



CASE STUDY

Manufacturer Chooses Bypass for Deployment of Next Gen Firewall

Standalone Bypass Supports Fail-Safe Operation of Cisco Security Appliance

After a demonstration that showed information leaving the company and going to China in an unsecure fashion, this Global 500 manufacturer of HVAC equipment and automotive devices received CFO approval to purchase the appliances necessary for inline security monitoring.

They chose the Cisco ASA with FirePOWER™ for its advanced functionality, and the network team looked for a way to support real-time monitoring, while also protecting network availability. Ixia provided the solution they needed.

The Need for Failover

The company's previous firewall solution failed closed – meaning that if it lost power or stopped functioning, traffic was not forwarded on.

However, Cisco's ASA with FirePOWER needs to be able to fail open. It must be set up in a way that permits network traffic to continue flowing, even when the device goes down. This is because ASA FirePOWER is more than just a firewall.



Company:

- Global equipment manufacturer

Key Issues:

- Minimize downtime during deployment of FirePOWER in 1000 locations
- Protect network against future appliance failure

Solutions:

- Ixia iBypass and IndigoPro

Results:

- Faster, consistent deployment
- Reduced risk of downtime due to real-time traffic inspection

It brings an Intrusion Prevention System (IPS) and a Next Generation Firewall (NGFW) together, in a single device. FirePOWER appliances must fail open and keep traffic flowing to allow:

- IPS policies to be reconfigured
- The appliance to be serviced or upgraded
- The appliance to be moved from one network segment to another

... all without impacting network traffic and causing costly network downtime.

Ixia's external bypass switch is designed to do exactly that using the industry's fastest heartbeat, to fail open as fast as possible in the event of a failure. Using a bypass switch in tap mode also allows the IPS to function as an Intrusion Detection System (IDS) – passively monitoring network traffic without affecting it, for even more flexibility.



The simple addition of an external bypass switch took the fear out of implementing real-time security monitoring

Fastest Time to Value

The company did a head-to-head comparison of multiple bypass solutions and chose the Ixia iBypass VHD, the highest density bypass switch available. Fast, accurate deployment was essential, as the company wanted to implement security appliances in over 1000 locations across six continents. A slow complicated process would have cost the manufacturer too much time and disrupted business. Ixia's solution helped them avoid this.

Ixia's iBypass is preconfigured to automatically integrate with Cisco security appliances via a single click, to limit potential configuration errors and deploy tools in minutes, instead of hours.

Control and Configuration Made Easy

Ixia iBypass switches were deployed along with Ixia Indigo Pro: a centralized system for configuration and management of an organization's taps, bypasses, monitoring switches, and network packet brokers. With dozens of bypasses installed in multiple locations across the globe, the company needed a streamlined and cost-effective way to manage them all remotely, from a single pane of glass.

Indigo Pro allows the company to push configurations and updates to every device – across the globe – at the touch of a button. According to the network team, Ixia's competitors were unable to offer this level of functionality. Without Indigo Pro, they would have been forced to update, revise, patch, or push configurations to each device, one by one. Indigo Pro was a key component of the deployment process, saving the company hours of IT admin. Furthermore, the network team was particularly impressed with the highly-visual user interface that Ixia offered, in contrast to competitive solutions.

Security, Stability, and Seamless Control

As a supplier to governments around the world, the manufacturer needed to maintain the highest level of security over customer contracts and information. A breach leading to the unauthorized disclosure of sensitive data could damage the trust and confidence of customers, and severely impact future business.

Working with Ixia, the company was able to take advantage of the additional security provided by the Cisco ASA with FirePOWER, without impacting network availability. Ixia's external bypass technology allows configuration changes or software upgrades to Cisco appliances without waiting for a maintenance window, and promotes network stability – a 'must have' for a global manufacturer of this size.

For this manufacturer, the simple addition of an external bypass switch took the fear out of performing real-time monitoring, to strengthen security and protect their business.

Learn more at: www.keysight.com

For more information on Keysight Technologies' products, applications or services, please contact your local Keysight office. The complete list is available at: www.keysight.com/find/contactus

