ZYXEL

NSG50/100/200/300

Nebula Cloud Managed Security Gateway

The Zyxel Nebula Cloud Managed Security Gateway is built with remote management and ironclad security for organizations with multiple distributed sites. With an extensive suite of security features including ICSA-certified firewall, IPsec VPN connectivity, Intrusion Detection Prevention (IDP) and Application Patrol, Content Filtering as well as Anti-virus the NSG provides deep, extensive protection to meet everything that small- to mid-sized businesses need.

As the Zyxel Nebula Security Gateway has been designed from the ground up to be cloud managed, installation and management is as simple as 1-2-3. Through Nebula's cloud interface, administrators can create site-wide policies and monitor all branch sites effortlessly, even without training.

- Complete network, security, and application control from anywhere via the cloud
- Zero-touch site-to-site VPN
- Secure networks with IDP and Application Patrol, Content Filtering and Anti-Virus
- Built-in DHCP, NAT, QoS, and VLAN management
- Static route and dynamic DNS support
- Identity-based security policies and application management
- Cloud management and cloud statistics

Benefits

Out-of-the-box cloud-managed gateway

Every Zyxel Nebula Security Gateway can be quickly and easily deployed at a remote location through nearly zero-touch cloud provisioning. It automatically pulls policies and configuration settings, receives seamless firmware upgrades and security signature updates from the cloud without the need for on-site networking expertise.

Easy setup, simple management

Traditional gateways require administrators to manage configurations and security policies separately for every device, eating up considerable time and effort. Nebula provides a single point of management for all Nebula gateways, allowing administrators to synchronize security settings

nebula

Datasheet NSG50/100/200/300

across thousands of sites to every device all at once. The cloud interface provides site-wide visibility and control that enable administrators to monitor and manage event logs, traffic statistics, bandwidth consumption, networked clients, and application usage without access to the individual devices.

Zero-touch VPN connections

Establishing a virtual private network to keep branch locations securely connected is easier than ever. With the Zyxel Nebula Security Gateway, either site-to-site or hub-and-spoke VPN connections can be configured with just a few clicks in the Nebula Control Center and no complex VPN configuration steps. The intuitive cloud management interface lets administrators monitor VPN connectivity between multiple locations in real time.

Streamlined policy management

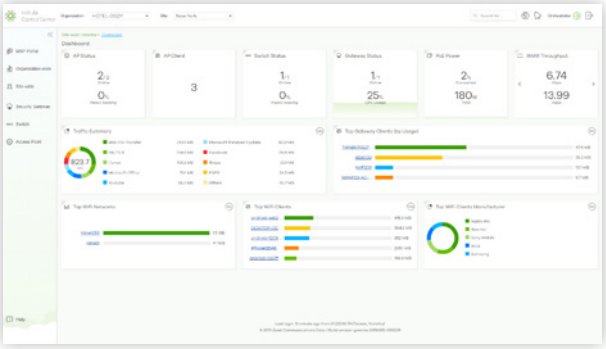
The Zyxel Nebula Security Gateway streamlines the configuration of firewalls and every security feature for faster, easier, and more consistent policy settings. It does so by supporting object-based management and a unified configuration approach for all security related policies, with which users can easily apply all policy criteria to every security feature. Moreover, any configuration made in the Nebula Control Center can be automatically propagated to all connected Nebula gateways.

Effective network protection

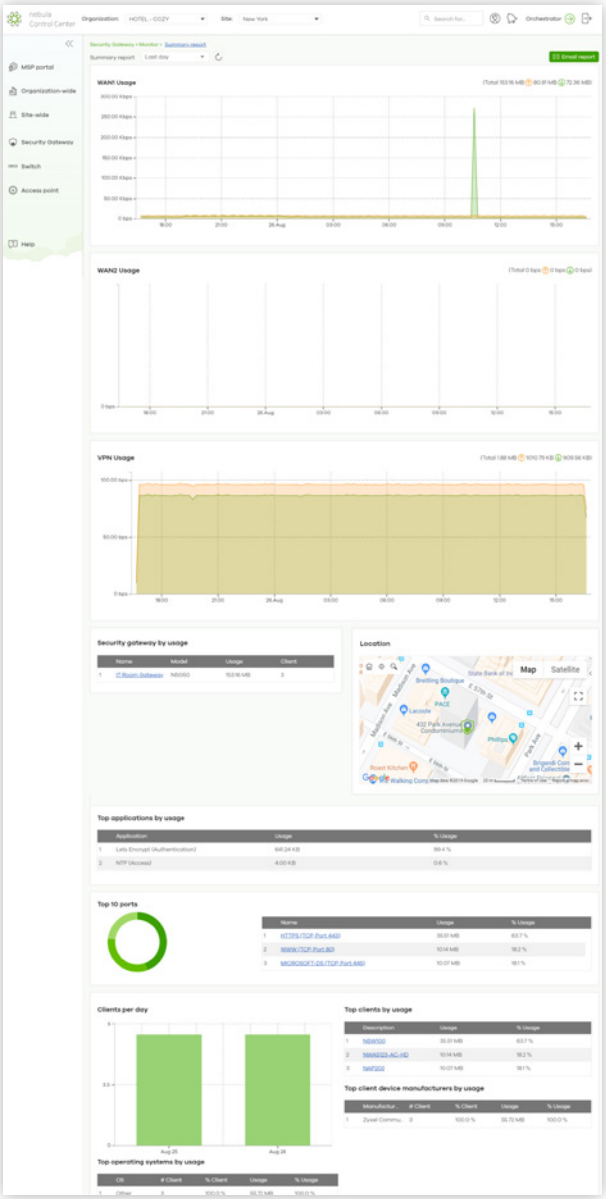
Nebula's IDP system scans multiple layers and protocols to inspect vulnerabilities invisible to simple port and protocol-based firewalls by utilizing deep packet inspection (DPI) technology that eliminates false positives with a database of malware signatures and provides effective protection against intrusions from unknown backdoors.

Powerful security pack free for a year

Every Nebula Security Gateway comes bundled with a one-year subscription to the Nebula Security Pack, which better protects your networks through IDP, Application Patrol, Content Filtering, and Anti-Virus security services. IDP guards your business from a wide range of attacks and suspicious activities such as SQL injection and DoS; Application Patrol helps boost productivity and prevent bandwidth abuse by prioritizing, throttling, and blocking unnecessary applications; and Content Filtering uses categorization and URL filtering to stop users from accessing malicious and inappropriate sites. Finally, the Anti-Virus acts as a bulwark against malware including viruses, Trojans, worms, spyware, and rogue ware, being the first line of defense for your networks.



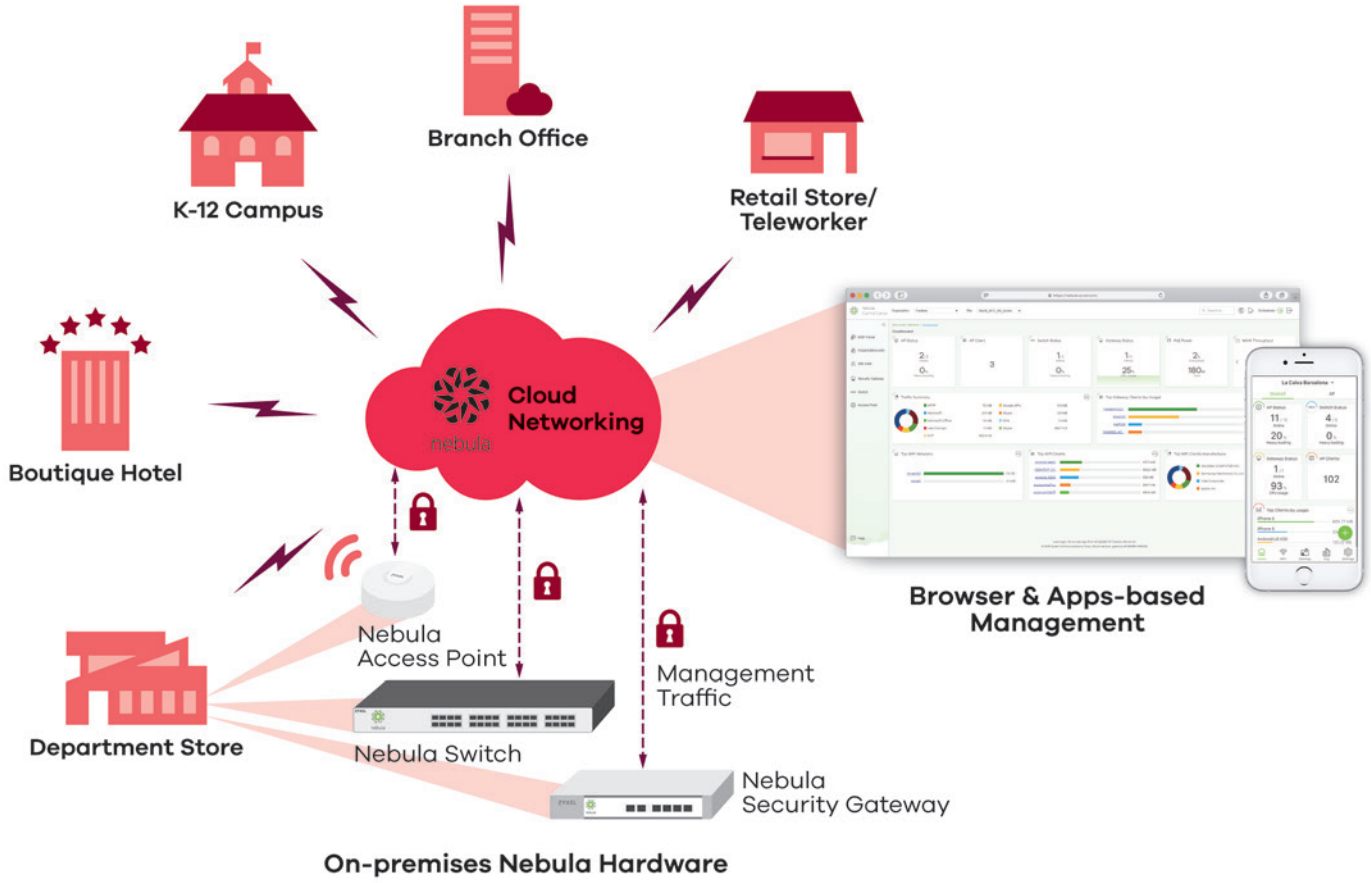
Real-time control of all devices from a single pane of glass



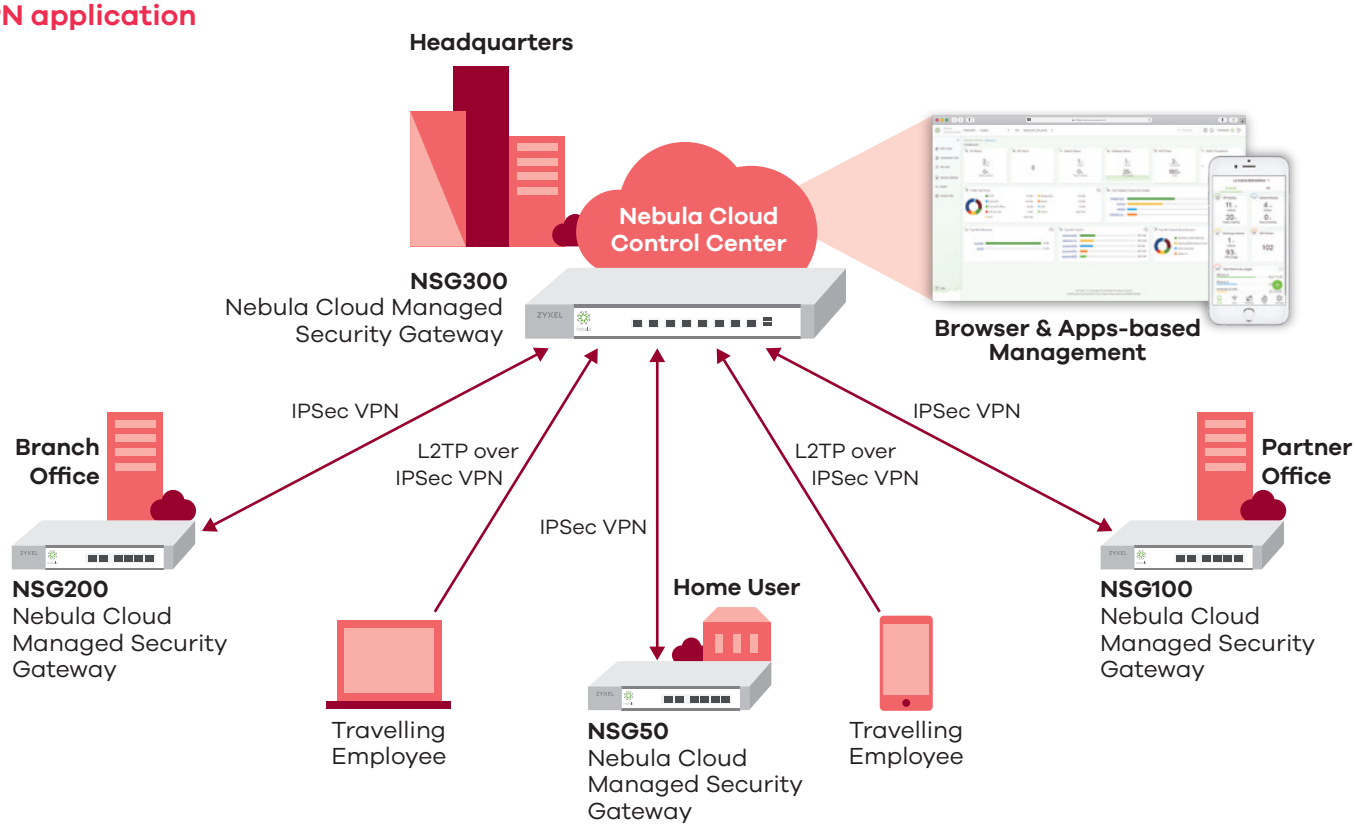
Use the intuitive management interface to view WAN usage, client and application reports for different time intervals, and historical status records

Applications Diagram

Nebula cloud management architecture



VPN application



Specifications

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	32	64
Key Software Features				
Firewall	Yes	Yes	Yes	Yes
Virtual Private Network (VPN)	Yes (IPSec, L2TP over IPSec)	Yes (IPSec, L2TP over IPSec)	Yes (IPSec, L2TP over IPSec)	Yes (IPSec, L2TP over IPSec)
Bandwidth management	Yes	Yes	Yes	Yes
Logging and Monitoring	Yes	Yes	Yes	Yes
Unified Security Policy	Yes	Yes	Yes	Yes
Intrusion Detection and Prevention (IDP)	Yes	Yes	Yes	Yes
Application Patrol	Yes	Yes	Yes	Yes
Content Filtering	Yes	Yes	Yes	Yes
Anti-Virus	Yes	Yes	Yes	Yes
WAN Failover	Yes	Yes	Yes	Yes
Power Requirements				
Power input	12 V DC, 2.0 A max.	12 V DC, 2.5 A max.	12 V DC, 3.33 A max.	100-240 V AC, 50/60 Hz, 1.3 A max.
Max. power consumption (watts)	12.0	19.0	37.0	58.5
Heat dissipation (BTU/hr)	40.95	64.83	199.61	199.61

Model		NSG50	NSG100	NSG200	NSG300
Physical Specifications					
Item	**Dimensions (WxDxH)(mm/in.)**	216 x 147.1 x 33/ 8.50 x 5.79 x 1.30	242 x 175.5 x 35.5/ 9.53 x 6.91 x 1.40	300 x 187.6 x 43.5/ 11.81 x 7.38 x 1.71	430 x 260.5 x 43.5/ 16.93 x 10.24 x 1.71
	Weight (kg/lb.)	1.04/2.29	1.25/2.76	2.0/4.4	3.3/7.28
Packing	**Dimensions (WxDxH)(mm/in.)**	276 x 185 x 98/ 10.87 x 7.28 x 3.86	394 x 240 x 101/ 15.51 x 9.45 x 3.98	351 x 243 x 149/ 13.82 x 9.57 x 5.87	519 x 392 x 163/ 20.43 x 15.43 x 6.42
	Weight (kg/lb.)	1.41/3.11	2.25/4.96	3.264/7.20	4.8/10.58
Included accessories		• Power adapter (with plug) • RJ45-RS232 console cable	• Power adapter • Rack mounting kit	• Power cord • Power adapter • 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)		655,130	815,463.9	787,109.3	560,811.50
Certifications					
EMC		FCC Part 15 (Class B), IC, CE EMC (Class B), RCM, 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		BSMI, UL	LVD (EN60950-1), BSMI	LVD (EN60950-1), BSMI	LVD (EN60950-1), BSMI

*1: Actual performance may vary depending on network conditions and activated applications.
*2: Maximum throughput based on RFC 2544 (1,518-byte UDP packets), and without enabling Intrusion Detection and Prevention.
*3: VPN throughput measured based on RFC 2544 (1,424-byte UDP packets), and without enabling Intrusion Detection and Prevention.
*4: IDP throughput measured using the industry standard HTTP performance test (1,460-byte HTTP packets). Testing was done with multiple sessions.
*5: Maximum sessions measured using the industry-standard IXIA IxLoad testing tool.
*6: Including Gateway-to-Gateway and Client-to-Gateway.

Features

Firewall

- Stateful packet inspection
- VLAN
- PPPoE
- Static route

IPSec VPN

- Topology: Site-to-site, hubs-and-spoke, server-and-client
- Encryption: AES (256-bit), 3DES and DES
- Authentication: SHA-2 (512-bit), SHA-1 and MD5
- Perfect forward secrecy (DH groups) support 1, 2, 5, 14
- IPSec NAT traversal
- Dead peer detection and relay detection
- VPN auto-reconnection
- L2TP over IPSec

Intrusion Detection and Prevention (IDP)*

- Signature-based
- Behavior-based scanning
- Automatic signature updates

Application Patrol*

- Granular control over the most important applications
- Identifies and controls applications and behaviors
- Top application usage record

Content Filtering*

- Social media filtering
- Malicious Website filtering
- URL blocking
- Blacklist and whitelist support
- Dynamic, cloud-based URL filtering database
- Unlimited user license support
- Customizable warning messages and redirection URL
- HTTPs Domain filtering

Anti-Virus*

- Supports Anti-Virus signatures
- Identifies and blocks over 650,000 viruses
- Stream-based Anti-Virus engine
- HTTP, FTP, SMTP, POP3 and IMAP4 protocol support
- Automatic signature updates
- No file size limitation

Streamlined Policy Management

- Unified policy management interface
- Supported exclusive security features: IDP, Application Patrol, firewall (ACL)
- Policy criteria: Source and destination IP address, destination port, time

Networking

- Routing mode
- Ethernet and PPPoE
- NAT
- VLAN tagging (802.1Q)
- DHCP client/server/relay
- Dynamic DNS support
- Maximum bandwidth
- Bandwidth limit per client IP

Authentication

- Microsoft Windows Active Directory integration
- External RADIUS user database
- Nebula Cloud (Nebula Control Center) authentication

Captive Portal

- Web-based authentication
- Forced user authentication (transparent authentication)
- Sign-on or click-to-continue authentication
- Multiple instances of captive portal
- Customizable portal templates
- Internal or external captive portal redirect
- Walled garden support

System Management

- Cloud managed
- Role-based administration
- SNMP v2c (MIB-II)
- System configuration rollback
- Cloud firmware upgrade

Logging and Monitoring

- Comprehensive local logging
- Syslog (up to 2 servers)
- Real-time traffic monitoring
- Nebula Security Service (NSS) analysis report*

* IDP and Application Patrol, Content Filtering and Anti-Virus services in NSS-SP (Nebula Security Service-Security Pack) license will be co-terminated separately from NCC Pro Pack (Nebula Control Center Professional Pack) service license.

For more product information, visit us on the web at www.zyxel.com

24/02/20