ZyWALL NS5000/NS7000

Security Firewall

Next-Gen Firewall for SMBs

The Zyxel ZyWALL NS5000/NS7000 series is a Security 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. An infographic dashboard is also included, delivering high performance and ensuring comprehensive protection as a self-evolving solution.

- Sandboxing defeats unknown threats
- 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

Benefits

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 NS series Firewall Series is preventive measure for zero-day attacks of all sorts.
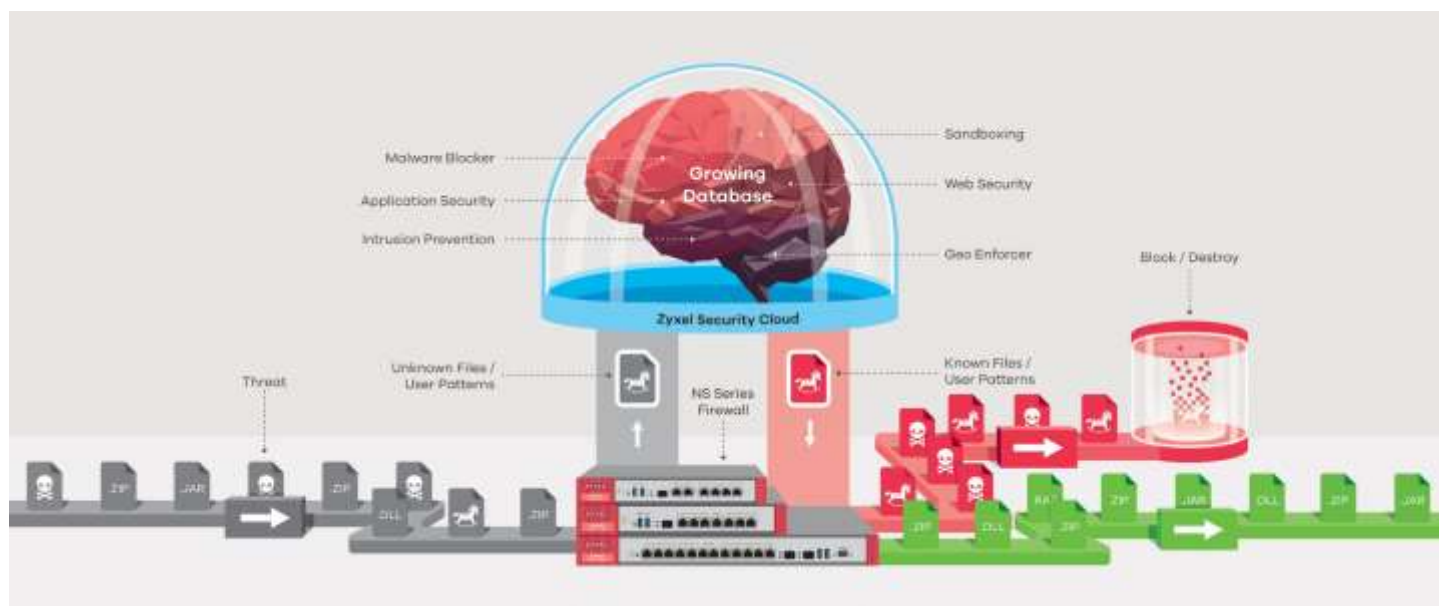
High assurance multi-layered protection

NS 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.
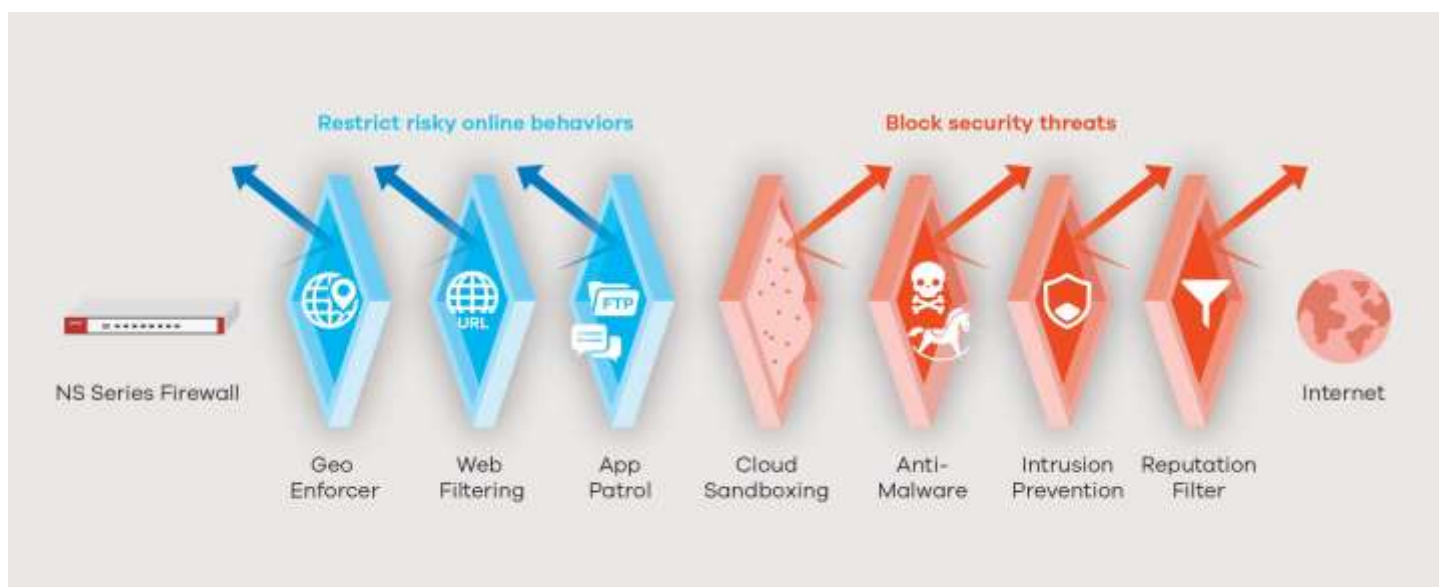
Deep insight into all your device

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.
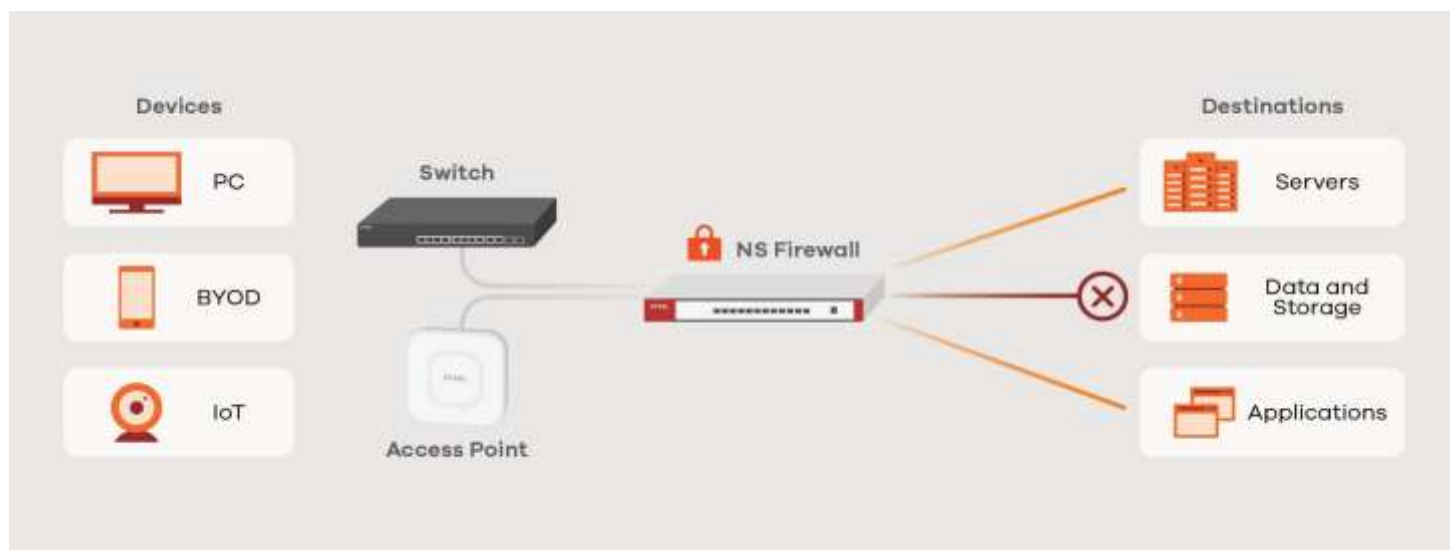
Comprehensive Web Filtering service

NS 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 NS Firewall series now supports monitoring or blocking the use of DoH/DoT for better managing internet activities.

Hybrid scanning leveling up malware blocking

NS 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.
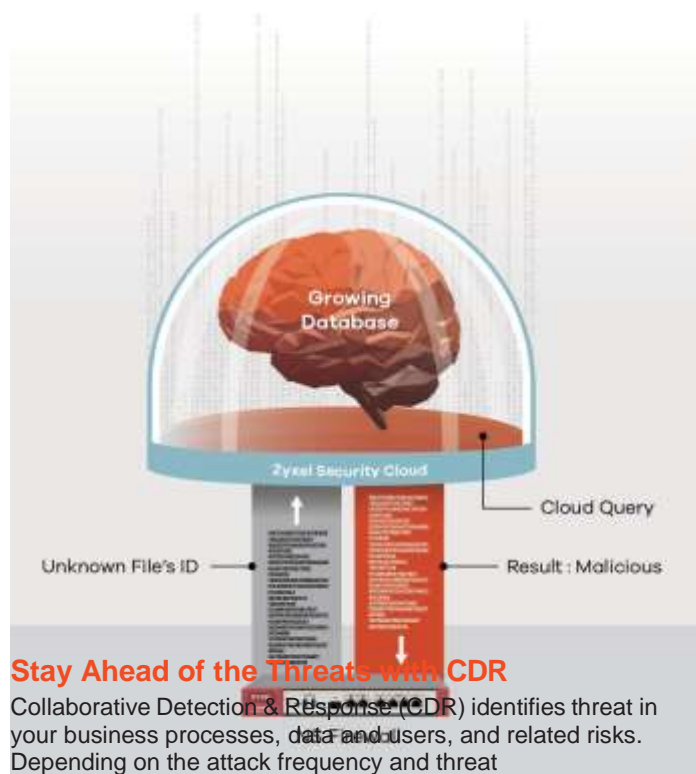

Stay Ahead of the Threats with CDR

Collaborative Detection & Response (CDR) identifies threat in your business processes, data and users, and related risks. Depending on the attack frequency and threat level, it generates a protection rule. NS Firewall takes a

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 NS Firewall.

great leap forward to adopt this generated protection rule to automatically stop threats at the network edge. It's perfect fit for SMB(s) to address the requirements of a decentralized, IoT-driven network infrastructure.
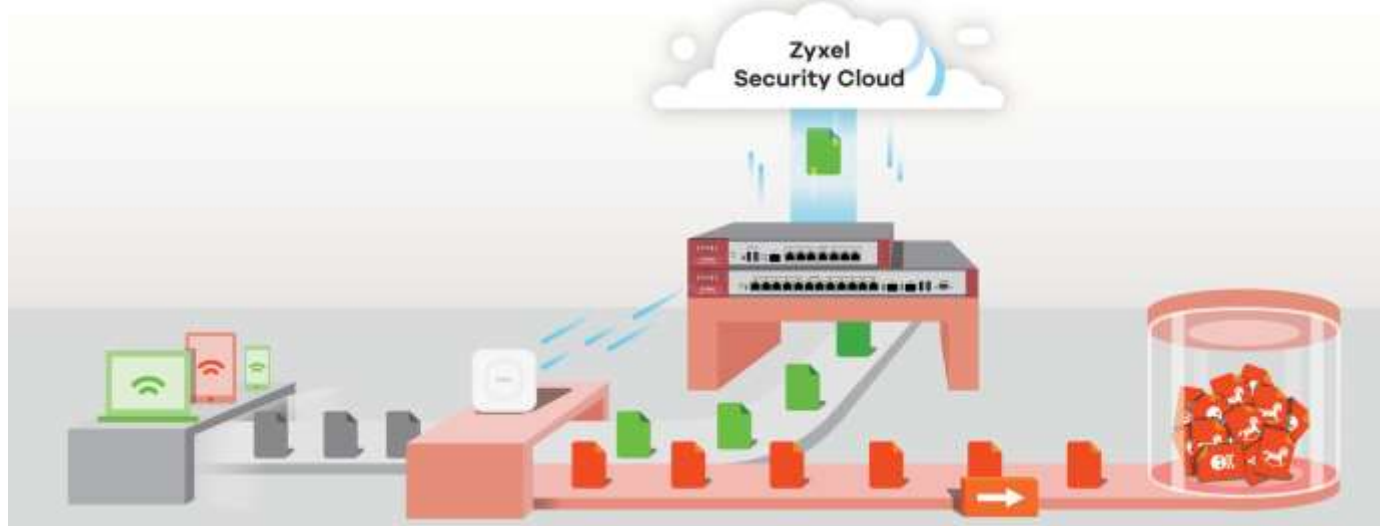
Analytics report and enhanced insights

NS 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.
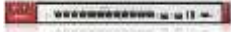
Services and Licenses

Licensed Service	Feature	NS5000/7000
		Gold Security Pack (1 Year/3 Years)
Web Filtering	Content Filter	Yes
App Patrol	Application visibility and control	Yes
Email Security	Anti-Spam	Yes
Anti-Malware	Anti-Malware with Hybrid Mode	Yes
	Threat Intelligence Machine Learning	Yes
Reputation Filter	IP Reputation	Yes
	DNS Threat Filter	Yes
	URL Threat Filter	Yes
Sandboxing	Sandboxing	Yes
SecuReporter	SecuReporter	Yes
CDR	Collaborative Detection & Response	Yes

Model	ZyWALL NS5000	ZyWALL NS7000
Product photo		

Hardware Specifications		
Interface	7 (configurable), 1x SFP	12 (configurable), 2x SFP (configurable)
USB 3.0 ports	2	2
Console port	DB9	DB9
Rack-mountable	Yes	Yes
Fanless	-	-

System Capacity & Performance[1]		
SPI firewall throughput (Mbps)[2]	2,600	6,000
VPN throughput (Mbps)[3]	900	1,200
IPS throughput (Mbps)[4]	1,700	2,200
Anti-malware throughput (Mbps)[4]	900	1,600
UTM throughput (Anti-Malware and IPS, Mbps)[4]	890	1,500
Max. TCP concurrent sessions[5]	1,000,000	1,600,000
Max. concurrent IPsec VPN tunnels[6]	300	500
Recommended gateway-to-gateway IPsec VPN tunnels	150	300
Concurrent SSL VPN users	150	150
VLAN interface	64	128

Speedtest Performance		
SPI firewall throughput (Mbps)[7]	900	930

Key Features			
Security Service	Sandboxing[8]	Yes	Yes
	Web Filtering[8]	Yes	Yes
	Application Patrol[8]	Yes	Yes
	Anti-Malware[8]	Yes	Yes
	IPS[8]	Yes	Yes
	Reputation Filter[8]	Yes	Yes
	Geo Enforcer	Yes	Yes
	SecuReporter[8]	Yes	Yes
	Collaborative Detection & Response[8]	Yes	Yes
	Device Insight	Yes	Yes
	SSL (HTTPS) Inspection	Yes	Yes
	2-Factor Authentication	Yes	Yes
VPN Features	VPN	IKEv2, IPSec, SSL, L2TP/IPSec	IKEv2, IPSec, SSL, L2TP/IPSec
WLAN Management	Default number of managed AP	8	8
	Recommend max. AP in 1 AP Group	60	200

Model		ZyWALL NS5000	ZyWALL NS7000
Key Features			
WLAN Management	**Secure WiFi Service*⁸**	Yes	Yes
	Maximum Number of Tunnel-Mode AP	18	66
	Maximum Number of Managed AP	72	264
Connectivity Management	**Device HA Pro**	Yes	Yes
	Link Aggregation (LAG)	Yes	Yes
	Concurrent devices logins (max.)	300	1500
Power Requirements			
Power input		12 V DC, 4.17 A	100-240V AC, 50/60Hz, 2.5A max.
Max. power consumption (watt)		24.1	46
Heat dissipation (BTU/hr)		82.23	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
	Weight (kg/lb.)	1.65/ 3.64	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
	Weight (kg/lb.)	2.83/ 6.24	4.8/ 10.58
Included accessories		• Power adapter • 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
	Humidity	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
	Humidity	10% to 90% (non-condensing)	10% to 90% (non-condensing)
MTBF (hr)		529,688.2	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
Certifications			
EMC		BSMI	BSMI
Safety		BSMI	BSMI

*: This matrix with firmware ZLD5.31 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).
*4: 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.
*5: Maximum sessions measured using the industry standard IXIA IxLoad testing tool.
*6: Including Gateway-to-Gateway and Client-to-Gateway.
*7: 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.

Software Features

Security Service

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

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

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
- 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
- Transparent mail interception via SMTP and POP3 protocols
- Spam, Phishing, mail detection
- Block 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 blacklist

Web Filtering
- HTTPs domain filtering
- SafeSearch support
- 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

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

SSL VPN
- Supports Windows and macOS
- 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
- 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

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 (Google Authenticator, SMS/Email)

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
- Dual firmware images

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

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

Access Point Compatibility List

Secure Tunnel for Remote AP

Product	Remote AP	Number of Tunnel Mode AP	Supported Remote AP
NS	NS5000	18	• WAX655E
	NS7000	66	• WAX650S
USG FLEX	USG FLEX 100(W)	6	• WAX640S-6E
	USG FLEX 200	10	• WAX630S
	USG FLEX 500	18	• WAX620D-6E
	USG FLEX 700	130	• WAX610D
VPN	VPN50	10	• WAX510D
	VPN100	18	• WAC500
	VPN300	130	• WAC500H
	VPN1000	258	

Managed AP Service

Product	Unified AP		Unified Pro AP	
Models	• NWA5301-NJ	• WAC5302D-Sv2	• WAC6103D-I	• WAX650S
	• NWA5121-NI	• WAC500*	• WAC6503D-S	• WAX630S
	• NWA5123-AC HD*	• WAC500H*	• WAC6502D-S	• WAX610D
	• NWA5123-AC		• WAC6303D-S	• WAX640S-6E
	• NWA5123-NI		• WAC6553D-E	• WAX620D-6E
	• WAC5302D-S		• WAC6552D-S	• WAX655E
	• WAX510D*		• WAC6502D-E	

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
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

*: SFP-BX1310-10-D & SFP-BX1490-10-D, SFP-BX1310-E & SFP-BX1550-E must be used in pairs.

10/05/23