What Firewall should I use?

Are you struggling to find the best firewall model for your next deployment?

Hopefully, this article may help you!

We first have to divide our firewalls into two categories:

Cloud-managed Firewalls (Nebula)

- USGFlex-series (Q2, 2021)

and;

- NSG-series

Stand-alone managed Firewalls

- USGFlex-series

- VPN-series

- ATP-series

Note! Security (UTM) Features are license-based.

USG Flex-series

This firewall series is our newest edition of firewalls, where increased throughput of both SPI and UTM is defining this firewall. It is a Flex-model which means it can be managed in Nebula (Q2, 2021). This is our standardized model which can be deployed at small and medium-sized sites.

Model	USG FLEX 100	USG FLEX 200	USG FLEX 500
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 x (Configurable), 1 x SFP
USB3.0 ports	1	2	2
Console port	Yes (RJ-45)	Yes (DB9)	Yes (DB9)
Rack-mountable	–	Yes	Yes
Fanless	Yes	Yes	–
System Capacity & Performance[1]			
SPI firewall throughput (Mbps)[2]	900	1,800	2,300
VPN throughput (Mbps)[3]	270	450	810
IDP throughput (Mbps)[4]	540	1,100	1,150
AV throughput (Mbps)[4]	360	570	800
UTM throughput (AV and IDP)[4]	360	550	800
Max. TCP concurrent sessions[5]	300,000	600,000	1,000,000
Max. concurrent IPsec VPN tunnels[6]	40	100	300
Concurrent SSL VPN users	30	60	150
VLAN interface	8	16	64
Concurrent devices logins (default/max.)[7][8]	64	200	200 / 300

UTM features include:

Security Service
Anti-Malware[7]
IPS (IDP)
Application Patrol[7]
Email Security
Web filtering (CF)[7][9]
SecuReporter Premium[7]

ATP-series

If your customer value top-security for a reasonable price, this is definitely your choice of a firewall. The ATP-series are equipped with not only the security (UTM) features of a USG Flex, but also sandboxing and botnet filter as well.

Sandboxing is taking the threat to an isolated environment where it's identified and analyzed in real-time (read more here: https://support.zyxel.eu/hc/en-us/articles/360003588639-ATP-Series-Why-do-you-need-a-sandbox-).

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 & Performance[*1]				
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

VPN-series

If you need a simple firewall for using device-only (without UTM) as well as VPN-use - this is your choice. It is equipped with SD-WAN which optimizes your VPN path, especially for international organizations (read more here: https://support.zyxel.eu/hc/en-us/articles/360015692259). It also is possible to enable the content filter and GeoIP.

Model	ZyWALL VPN50	ZyWALL VPN100	ZyWALL VPN300
Product photo			
Hardware Specifications			
Interfaces	4 x LAN/DMZ, 1 x WAN, 1 x SFP	4 x LAN/DMZ, 2 x WAN, 1 x SFP	7 x GbE (Configurable), 1 x SFP
USB3.0 ports	1	2	2
Console port	Yes (RJ-45)	Yes (DB9)	Yes (DB9)
Rack-mountable	-	Yes	Yes
System Capacity & Performance[*1]			
SPI firewall throughput (Mbps)[*2]	800	2,000	2,600
VPN throughput (Mbps)[*3]	150	500	1,000
Max. TCP concurrent sessions[*4]	400,000	800,000	2,000,000
Max. concurrent IPSec VPN tunnels[*5]	50	100	300
Concurrent SSL VPN users (default/max.)[*6]	10/50	30/200	50/300
VLAN interface	8	16	64
Concurrent device logins (default/max.)[*6*7]	64	200/300	500/800

NSG-series

If you are trying to simplify your devices' management and are ready for deploying a cloud-based management system that takes advantage of centralizing your customers (i.e. managing all your customers in one place), this is definitely your choice.

It has a simplified management system where no extra hardware or software has to be purchased, a no touch-deployment where scanning of QR-codes is registering your device for configuring instantaneously instead of inserting the MAC & S/N manually of your device. Configuration can then be done even before you connect your device to the internet.

Model	NSG50	NSG100	NSG200	NSG300
Product name	Nebula Cloud Managed Security Gateway	Nebula Cloud Managed Security Gateway	Nebula Cloud Managed Security Gateway	Nebula Cloud Managed Security Gateway
Hardware Specifications				
CPU	Single-core	Multi-core	Multi-core	Multi-core
Memory	2GB	1GB	1GB	4GB
10/100/1000 Mbps RJ-45 ports	4 x LAN (GbE) 2 x WAN (1x SFP, 1x GbE)	4 x LAN (GbE) 2 x WAN (GbE)	5 x LAN (GbE) 2 x WAN (GbE)	6 x Individual LAN (GbE) 2 x WAN (GbE)
Port grouping	Yes	Yes	Yes	No
USB ports	1	2	2	2
Console port	Yes (RJ-45)	Yes (DB9)	Yes (DB9)	Yes (DB9)
Rack-mountable	No	Yes	Yes	Yes
Wall-mountable	Yes	No	No	No
Fanless	Yes	Yes	No	No
System Capacity & Performance[1]				
SPI firewall throughput (Mbps)[2]	300	450	1,250	4,000
VPN throughput (Mbps)[3]	100	150	500	750
IDP throughput (Mbps)[4]	110	160	500	950
AV throughput (Mbps)[4]	50	90	300	450
SP throughput (Mbps, AV and IDP)[4]	50	90	300	450
Unlimited user	Yes	Yes	Yes	Yes
Max. TCP concurrent sessions[5]	20,000	40,000	80,000	500,000
Max. TCP session rate	2,000	2,000	8,000	10,000
Max. concurrent IPsec VPN tunnels[6]	10	40	200	300
VLAN interface	8	16	16	16

Interested in Nebula?

Read more here:
https://www.zyxel.com/solutions/Nebula-Commercial-Cloud-Networking-Solution-20161018-771782.shtml

Test out Nebula for yourself here:

https://nebula.zyxel.com