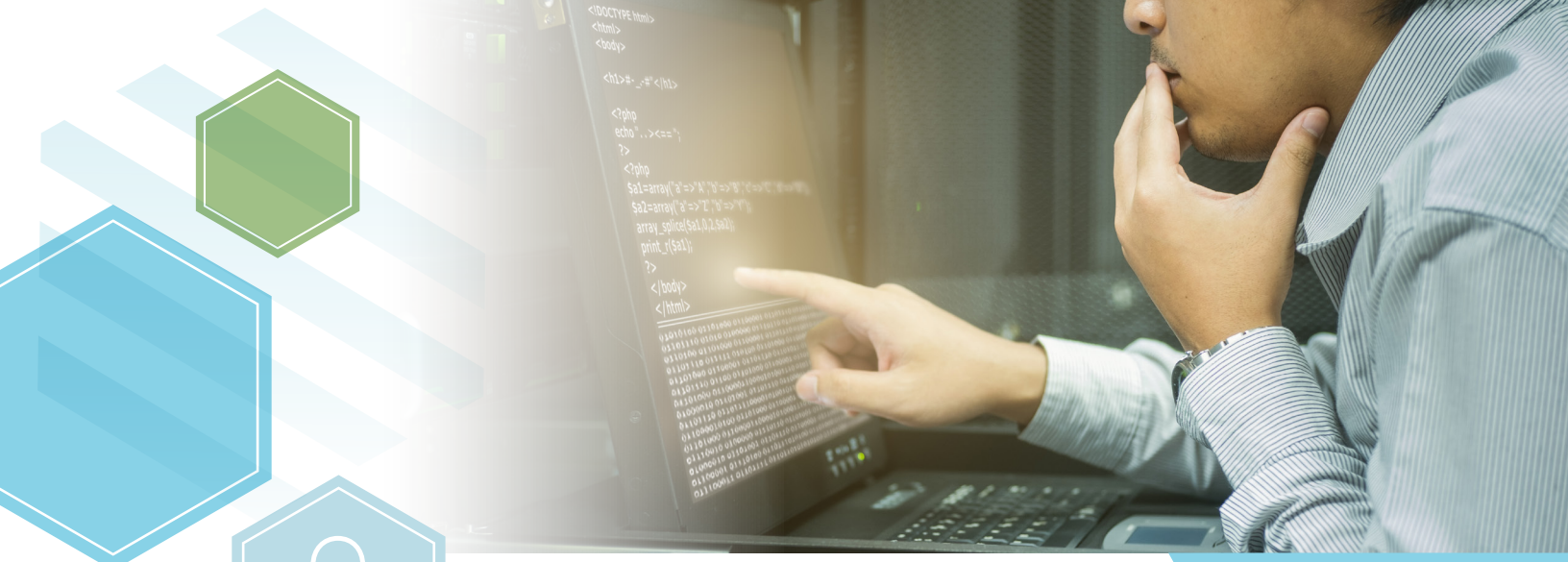

CASE STUDY

Service Provider Strengthens Defense Against Cyberattacks

INLINE MONITORING IMPROVED AND NETWORK AVAILABILITY PROTECTED

Company:
High-profile service provider in Japan

Key Issues:
- Extraordinary volume of network traffic
- Daily exposure to cyberattacks
- Business dependent on network availability
- Pressue to control costs

Solution:
- Ixia external iBypass switch deployed in front of each IPS protects network availability
- Ixia Net Tool Optimizer aggregates, filters, and delivers traffic to tools at high speed

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

ixia
A Keysight Business

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 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

915-8131-01-4071 Rev A

deployed inline as insurance against an unexpected outage. Ixia 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.

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 filter the traffic delivered to the IPS and deliver it with minimal latency to increase efficiency and maintain a satisfactory customer experience.

"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

The IT team also realized the company's filtering needs would change over time as cyber threats evolved. This led them to request a solution in which the filters 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 Ixia network packet broker with intelligent filtering capabilities and an easy-to-use graphical interface. The Ixia Network Tool Optimizer® (NTO) solution aggregates traffic collected by the network taps and filters it according to rules provided by the IT staff, delivering only relevant data to each security appliance. Filtering reduces the appliance's overall workload and eliminates unproductive processing that uses up valuable capacity. For instance, traffic that is not transactional in nature, such as Netflix video traffic, can be passed around IPS devices that are looking for vulnerability exploits. With less data to process, the company can delay upgrading or scaling its security appliances, preserving budget for other projects.

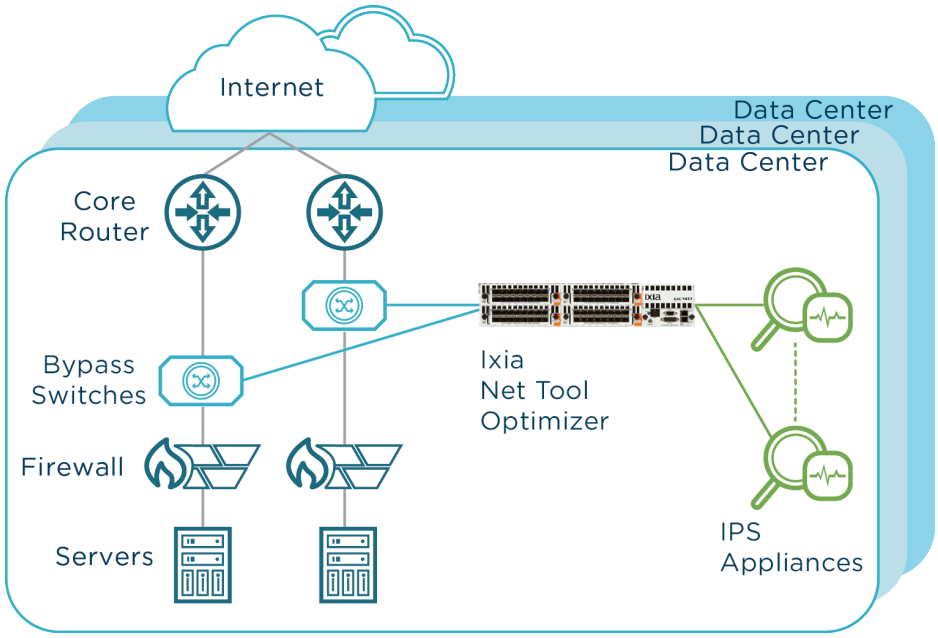

Figure 1. Ixia Inline Security Solution

915-8131-01-4071 Rev A

USE EXISTING TOOLS WITH HIGHER SPEED NETWORK LINKS

Since the Ixia NTO 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.

"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

SIMPLIFY MANAGEMENT WITH SUPERIOR INTERFACE

The provider tried similar products for comparison prior to adopting the Ixia solution and saw a strong advantage in Ixia's intuitive and user-friendly interface. This feature allowed them to start using the Ixia NTO right away, without any special training. The interface lets them easily identify information such as which traffic is being inspected and what kind of filter is being applied, to simplify security and let the IT team focus more on creating the new services customers want.

Since deployment of its new security architecture, the provider has also discovered another advantage. The Ixia NTO packet broker provides a filtering library with multiple types of preconfigured filtering criteria. Using the library, the team can easily create new filters, and also export an existing filter to another network segment or data center, simplifying the process of updating the company's very large network infrastructure.

IXIA WORLDWIDE

26601 W. Agoura Road
Calabasas, CA 91302

(Toll Free North America)
1.877.367.4942

(Outside North America)
+1.818.871.1800

(Fax) 1.818.871.1805

www.ixiacom.com

IXIA EUROPE

Clarion House, Norreys Drive
Maidenhead SL64FL
United Kingdom

Sales +44.1628.408750
(Fax) +44.1628.639916

IXIA ASIA PACIFIC

101 Thomson Road,
#29-04/05 United Square,
Singapore 307591

Sales +65.6332.0125
(Fax) +65.6332.0127