ZYXEL

ATP800

ZyWALL ATP Next Generation Firewall

Overview

ZyXEL ZyWALL ATP는 클라우드 인텔리전스로 강화된 통합 보안장비로써 Web Filtering, Application Patrol, Anti-Malware, Email-Security 등과 같은 보안 서비스를 지원하여 바이러스, 웜, 피싱, 스파이웨어, 스팸 등 외부 불법 침입 시도의 차단과 내부에서의 부적절한 어플리케이션 프로그램의 사용 또는 악성 웹사이트의 접근을 제한하는 다양한 유형의 위협에 대하여 다중 보호기능을 제공합니다.

새롭게 추가된 Reputation Filter, Sandboxing, CDR 등의 보안 기능과 SecuReporter가 포함된 ZyWALL ATP는 IP Reputation 기반으로 탐지한 악성 IP 차단 데이터, Sandboxing 스캔 결과에 대한 데이터와 DNS 쿼리 유형 등의 포괄적인 보안 분석 내용을 포함하는 시각화된 보안 보고서를 제공합니다.

특히, 클라우드 인텔리전스는 알려지지 않은 새로운 위협에 대하여 클라우드 머신 러닝에서 실시간으로 수집된 정보를 ATP 장비와 지속적인 동기화를 통해 네트워크 보호 수준을 항상 최신 상태로 유지합니다.

또한, 무선 AP 컨트롤러를 내장하여 최대 520대의 AP를 중앙 집중 관리 할 수 있으며, Secure Wi-Fi 서비스로 원격지에 설치된 AP들의 무선네트워크 보안을 지원합니다.

.

- 대규모 비즈니스를 위한 올인원 통합 방화벽 기능
- 라이선스기반의 통합보안장비
  - Web Filtering, Reputation Filter ,IPS, Application Patrol, Anti - Malware, CDR(Collaborative - Detection & Response), Email - Security, Sandboxing
- Gold Security Pack 라이선스 1년간 Bundle 제공
  - 30일 Trial 기간 제공
  - 총 13개월 사용 무상 지원
- Nebula Professional Pack
- SecuReporter
  - 클라우드 기반 각종 보안 및 트래픽 분석, Daily & Weekly Report 제공
- Hybrid VPN 지원
  - SSL, IPSec, L2TP
- Secure WiFi
  - 원격지 무선 네트워크 보안 터널 구성
- 2FA Network Access 구성
- AWS, Azure 공식 인증
- 무선AP 컨트롤러 기능 탑재
  - 기본 8대, 라이선스 추가시 최대 520
- 3단계 High Availability 무중단 구성
  - WAN HA, VPN HA, Device HA
- 타 벤더 장비 호환성
  - ICSA LAB 국제 평가기관 인증 획득
- NAT 및 DHCP 기능 지원
- ZyXEL One Network
  - ZON Utility, Smart Connect
- IPv6 지원

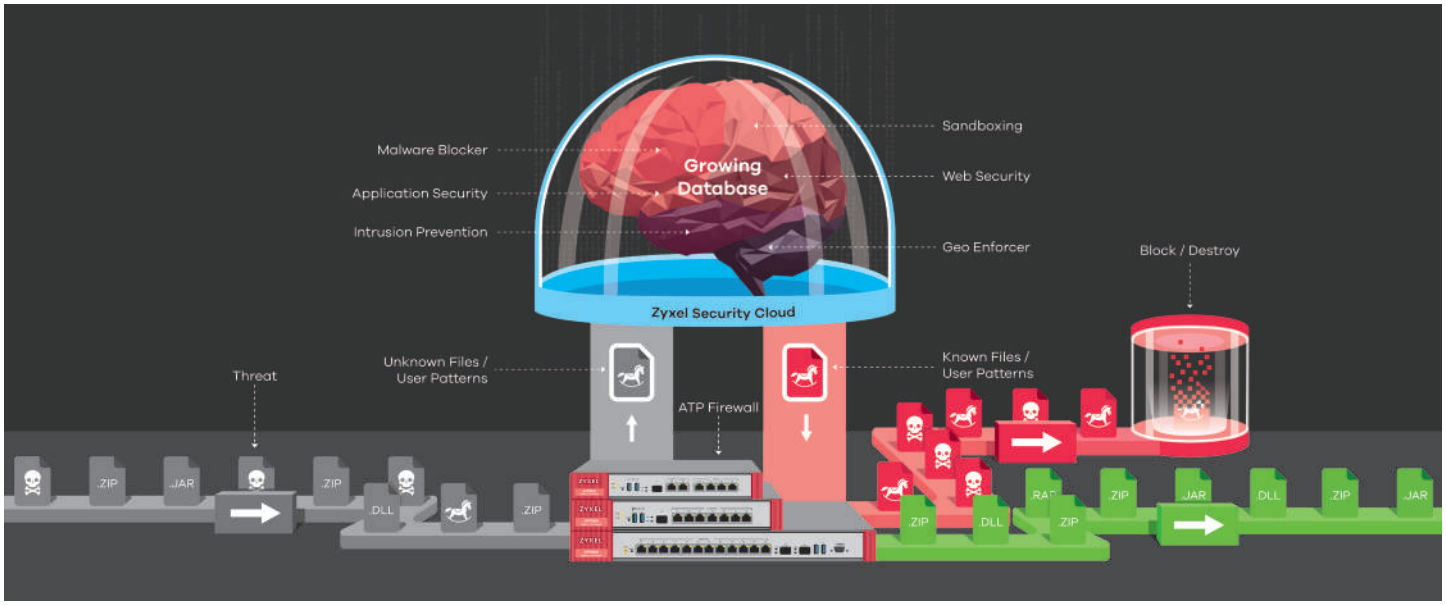
Zyxelone network
Redefining network integration

aws

Microsoft Azure

ICSA labs CERTIFIED IPSEC - BASIC

ICSA labs CERTIFIED FIREWALL - SMB



GbE 인터페이스 및 USB 포트 지원

ZYXEL ZyWALL ATP의 인터페이스는 각 포트당 10/100/1000 Mbps 속도를 지원하며, 각각의 인터페이스에 Routing, NAT, VLAN, Bridge 구성이 가능합니다. DHCP Server 및 Relay 기능을 활용할 수 있으며, 사용자 환경에 대해 Zone 영역 구성을 통해 WAN, LAN 혹은 VLAN 인터페이스 영역으로 구성할 수 있습니다. 또한 로그파일을 별도로 저장할 수 있도록 USB 포트가 장착되어 있습니다.

고성능 방화벽 및 VPN 처리 성능

ZYXEL ZyWALL ATP는 다양한 site-to-client and site-to-site VPN 구축을 위한 높은 처리량의 IPSec, L2TP, SSL VPN 방식을 지원하여 원격의 ZyXEL 장비들과 사용자 보안 통신을 위한 안정적인 인프라를 구성할 수 있습니다. 특히, SSL VPN 설정이 쉽고 간단하며 라이선스 적용으로 원격의 사용자들이 내부 시스템의 접근 공유가 편리하고 사용자 OS 환경에 따른 세션 분류 및 연결 제어가 가능하여 사용자 기반의 보안 터널 통신이 가능하도록 설계 되었습니다.

Multi-WAN & 장비 이중화

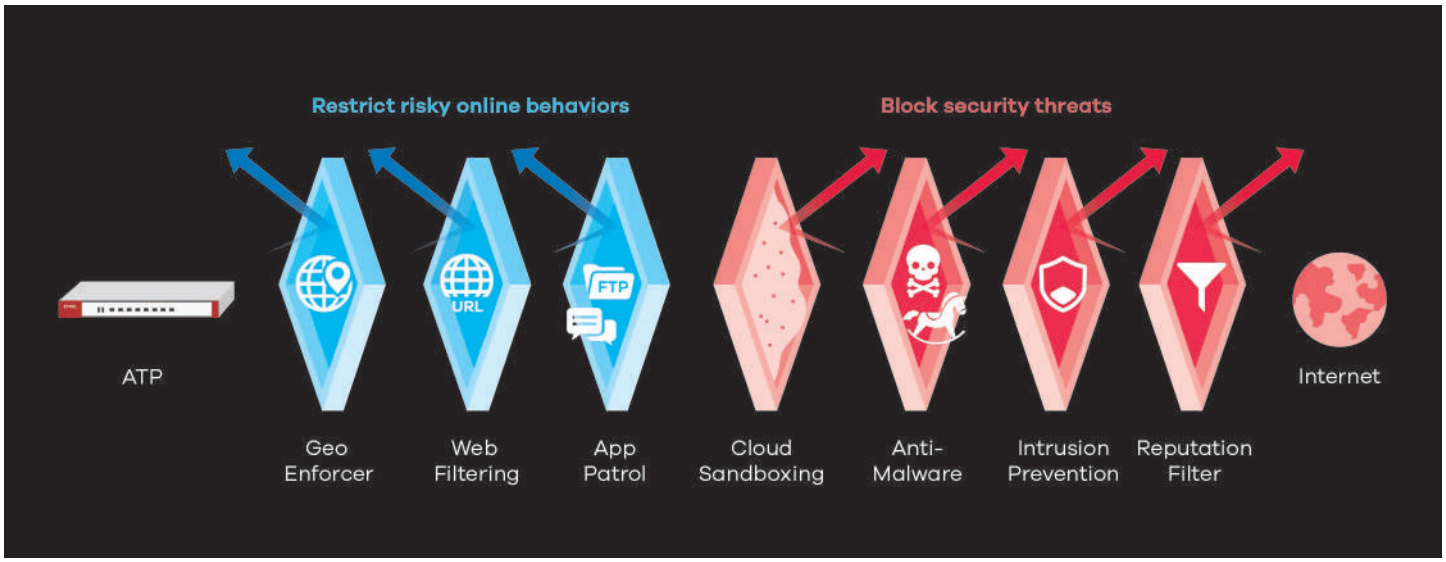
단일 WAN 인터페이스 환경에서는 물리적인 장애나 과다한 트래픽으로 인하여 운영중인 서비스가 중단되는 결과를 초래할 수 있습니다. ZyXEL ZyWALL ATP 에서는 단일 WAN 구성의 네트워크 부하를 줄이기 위해 WAN 인터페이스를 이중화하여 active-active 로드밸런싱(Load-Balancing) 구성 및 active-passive failover 구성이 가능하며, 회선 이중화 및 정책 라우터 방식을 통해서 다양한 서비스 경로를 제어할 수 있습니다. 또한 단일 장비 운영 중에 발생되는 네트워크 장애를 사전에 방지하고자 두 대의 장비를 동일 구성으로 하드웨어 이중화를 구성할 수 있습니다. 마스터 장비에 장애가 발생하게 되면 백업 장비로 연결되는 active-passive failover 방식으로 무중단 시스템 운영이 필요한 네트워크 구조에 적합한 이중화 구성이 가능합니다.

Sandboxing

샌드박싱은 기존 보안 서비스로 식별할 수 없는 알 수 없는 파일을 격리된 클라우드 환경으로 에뮬레이션 하여 악성 여부를 식별합니다. 패킷을 격리하여 검사하고 기존의 정적 보안 메커니즘이 탐지하지 못하는 새로운 악성 코드 유형을 식별하여 제로 데이 공격에 대한 예방을 할 수 있습니다.

다중 계층 보호

ZyXEL ZyWALL ATP는 외부와 내부에서 여러 유형의 위협에 대하여 다중 계층 보호로 설계되었습니다. Sandboxing, Anti-Malware, Reputation Filter 및 Intrusion Prevention은 외부 공격을 차단하고 Application Patrol 및 Web Filtering은 사용자의 부적절한 애플리케이션 사용의 제어와 불필요한 웹 액세스를 제한할 수 있습니다.



2FA with Google Authenticator

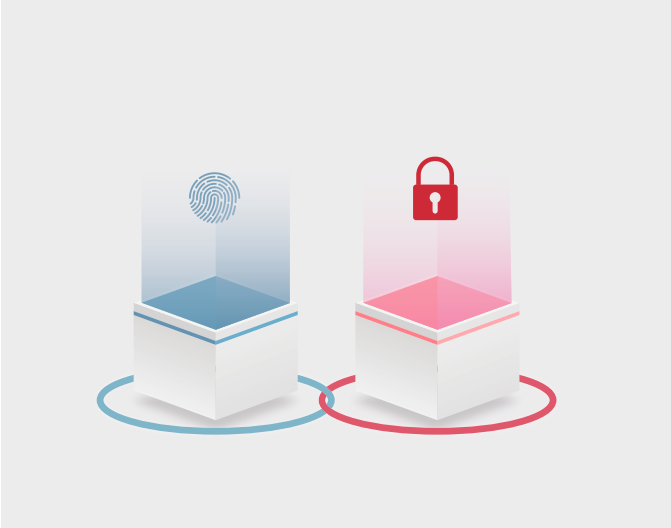
보안 터널을 통한 원격지 무선 네트워크 보안으로 기업 네트워크 접근 시 ID/PW 인증 뿐 아니라 Google OTP 이중 인증으로 등록 되지 않은 사용자의 내부 네트워크 접근을 제한하여 보안성을 확보하였습니다.

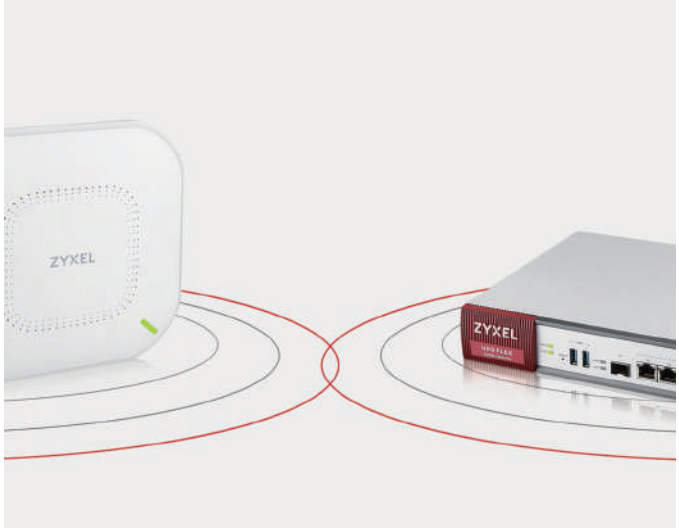
WPA2 Enterprise 인증보안

WPA2 로컬 유저 인증으로 침입자가 암호를 도용하여 내부 네트워크에 접근하는 것을 방지하여 사무실 네트워크 접근 시 사전에 등록된 ID와 PW 인증으로 등록되지 않은 사용자 접근을 제어합니다.

CDR (Collaborative Detection & Response)

IDP, Anti-Malware, URL Threat Filter 시그니처 데이터 베이스를 기반으로 유/무선 내부 네트워크 사용자가 악성 사이트에 접근하거나 비정상 트래픽을 발생시키는 시도가 감지되면 관리자에게 알림 메일을 전송합니다. 사용자가 악성 웹사이트에 일정 횟수 연결 시도가 감지되어 임계치에 도달하면 유선 사용자의 경우 IP를 차단하여 다른 네트워크 대역에 통신을 차단합니다. 무선 사용자의 경우에는 AP에서 연결을 해제하고 재연결 시 격리된 VLAN IP를 할당 하여 추가 감염의 확산을 방지합니다.



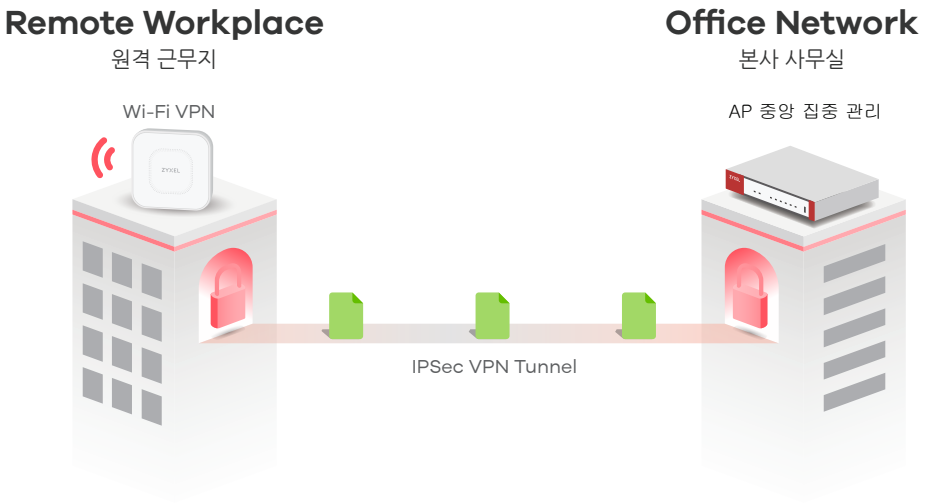


IDNS Content filter

기존의 Web(URL) Content filter는 클라이언트의 HTTPS/ TLS Hello 메시지의 SNI로 도메인을 분류 하였습니다. 새롭게 출시된 TLS1.3버전은 대다수의 웹 브라우저에서 점차 지원되고 있으며, ESNI를 사용하여 도메인이 암호화 되어있기 때문에 Web Content filter만으로 분류가 어렵습니다. USG FLEX 시리즈에서 새롭게 출시된 기능인 DNS Content filter는 DNS query 메시지에서 도메인을 분류하기때문에 Web Content filter와 함께 안정적인 도메인 접근을 제어 할 수 있습니다.

Secure WiFi

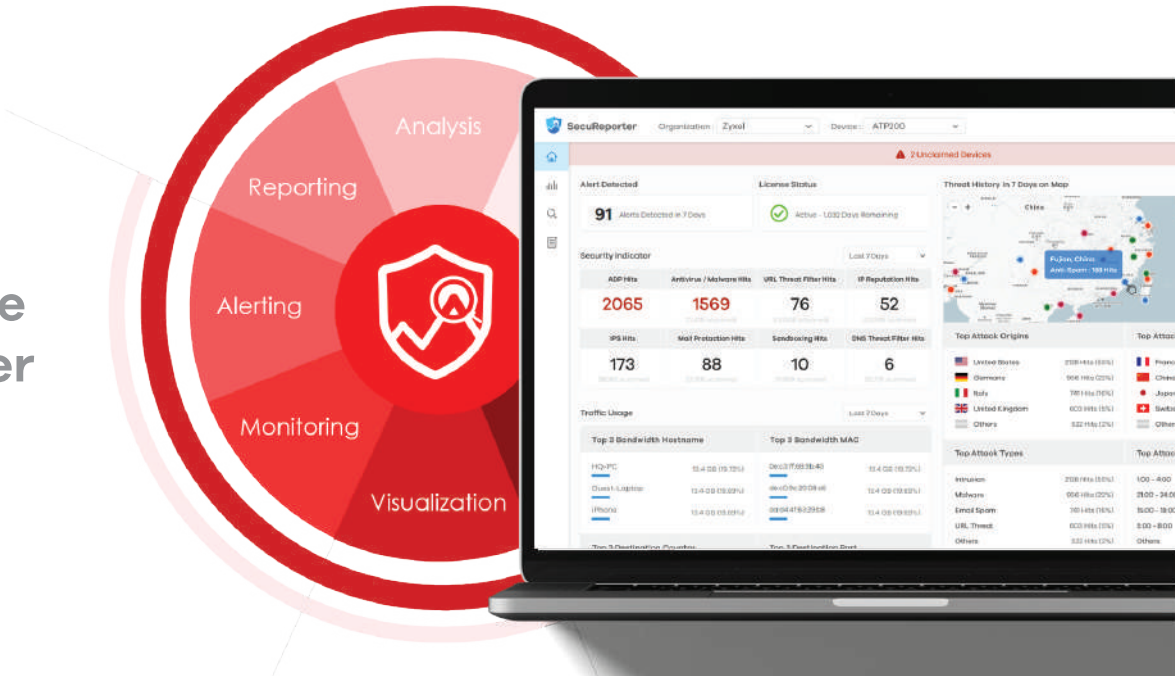
Secure WiFi는 USG FLEX와 원격지의 AP간 보안 터널을 생성하여 무선 네트워크의 보안을 강화합니다. Secure WiFi 기능으로 보안 터널이 맺어진 원격지에서는 USG FLEX의 SSID 정책을 동일하게 적용할 수 있습니다. 또한, 3rd party 게이트웨이 구성으로도 VPN 통신이 가능하며, 별도의 게이트웨이가 없어도 DHCP 서비스가 제공됩니다. Plug-n-play 옵션을 지원하여 네트워크 관리자는 원격지에서 손쉽게 네트워크를 확장할 수 있습니다. (* 지원 가능한 무선 AP : WAC500, WAX650S, WAX610D)



SecuReporter

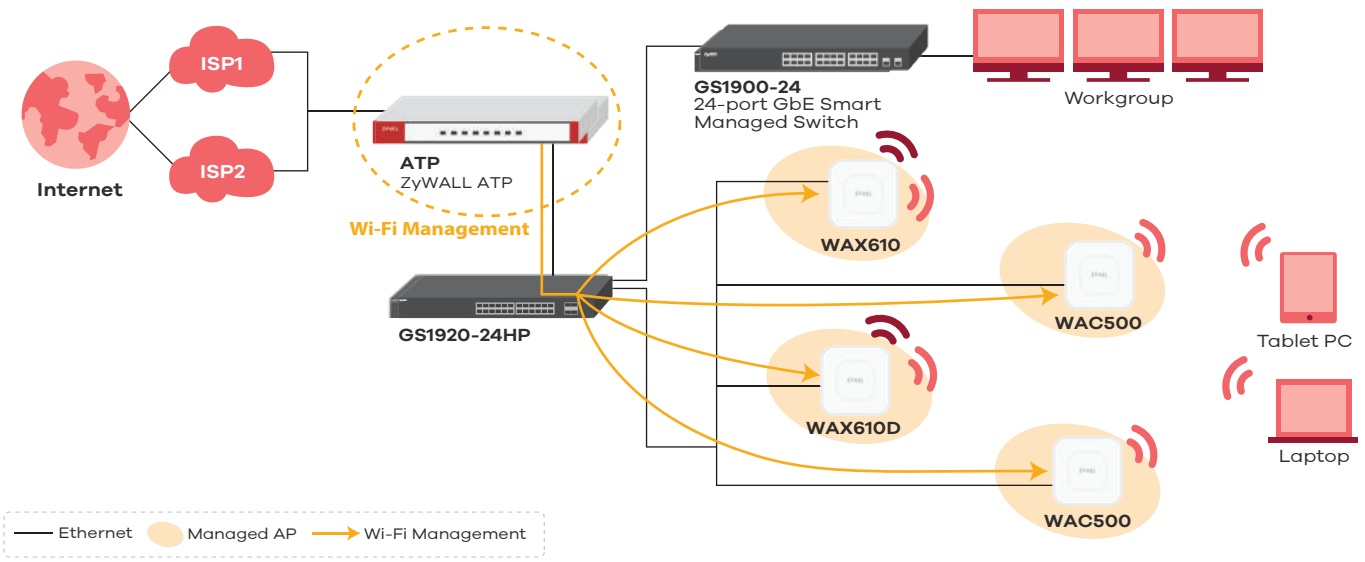
SecuReporter는 클라우드 기반의 지능형 보안 분석 리포트 서비스입니다. ZYXEL ZyWALL ATP에서 실시간 수집 된 데이터를 기반으로 Dashboard를 통해 보안 검출 내역 및 실시간 트래픽 데이터를 한눈에 확인 할 수 있습니다. Malware / IPS / Block Website 탐지 등 보안 필터에 의해 차단된 데이터는 Analyzer를 통해 그래프, 차트 형식으로 표시되어 손쉽게 파악이 가능합니다. 또한 비정상적인 데이터가 탐지되면 자동으로 지정된 메일로 알람을 보내주는 Alert 기능을 제공하여 네트워크 관리자는 비정상적인 데이터에 대해 빠른 대처가 가능합니다. 분석된 모든 데이터는 관리자가 지정한 메일로 일자별, 주간별 리포트가 PDF 파일로 제공되어 네트워크 관리자는 네트워크 보안 환경을 쉽고 편리하게 관리할 수 있습니다.

What's inside SecuReporter



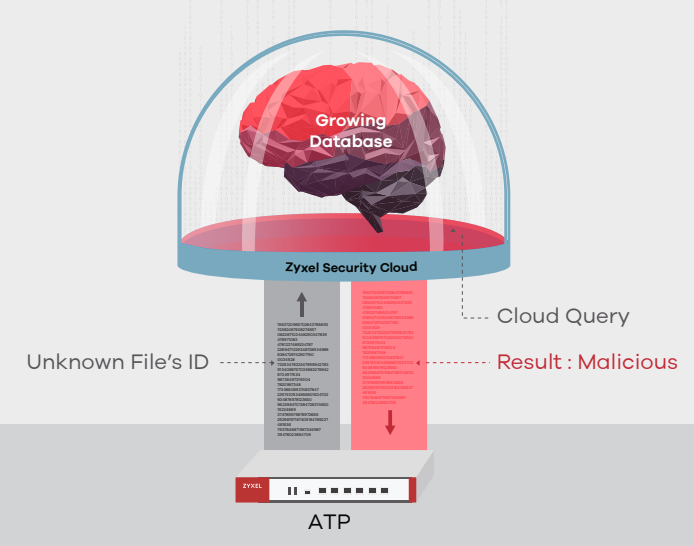
무선AP 컨트롤러 기능 APC(AP Controller) 탑재

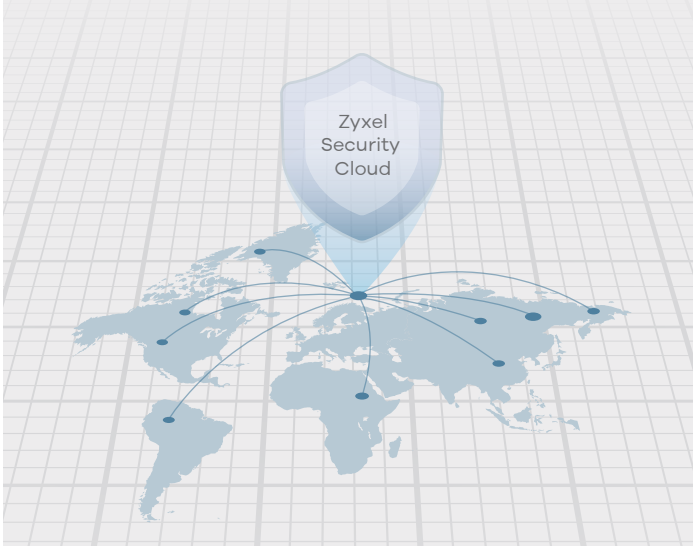
ZyXEL ZyWALL ATP는 무선 네트워크의 관리, 인증, 게스트 접속뿐 만 아니라 AP 구축 설계, 배치, 모니터링 기능을 하나로 담은 지능형 무선AP 컨트롤러 기능이 탑재된 된 통합 유무선 보안 장비입니다. 기본적으로 8개의 AP를 관리할 수 있으며, 라이선스를 추가하여 최대 520대 AP까지 연결할 수 있는 확장성을 갖추어 소규모 사무실, 병원, 학교 등 각 지사의 보안 및 무선 네트워크 관리가 필요한 장소에 방화벽과 함께 최적화된 무선 보안 솔루션을 제공합니다.



하이브리드 스캐닝을 이용한 멀웨어 차단

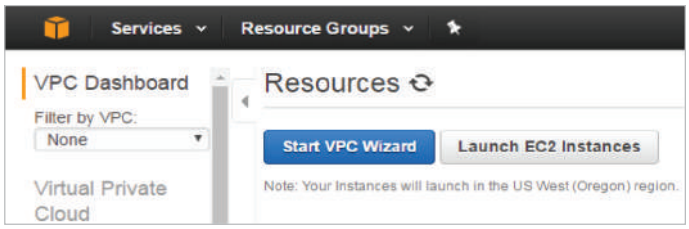
Zyxel ZyWALL ATP는 바이러스 및 기타 위협에 대해 장비에서 파일을 스캔하는 스트림 기반 엔진을 지원할 뿐만 아니라 머신 러닝 인텔리전스인 ZYXEL 보안 클라우드로 쿼리를 동시에 실행하여 알려지지 않은 위협에 대처할 수 있는 다중 소스 데이터베이스를 활용합니다.
하이브리드 모드는 처리량을 희생하지 않고 멀웨어 탐지율을 최대화합니다.

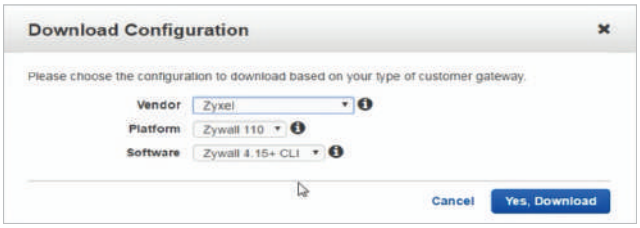


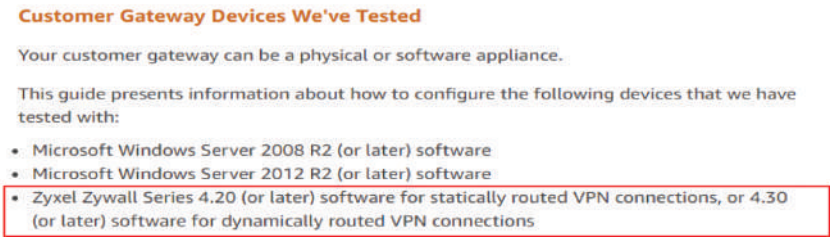


AWS 공식 인증 제품

Amazon VPN Firewall Gateway와 VPN을 연결하여 AWS Public Cloud 하단에 있는 VPC와 연결합니다. 이 연결을 통해 가상 네트워크 AWS 리소스를 사용하며, 가상 네트워킹 환경을 제어할 수 있습니다.



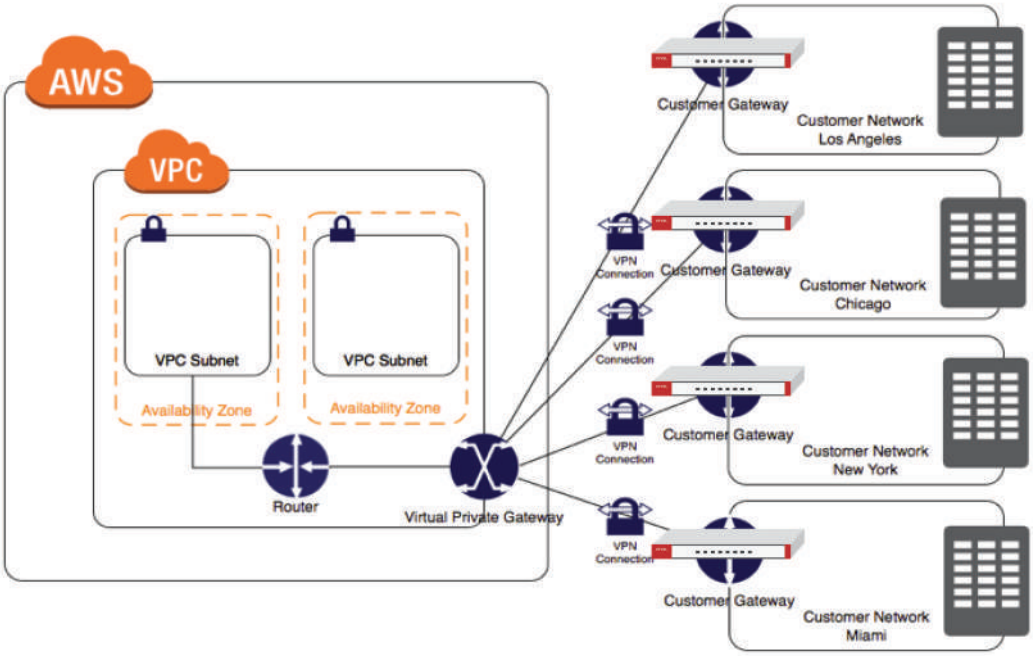




Azure 공식 인증 제품

Microsoft Azure의 VnetGateway와 VPN을 통하여 Azure의 Virtual Network 와 연결합니다.
네트워크 확장성과 유연성을 가지도록 BGP(Border Gateway Patrol)와 VTI(Virtual Tunnel Interface) 를 이용하여 구성할 수 있습니다.

VPN diagram

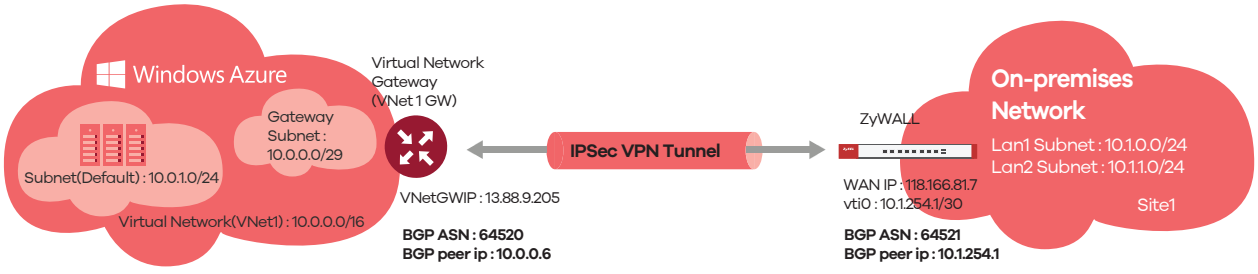


확인된 VPN 디바이스 및 디바이스 구성가이드

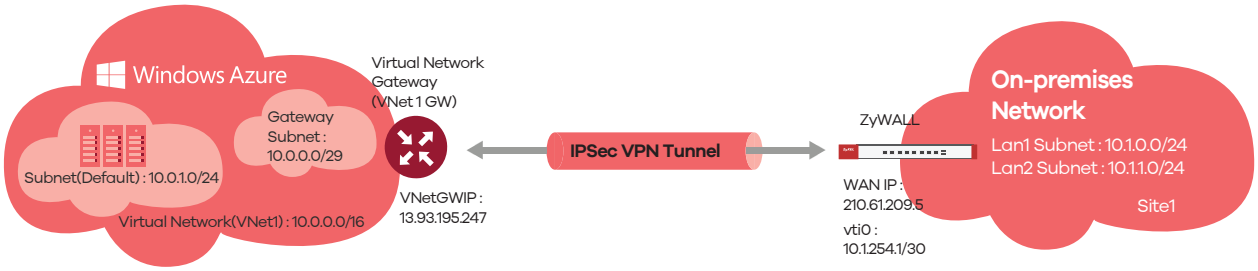
디바이스 공급업체와 협력하여 표준 VPN 디바이스 집합의 유효성을 검사했습니다. 다음 목록에 포함된 디자이스 제품군의 모든 디바이스는 VPN 게이트웨이에서 작동합니다. 구성하려는 VPN Gatewqy 솔루션의 VPN 유형(정책 기반 또는 경로 기반)을 이해하려면 VPN Gateway 설정 정보를 참조하세요.

디바이스 시리즈	OS 버전	VPN 유형
UTM 시리즈	ZLD v4.32+	IKEv2/IPsec을 통한 VTI IKEv2/IPsec을 통한 BGP
VPN 시리즈		
ATP 시리즈		

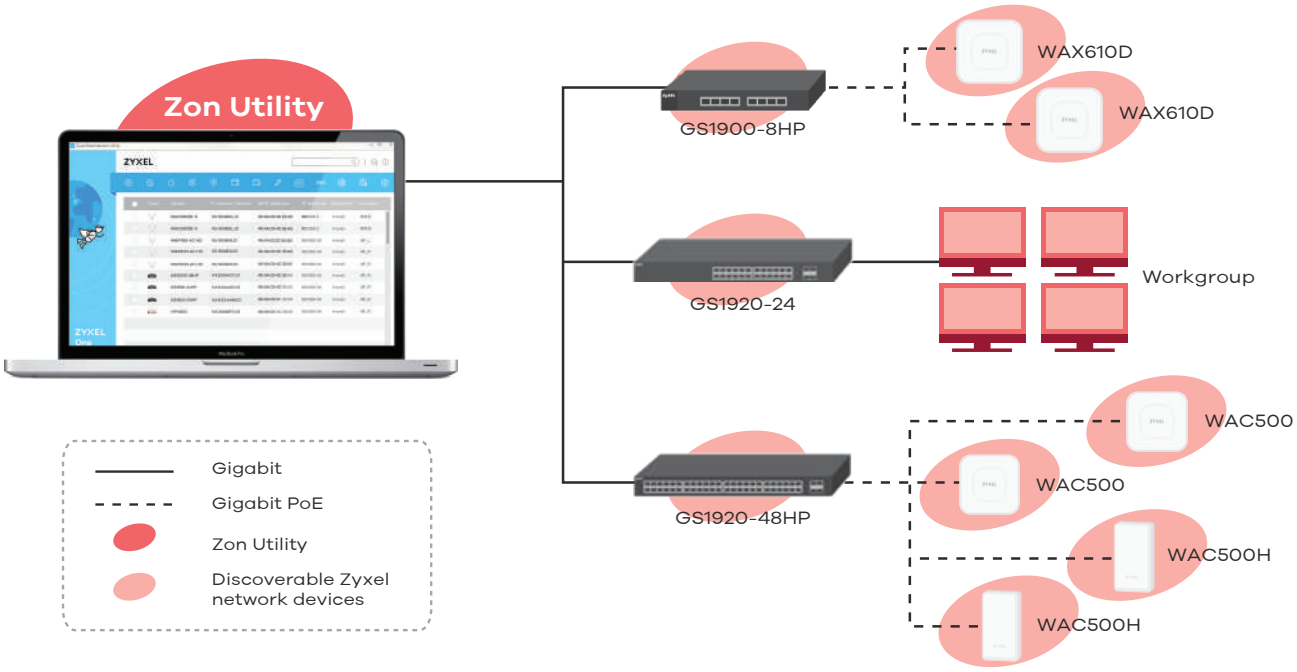
* BGP(Border Gatway Patrol) 구성



* VTI(Virtual Tunnel Interface) 구성

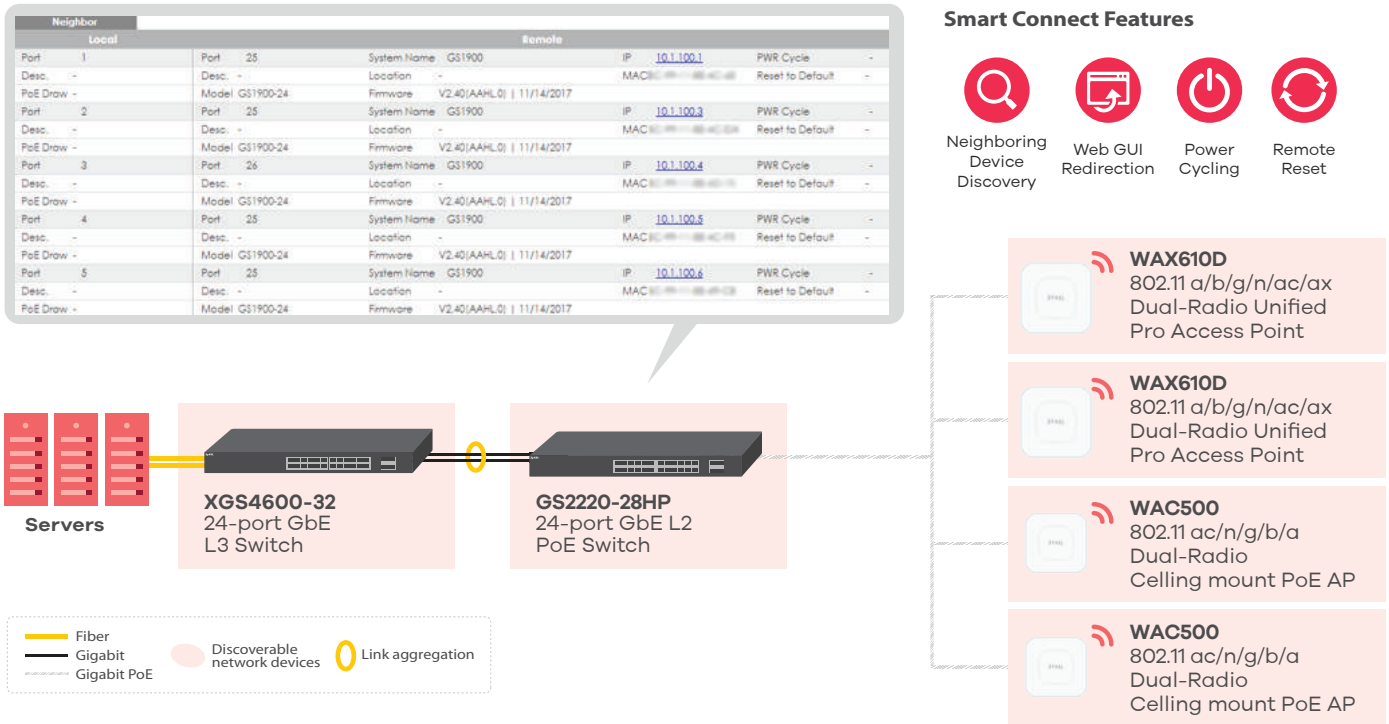


ZyXEL One Network - 네트워크 통합 관리 솔루션



Smart Connect

Smart Connect 기능이 탑재된 스위치나 AP를 통해 1)근접된 자이젤 네트워크 장비(스위치, AP, UTM)를 검색하고 2)원격에서 네트워크 장비 설정이 가능하도록 다른 자이젤 네트워크 장비의 Web GUI 화면을 연동하거나 3)장비의 재부팅 및 4)설정 초기화가 가능하여 네트워크 장애가 발생할 경우 빠른 원인 파악이 가능할 뿐만 아니라 장애 복구 시간을 단축할 수 있습니다.



ZON Utility, Smart Connect와 ZyXEL iStacking 과 같은 네트워크 통합 관리 솔루션을 통해 네트워크 구축시 초기 투자 비용을 줄이고 반복적이고 비효율적인 작업을 최소화할 수 있습니다.

Hardware Included License

Licensed Service	Feature	ZyWALL ATP800*
		Gold Security Pack (1 Year)
Web Filtering	Content Filter	Yes
App Patrol	Application visibility and control	Yes
Email Security*[3]	Anti-Spam	Yes
Anti-Malware	Anti-Malware with Hybrid Mode	Yes
	Threat Intelligence Maching Learing	Yes
IPS	Intrusion Detection & Prevension	Yes
Reputation Filter	IP Reputation	Yes
	DNS Threat Filter	Yes
	URL Threat Filter	Yes
Sandboxing	Sandboxing	Yes
SecuReporter	SecuReporter Premium	Yes
Secure WiFi	Secure Tunnel for Remote AP	Yes
	Managed AP Service	Unlock to Max
CDR	Collaborative Detection & Response	Yes
Security Profile Sync*	Sync up security profiles across networks	Yes
Nebula Professional Pack	Cloud Networking Management	Yes

* Gold Security Pack은 기본 1년 + 30일 Trial 라이선스가 Bundle로 되어 있습니다.
* Secure WiFi 는 라이선스는 Bundle 상품이 아니므로 별도 구매시 사용 가능합니다.
* Security Profile Sync는 Nebula clould 모드에서만 지원합니다.

Secure WiFi

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

Applied Products	Number Tunnel Mode AP	Supported Remote AP
ATP800	130	WAX650S / WAX610D / WAC500 / WAC500H

Specifications

Model		ZyWALL ATP800
Product photo		
Hardware Specifications		
Interface		12 (configurable), 2x SFP (configurable)
USB 3.0 ports		2
Console port		DB9
Rack-mountable		Yes
Fanless		-
System Capacity & Performance*1		
SPI firewall throughput (Mbps)*2		8,000
VPN throughput (Mbps)*3		1,500
IPS throughput (Mbps)*4		2,700
Anti-malware throughput (Mbps)*4		2,000
UTM throughput (AV and IDP, Mbps)*4		1,900
Max. TCP concurrent sessions*5		2,000,000
Max. concurrent IPsec VPN tunnels*6		1,000
Recommended gateway-to-gateway IPsec VPN tunnels		300
Concurrent SSL VPN users		500
VLAN interface		128
Speedtest Performance		
SPI firewall throughput (Mbps)*7		930
Key Features		
Security Service	Sandboxing*8	Yes
	Web Filtering*8	Yes
	Application Patrol*8	Yes
	Anti-Malware*8	Yes
	IPS*8	Yes
	Reputation Filter*8	Yes
	Geo Enforcer	Yes
	SecuReporter Premium*8	Yes
	Collaborative Detection & Response*8	Yes
	Device Insight	Yes
	Security Profile Sync (SPS)*8	Yes
	SSL (HTTPS) Inspection	Yes
	2-Factor Authentication	Yes
VPN Features	VPN	IKEv2, IPSec, SSL, L2TP/IPSec
	Microsoft Azure	
	Amazon VPC	Yes
Key Features		
WLAN Management	Default number of managed AP	8
	Recommend max. AP in 1 AP Group	300

Model		ZyWALL ATP800
Key Features		
WLAN Management	Secure WiFi Service*8	Yes
	Maximum Number of Tunnel-Mode AP	130
	Maximum Number of Managed AP	520
Connectivity Management	Nebula Cloud Managed Mode	Yes
	Device HA Pro	Yes
	Link Aggregation (LAG)	Yes
	Concurrent devices logins (max.)	1500
Power input		100-240 V AC, 50/60 Hz, 2.5 A max.
Max. power consumption (watt)		46
Heat dissipation (BTU/hr)		120.1
Physical Specifications		
Item	Dimensions (WxDxH) (mm/in.)	430 x 250 x 44/ 16.93 x 9.84 x 1.73
	Weight (kg/lb.)	3.3/ 7.28
Packing	Dimensions (WxDxH) (mm/in.)	519 x 392 x 163/ 20.43 x 15.43 x 6.42
	Weight (kg/lb.)	4.8/10.58
Included accessories		• Power cord • Rack mounting kit
Environmental Specifications		
Operating environment	Temperature	0°C to 40°C/ 32°F to 104°F
	Humidity	10% to 90% (non-condensing)
Storage environment	Temperature	-30°C to 70°C/ -22°F to 158°F
	Humidity	10% to 90% (non-condensing)
MTBF (hr)		947,736
Acoustic noise		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
Safety		LVD (EN60950-1), BSMI

*: This matrix with firmware ZLD5.3 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.
*8: Enable or extend feature capacity with Zyxel service license.

Access Point Compatibility List

Secure Tunnel for Remote AP

Product	Remote AP	Number of Tunnel Mode AP	Supported Remote AP
ATP	ATP800	130	• WAX650S • WAX610D • WAC500 • WAC500H
USG FLEX	USG FLEX 100	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	• NWA5301-NJ • WAC500* • WAC500H*	• WAX650S • WAX610D • WAC6103D-I • WAC6552D-S

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.

Software Features

Security Service

Firewall

- ICSA-certified corporate firewall
- Routing and transparent (bridge) modes
- Stateful packet inspection
- SIP NAT traversal
- H.323 NAT traversal*2
- 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*2

Intrusion Prevention System (IPS)

- Support both intrusion detection and prevention
- Support allowlist (whitelist) to deal with false positives involving known benign activity*2
- Support rate-based IPS signatures to protect networks against application-based DoS and brute force attacks*2
- 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*2
- Inspection on various protocols: HTTP, FTP, SMTP, POP3, and IMAP
- Inspection on various protocols: HTTPs, FTPs, SMTPs, POP3s, and IMAPs*2
- Customizable signature & protection profile*2
- 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*2

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*2
- 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*2
- 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*2
- GRE Tunnel for Campus AP
- SSL inspection support*2

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*2
- Agentless Scanning for discovery and classification of devicess
- Provide the dashboard to view all devices on the network, including wired, wireless, BYOD, IoT, and SecuExtender (remote endpoint)
- Extended view of the inventory 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*2
- NAT over IPSec
- L2TP over IPSec
- SecuExtender Zero Trust VPN Client provisioning
- Support native Windows, iOS/macOS and Android (StrongSwan) client provision*2
- Support 2FA Email/SMS*2
- Support 2FA Google Authenticator

SSL VPN*2
- 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*2
- Supports AP Controller (APC) version 3.60
- 802.11ax Wi-Fi 6 AP and WPA3 support
- 802.11k/v/r support
- 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*2
- 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)
- 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
- NAT Virtual Server Load Balancing
- VLAN tagging (802.1Q)
- Virtual interface (alias interface)
- Policy-based routing (user-aware)*2
- Policy-based NAT (SNAT)
- GRE*2
- 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*2
- Bandwidth limit per IP
- Bandwidth management by application
- Link Aggregation support*1*2

Management

Nebula Cloud Management*3
- 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

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)
- 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*2

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
*1: Supported models ATP500/700/800
*2: Only supported in On-Premise mode
*3: Only supported in Cloud mode