ZYXEL

ZyWALL USG FLEX 100 / 200 / 500 / 700

Overview

ZyXEL USG FLEX 시리즈는 Zero-Trust Network 기반의 통합 보안장비로써 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.

새로 설계된 Multi-Core하드웨어 플랫폼을 바탕으로 컴퓨팅 파워 사용량을 최소화하여 방화벽 성능과 UTM 성능을 극대화하였으며, Bitdefender, McAfee, Trend Micro 와 같은 세계 최고의 보안 회사의 엔진을 탑재하여 주기적인 업데이트를 통해 최신 보안 위협으로부터 빠르고 정확하게 보호합니다.

점점 증가되는 재택근무 환경에서도 안전하게 사내 네트워크 자산을 보호할 수 있도록 SSL, IPSec, L2TP 와 같이 다양한 VPN 알고리즘 및 호환성을 지원하여 보안이 강화된 원격 접속을 제공하며, 사내 네트워크 접근 시 구글 OTP 서비스를 이용한 2단계 인증으로 한층 더 강화된 보안 인증 서비스를 제공합니다.

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

ZyXEL USG Flex 시리즈는 통합 보안 네트워크를 구축하고자 하는 기업 사무실, 공유오피스, 프랜차이즈와 같이 불특정 다수가 이용하는 내부 네트워크 환경의 보안과 더불어 원격지 보안 네트워크 환경을 구축해야 하는 고객을 위한 최적의 통합 보안 솔루션입니다.

- 중소규모 비즈니스를 위한 올인원 통합 방화벽 기능
- 라이선스기반의 통합보안장비
  - Web Filtering
  - IPS
  - Application Patrol
  - Anti Malware
  - CDR(Collaborative Detection & Response)
  - Email Security
- UTM 라이선스 1년간 Bundle 제공
  - 30일 Trial 기간 제공
  - 총 13개월 사용 무상 지원
- 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 520대
- 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 USG Flex의 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 로그를 별도로 저장할 수 있도록 USB 포트가 장착되어 있습니다.

고성능 방화벽 및 VPN 처리 성능

ZYXEL USG Flex는 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

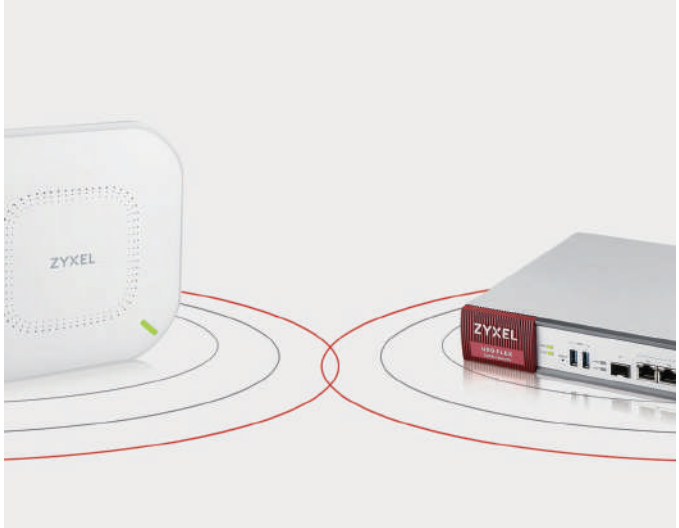
단일 WAN 인터페이스 환경에서는 내부의 트래픽을 전부 단일 인터페이스에서 처리하게 될 경우 과다한 트래픽으로 인해 장애가 발생 하여 결국 운영중인 서비스가 중단되는 결과를 초래할 수 있습니다. ZyXEL USG Flex 에서는 단일 WAN 구성의 네트워크 부하를 줄이기 위해 각각 다른 통신사 회선을 이중화하여 active-active 로드밸런싱(Load-Balancing) 설정 및 active-passive failover 구성이 가능하며, 회선 이중화 및 정책 라우터 방식을 통해서 다양한 서비스 경로를 제어할 수 있습니다. 또한 단일 장비 운영으로 인해 불안한 네트워크의 장애를 사전에 방지하고자 두 대의 장비를 동일 구성으로 하드웨어 이중화를 구성할 수 있습니다. active-passive failover 구성 뿐 만 아니라 마스터 장비에 장애가 발생하게 되면 백업 장비 쪽에서 마스터의 가상 라우터 (VRRP)를 모두 종료하고 백업 장비로 연결되는 active-active 방식으로 무중단 시스템 운영이 필요한 네트워크 구조에 적합한 이중화 구성이 가능합니다.

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.

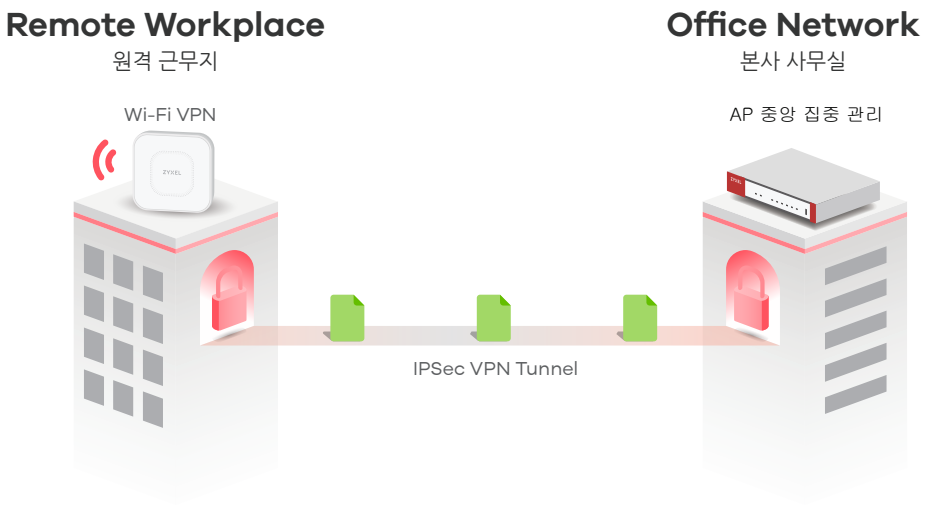
DNS Content filter

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 filter 만으로 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 : WAC500H, WAC500, WAX650S, WAX610D)

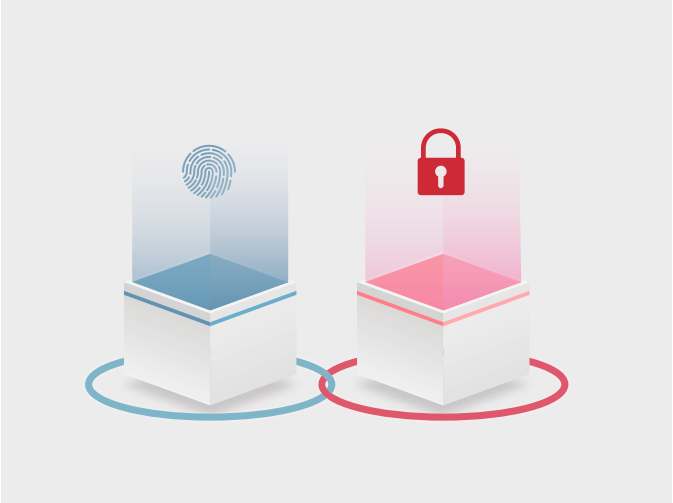


WPA2 Enterprise 인증 보안

WPA2 로컬 유저 인증으로 침입자가 암호를 도용하여 내부 네트워크에 접근하는것을 방지하여 사무실 네트워크 접근시 사전에 등록된 ID와 PW 인증으로 등록되지 않은 사용자 접근을 제어합니다.

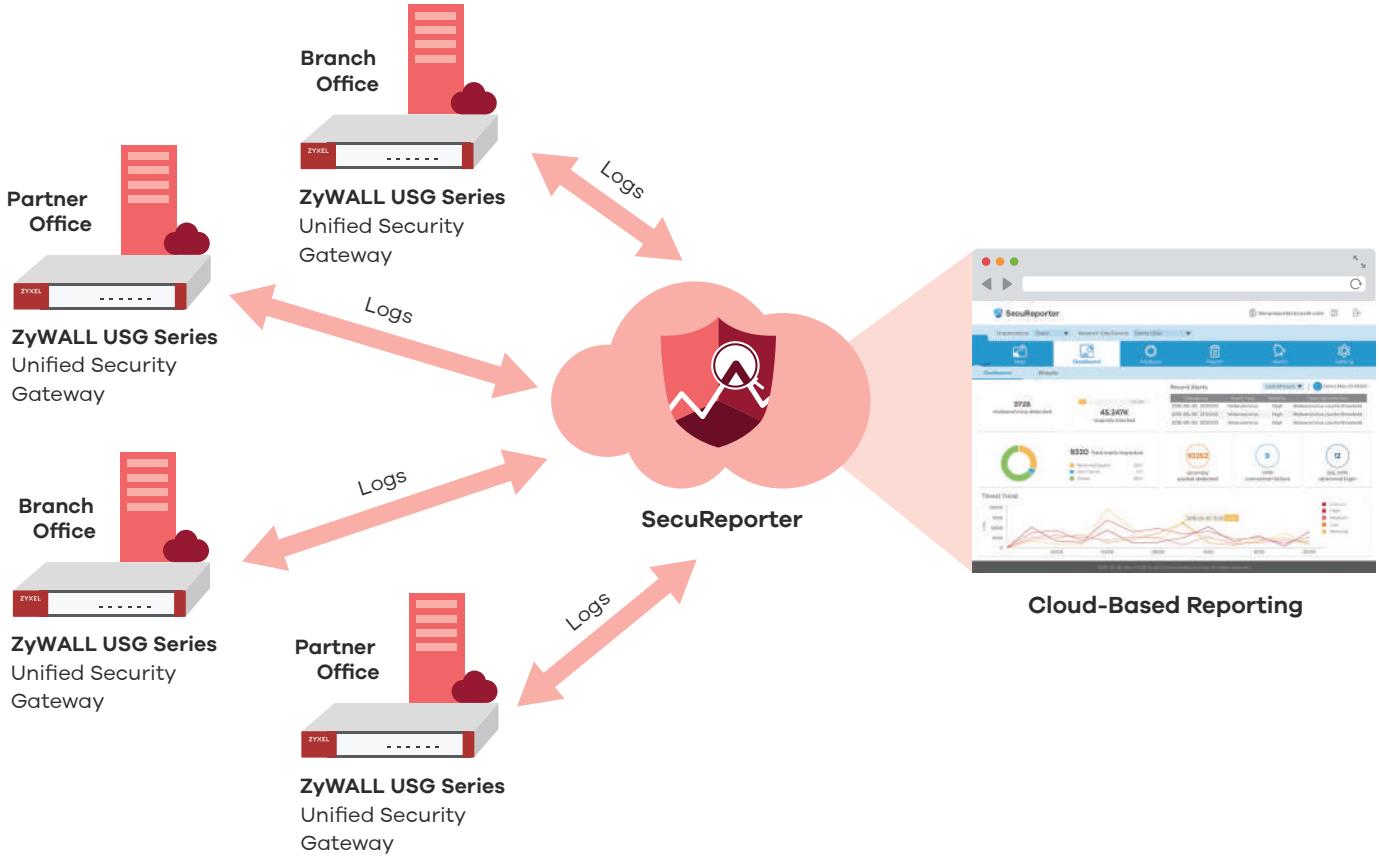
2FA with Google Authenticator

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.



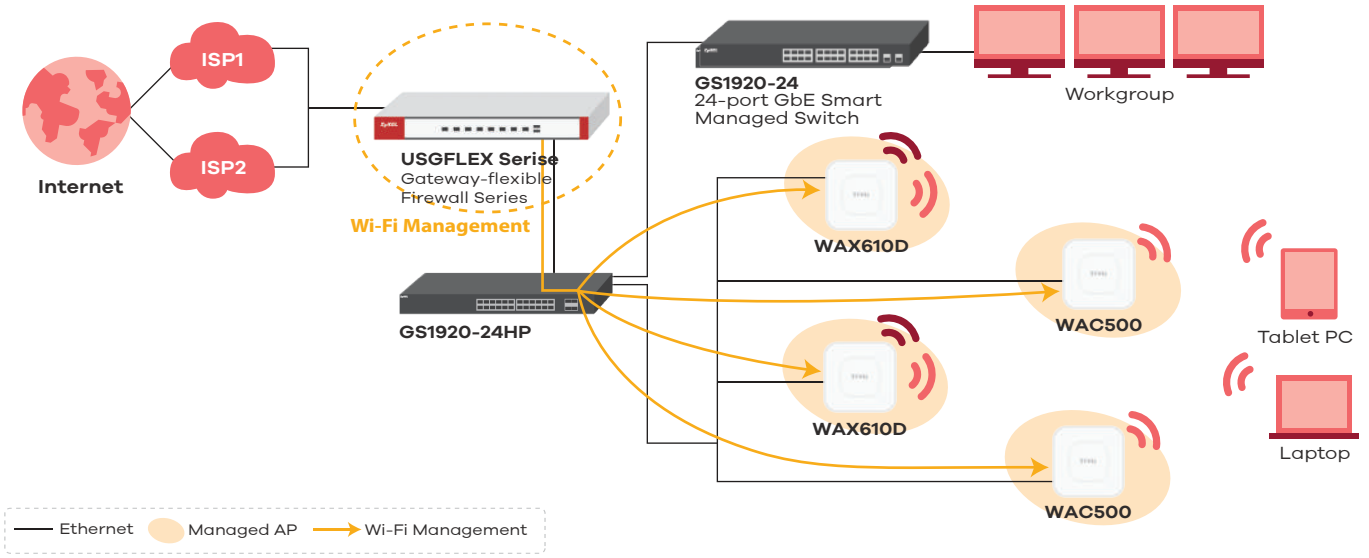
SecuReporter

SecuReporter는 클라우드 기반의 지능형 보안 분석 리포트 서비스입니다. ZYXEL USG Flex에서 실시간 수집 된 데이터를 기반으로 Dashboard를 통해 보안 검출 내역 및 실시간 트래픽 데이터를 한눈에 확인 할 수 있습니다. Malware / IDP / 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.



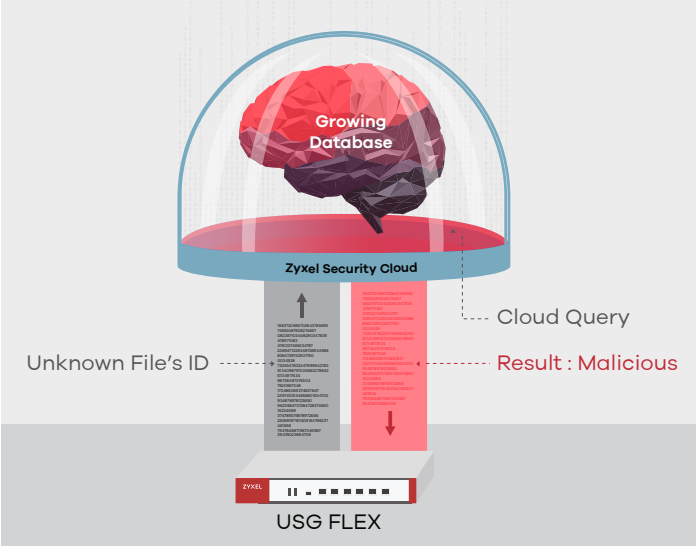
무선 AP 컨트롤러 기능 APC(AP Controller) 탑재

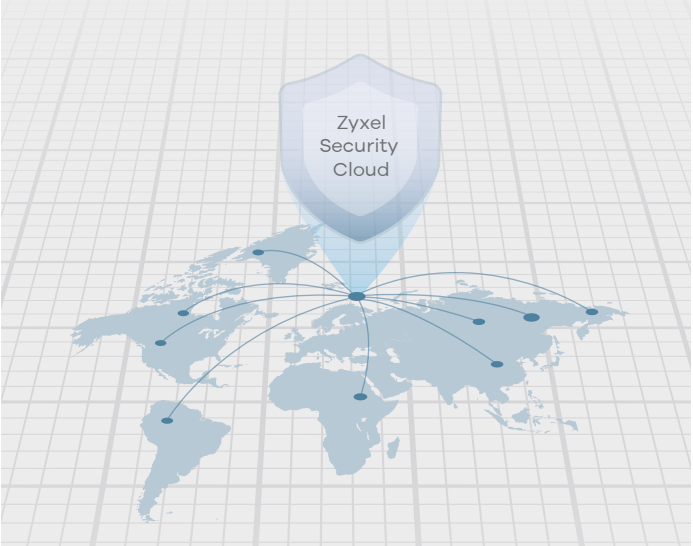
ZyXEL USG Flex 는 무선 네트워크의 관리, 인증, 게스트 접속 뿐 만 아니라 AP 구축 설계, 배치, 모니터링 기능을 하나로 담은 지능형 무선AP 컨트롤러 기능이 탑재된 된 통합 유무선 보안 장비입니다. 기본적으로 8개의 AP를 관리할 수 있으며, 라이선스를 추가하여 최대 520대 AP까지 연결 할 수 있는 확장성을 갖추어 소규모 사무실, 병원, 학교 등 각 지사의 보안 및 무선 네트워크 관리가 필요한 장소에 방화벽과 함께 최적화된 무선 보안 솔루션을 제공합니다.



Email Security

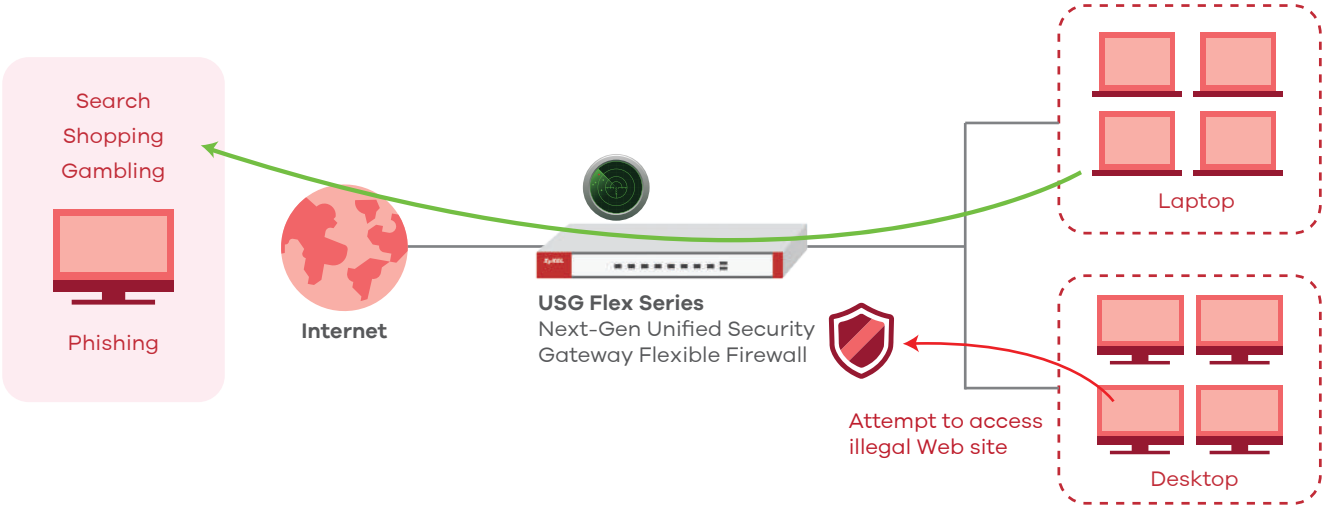
Email Security 는 스팸, 피싱, 바이러스가 포함된 이메일을 감지하고 차단할 수 있습니다. McAfee의 데이터센터와 다중 트래픽 수집 노드를 포함하여 매일 10 억건이상의 인터넷 메일을 수집하며, RPD(Recurrent Pattern Detection)기술은 이렇게 수집된 메일 트래픽을 자동으로 분석하여 전 세계적으로 유포되는 스팸 메일을 탐지합니다. 또한 원하지 않는 메일의 80% 이상을 차단할 수 있으며, 의심스러운 메시지를 차단하거나 지연시키는 바이러스 발생 방지 기능을 적용할 수 있습니다.





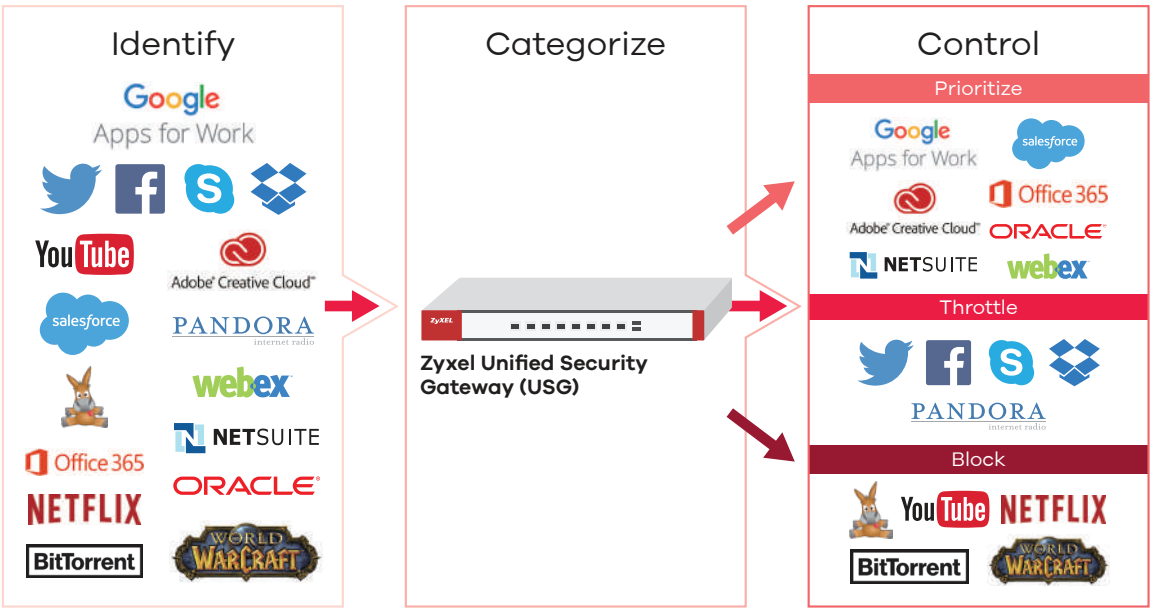
Content Filtering

Content Filtering은 관리자가 직접 각각의 URL을 개별적으로 차단하지 않고도 부적절한 사이트와 소셜 네트워킹 사이트 등 특정 유형의 웹 콘텐츠 를 쉽게 차단할 수 있습니다. 지속적으로 분석하고 추척한 1,400억개 이상의 대규모 클라우드 기반 URL 데이터베이스를 바탕으로 악성 웹 콘텐츠에 대해 높은 정확도와 광범위하고 즉각적인 보호를 제공합니다.



Application Patrol

App patrol은 최대 19개의 카테고리와 수천 개의 어플리케이션을 관리 및 제어 기능을 제공하며, DPI 엔진을 사용하여 관리자가 어플리케이션을 식별하고 분류할 수 있도록 합니다. 필터링 외에 다양한 컨트롤모드(Prioritize, BWM, Block)를 제공하며 소셜 미디어, 게임, P2P 및 기타 웹 어플리케이션에 효과적인 정책을 적용할 수 있습니다.

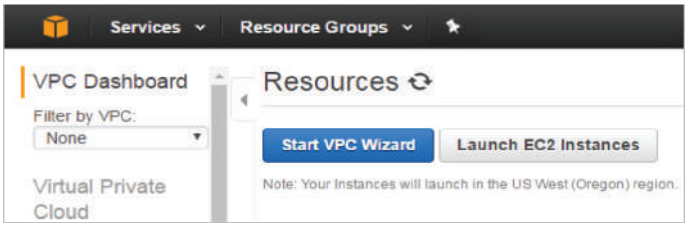


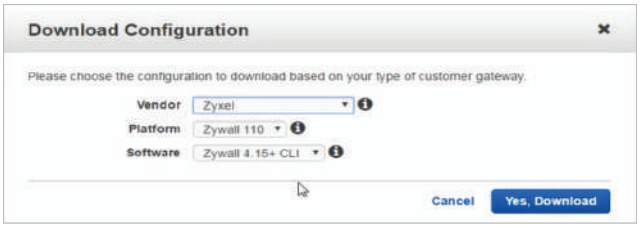
실시간 침입 탐지 방어(IDP)

Intrusion Detection and Prevention(IDP)는 내부 네트워크에 침투할 수 있는 트로이 목마나 백도어 같이 악의적인 응용 프로그램을 실시간 감지 하고 차단할 수 있는 침입 탐지 방어 기능입니다. 간단한 포트나 프로토콜 기반의 방화벽으로 확인되지 않는 취약점을 점검하기 위해 다양한 계층과 프로토콜을 모니터링하는 Deep Packet Inspection(DPI) 기술을 사용하고, 트로이 목마나 백도어 같이 잘 알려진 응용 프로그램에 대한 8,000개 이상의 시그니처를 지원하여 네트워크를 보호합니다. 또한, 계속 진화하는 IM/P2P 응용프로그램에 대응하기 위해 App Patrol을 활용하여 3,000 개 이상의 소셜, 게임 및 기타 응용 프로그램을 식별, 분류 및 제어하며 사용자의 생산성을 향상시키고 대역폭 남용을 방지하기 위해 응용 프로그램 들의 우선순위를 지정할 수 있습니다.

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.





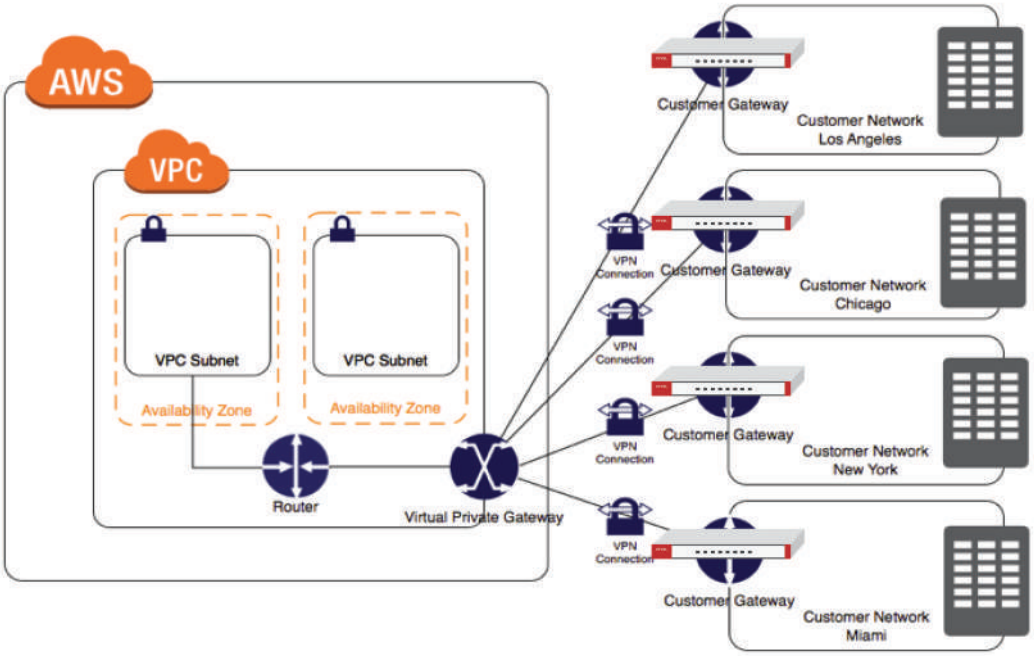
Customer Gateway Devices We've Tested

Your customer gateway can be a physical or software appliance.

This guide presents information about how to configure the following devices that we have tested with:

- Microsoft Windows Server 2008 R2 (or later) software
- Microsoft Windows Server 2012 R2 (or later) software
- Zyxel Zywall Series 4.20 (or later) software for statically routed VPN connections, or 4.30 (or later) software for dynamically routed VPN connections

VPN diagram



Azure 공식 인증 제품

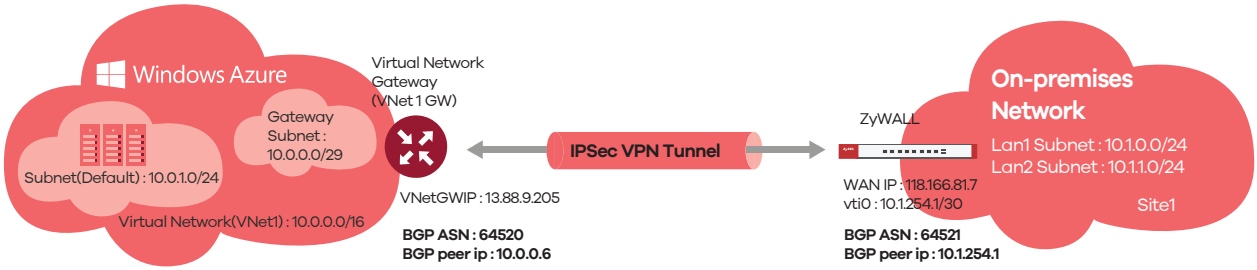
Microsoft Azure의 VnetGateway와 VPN을 통하여 Azure의 Virtual Network 와 연결합니다.
네트워크 확장성과 유연성을 가지도록 BGP(Border Gateway Patrol)와 VTI(Virtual Tunnel Interface) 를 이용하여 구성할 수 있습니다.

확인된 VPN 디바이스 및 디바이스 구성가이드

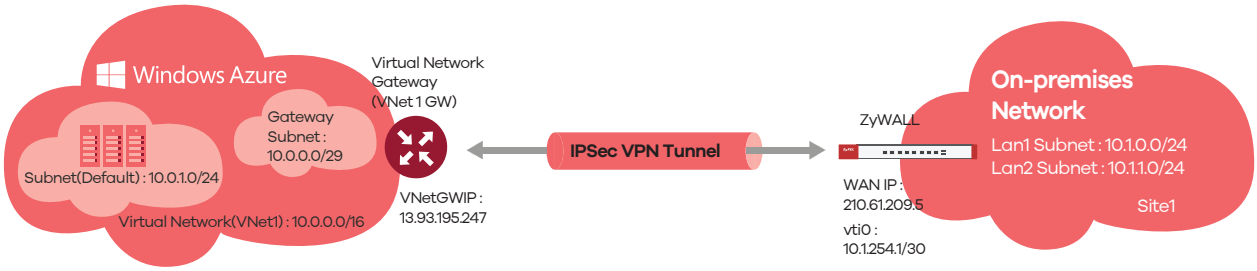
디바이스 공급업체와 협력하여 표준 VPN 디바이스 집합의 유효성을 검사했습니다. 다음 목록에 포함된 디자이스 제품군의 모든 디바이스는 VPN 게이트웨이에서 작동합니다. 구성하려는 VPN Gateway 솔루션의 VPN 유형(정책 기반 또는 경로 기반)을 이해하려면 VPN Gateway 설정 정보를 참조하세요.

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

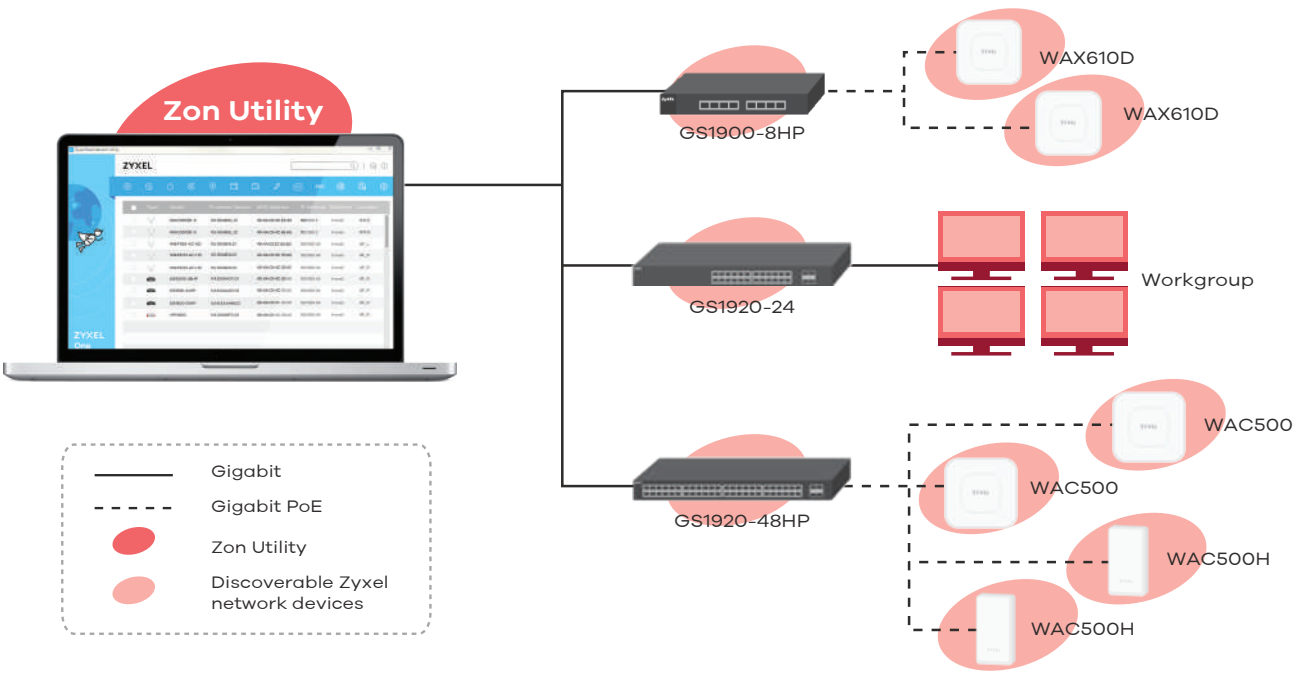
* BGP(Border Gatway Patrol) 구성



* VTI(Virtual Tunnel Interface) 구성

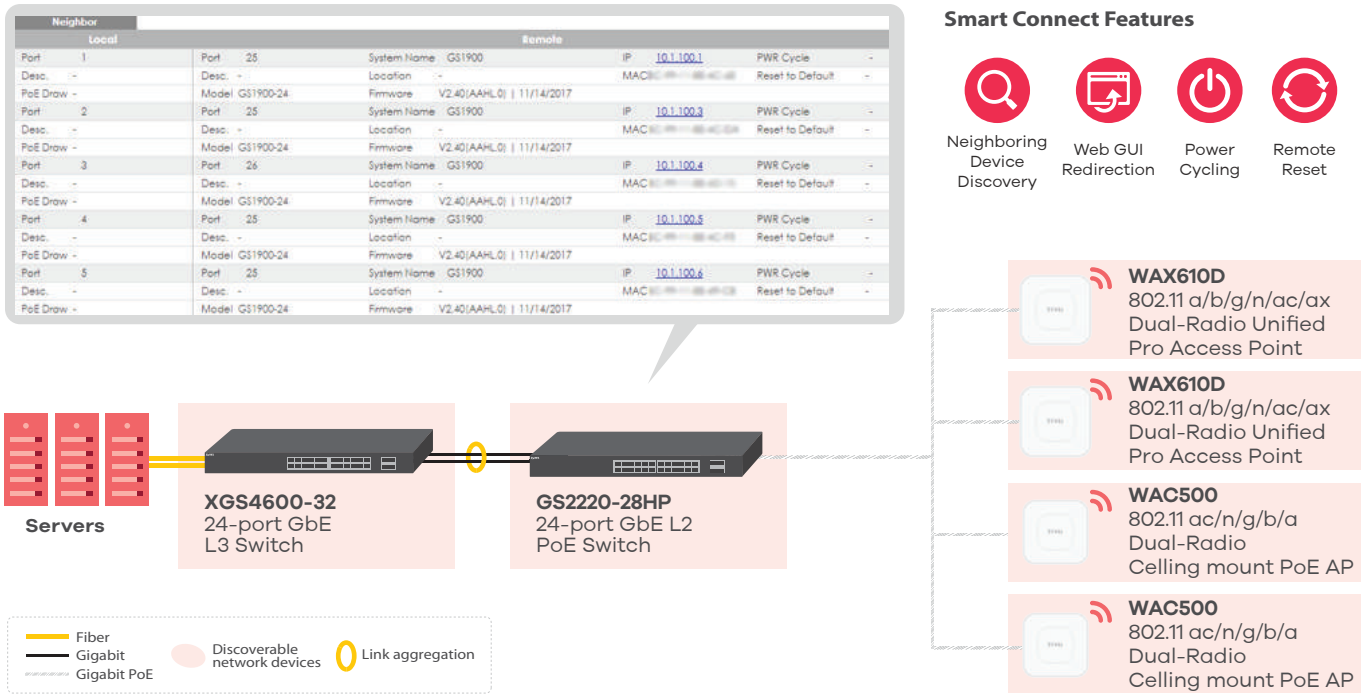


ZyXEL One Network - 네트워크 통합 관리 솔루션



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

	Service/Component	Bundle License	Single License
UTM	Web Filtering	●	-
	Anti-Malware	●	-
	IPS	●	-
	Application Patrol	●	-
	SecuReporter	●	-
	Collaborative Detection & Response	●	-
	Email Security	●	-
	Security Profile Sync	-	-
Hospitality	Hotspot Management service	●	-
	Concurrent Device Upgrade	●	-
Secure WiFi	Secure tunnel & Managed AP Service	-	●

* UTM Pack은 기본 1년 + 30일 Trial 라이선스가 Bundle로 되어 있습니다.
* Secure WiFi 는 라이선스 Bundle 상품이 아니므로 별도 구매시 사용이 가능합니다.

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
USG Flex 100	6	WAX650S / WAX610D / WAC500 / WAC500H
USG Flex 200	10	
USG Flex 500	18	
USG Flex 700	130	

Managed AP Service (on-premise only)

- 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
- ACustomizable captive portal page
- WiFi Multimedia (WMM) wireless QoS
- CAPWAP discovery protocol
- Multiple SSID with VLAN
- Supports ZyMesh
- Supports AP Controller (APC)

Managed AP Service	Applied Products	Number of Managed AP(Default/Maximum)
APC	USG Flex 100	8/ 24
	USG Flex 200	8/ 40
	USG Flex 500	8/ 72
	USG Flex 700	8/ 520

Model	USG FLEX 100	USG FLEX 200	USG FLEX 500	USG FLEX 700
Product photo				
Hardware Specifications				
10/100/1000 Mbps RJ-45 ports	4 x LAN/DMZ, 1 x WAN	4 x LAN/DMZ, 2 x WAN 1 x SFP	7 (configurable), 1 x SFP (configurable)	12 (configurable), 2 x SFP (configurable)
USB3.0 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 & Performance*1				
SPI firewall throughput (Mbps)*2	900	1,800	2,300	5,400
VPN throughput (Mbps)*3	270	450	810	1,100
VPN IMIX throughput (Mbps)*3	100	160	240	550
IDP throughput (Mbps)*4	540	1,100	1,500	2,000
AV throughput (Mbps)*4	360	570	800	1,450
UTM throughput (AV and IDP)*4	360	550	800	1,350
Max. TCP concurrent sessions*5	300,000	600,000	1,000,000	1,600,000
Max. concurrent IPsec VPN tunnels*6	40	100	300	500
Concurrent SSL VPN users	30	60	150	150
VLAN interface	8	16	64	128
Concurrent devices logins (default/max.)*7*8	64	200	200/300	500/2000
Speedtest Performance				
SPI firewall throughput (Mbps)*11	760	810	810	840
Security Features				
Anti-Malware*7	Yes	Yes	Yes	Yes
IPS*7	Yes	Yes	Yes	Yes
Application Patrol*7	Yes	Yes	Yes	Yes
Email Security	Yes	Yes	Yes	Yes
Web filtering*7	Yes	Yes	Yes	Yes
SecuReporter Premium*7	Yes	Yes	Yes	Yes
Collaborative Detection & Response*7	Yes	Yes	Yes	Yes
SSL (HTTPS) Inspection	Yes	Yes	Yes	Yes
2-Factor Authentication	Yes	Yes	Yes	Yes
VPN Features				
VPN	IKEv2, IPSec, SSL, L2TP/IPSec	IKEv2, IPSec, SSL, L2TP/IPSec	IKEv2, IPSec, SSL, L2TP/IPSec	IKEv2, IPSec, SSL, L2TP/IPSec
Microsoft Azure	Yes	Yes	Yes	Yes
Amazon VPC	Yes	Yes	Yes	Yes
WLAN Management				
Default Number of Managed AP	8	8	8	8
Recommend max. AP in 1 AP Group	10	20	60	200
Secure WiFi Service*7	Yes	Yes	Yes	Yes
Maximum No. of Tunnel-Mode AP	6	10	18	130
Maximum No. of Managed AP	24	40	72	520

Model		USG FLEX 100	USG FLEX 200	USG FLEX 500	USG FLEX 700
Connectivity Management					
Cloud-managed (Nebula) Mode		Yes	Yes	Yes	Yes
Hotspot Management*7		-	Yes	Yes	Yes
Ticket printer support*9/ Support Qty (max.)		-	Yes (SP350E) / 10	Yes (SP350E) / 10	Yes (SP350E) / 10
Device HA Pro		-	-	Yes	Yes
Power Requirements					
Power input		12V DC, 2A max.	12V DC, 2.5A max.	12V DC, 4.17A	100-240V AC, 50/60Hz, 2.5A max.
Max. power consumption (Watt Max.)		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 147.3 x33/ 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/ 16.93 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.)	1.40/3.09	2.23 (W/O bracket) 2.42 (W/ bracket)	2.83/6.24	4.8/10.58
Included accessories		• Power adapter • RJ-45 - RS-232 Cable for console connection	• Power adapter • Rack mounting kit	• Power adapter • Power cord • Rack mounting kit	• Power cord • Rack mounting kit
Environmental Specifications					
Operating	**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	**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)		989810.8	529688.2	529688.2	947736
Acoustic Noise		-	-	24.5dBA on < 25degC Operating Temperature, 41.5dBA on full FAN speed	24.5dBA on < 25degC Operating Temperature, 41.5dBA on full FAN speed
Certifications					
EMC		FCC Part 15 (Class B), CE EMC (Class B), C-Tick (Class B), BSMI	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	LVD (EN60950-1), BSMI

*: This matrix with firmware ZLD4.50 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 measurement are based on RFC 2544 (1,424-byte UDP packets); IMIX: UDP throughput based on a combination of 64 byte, 512 byte, and 1424 byte packet sizes.
*4: AV (with Express Mode) 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: Including Gateway-to-Gateway and Client-to-Gateway.
*7: With Zyxel service license to enable or extend the feature capacity.
*8: This is the recommend maximum number of concurrent logged-in devices.
*9: SafeSearch function in CF need to enable SSL inspection firstly and not for small business models.
*10: With Hotspot Management license support
*11: 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

- 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

Anti-Malware

- Stream-based scan engine (Stream Mode)
- HTTP, FTP, SMTP, and POP3 protocol supported
- No file size limitation
- Automatic signature updates

E-mail Security

- Transparent mail interception via SMTP and POP3 protocols
- Spam and Phishing mail detection
- Blacklist and whitelist support
- Supports DNSBL checking

URL Threat Filter

- Botnet C&C websites blocking
- Malicious URL blocking
- Supports External URL blacklist

Content Filtering

- HTTPs domain filtering
- SafeSearch support
- Whitelist websites enforcement
- URL blacklist and whitelist 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

IP Exception

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

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
- 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

- 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

- 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*1

Management

Nebula Cloud Management

- Unlimited Registration & Central Management (Configuration, Monitoring, Dashboard, Location Map

& Floor Plan Visual) of Nebula Devices
- Network Function Scheduling (SSID/ PoE/Firewall Rules)
- MAC-Based and 802.1X Authentication
- Captive Portal Authentication

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 with Google Authenticator as the second factor for administrator account

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
- 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