ZYXEL USGFLEX100HP

Zyxel USGFLEX100HP ZyWALL Firewall Instruction Manual

High Speed Cyber Security Firewall with PoE+

1. Product Overview

The Zyxel USGFLEX100HP ZyWALL Firewall is a high-performance network security appliance designed for small to medium-sized businesses. It offers robust cyber security features, flexible port configurations, and integrated Power over Ethernet (PoE+) capabilities. This device supports up to 50 users and internet speeds of up to 500 Mbps, providing comprehensive protection and efficient network management.

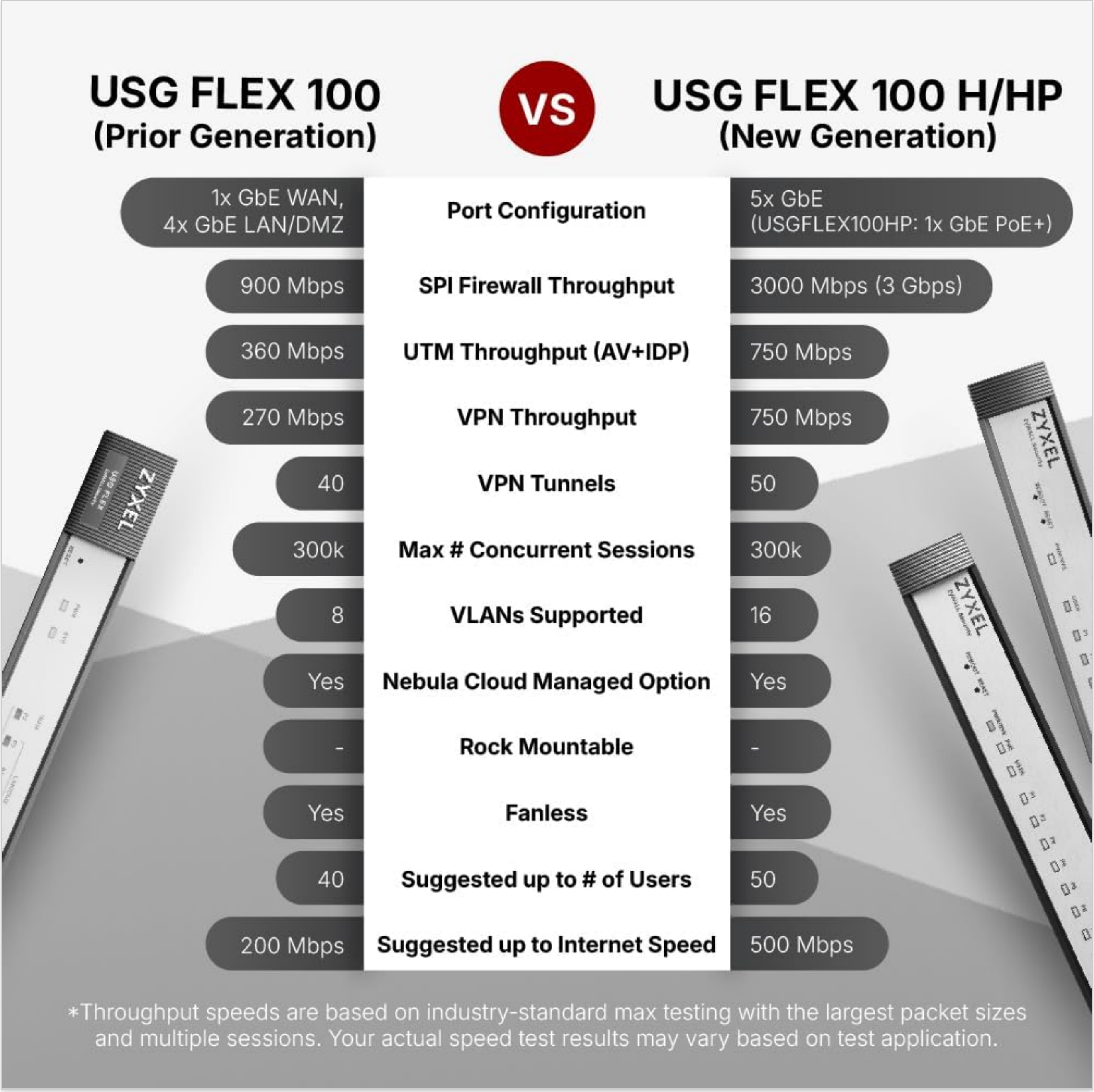
Your browser does not support the video tag.

Video 1: Overview of the Zyxel USG FLEX H Firewall Series. This video highlights the key features and benefits of the firewall series, including network protection, integrated PoE+ ports, and Nebula App management.

2. Package Contents

Verify that all items are present in the package. If any item is missing or damaged, contact your vendor immediately.

- Zyxel USGFLEX100HP ZyWALL Firewall Unit
- Power Adapter and Power Cord
- Ethernet Cable
- Console Cable (RJ45 to DB9)
- Mounting Brackets (for rack or wall mounting)
- Rubber Feet
- Quick Start Guide



USG FLEX 100 (Prior Generation)	VS	USG FLEX 100 H/HP (New Generation)
1x GbE WAN, 4x GbE LAN/DMZ	Port Configuration	5x GbE (USGFLEX100HP: 1x GbE PoE+)
900 Mbps	SPI Firewall Throughput	3000 Mbps (3 Gbps)
360 Mbps	UTM Throughput (AV+IDP)	750 Mbps
270 Mbps	VPN Throughput	750 Mbps
40	VPN Tunnels	50
300k	Max # Concurrent Sessions	300k
8	VLANs Supported	16
Yes	Nebula Cloud Managed Option	Yes
-	Rock Mountable	-
Yes	Fanless	Yes
40	Suggested up to # of Users	50
200 Mbps	Suggested up to Internet Speed	500 Mbps

*Throughput speeds are based on industry-standard max testing with the largest packet sizes and multiple sessions. Your actual speed test results may vary based on test application.

Image 1: Contents of the Zyxel USGFLEX100HP package. This image displays the firewall unit, power supply, console cable, and other accessories included in the box.

Your browser does not support the video tag.

Video 2: Unboxing of a Zyxel USGFLEX H Series Firewall. This video demonstrates the unboxing process and shows the various components included in the product package.

3. Physical Description

3.1 Front Panel

The front panel of the USGFLEX100HP features status LEDs and a USB 3.0 port.

- **Status LEDs:** Indicate power, system status, PoE activity, and individual port activity (P1-P8).
- **USB 3.0 Port:** For connecting external storage or other compatible USB devices.
- **REBOOT/RESET Buttons:** Used for restarting the device or performing a factory reset.

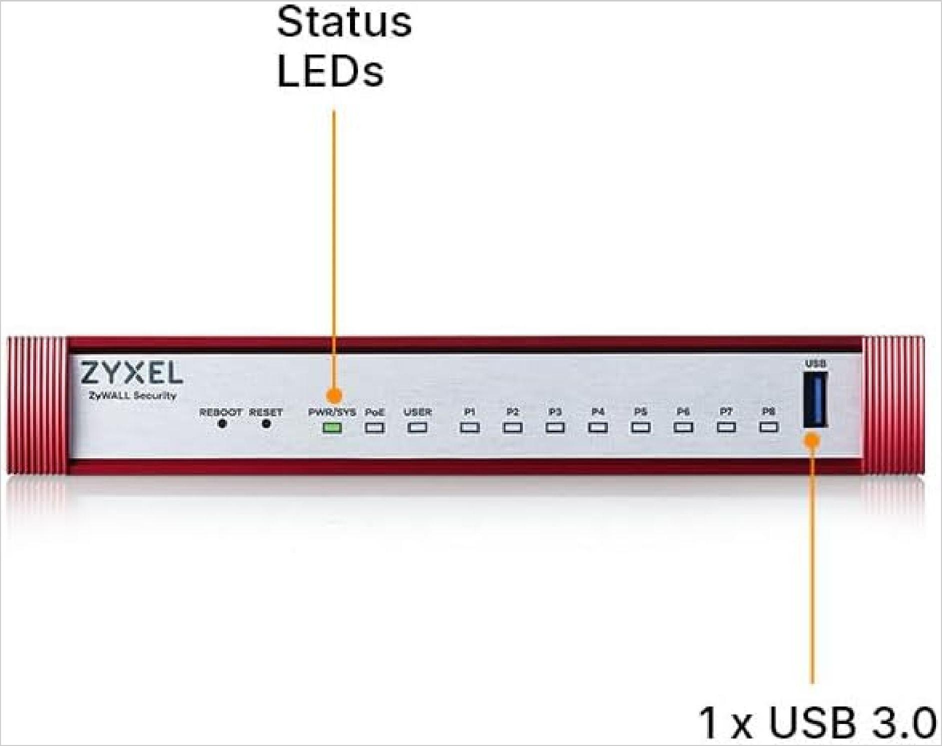


Image 2: Front view of the Zyxel USGFLEX100HP, highlighting the status LEDs and the USB 3.0 port.

3.2 Rear Panel

The rear panel provides various connectivity options, including Gigabit Ethernet ports, a console port, and the power input.

- **7 x 1G Ethernet Ports:** Configurable Gigabit Ethernet ports for flexible WAN/LAN connectivity.
- **1 x 1G PoE+ Port:** A Gigabit Ethernet port with Power over Ethernet Plus (30W) capability, ideal for powering access points, IP cameras, or IP phones.
- **1 x Console Port (RJ45):** For direct command-line interface (CLI) access and initial configuration.
- **Power Supply Input:** Connects to the provided power adapter.

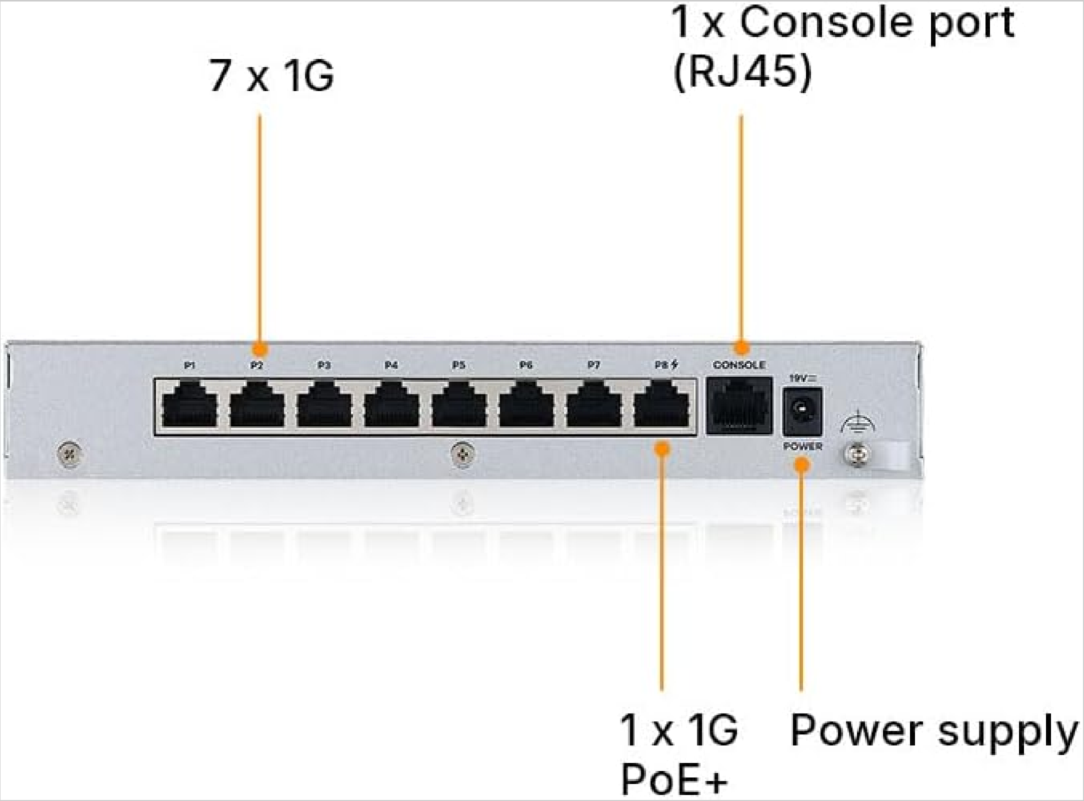


Image 3: Rear view of the Zyxel USGFLEX100HP, detailing the Ethernet ports, PoE+ port, console port, and power input.

4. Setup

Follow these general steps for initial setup:

1. **Physical Placement:** Place the firewall on a stable, flat surface or mount it using the provided brackets. Ensure adequate ventilation.
2. **Connect Network Cables:** Connect your internet modem to a designated WAN port (refer to the Quick Start Guide for specific port assignments). Connect your internal network devices (switches, computers) to the LAN ports.
3. **Connect Power:** Connect the power adapter to the firewall's power input and then to a power outlet. The device will power on automatically.
4. **Initial Configuration:** Access the device's web-based management interface via a connected computer or use the Zyxel Nebula Cloud Management solution for simplified setup.

5. Operating Instructions

The Zyxel USGFLEX100HP operates as a central security gateway for your network. Once configured, it will automatically enforce security policies and manage network traffic. Key operational aspects include:

- **Traffic Management:** The firewall inspects incoming and outgoing network traffic based on configured rules.
- **VPN Connectivity:** Supports Virtual Private Network (VPN) connections for secure remote access.
- **PoE+ Functionality:** The dedicated PoE+ port provides power and data to compatible devices, simplifying deployment.
- **Monitoring:** Monitor network status, traffic logs, and security events through the web interface or Nebula Cloud.

6. Nebula Cloud Management

The Zyxel USGFLEX100HP can be managed through Zyxel's Nebula Cloud Management platform, offering a centralized and simplified approach to network operations.

- **Unified Security:** Synchronizes security policies across multiple devices.
- **Real-time Monitoring:** Provides live insights into network performance and security events.
- **Cloud-based Control:** Configure and manage your firewall remotely from anywhere.
- **Mobile App:** Get up and running in minutes via the Nebula mobile app for quick setup and monitoring.

Your browser does not support the video tag.

Video 3: Zyxel USGFLEX H Series Firewalls. This video showcases the Nebula Cloud integration for easy management and monitoring of the firewall.

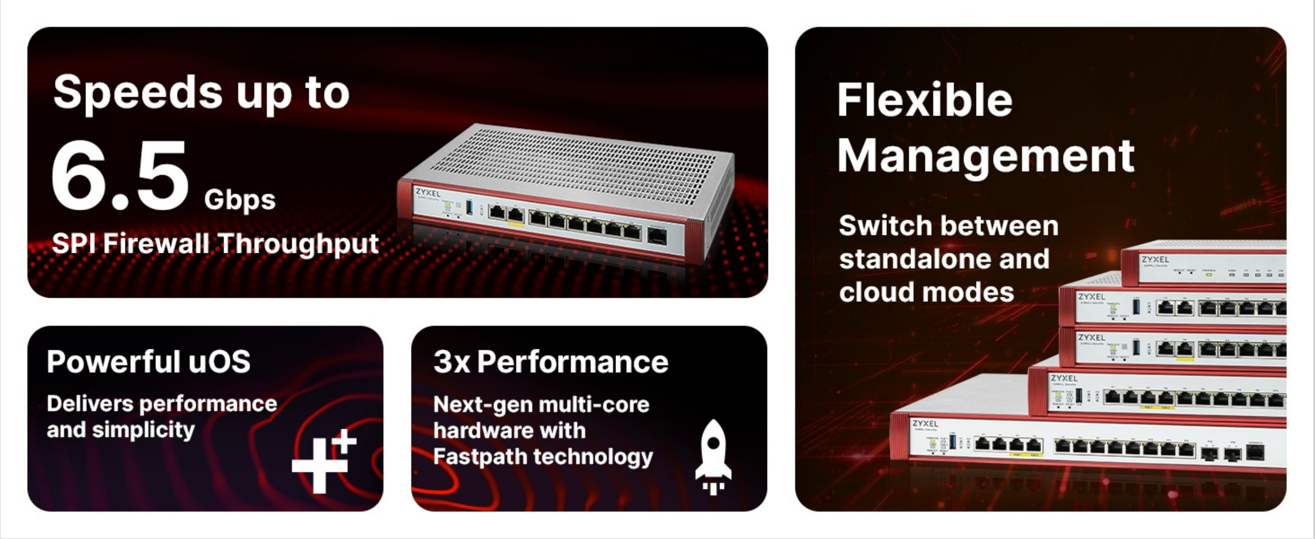
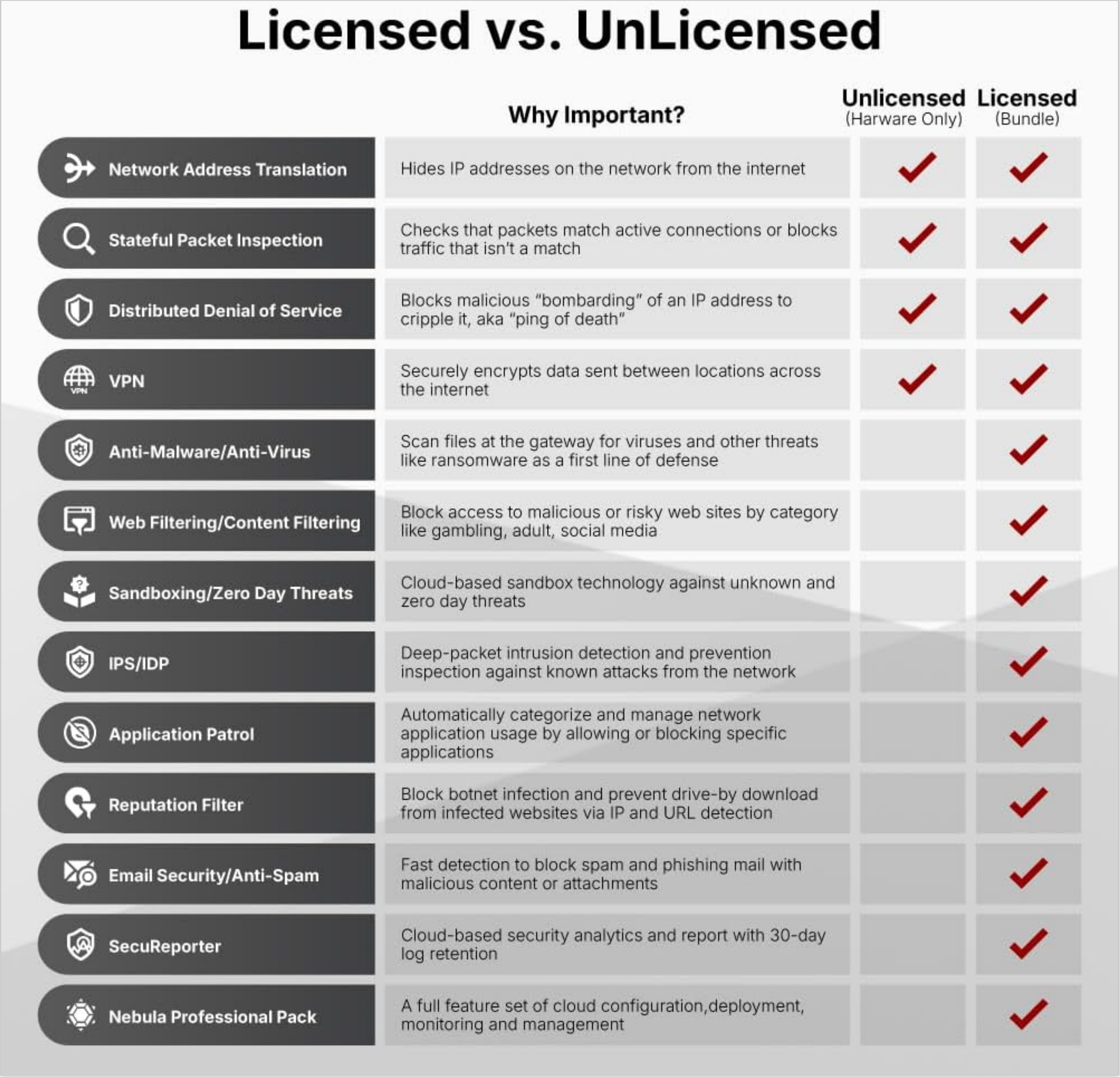

Speeds up to
6.5 Gbps
SPI Firewall Throughput
Flexible Management
Switch between standalone and cloud modes
Powerful uOS
Delivers performance and simplicity
3x Performance
Next-gen multi-core hardware with Fastpath technology
ZYXEL

Image 4: Illustration of Cloud & On-Premise Sync with Zyxel Nebula, simplifying network operations.

7. Security Features

The USGFLEX100HP provides robust security to protect your network from various cyber threats. Many advanced features require a security license.

- **Network Address Translation (NAT):** Hides internal IP addresses from the internet.
- **Stateful Packet Inspection (SPI):** Checks packets against active connections and blocks non-matching traffic.
- **Distributed Denial of Service (DDoS) Protection:** Blocks malicious traffic aimed at overwhelming the network.
- **VPN:** Securely encrypts data sent between locations.
- **Anti-Malware/Anti-Virus (Licensed):** Scans files at the gateway for viruses and other threats.
- **Web Filtering/Content Filtering (Licensed):** Blocks access to malicious or inappropriate websites.
- **Sandboxing/Zero Day Threats (Licensed):** Cloud-based sandbox technology for unknown threats.
- **Intrusion Prevention System/Intrusion Detection System (IPS/IDP) (Licensed):** Deep-packet inspection for known attacks.
- **Application Patrol (Licensed):** Categorizes and manages network application usage.
- **Reputation Filter (Licensed):** Blocks botnet infection and drive-by downloads.
- **Email Security/Anti-Spam (Licensed):** Fast detection to block spam and phishing mail.
- **SecuReporter (Licensed):** Cloud-based security analytics and reporting.



Licensed vs. UnLicensed

	Why Important?	Unlicensed (Harware Only)	Licensed (Bundle)
Network Address Translation	Hides IP addresses on the network from the internet	✓	✓
Stateful Packet Inspection	Checks that packets match active connections or blocks traffic that isn't a match	✓	✓
Distributed Denial of Service	Blocks malicious "bombarding" of an IP address to cripple it, aka "ping of death"	✓	✓
VPN	Securely encrypts data sent between locations across the internet	✓	✓
Anti-Malware/Anti-Virus	Scan files at the gateway for viruses and other threats like ransomware as a first line of defense		✓
Web Filtering/Content Filtering	Block access to malicious or risky web sites by category like gambling, adult, social media		✓
Sandboxing/Zero Day Threats	Cloud-based sandbox technology against unknown and zero day threats		✓
IPS/IDP	Deep-packet intrusion detection and prevention inspection against known attacks from the network		✓
Application Patrol	Automatically categorize and manage network application usage by allowing or blocking specific applications		✓
Reputation Filter	Block botnet infection and prevent drive-by download from infected websites via IP and URL detection		✓
Email Security/Anti-Spam	Fast detection to block spam and phishing mail with malicious content or attachments		✓
SecuReporter	Cloud-based security analytics and report with 30-day log retention		✓
Nebula Professional Pack	A full feature set of cloud configuration,deployment, monitoring and management		✓

Image 5: Detailed comparison of security features available with and without a license for Zyxel firewalls.

Your browser does not support the video tag.

Video 4: "Work smarter, not harder" - This video illustrates the importance of robust network security and how Zyxel solutions protect businesses from cyber threats.

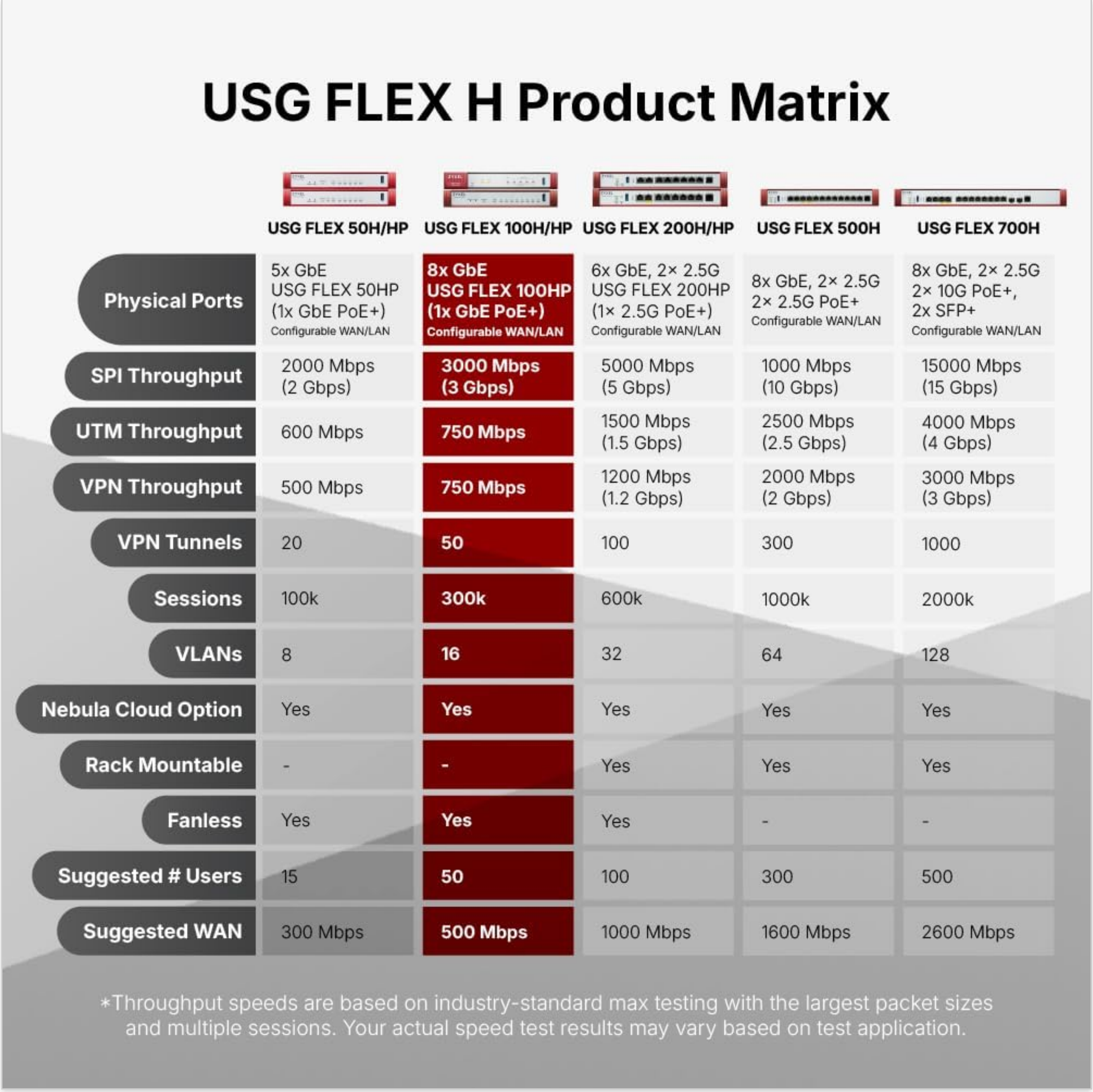
8. Performance Specifications

The Zyxel USGFLEX100HP is engineered for high performance in business environments.

Feature	Specification
SPI Firewall Throughput	3000 Mbps
UTM Throughput (AV+IDP)	750 Mbps
VPN Throughput	750 Mbps
Concurrent Sessions	300,000
VPN Tunnels	50

Feature	Specification
VLANs Supported	16
Suggested Users	Up to 50
Suggested Internet Speed	Up to 500 Mbps
Physical Ports	7x GbE, 1x GbE PoE+
Item Weight	4.31 pounds
Product Dimensions	1 x 11.7 x 8 inches
Upper Temperature Rating	40 Degrees Celsius

Note: Throughput speeds are based on industry-standard max testing with large packet sizes and multiple sessions. Actual speed test results may vary based on application and network conditions.



USG FLEX H Product Matrix

	USG FLEX 50H/HP	USG FLEX 100H/HP	USG FLEX 200H/HP	USG FLEX 500H	USG FLEX 700H
Physical Ports	5x GbE USG FLEX 50HP (1x GbE PoE+) Configurable WAN/LAN	8x GbE USG FLEX 100HP (1x GbE PoE+) Configurable WAN/LAN	6x GbE, 2× 2.5G USG FLEX 200HP (1× 2.5G PoE+) Configurable WAN/LAN	8x GbE, 2× 2.5G 2× 2.5G PoE+ Configurable WAN/LAN	8x GbE, 2× 2.5G 2× 10G PoE+, 2x SFP+ Configurable WAN/LAN
SPI Throughput	2000 Mbps (2 Gbps)	3000 Mbps (3 Gbps)	5000 Mbps (5 Gbps)	1000 Mbps (10 Gbps)	15000 Mbps (15 Gbps)
UTM Throughput	600 Mbps	750 Mbps	1500 Mbps (1.5 Gbps)	2500 Mbps (2.5 Gbps)	4000 Mbps (4 Gbps)
VPN Throughput	500 Mbps	750 Mbps	1200 Mbps (1.2 Gbps)	2000 Mbps (2 Gbps)	3000 Mbps (3 Gbps)
VPN Tunnels	20	50	100	300	1000
Sessions	100k	300k	600k	1000k	2000k
VLANs	8	16	32	64	128
Nebula Cloud Option	Yes	Yes	Yes	Yes	Yes
Rack Mountable	-	-	Yes	Yes	Yes
Fanless	Yes	Yes	Yes	-	-
Suggested # Users	15	50	100	300	500
Suggested WAN	300 Mbps	500 Mbps	1000 Mbps	1600 Mbps	2600 Mbps

*Throughput speeds are based on industry-standard max testing with the largest packet sizes and multiple sessions. Your actual speed test results may vary based on test application.

Image 6: USG FLEX H Product Matrix, providing a detailed comparison of specifications across various models in the series.

Image 7: Comparison between the prior generation USG FLEX 100 and the new generation USG FLEX 100 H/HP, highlighting performance improvements and new features.

9. Troubleshooting

If you encounter issues with your Zyxel USGFLEX100HP, consider the following troubleshooting steps:

- **No Power:** Ensure the power adapter is securely connected to both the device and a working power outlet. Check the power LED on the front panel.
- **No Internet Access:** Verify that your modem is working correctly and connected to the designated WAN port. Check the WAN port's LED indicator. Confirm your internet service provider (ISP) connection is active.
- **Network Connectivity Issues:** Check Ethernet cable connections to LAN ports. Ensure devices are receiving IP addresses from the firewall (if acting as a DHCP server).
- **Slow Performance:** Review your security policy configurations. High-level security features can impact throughput. Check for excessive network traffic or potential malware.
- **Accessing Web Interface:** Ensure your computer is on the same network segment as the firewall and that you are using the correct IP address for the management interface.
- **Factory Reset:** If all else fails, a factory reset can restore the device to its default settings. Refer to the Quick Start Guide for instructions on performing a reset.

10. Maintenance

Regular maintenance ensures optimal performance and security for your Zyxel USGFLEX100HP firewall:

- **Firmware Updates:** Regularly check for and apply the latest firmware updates from the Zyxel website or through Nebula Cloud. Firmware updates often include security patches and performance enhancements.
- **Configuration Backups:** Periodically back up your device configuration. This allows for quick restoration in case of unexpected issues or misconfigurations.
- **Security Policy Review:** Regularly review and update your security policies to adapt to evolving threat landscapes and changing network requirements.
- **Physical Inspection:** Ensure the device is free from dust and debris, especially around ventilation areas, to prevent overheating.

- **Log Monitoring:** Monitor system and security logs for unusual activity or potential threats.

11. Warranty and Support

Your Zyxel USGFLEX100HP ZyWALL Firewall comes with a standard manufacturer's warranty. For detailed warranty information, please refer to the warranty card included in your package or visit the official Zyxel website.
For technical support, product documentation, and software downloads, please visit the Zyxel support portal:

- **Zyxel Support Portal:** www.zyxel.com/support
- **Zyxel Nebula Cloud:** nebula.zyxel.com

Additional protection plans may be available for extended coverage. Contact your reseller for more information.