Multi-Homing Gateway
MHG - 2 5 0 0

Relying on a single WAN link is risky for any company due to the consequences of Internet disconnections. To avoid profit loss, the best tactic is to implement a fault tolerance mechanism for ensuring network continuity. Accordingly, Nusoft MHG-2500 comes equipped with link failover, load balancing and policy-based routing (PBR) to achieve fault tolerance. It also integrates with firewall, QoS manager, Web filter, AAA server (Authentication, Authorization, and Accounting), application blocker, anomaly traffic detection, full VPN connectivity (SSL / IPsec / PPTP VPN and trunking) and more, presenting you an all-in-one solution to simplify network management cost-effectively.

Product Features

Full IPv6 Compatibility
MHG-2500 is fully compatible with IPv6 addressing, the mainstream Internet protocol in the future. No additional budget is required for implementing another IPv6-based gateway simply for IPv4-to-IPv6 address translation.

Customizable & Scalable NIC Modules
Up to 10 to 18 GbE RJ45 ports (replaceable with mini-GBIC ports and expandable by using Virtual WAN feature) are available for defining as LAN, WAN, DMZ, or isolated NIC groups. Accordingly, MHG-2500 can physically segment a network, adding advanced controls (authentication, QoS, etc.) by serving as an internal firewall to improve management over networks.

Bi-directional Load Balancing & Policy-based Routing
With the multi-WAN module, outbound traffic are distributed across WAN links by load-balancing algorithms, due to which it delivers bandwidth aggregation and link failover capabilities, making the most of bandwidth, and yet connecting reliably. Besides, inbound traffic to your company website can be evenly load-balanced across each link to mitigate the load of Web requests, ensuring the accessibility to the website should any link failure occur.

Moreover, the network traffic generated from a specific service or user can be routed through a designated WAN link based on the company's network policies.

Total VPN Solution
Unlike conventional firewalls, MHG-2500’s VPN Trunking feature delivers link failover and bandwidth aggregation capabilities to IPsec / PPTP tunnels, greatly increasing the speed and stability of VPN connections. In addition, hardware authentication is incorporated into SSL Web VPN connectivity, which allows user authentication to base on hardware information, such as CPU ID, hard disk serial number, etc. Branch offices and road warriors will be provided with VNC connectivity and Wake-on-LAN capability, as well as a fast and easy VPN access along with advanced controls (authentication, QoS, etc.).

Flexible Bandwidth Management
Global Quality of Service (QoS), individual QoS and P2P QoS are provided as tools to base bandwidth allocation on network policies, preventing the bandwidth being exhausted by minorities.

AAA Server
Authentication: Manages the Internet access by internal or external (RADIUS / POP3 / LDAP) authentication.
Authorization: Permits access to a specific resource or service.
Accounting: Provides detailed connection logs for network policy adjustment.

Nusoft Internet Security Fighter
Web Filtering
The Web Filtering feature employs a cloud-based URL database which is categorized into Anti-Social and Illegal, Pornographic and Abusive, Gaming and Gambling, Society and Commerce, Communication and Technology, Leisure, Information and Education, Other, and further categorized into sixty-four subcategories. Web access can be easily managed by category instead of a URL, keyword, etc. Additionally, network administrators are allowed to restrict file transfers, MIME types and browser scripts, as well as provided with detailed logs and statistics for diagnosis.

Internet-based Application Blocking
The increasing popularity of instant messaging (Skype, WhatsApp, Line, ICQ, QQ, Yahoo, etc.), P2P file sharing (BitTorrent, eDonkey, Foxy, etc.), anonymous web browsing (Freegate, UltraSurf, etc.) has raised the risks of trade secret leak and security threats. Accordingly, MHG-2500 features Application Blocking to help manage the use of IM messengers (chats and file transfers) and avoid bandwidth being abused or misused by minorities. In addition, the use of multimedia streaming, Web-based email service, online gaming and remote controlling can also be effortlessly blocked by their packet signatures.

Anomaly Traffic Detection & Switch Co-Defense
MHG-2500 is capable of proactively blocking packet-flooding attacks and notifying related personnel of such an event. A core switch may be incorporated to perform a co-defense against DoS or DDoS attack by disabling the switch port containing the source of the attack.

One-Time Password Authentication
An unpredictable and unrepeatable password can be generated at each login using Nusoft OTP (available for iOS and Android devices), offering users a more secure identity verification along with their account credentials.

Deployment
Various authentication mechanisms

Greatly increases the network security by using hardware information (CPU ID, hard disk serial number, etc.) and one-time password for user authentication.

Network security is at risk due to sole reliance on user credentials for authentication.

Policy-based routing

Allows in-/outbound traffic to be routed based on network policies.

Only comes in outbound routing capability and has no manageability.

Flexible bandwidth management

Adds flexibility to bandwidth management by providing global QoS, individual QoS and P2P QoS.

Lacks flexibility in bandwidth management due to the only option being maximum bandwidth.

Total VPN solution

Secures LAN networks with anomaly flow detection and switch co-defense capabilities, as well as serves as internal firewall.

No protection against attacks initiated from within the network.

LAN security mechanisms

Provides an effortless network management through a unified user interface.

Merely a firewall equipped with simple security mechanisms and cluttered management interfaces; operation requires a separate configuration for each feature.

Unified network management

Greater increases the network security by using hardware information and one-time password for user authentication.

Network security is at risk due to sole reliance on user credentials for authentication.

Policy-based routing

Allows in-/outbound traffic to be routed based on network policies.

Only comes in outbound routing capability and has no manageability.

Flexible bandwidth management

Adds flexibility to bandwidth management by providing global QoS, individual QoS and P2P QoS.

Lacks flexibility in bandwidth management due to the only option being maximum bandwidth.

Total VPN solution

Secures LAN networks with anomaly flow detection and switch co-defense capabilities, as well as serves as internal firewall.

No protection against attacks initiated from within the network.

LAN security mechanisms

Provides an effortless network management through a unified user interface.

Merely a firewall equipped with simple security mechanisms and cluttered management interfaces; operation requires a separate configuration for each feature.

Unified network management

Greater increases the network security by using hardware information and one-time password for user authentication.

Network security is at risk due to sole reliance on user credentials for authentication.

Policy-based routing

Allows in-/outbound traffic to be routed based on network policies.

Only comes in outbound routing capability and has no manageability.

Flexible bandwidth management

Adds flexibility to bandwidth management by providing global QoS, individual QoS and P2P QoS.

Lacks flexibility in bandwidth management due to the only option being maximum bandwidth.

Total VPN solution

Secures LAN networks with anomaly flow detection and switch co-defense capabilities, as well as serves as internal firewall.

No protection against attacks initiated from within the network.

LAN security mechanisms

Provides an effortless network management through a unified user interface.

Merely a firewall equipped with simple security mechanisms and cluttered management interfaces; operation requires a separate configuration for each feature.

Unified network management

Greater increases the network security by using hardware information and one-time password for user authentication.

Network security is at risk due to sole reliance on user credentials for authentication.

Policy-based routing

Allows in-/outbound traffic to be routed based on network policies.

Only comes in outbound routing capability and has no manageability.

Flexible bandwidth management

Adds flexibility to bandwidth management by providing global QoS, individual QoS and P2P QoS.

Lacks flexibility in bandwidth management due to the only option being maximum bandwidth.

Total VPN solution

Secures LAN networks with anomaly flow detection and switch co-defense capabilities, as well as serves as internal firewall.

No protection against attacks initiated from within the network.

LAN security mechanisms

Provides an effortless network management through a unified user interface.

Merely a firewall equipped with simple security mechanisms and cluttered management interfaces; operation requires a separate configuration for each feature.

Unified network management

Greater increases the network security by using hardware information and one-time password for user authentication.

Network security is at risk due to sole reliance on user credentials for authentication.

Policy-based routing

Allows in-/outbound traffic to be routed based on network policies.

Only comes in outbound routing capability and has no manageability.

Flexible bandwidth management

Adds flexibility to bandwidth management by providing global QoS, individual QoS and P2P QoS.

Lacks flexibility in bandwidth management due to the only option being maximum bandwidth.

Total VPN solution

Secures LAN networks with anomaly flow detection and switch co-defense capabilities, as well as serves as internal firewall.

No protection against attacks initiated from within the network.

LAN security mechanisms

Provides an effortless network management through a unified user interface.

Merely a firewall equipped with simple security mechanisms and cluttered management interfaces; operation requires a separate configuration for each feature.

Unified network management

Greater increases the network security by using hardware information and one-time password for user authentication.

Network security is at risk due to sole reliance on user credentials for authentication.

Policy-based routing

Allow...
## MHG Series Product Comparison

### Specifications

<table>
<thead>
<tr>
<th>Model</th>
<th>MHG-800</th>
<th>MHG-1000</th>
<th>MHG-1500</th>
<th>MHG-2500</th>
<th>MHG-3500</th>
</tr>
</thead>
<tbody>
<tr>
<td>No. of NIC Ports</td>
<td>4 GbE</td>
<td>4 GbE</td>
<td>6 GbE</td>
<td>10~18 GbE</td>
<td>10~26 GbE</td>
</tr>
<tr>
<td>Connector Type</td>
<td>RJ45</td>
<td>RJ45</td>
<td>RJ45</td>
<td>RJ45/miniGBIC</td>
<td>RJ45/miniGBIC</td>
</tr>
<tr>
<td>Custom NIC Ports</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>0dBaFanless Design</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Power Redundancy</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Form Factor</td>
<td>9“ Desktop</td>
<td>1U Rackmount</td>
<td>1U Rackmount</td>
<td>1U Rackmount</td>
<td>2U Rackmount</td>
</tr>
</tbody>
</table>

### Features

<table>
<thead>
<tr>
<th>Feature</th>
<th>MHG-800</th>
<th>MHG-1000</th>
<th>MHG-1500</th>
<th>MHG-2500</th>
<th>MHG-3500</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 Compatibility</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>NIC Teaming</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Virtual WAN</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>SPI / Internal Firewall</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Web Filtering Database [Optional]</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Load Balancing</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Outbound</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Inbound</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Policy-based Routing</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>AAA Server</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Authentication</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Authorization</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Accounting</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Global QoS</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Individual QoS</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>P2P QoS</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Up-/Download Blocking</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Application Blocking</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>VPN Connectivity</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>IPSec / PPTP VPN</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>VPN Trunking</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>SSL Web VPN</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>SSL Application</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Hardware Authentication</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>VLAN / VLAN Trunking</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>High Availability</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>OTP Authentication</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
</tbody>
</table>

### Performance

<table>
<thead>
<tr>
<th>Feature</th>
<th>MHG-800</th>
<th>MHG-1000</th>
<th>MHG-1500</th>
<th>MHG-2500</th>
<th>MHG-3500</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU Cores / Threads</td>
<td>1 / 1</td>
<td>1 / 1</td>
<td>2 / 2</td>
<td>2 / 4</td>
<td>4 / 8</td>
</tr>
<tr>
<td>Firewall Throughput</td>
<td>470 Mbps</td>
<td>810 Mbps</td>
<td>1.1 Gbps</td>
<td>2.5 Gbps</td>
<td>2.9 Gbps</td>
</tr>
<tr>
<td>Max. Concurrent Sessions</td>
<td>1,000,000</td>
<td>1,000,000</td>
<td>1,000,000</td>
<td>2,000,000</td>
<td>4,000,000</td>
</tr>
</tbody>
</table>