Joint Solution Brief

Check Point Optimizes Security with Gigamon's Full Network Visibility

The Challenge

Due to the growing frequency and sophistication of security threats, there is a need for a fully integrated and centrally managed security infrastructure. Ensuring traffic visibility for the devices in this infrastructure along with the ability to fully coordinate enforcement by applying policy broadly and consistently is essential.

Integrated Solution

Check Point's Next Generation Threat Prevention solution, including Check Point's SandBlast Zero-Day Protection and Check Point's Next-Generation Threat Prevention Platform, offers customers a multi-layered line of defense with extensive security. Gigamon provides high-availability design options and the ability to deploy easily in asymmetrically routed networks as well as a mechanism to easily change deployment modes of devices without time-consuming physical re-cabling and change orders.

Joint Solution Benefits

- Enable visibility to the entire network; route traffic from branch locations, virtualized segments and key physical links
- Ensure controllable network connectivity even in the event of device failure
- Manage asymmetric traffic flows to ensure efficient performance of your firewall
- Deploy firewalls out of band with full functionality to test performance and then move inline at the touch of a button
- Aggregate or load balance traffic flows to optimize device performance
- Off-load SSL decryption to maximize performance
- Filter selected traffic to avoid unnecessary processing
- Generate metadata (NetFlow/IPFIX) from any traffic flow to avoid unnecessary processing

Introduction

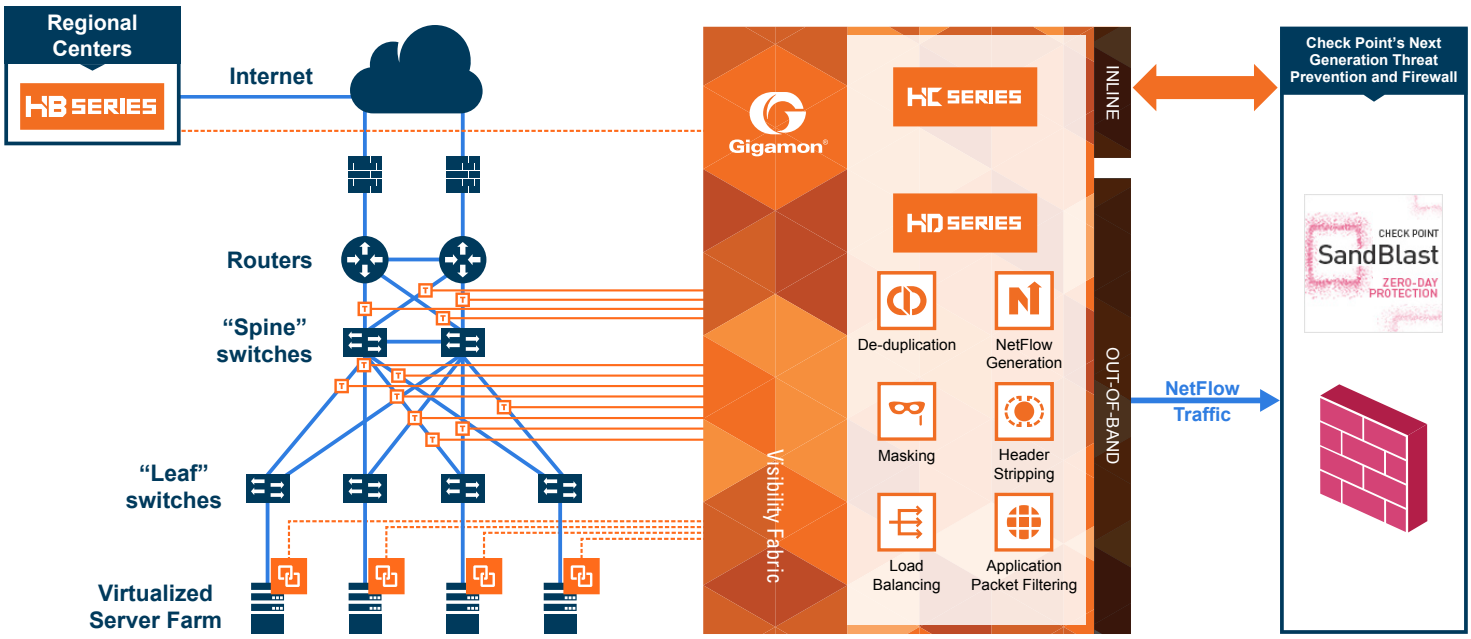
Cyber security professionals believe that today's threat landscape presents an overwhelming challenge due to increasing threat volume and sophistication. The advantage is that attackers have many places to exploit: BYOD, mobile communications and virtualization all add to a vastly expanded network perimeter. To combat attacks, organizations need to protect this valuable data using multi-layered defenses. Network operators and security teams need to carefully design their implementations to ensure security is maintained while performance is not negatively impacted by additional analytics and controls. In order to do all of this, security devices must have efficient access to the traffic they need to monitor, operate seamlessly even in unwelcoming routing schemes, and never introduce a single point of failure into the network.

The Gigamon and Check Point Joint Solution

Check Point's Next-Generation Threat Prevention Platform delivers a multi-layered line of defense and extensive security intelligence coverage to help combat today's threats. Check Point's SandBlast Zero-Day Protection catches and proactively prevents malware from infiltrating a customer's network. The Threat Prevention Appliances and Software stop application-specific attacks, botnets, targeted attacks, APTs and zero-day threats while easily and confidently managing access to millions of websites. Check Point's integrated Next-Generation Firewall provides customers of all sizes with the latest data and network security protection while reducing complexity and lowering the total cost of ownership. Gigamon's GigaSECURE® Security Delivery Platform helps network owners get the most from their investment in Check Point's technology. The integrated Check Point and Gigamon solution provides an efficient, high fidelity way to spot and respond to threats across the network. Key features for Check Point's deployments include:

Full Visibility: The GigaSECURE platform provides visibility across the entire network and can deliver traffic from multiple locations, like branch offices and virtualized data center segments back to centrally located Check Point devices.

Bypass Protection: Deploy Check Point's devices inline and use the GigaSECURE functionality to provide physical bypass traffic protection in the event of power loss and logical bypass traffic protection in the event of an inline tool failure.



Manage Asymmetric Routing: Most security devices, including those from Check Point, require inspection of all the packets in a session to be performed by the same device. GigaSECURE provides an intelligent and efficient way to ensure this happens.

Traffic Distribution: Improve the scalability of inline security by distributing the traffic across multiple security devices, allowing them to share the load and inspect more traffic or aggregate multiple traffic flows into a single flow for efficient port utilization on the firewall.

Traffic Filtering: Send specific traffic to your Check Point devices based on Layer 2 to Layer 4 rules so that applications and services are protected while safe traffic can bypass inspection.

Agile Deployment: Add, remove, and/or upgrade firewalls without disrupting network traffic; convert tools from out-of-band monitoring to inline inspection on the fly without rewiring.

NetFlow Generation and SSL Decryption: If desired, processing intensive tasks can be offloaded from the Check Point devices by using GigaSECURE's functionality for generating unsampled, enhanced metadata (NetFlow/IPFIX) from any selected traffic stream. Similarly, the Security Delivery Platform can be used to decrypt SSL traffic for inspection by Check Point devices.

Learn More

For more information on the Check Point and Gigamon solution, contact:

Check Point® SOFTWARE TECHNOLOGIES LTD.
www.checkpoint.com

Gigamon®
www.gigamon.com

3186-01 04/16