Technology Overview

Gigamon Resilient Inline Protection

Maximizing both network uptime and network security is a challenge for any organization. As more tools move from an out-of-band detection mode to an inline active protection mode, network resiliency becomes a particular concern. Redundant network architectures are designed to be fault-resilient, but they present their own challenges when it comes to inline inspection of traffic.

Gigamon has developed a resilient inline architecture that utilizes the GigaVUE-HC2 to address these concerns as part of the GigaSECURE® Security Delivery Platform—Gigamon Resilient Inline Protection (GRIP™).

Inline security appliances represent potential points of failure in the network. Whether due to a power outage, software malfunction, or processing bottleneck, failing inline tools can disrupt the very applications and services they are meant to protect. This problem is addressed on two fronts: deploying redundant inline tools and utilizing bypass protection.

Redundant Inline Tools

Redundant inline tools address resiliency with the simple principle that if one tool fails, the redundant tool takes over. This is also known as 1+1 protection. An inline visibility node is required to detect the failure of the active tool and redirect traffic to the standby tool. The health of an inline tools is determined by monitoring the state of the link and optionally sending bidirectional heartbeat packets that verify the tool is passing traffic. The parameters of the heartbeat packets can also be fine-tuned to trigger a failover to the standby tool when the latency of the active tool becomes too great.

Rather than have an active/standby arrangement, the visibility node can distribute traffic across multiple inline tools. Not only does this allow security monitoring to scale up to the speed of the network, but also in the event of a tool failure, the traffic can be redistributed to the remaining healthy tools. In addition, a dedicated standby tool can be deployed to provide N+1 protection (see Figure 1).

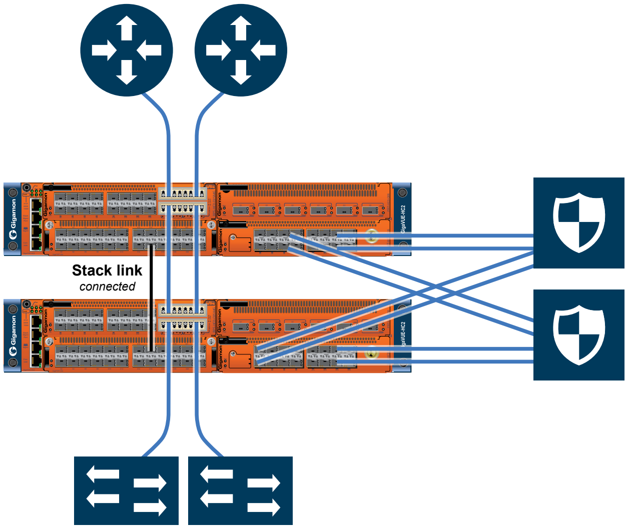

Figure 1: The Visibility Fabric node can distribute traffic across multiple inline tools; in the event of a tool failure, the traffic can be redistributed to the remaining healthy tools or to a dedicated standby tool (1+1 protection shown)

Bypass Protection

Bypass protection comes in two varieties: logical and physical. Both operate on the principle that traffic continuity must be maintained even if the traffic cannot be inspected. This is also known as fail to wire.

> Many organizations deploy a security policy that forbids fail to wire. In highly sensitive environments, it may be preferable to have a disruption in network traffic than allow uninspected traffic into the network. These cases can still benefit from deploying redundant tools, but would not benefit from bypass protection or GRIP™.

With logical bypass, the traffic is forwarded to the network should the inline tool fail. When deploying redundant inline tools, bypass protection is applied if/when both the active and standby tool is down. Or if multiple tools are present, traffic is bypassed when a certain number of the tools have failed.

In order to optimize inline tool performance, the visibility node can be configured to only send a portion of the network traffic to the tool and bypass the rest. For example, a tool that is designed to inspect a particular type of application, such as database or email traffic, will benefit if only that type of traffic is sent to the tool. The processing load on the tool can be reduced and the performance enhanced by only sending it traffic on specific subnets, VLANs, or TCP/UDP ports, and bypassing the rest. The power of inline Flow Mapping® technology allows the GigaVUE-HC2 fabric node to send different traffic to separate tools for inspection.

Physical bypass protection avoids any problem with power failure of the visibility node itself. In the event of a power failure, relays complete the network circuit and keep traffic flowing. The relays are designed such that they require power to access the network traffic (so that it can be forwarded to the inline tools) and switching to protected mode occurs automatically and without software intervention upon the loss of power.

How GRIP Works

GRIP supports a variety of different deployment options, including single or multiple network paths protected by one or more inline tools. Below is a description of one common arrangement in which two redundant network paths are protected by two Intrusion Protection Systems (IPSes) deployed inline. Two GigaVUE-HC2 nodes provide additional resiliency; one is designated as primary and one is secondary. Both are connected to both inline IPSes.

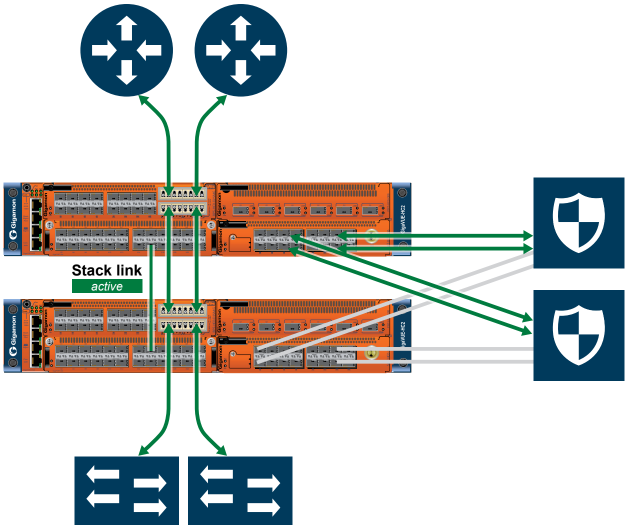

Figure 2: Traffic path while the primary GigaVUE-HC2 fabric node is up

In standard operation, the primary GigaVUE-HC2 forwards network traffic to the IPSes. The secondary GigaVUE-HC2 node is in a standby mode with its inline network ports physically bypassing the traffic. Thus, only a single copy of the traffic is sent to the IPSes. The two GigaVUE-HC2 nodes are also connected via a 10G status link that the secondary GigaVUE-HC2 fabric node uses to monitor the state of the primary node.

If the primary GigaVUE-HC2 node loses power, the status link will turn off and the secondary node is triggered to disengage its physical bypass relay and begin sending traffic to the inline tools. When the primary GigaVUE-HC2 node recovers and the signaling link returns, the secondary node again engages its physical bypass.

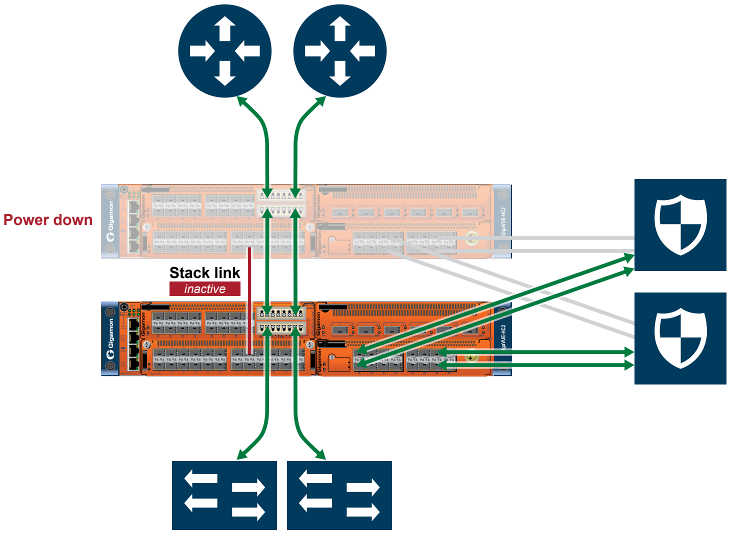

Figure 3: Traffic path should the primary GigaVUE-HC2 fabric node lose power; the secondary node forwards the traffic to the security tools

Should both the primary and secondary GigaVUE-HC2 nodes lose power, both sets of physical bypass relays will be engaged, preserving network continuity. Thus, GRIP provides three layers of resiliency: support for redundant network architectures, redundant inline tools, and redundant visibility nodes.

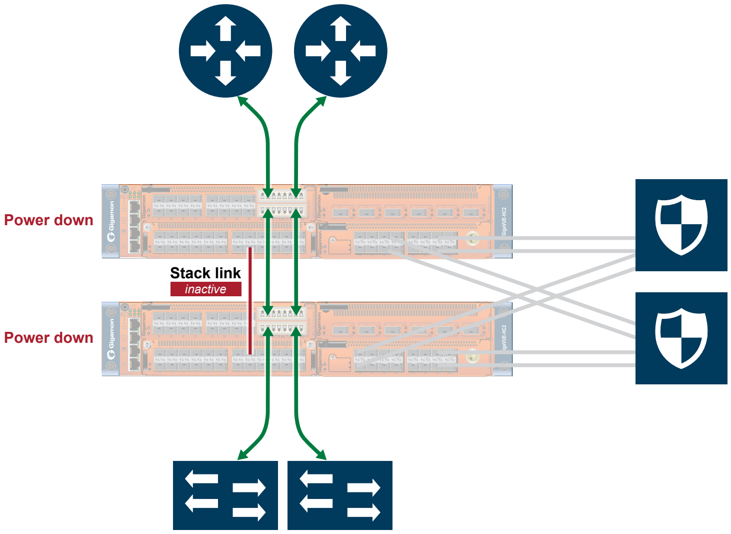

Figure 4: If both the primary and secondary GigaVUE-HC2 nodes go down, network traffic integrity is maintained

Variations

GRIP also works with out-of-band security tools, either instead of or in concert with inline tools. In addition, more complex and sophisticated arrangements of inline tools is also supported. For example, GRIP can be configured with multiple inline tools arranged serially, each inspecting network traffic, such as IPS, data loss prevention (DLP), and anti-malware appliances.

About Gigamon

Gigamon provides an intelligent Unified Visibility Fabric™ to enable the management of increasingly complex networks. Gigamon technology empowers infrastructure architects, managers and operators with pervasive visibility and control of traffic across both physical and virtual environments without affecting the performance or stability of the production network. Through patented technologies, centralized management and a portfolio of high availability and high density fabric nodes, network traffic is intelligently delivered to management, monitoring and security systems. Gigamon solutions have been deployed globally across enterprise, data centers and service providers, including over half of the Fortune 100 and many government and federal agencies.

For more information about the Gigamon Unified Visibility Fabric visit: **www.gigamon.com**