Interface Masters
TECHNOLOGIES
Innovative Network Solutions

CISCO IPS and Interface Masters Qualification

Maximize network visibility

The modern enterprise runs on a dizzying array of large- to medium-scale commercial and customized applications. The data within those applications is exactly what attackers are targeting. Utilizing a Cisco IPS provides critical application and infrastructure protection for the data center or network core.

Uptime in the network

If the CISCO IPS fails for any reason due to power loss, or if it simply is not passing traffic, that is the bottleneck and point of failure on the network. The Niagara bypass unit will detect this failure and reroute all network traffic to bypass the IPS system, keeping the traffic flowing on the network.

The Niagara bypass units can also be configured to not allow traffic to flow if it detects failure in the CISCO IPS. This feature is useful for networks that have redundant paths. The networking devices on the network will detect that the traffic is not flowing on the route where the Niagara bypass unit is present, and will then reroute the traffic using the backup path.

The Niagara bypass units will send out a layer 2 Ethernet frame heartbeat (by default) in order to verify appliance health. The heartbeat can be configured to be ICMP, TCP Syn, IPX or UDP packet. The CISCO IPS will process the packet and forward the heartbeat from its input port to its output port with no configuration by default.

Qualified Systems

The CISCO IPS 4345, IPS 4360, IPS 4510, IPS 4520 systems have been verified and tested with the Niagara 2299, a 1Gbs External Bypass Switch. The Niagara 2299 supports maximum flexibility and scalability by offering four independent Gigabit Ethernet interface segments with various media combinations including copper, single-mode fiber, multi-mode fiber, multi-mode fiber to single-mode fiber conversion and copper to fiber conversion options.
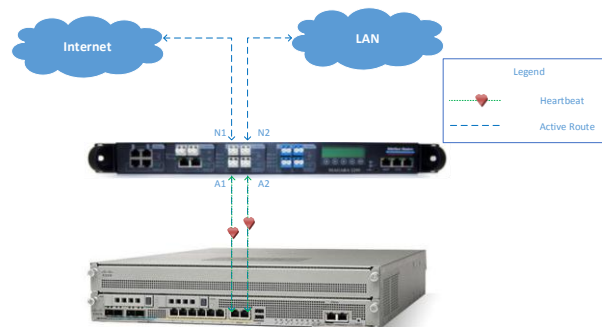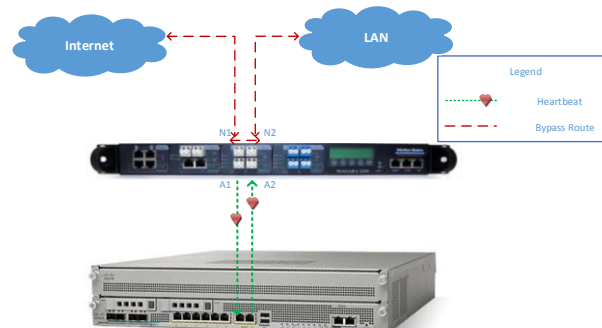

Figure 1: Inline Mode

Figure 2: Bypass Mode

The CISCO IPS 4510, IPS 4520, IPS 4520-XL system has also been tested and verified

with the Niagara 2818. The Niagara 2818 is a 10G quad-segment Bypass switch. This can also provide network protection for up to four 10Gbps Appliances. The Niagara 2818 also has a high availability mode where if two appliances are connected, and if the primary appliance fails, all traffic will be re-routed to the secondary appliances. The Niagara 2818 supports 1G and 10G fiber while the appliance ports can support 1G copper SFPs as well.

The interface Masters Bypass systems are provided with dual power supplies for maximum availability while they enable secure configuration via CLI secure shell or WEB UI (HTTPS). The system will also notify the system administrator on events like power supply failure, network bypass, system reboot and others.

About Interface Masters Technologies

Interface Masters Technologies is a leading vendor in the network monitoring and visibility market including Bypass, TAP, switches and smart NICs products, based in the heart of the Silicon Valley. Interface Masters' expertise lies in Gigabit, 10GbE and 40GbE networking solutions that integrate with monitoring, inline networking, IPS, UTM, Load Balancing, WAN acceleration, and other mission-critical IT and security appliances. Flagship product lines include PacketMaster® Network Packet Broker, specialized 10GE internal server adapter cards, switches, 10Gb and 40Gb external intelligent Network TAP and Bypass and failover systems. Company Headquarters are located in San Jose, CA with satellite offices in Hong Kong and Europe. For more information, contact: sales@interfacemasters.com or visit www.interfacemasters.com.

For more information on Cisco IPS, visit http://www.cisco.com/go/ips.