# ZYXEL

# NSG100

## Nebula Cloud Managed Security Gateway

The Zyxel Nebula NSG100 Cloud Managed Security Gateway is built with remote management and ironclad security for organizations with growing numbers of distributed sites. With the extensive suite of security features that includes ICSA-certified firewall, IPsec VPN connectivity, Intrusion Detection and Prevention (IDP) as well as Application Patrol, the NSG100 provides deep, extensive protection to meet everything that small- to mid-size businesses would need.

As the Zyxel Nebula NSG100 has been completely designed for cloud managed, the installation and management become simpler than ever. Through Nebula's cloud interface, administrators are able to create site-wide policies and monitor all the branch sites effortlessly even without training.

## Benefits

### Out-of-the-box cloud-managed gateway

The Zyxel Nebula NSG100 can be quick and easy 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 gateway requires administrators to perform configuration and to manage security policies on each device one by one but it costs considerable time and effort. The Zyxel Nebula provides a single point of management to all the Nebula gateways for administrators to synchronize security settings

Datasheet NSG100

- Complete networking, security and application control over the cloud
- Zero-touch site-to-site VPN
- Secure networks with Next-Gen Firewall, IDP and Application Patrol*
- Built-in DHCP, NAT, QoS and VLAN management
- Static route and dynamic DNS support
- Identity-based security policies and application management

\* Every NSG100 is pre-bundled with one year IDP and Application Patrol service.

nebula

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

## Zero-touch VPN connections

Establish VPN to keep branch locations securely connected is easier than ever. With the Zyxel Nebula NSG100, either site-to-site or hub-and-spoke VPN connections can be configured with complete simplicity through few clicks in the Nebula Control Center, without complex VPN configuration steps. The intuitive cloud management interface gives administrators a real-time view to monitor VPN connectivity between multiple locations.

## Streamlined policy management

The Zyxel Nebula NSG100 streamlines configuration of firewall and every security feature for faster, easier and more consistent policy settings 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 automatically propagate to all the connected Nebula gateways.

## Effective network protection

Nebula's IDP (Intrusion detection and prevention) 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 back doors.

## Powerful application security

The Zyxel Nebula NSG100 supports Application Patrol that can identify, categorize and control social, gaming, productivity and other Web applications and behaviors. Users can block undesirable applications to boost productivity and to prevent bandwidth abuse.
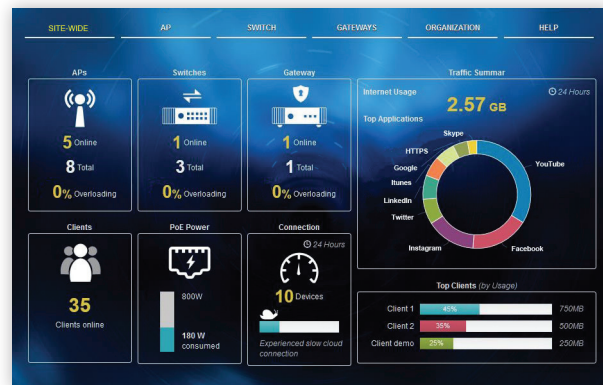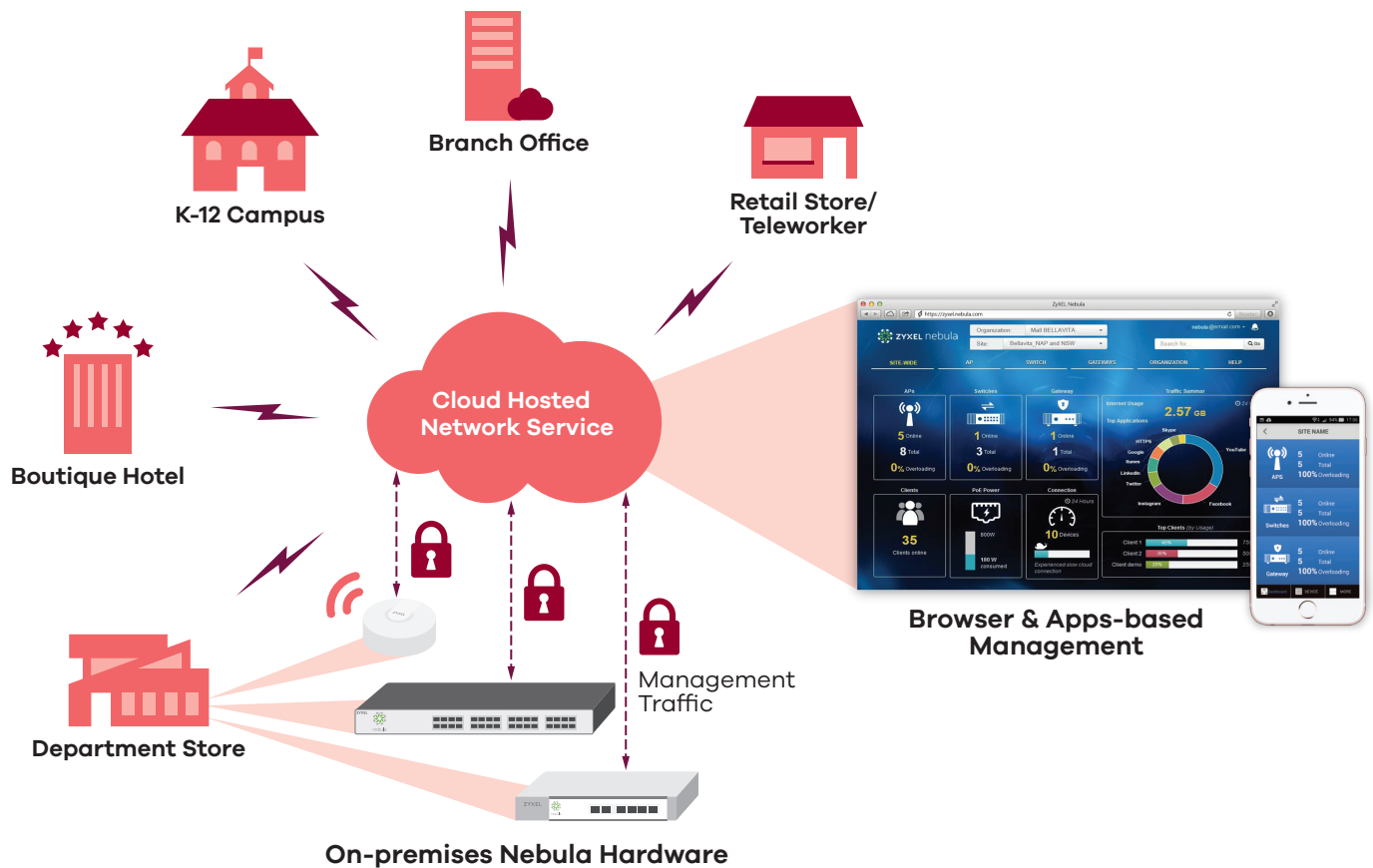


Real-time control of all the devices through a single pane of glass
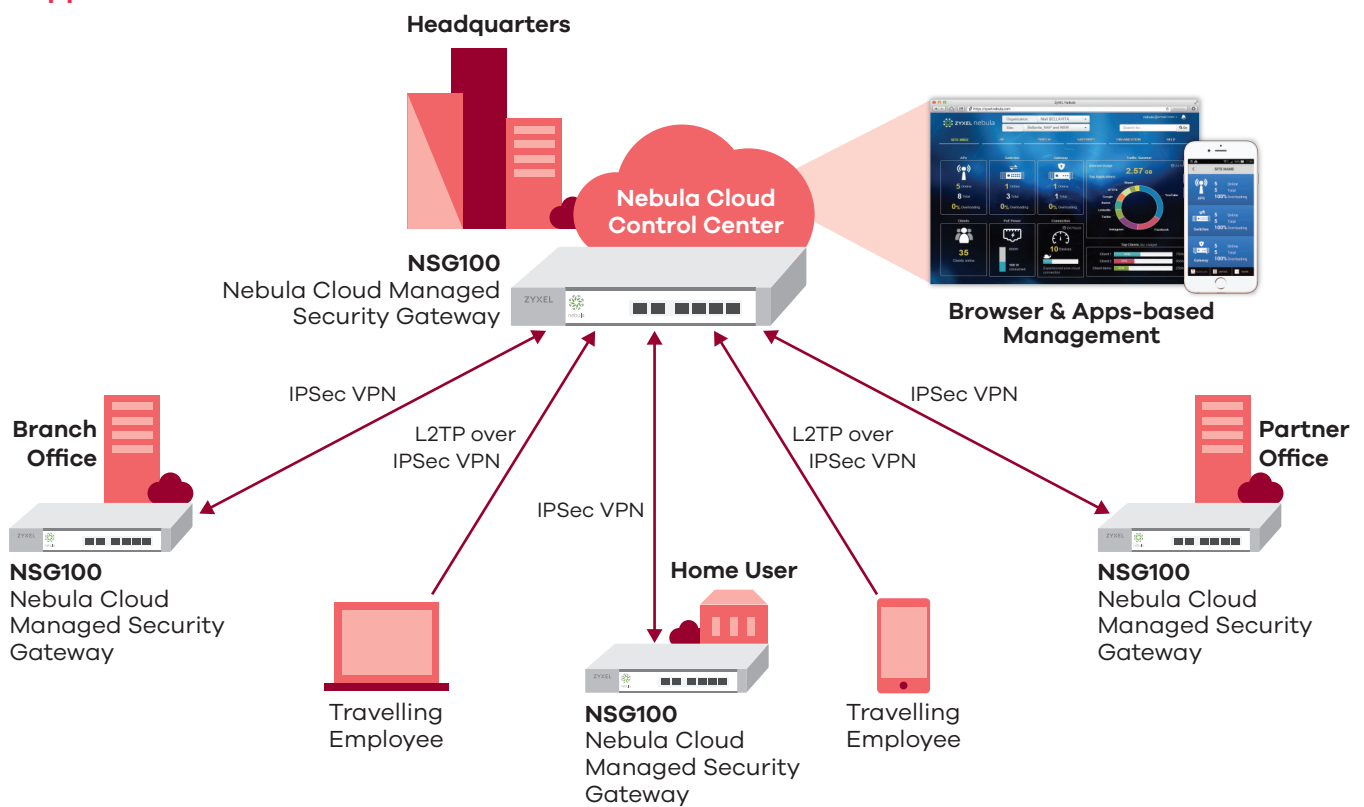


Monitor WAN usage, client and application report by different time intervals and view historical status record with the intuitive management interface

# Applications Diagram

## Nebula cloud management architecture



K-12 Campus

Branch Office

Retail Store/
Teleworker

Boutique Hotel

Cloud Hosted
Network Service

Browser & Apps-based
Management

Department Store

Management
Traffic

On-premises Nebula Hardware

## VPN application



Headquarters

Nebula Cloud
Control Center

Browser & Apps-based
Management

NSG100
Nebula Cloud Managed
Security Gateway

IPSec VPN

L2TP over
IPSec VPN

L2TP over
IPSec VPN

IPSec VPN

Branch
Office

IPSec VPN

Partner
Office

NSG100
Nebula Cloud
Managed Security
Gateway

Travelling
Employee

Home User

Travelling
Employee

NSG100
Nebula Cloud
Managed Security
Gateway

NSG100
Nebula Cloud
Managed Security
Gateway

# Specifications

| Model | NSG100 |
|---|---|
| Product name | Nebula Cloud Managed Security Gateway |



| Hardware Specifications | |
|---|---|
| 10/100/1000 Mbps RJ-45 ports | 4 x LAN, 2 x WAN |
| USB ports | 2 |
| Console port | Yes (DB9) |
| Rack-mountable | Yes |
| Fanless | Yes |
| **System Capacity & Performance**[1] | |
| SPI firewall throughput (Mbps)[2] | 650 |
| VPN throughput (Mbps)[3] | 140 |
| IDP throughput (Mbps)[4] | 180 |
| Unlimited user | Yes |
| Max. TCP concurrent sessions[5] | 40,000 |
| Max. concurrent IPsec VPN tunnels[6] | 40 |
| Customizable zones | Yes |
| VLAN interface | 8 |
| **Key Software Features** | |
| Firewall | Yes |
| Virtual Private Network (VPN) | Yes (IPSec, L2TP over IPSec) |
| Application Patrol | Yes |
| Intrusion Detection and Prevention (IDP) | Yes |
| Bandwidth management | Yes |
| **Power Requirements** | |
| Power input | 12 V DC, 3.0 A max. |
| Max. power consumption (watts) | 19.0 |
| Heat dissipation (BTU/hr) | 64.83 |

| Physical Specifications | | |
|---|---|---|
| Item | Dimensions (WxDxH)(mm/in.) | 242 x 175 x 36/9.53 x 6.89 x 1.42 |
| | Weight (kg/lb.) | 1.25/2.76 |
| Packing | Dimensions (WxDxH)(mm/in.) | 394 x 240 x 101/15.51 x 9.45 x 3.98 |
| | Weight (kg/lb.) | 2.25/4.96 |
| Included accessories | • Power adapter      • Rack mounting kit | |

| Environmental Specifications | | |
|---|---|---|
| Operating | Temperature | 0°C to 40°C/32°F to 104°F |
| | Humidity | 10% to 90% (non-condensing) |
| Storage | Temperature | -30°C to 70°C/-22°F to 158°F |
| | Humidity | 10% to 90% (non-condensing) |
| MTBF (hr) | | 815,463.9 |

| Certifications | |
|---|---|
| EMC | FCC Part 15 (Class B), CE EMC (Class B), C-Tick (Class B), BSMI |
| Safety | 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).
*3: VPN throughput measured based on RFC 2544 (1,424-byte UDP packets).

*4: IDP throughput measured using the industry-standard HTTP performance test (1,460-byte HTTP packets). Tests were 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

# Features

## Firewall

- Stateful packet inspection
- User-aware policy enforcement
- VLAN
- PPPoE
- Static route
- Firewall
- Intrusion Detection and Prevention (IDP)
- Application Patrol

## IPSec VPN

- Topology: Site-to-site, hubs-and-spoke
- 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

## 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

## 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

## System Management

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

## Logging and Monitoring

- Comprehensive local logging
- Syslog (to up to 2 servers)
- Real-time traffic monitoring

* IDP and Application Patrol services need to be purchased on top of Nebula Control Center (NCC) service license, and will not be co-terminated along with NCC service license.

Datasheet NSG100