CASE STUDY

Service Provider Strengthens Defense Against Cyberattacks

Inline Monitoring Improved And Network Availability Protected

The massive network of this high-profile provider of Internet services (including search, shopping, auctions, and news) is exposed to cyberattacks on a daily basis. As a result, the company needed a strong security infrastructure that would identify and prevent cyberattacks in real time while minimizing network latency and any impact on its end users.

At the same time, the company needed to keep capital expenditures and operating costs under control to stay profitable in a highly competitive market. It wanted to minimize the time the information technology (IT) staff spent managing security to let them spend more time developing new services. And, although it was planning future network upgrades to keep up with traffic growth, the company also wanted to continue using as much of its existing security infrastructure as possible to keep costs from rising too quickly.

Enhance Security With IPS Traffic Inspection

The first step was to strengthen live traffic inspection with deployment of a new and powerful intrusion prevention system (IPS). The provider worked with security experts to deploy a solution that could help staff visualize the source and nature of incoming attacks and respond to them quickly.

In a business dependent on providing customers with fast access to their favorite services, the company needed to ensure traffic surges and cyberattacks meant to overwhelm security appliances do not cause overall network outages. The standard practice was to deploy an external bypass switch in front of each security solution deployed inline as insurance against an unexpected outage. Keysight iBypass switches also provided additional value by allowing IT managers to proactively take security devices offline for troubleshooting or software upgrades without having to wait for a network maintenance window.

Company:

High-profile service provider in Japan

Key Issues:

- Extraordinary volume of network traffic
- Daily exposure to cyberattacks
- Business dependent on network availability
- Pressure to control costs

Solutions:

- Keysight external iBypass switch deployed in front of each IPS protects network availability
- Keysight Vision ONE aggregates, manipulates, and delivers traffic to tools at high speed

Results:

- External bypass switch deployed in front of IPS protects network availability
- Traffic manipulation helps security appliances operate efficiently
- Extended use of lower-speed tools on higher-speed network
- Easier management of very large, complex network

KEYSIGHT TECHNOLOGIES

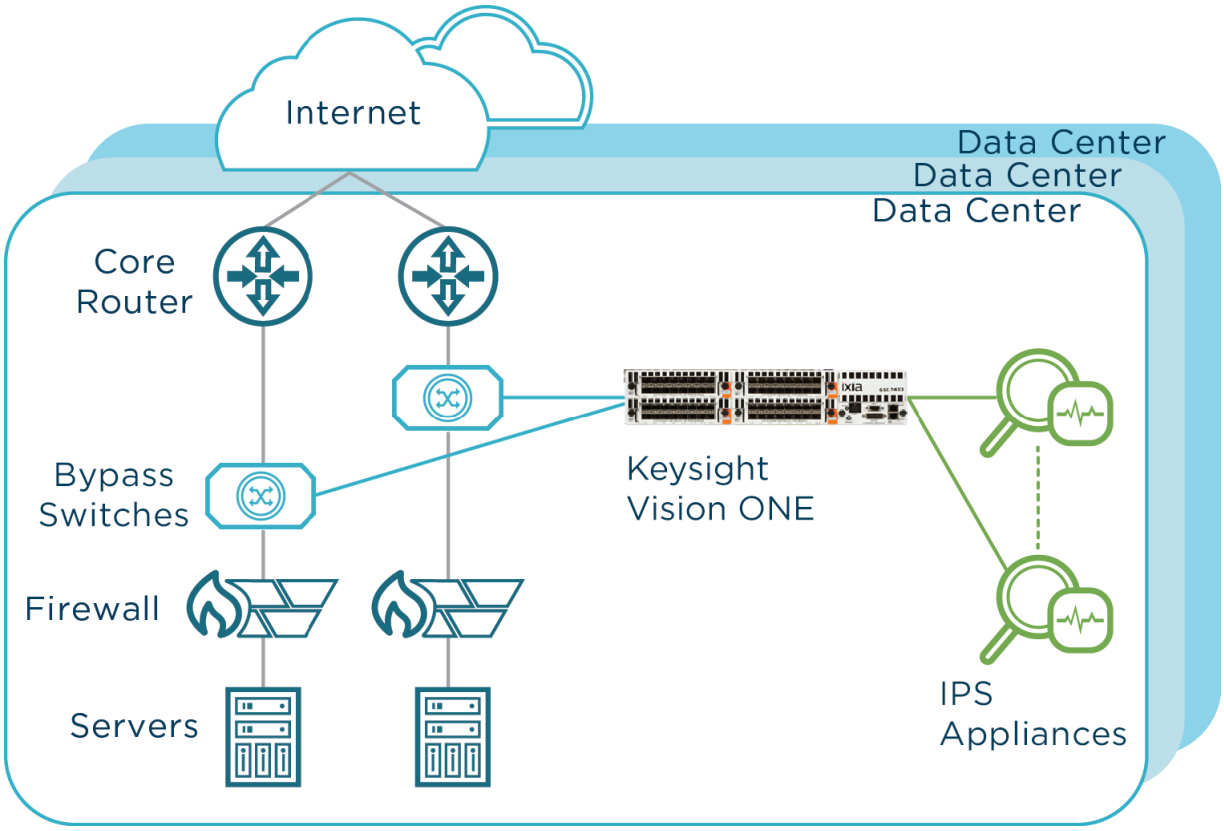
Increase IPS Efficiency By Delivering Only Relevant Data

Given the extraordinary volume of network traffic, the company also needed a solution that would let it selectively manipulate the traffic delivered to the IPS and deliver it with minimal latency to increase efficiency and maintain a satisfactory customer experience.

The IT team also realized the company's needs would change over time as cyber threats evolved. This led them to request a solution in which the solution could be changed and updated easily. With the scale and complexity of the network, the team also wanted to make system-wide changes easily from a central location to minimize the need for hands-on involvement.

The company ended up choosing an Keysight network packet broker and is easy-to-use graphical interface. The Keysight Vision ONE solution aggregates traffic collected by the network taps and optimizes it according to rules provided by the IT staff, delivering only relevant data to each security appliance.

"As part of our efforts to enhance network security, we wanted to keep track of the different types of incoming cyberattacks and respond to them automatically. Previously, IP addresses were the only information we had available on attacks. We wanted to implement security devices, such as IPS and WAF (web application firewall), to keep track of attacks in greater detail." -Manager, Network Security



Use Existing Tools With Higher Speed Network Links

Since the Keysight Vision ONE packet broker sits between the network taps and the security appliances, it also lets the provider continue using its existing lower speed security appliances, even after upgrading to a higher speed network. This allows the provider to upgrade security appliances over time, reducing the initial cost of a network upgrade.

Simplify Management With Superior Interface

The provider tried similar products for comparison prior to adopting the Keysight solution and saw a strong advantage in Keysight's intuitive and user-friendly interface. This feature allowed them to start using the Keysight Vision ONE right away, without any special training.

Since deployment of its new security architecture, the provider has also discovered another advantage. The Keysight Vision ONE packet broker provides a template library with multiple types of preconfigured filtering criteria. Using the library, the team can easily create new out-of band monitoring data filters, simplifying the process of updating the company's very large network infrastructure.

"A nice-looking GUI is a good thing, but as we later discovered, it also had a lot of operational advantages. We rarely make any configuration errors." - Network Security Engineer

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

KEYSIGHT TECHNOLOGIES