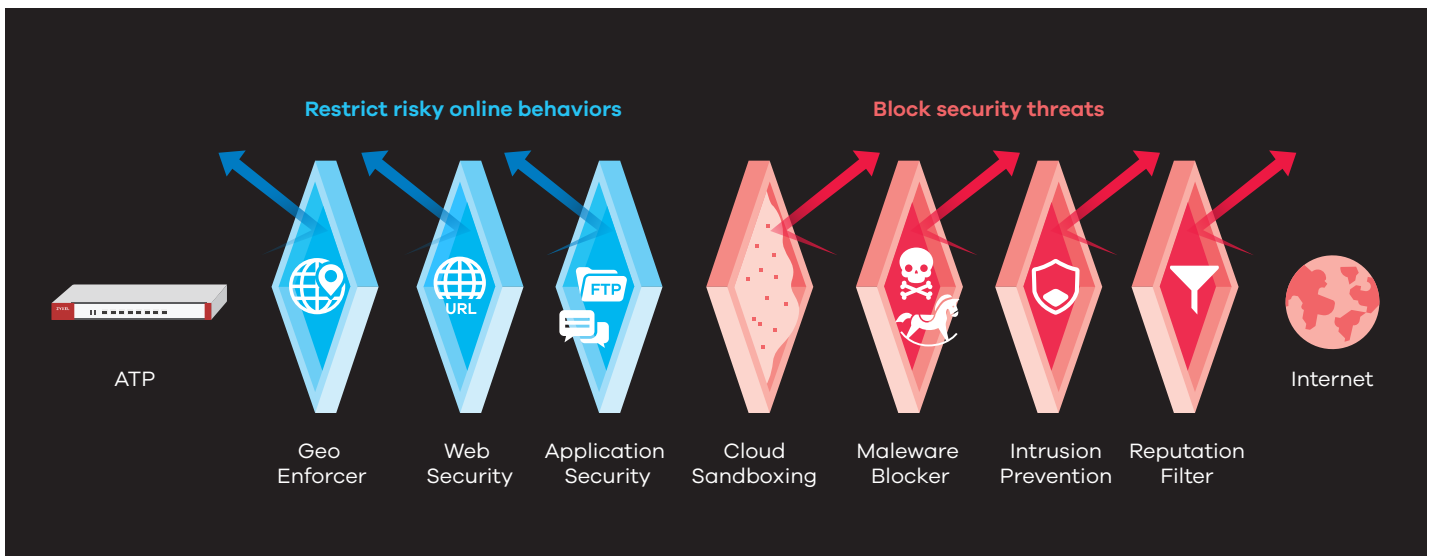
Sandboxing is an isolated cloud environment to contain unknown files that cannot be identified by existing security service on device and to emulate those unknown files to identify whether they are malicious or not. Key values from sandboxing is to inspect packet behavior in isolation so the potential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



Reputation Filter preemptive IP threat defense

Reputation Filter matches up IP addresses with a real-time cloud database that tracks malicious cyber activities and determines if its address is reputable or not. This improves blocking efficiency, reduces hardware utilization, giving

administrators additional network resources to quickly and easily address any issues. Reputation Filter also increases threat visibility in SecuReporter (included in bundle pack) which assists in tracing cyber threat sources.

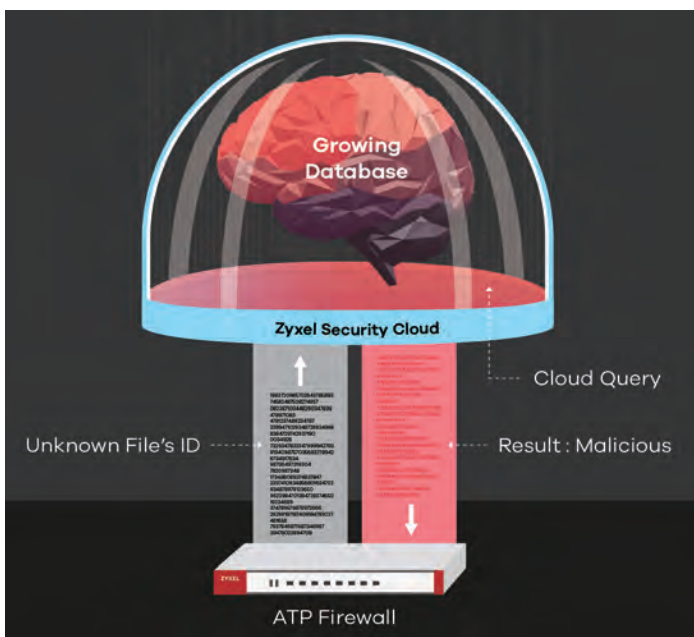


Cloud Query levels up ATP malware defense

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

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, security events, application usage, website usage, and traffic usage. Analyze sandboxing scanning activity detail and will send an alert mail to administrator if mail is detected as high risk. Botnet filter analytics/report show top N botnet threat web sites and their type, list which internal hosts are controlled by botnet web sites. IP Reputation analytics offer IP attack detail and its risk. ATP series with SecuReporter offer comprehensive protection and analytics.



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.



Sandboxing



Web Security



Application Security



Malware Blocker



Intrusion Prevention



Reputation Filter



Geo Enforcer



Managed AP Service



SecuReporter





License Packs

License Service	Feature	ZyWALL ATP100/200/500/800 ^{*1}
		Gold (1 Year/2 Years)
Sandboxing	Sandboxing	Yes
Web Security	Content Filter	Yes
	Botnet Filter	Yes
Application Security	App Patrol	Yes
	Email Security	Yes
Malware Blocker	Anti-Malware	Yes
	Cloud Query	Yes
	Threat Intelligence Machine Learning	Yes
Intrusion Prevention	IDP	Yes
Reputation Filter	IP Reputation Filter	Yes
Geo Enforcer	GeoIP	Yes
Managed AP Service^{*2}	Wireless Controller	Unlock to max
SecuReporter	SecuReporter Premium	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 (10 APs for ATP100, 18 APs for ATP200, 34 APs for ATP500, 130 APs for ATP800), only 2 APs will be supported if it's no longer renewed.

Specifications

Model	ZyWALL ATP100	ZyWALL ATP200	ZyWALL ATP500	ZyWALL ATP800
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, 2 x WAN, 1 x SFP	7 (Configurable), 1 x SFP	12 (Configurable), 2 x SFP (Configurable)
USB 3.0 ports	1	2	2	2
Console port	Yes (RJ-45)	Yes (DB9)	Yes (DB9)	Yes (DB9)
Rack-mountable	-	Yes	Yes	Yes
Fanless	Yes	Yes	-	-
System Capacity & Performance¹				
SPI firewall throughput (Mbps) ²	1,000	2,000	2,600	8,000
VPN throughput (Mbps) ³	300	500	900	1,500
IDP throughput (Mbps) ⁴	600	1,200	1,700	2,700
AV throughput (Mbps) ⁴	250	450	700	1,200
UTM throughput (AV and IDP) ⁴	250	450	700	1,200
Max. TCP concurrent sessions ⁵	300,000	600,000	1,000,000	2,000,000
Max. concurrent IPsec VPN tunnels ⁵	40	40	200	1,000
Concurrent SSL VPN users	10	10	50	100
VLAN interface	8	16	64	128
Speedtest Performance				
SPI firewall throughput (Mbps) ⁶	850	900	900	930
WLAN Management				
Managed AP number (1 Year bundled) ⁷	10	18	34	130
Security Services⁸				
Sandboxing	Yes	Yes	Yes	Yes
Web Security	Yes	Yes	Yes	Yes
Application Security	Yes	Yes	Yes	Yes
Malware Blocker	Yes	Yes	Yes	Yes
Intrusion Prevention (IDP)	Yes	Yes	Yes	Yes
Reputation Filter	Yes	Yes	Yes	Yes
Geo Enforcer	Yes	Yes	Yes	Yes
SecuReporter	Yes	Yes	Yes	Yes
Key Features				
VPN	IKEv2, IPsec, SSL, L2TP/IPsec	IKEv2, IPsec, SSL, L2TP/IPsec	IKEv2, IPsec, SSL, L2TP/IPsec	IKEv2, IPsec, SSL, L2TP/IPsec
SSL (HTTPS) Inspection	Yes	Yes	Yes	Yes
2-Factor Authentication	Yes	Yes	Yes	Yes
Microsoft Azure	Yes	Yes	Yes	Yes
Amazon VPC	Yes	Yes	Yes	Yes
Device HA Pro	-	-	Yes	Yes

Model		ZyWALL ATP100	ZyWALL ATP200	ZyWALL ATP500	ZyWALL ATP800
Power Requirements					
Power input		12 V DC, 2 A max.	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)		12.5	13.3	24.1	46
Heat dissipation (BTU/hr)		42.65	45.38	82.23	120.1
Physical Specifications					
Item	Dimensions (WxDxH) (mm/in.)	216 x 143 x 33/ 8.50 x 5.80 x 1.30	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.)	0.85/1.87	1.4/3.09	1.65/3.64	3.3/7.28
Packing	Dimensions (WxDxH) (mm/in.)	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	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.)	1.4/3.09	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 • RJ-45 cable • RS-232 cable 	<ul style="list-style-type: none"> • Power adapter • Rack mounting kit 	<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	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)	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	-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)	10% to 90% (non-condensing)
MTBF (hr)		989,810.8	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 (Class B), RCM (Class B), BSMI	FCC Part 15 (Class B), CE (Class B), RCM (Class B), BSMI	FCC Part 15 (Class A), CE (Class A), RCM (Class A), BSMI	FCC Part 15 (Class A), CE (Class A), RCM (Class A), BSMI
Safety		LVD, BSMI	LVD, BSMI	LVD, BSMI	LVD, BSMI

*: This matrix with firmware ZLD4.35 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: 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.

*7: Once Gold Pack has expired, 2 APs will only be supported.

*8: Enable or extend feature capacity with Zyxel service license.

Access Point Compatibility List

Product	Unified AP	Unified Pro AP		
Models	<ul style="list-style-type: none"> NWA5121-N NWA5121-NI NWA5123-AC NWA5123-AC HD NWA5123-NI 	<ul style="list-style-type: none"> NWA5301-NJ WAC5302D-S Forward Compatible APs* 	<ul style="list-style-type: none"> WAC6103D-I WAC6303D-S WAC6502D-E WAC6502D-S WAC6503D-S 	<ul style="list-style-type: none"> WAC6552D-S WAC6553D-E Forward Compatible APs*
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.

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
- 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

Reputation Filter

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

Botnet Filter

- Botnet C&C websites 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

IP Exception

- Provides granular control for target source and destination IP
- Supports security service scan bypass for IDP and Anti-Malware

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) support 1, 2, 5, 14, 15-18
- 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 3.40
- 802.11k/v/r support for wave 2 11ac AP
- 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
- 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

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-step authentication for administrator

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
- 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.

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 ATP100/200/500/800](#)

