How Scientific Atlanta Outsourced Intrusion Prevention System Management to Cisco Remote Operations Services

Twenty-four hour monitoring, plus explanations and recommended actions, enable swift response to security threats.

Cisco IT Case Study/Network Security/Cisco ROS Managed IPS Service: This case study describes why and how the Scientific Atlantic division takes advantage of the managed Intrusion Prevention System (IPS) service offered by Cisco® Remote Operations Services. Cisco customers can draw on Cisco IT's real-world experience in this area to help support similar enterprise needs.

Background

Scientific Atlanta, which became a Cisco company in February 2006, is a leading supplier of transmission networks for broadband access. The company is changing the way that consumers receive, use, and enjoy a variety of entertainment, information, and communication experiences provided by cable, telecom, wireless, and satellite service providers. Its 9000 employees, who work in global offices, represent more than 16 percent of Cisco's global workforce of 55,400.

Business Challenge

Scientific Atlanta outsourced the management of its Intrusion Prevention System (IPS) before it became a Cisco company. "After we became part of Cisco, we knew that we wanted to continue outsourcing IPS," says Scott Stanton, information security architect, Scientific Atlanta. "We simply do not have the staff to provide 24-hour monitoring of network security incidents, constantly update IPS sensors with new signatures, and tune the sensors to reduce false positives." However, the company wanted to work with a different managed security services provider that had a stronger commitment to communicating important information. For example, the previous provider did not always inform the company when sensors were offline. "Our top selection criteria were a commitment to communication, SLAs [service level agreements] for response times, and in-depth knowledge of Cisco IPS sensors," says Stanton.

> "The most important part of the Cisco ROS managed security service is converting raw sensor data into actionable information. Trouble tickets explain the significance of sensor data and recommend corrective actions, which helps our security team be more effective while spending less time."
>
> **Scott Stanton, Information Security Architect, Scientific Atlanta**

Network Solution

Cisco Remote Operations Services (ROS) offered a managed IPS service that met Scientific Atlanta's requirements. "Outsourcing to Cisco ROS gives us access to the engineers who developed the Cisco IPS solution and know it better than anyone else," says Stanton. Cisco ROS also offers SLAs for response times. "Whenever we detect an incident on a customer network, we have someone investigate it within 30 minutes," says Shane Mahon, customer support engineer, Cisco ROS.

EXECUTIVE SUMMARY

BACKGROUND

- Scientific Atlanta became a Cisco company in February 2006
- Company previously subscribed to a managed service for perimeter-based Intrusion Prevention Systems

CHALLENGE

- Build trusted relationship with managed security service provider
- Gain earlier awareness of network threats
- Avoid false positives and false negatives

SOLUTION

- Subscribed to managed IPS service from Cisco ROS
- Added internal IPS sensors to perimeter-based sensors

RESULTS

- Received more actionable information on security threats
- Reduced time spent on false positives

LESSONS LEARNED

- Convey relative value of network assets to Cisco ROS

Respond quickly to requests for information from Cisco ROS team

Pre-Implementation Meeting

When the engagement began, Cisco ROS and the Scientific Atlanta network security team met to discuss the business and technology requirements for the managed security service. Discussion topics included:

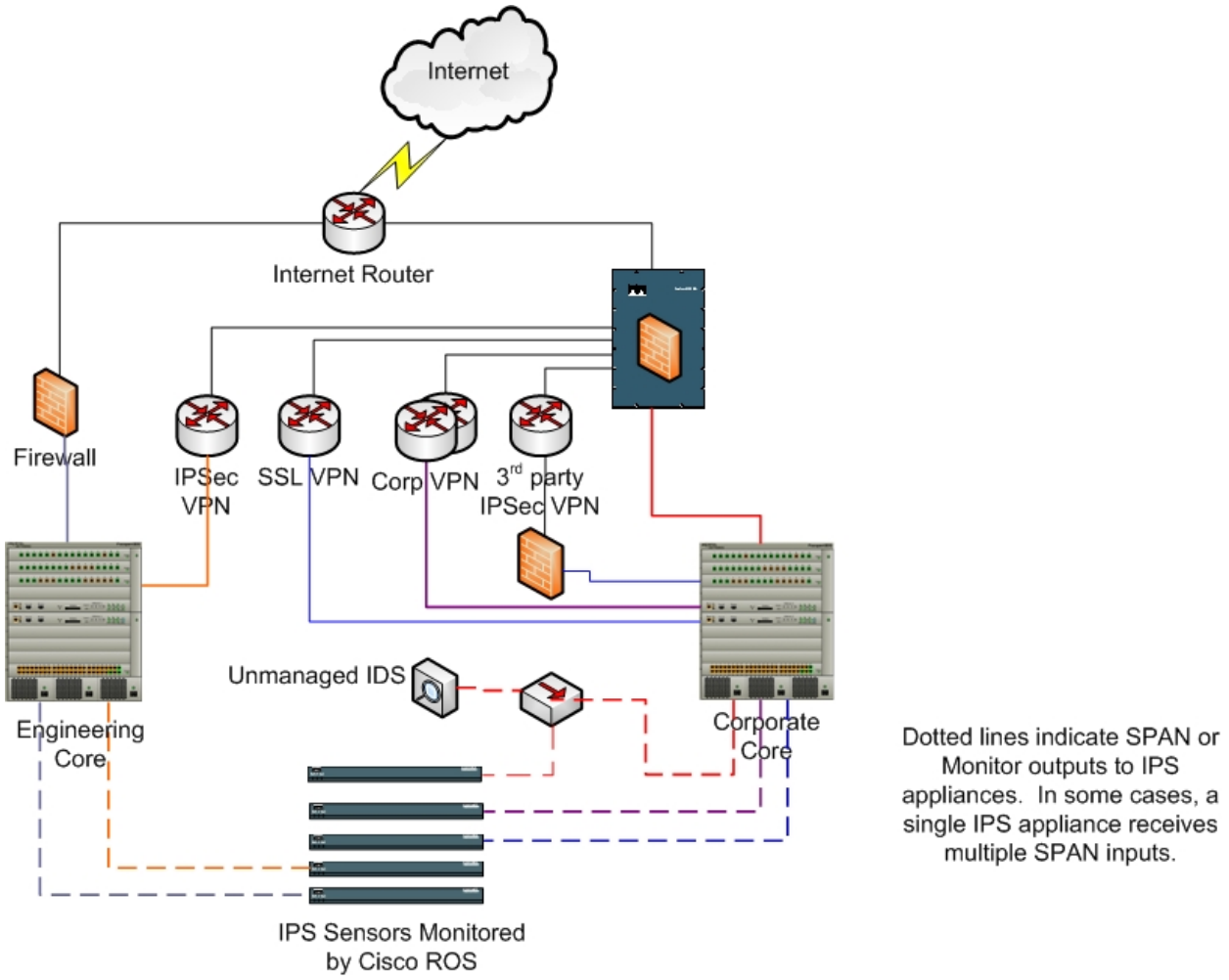
- Types of attacks requiring notification. Scientific Atlanta had the choice to be notified of probable attacks that were not confirmed, confirmed attacks in which the attacker researched network resources but did not steal data or compromise systems, or only confirmed attacks in which data was stolen or systems compromised. “Many customers initially want us to err on the side of too many trouble tickets,” says Chris Haugen, customer operations analyst, Cisco ROS. “Later, they often want to reduce e-mail volume, for example, by deciding to forego notification of reconnaissance events [network scanning].” The Scientific Atlanta network security team had already used a managed security service and felt confident not receiving notification of events that were unlikely to cause harm. The company also requested e-mail notification whenever Cisco ROS applied updates to the sensor software.
- Places in the network to monitor. With its previous managed security service, Scientific Atlanta only monitored the network perimeter. “But if a worm spreads through the internal network, perimeter-based IPS sensors do not detect it,” says Stanton. Therefore, Scientific Atlanta asked Cisco ROS to perform internal monitoring using the multiple interfaces of the Cisco IPS 4200 Series sensors to detect and mitigate threats spreading from one desktop to another, inside the data center, or from someone using a VPN. The additional network-based monitoring would give Scientific Atlanta two notifications of threats that started or ended at a user desktop and traveled across the perimeter: one each from the perimeter and internal IPS sensors. “If the threat does not register on both sensors, we know that something is not working,” says Stanton.
- Asset values. Scientific Atlanta indicated the value of various network devices to the business. Cisco ROS uses this information to create risk ratings, which, in combination with the threat severity level, determine whether events will be reported to Scientific Atlanta.
- Contact methods. Scientific Atlanta indicated who Cisco ROS should contact, at which time of day, and how, for example, by sending an e-mail or calling a mobile phone. “If an issue occurs on the Belgium network, Cisco ROS first calls the designated contact person at that site,” says Stanton. “This arrangement is convenient for our IT staff, because I don’t need to be contacted at 3:00 a.m. for an incident that someone else can resolve.”
- Types of Cisco IPS sensor required at different places in the network. Cisco ROS made the recommendation based on traffic patterns.

Two-Step Deployment

Deployment occurred in two phases: perimeter sensors and internal network sensors. During the first phase, Scientific Atlanta replaced its existing perimeter sensors with Cisco IPS 4240 Sensors (Figure 1). The perimeter IPS implementation mirrors low-bandwidth ports (less than or equal to 1Gbs) directly to the monitor inputs on the sensors. In places where multiple devices are needed to monitor traffic, a hub mirrors traffic to multiple destinations. The Cisco

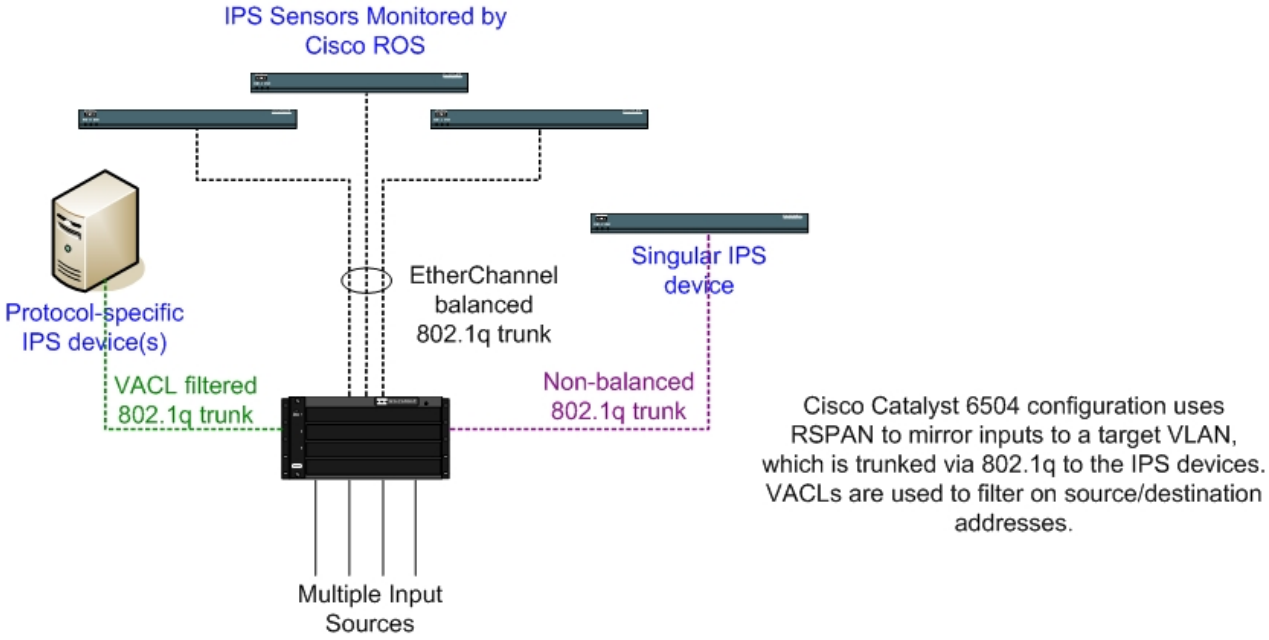
IPS 4200 Sensors can support up to four monitor inputs. “Our time commitment was limited to racking up the sensors and connecting the console cable to the modem,” says Stanton. “We notified Cisco ROS when each sensor was connected, and then they used a site-to-site VPN connection to place the sensors online within 24 hours.” To expedite deployment, Cisco ROS created a configuration template for the IPS sensors.

Figure 1. Perimeter IPS Implementation at Scientific Atlanta



During the second phase, Cisco ROS worked with Scientific Atlanta to determine where to place the internal, network-based IPS sensors. Cisco ROS recommended Cisco IPS 4255 Sensors for high-bandwidth (greater than 1Mbps) applications, such as data centers and inter-building 1GB links. Cisco Catalyst 6504 Switches provide filtering and load balancing of the sensor inputs (Figure 2). Some sensors monitor multiple network segments. The inputs are configured as a Remote Switched Port Analyzer (RSPAN). The destination is a VLAN carried by an 802.1q trunk, which is load-balanced using EtherChannel with source and destination IP address hashing. “This approach helps ensure that each appliance consistently receives traffic for a given source and destination IP address,” says Stanton. In VLANs where Scientific Atlanta only monitors a specific protocol, IP address, or service, such as HTTP, the company applies a VLAN access control list (VACL).

Figure 2. High-Bandwidth IPS Implementation



Monitoring

Cisco ROS remotely configures, manages, updates, tunes, and troubleshoots the sensors from its secure operations centers (SOC) in Austin, Texas and Bangalore, India. SOC personnel scrutinize all network traffic that meets pre-established criteria for the signature's severity rating and the asset's risk rating. "Our Cisco customer let us know that he cared about some events and not about others, which helps us save him time," says Mahon. Scientific Atlanta is especially interested in:

- Indications that one host is scanning many Scientific Atlanta systems:
  - One or two hosts performing reconnaissance scans of address ranges containing 20 to 50 or more nodes
  - Use of common, commercially available scanners
  - Internet Control Message Protocol (ICMP) pinging
  - Events in which the destination is unreachable
- The top 10 exploits listed by the Computer Security Institute and the Open Web Application Security Project (OWASP)
- One system attacking multiple systems on a specific port

Signatures for detecting the aforementioned events are built into Cisco IPS sensors. Cisco ROS developed custom signatures for other events of interest to Scientific Atlanta, such as:

- Multiple invalid page requests (Web server 4xx and 5xx messages)
- Many invalid logon attempts to Server Message Block (SMB), HTTP, Telnet, and File Transfer Protocol (FTP) servers

Cisco ROS regularly updates signatures, distributing them to the sensors over the VPN connection. The team waits until the new signatures' effectiveness has been proven before reporting results to Scientific Atlanta. "Best practices like these give us more accurate results and save time for our network security team," says Stanton.

Notification Methods and the Online Portal

To report lower-priority security events, Cisco ROS e-mails an event notification. To report higher-level alerts indicating active worms, viruses, or attacks, Cisco ROS phones the appropriate contact person, based on the event location and time of day.

When someone at Scientific Atlanta calls or e-mails Cisco ROS, the case is immediately updated. "We interact with the Cisco ROS SOC on day-to-day issues such as network traces to determine if the issue is a real threat," says Stanton. The case is escalated to a Cisco ROS engineer if the sensors need tuning to filter out false positives or false negatives. For example, after the managed security service had already been operational, Scientific Atlanta requested a modification of the signature for Internet Relay Chat (IRC) so that it would trigger on all ports, not just IRC ports, and to capture all related activities. "This tuning enables us to determine if a user is actually chatting or if a Trojan is communicating with a botnet," says Stanton.

To view more information about threats reported in e-mail trouble tickets, authorized members of the Scientific Atlanta network security team can use the Cisco ROS online portal, which shows Whois or Domain Name Server (DNS) information, TCP dump traces, and pcap capture results. "The information available on the online portal helps us determine if the event is real or a false positive," says Stanton.

According to Stanton, a major benefit of the Cisco ROS managed security service is that e-mailed trouble tickets also include explanations and recommended steps for remediation. For example, Cisco ROS once reported that Scientific Atlanta had a compromised host that was being remotely controlled by an IRC bot and scanning other parts of the network. "The trouble ticket provided the IP address of the host, what it was connected to, and by what port," says Stanton. "This information enabled us to shut down the host and take it off the network until it was remediated." Similarly, in mid-2007, Scientific Atlanta experienced a worm outbreak. Rather than simply reporting the outbreak, Cisco ROS provided all source addresses triggering the signature so that the Scientific Atlanta network security team could launch an investigation to contain and eradicate the infection.

Business Results

Early Awareness of Security Events

Having a dedicated team of humans looking at network traffic for patterns gives Scientific Atlanta early awareness of potential security threats. "Cisco ROS is very responsive," says Stanton. "If a sensor goes down, for example, they notify us immediately." Scientific Atlanta also receives timely notification when sensors require a software update. "Cisco ROS manages our infrastructure more proactively than other managed security service providers I've worked with," Stanton says. "Earlier awareness of viruses, worms, and other threats helps protect our business."

Reduced False Positives

The information that Scientific Atlanta provided to Cisco ROS about asset values and operating systems has helped to reduce false alarms. "On occasion, we have detected a recurring probable attack and not known whether it was malicious or benign," says Mahon. "We described the incident to Scott Stanton, who knew from his in-depth understanding of his organization's network traffic that the incident was benign. He gave us permission to filter it out."

Visibility into Security Events and Performance

Scientific Atlanta can view activity on its sensors 24 hours a day using the online portal. "Other managed security services providers cannot provide read-only access, but only operating-system level access," says Stanton. "The

Cisco IPS 4200 platform supports a read-only operator account, which is a good thing for Scientific Atlanta as well as Cisco ROS. We can monitor the sensors, and Cisco ROS can retain control of the configuration."

Scientific Atlanta augments the sensor monitoring from Cisco ROS by using Cisco Security Monitoring, Analysis, and Response System (MARS) to correlate IPS information with firewall information. "Cisco Security MARS gives us a second set of eyes on availability, performance, and bandwidth, and an early indication that we're being overloaded," says Stanton. "Human scrutiny provides an extra layer of defense."

Easy Access to Experienced Staff

Cisco ROS assigns experienced technical staff to Scientific Atlanta and its other customers. "Scientific Atlanta has its own team and, in addition, everyone else in the SOC is familiar with the Scientific Atlantic network," says Haugen.

Lessons Learned

Scientific Atlanta and Cisco ROS offer the following suggestions for organizations considering outsourcing their IPS solution:

- At the beginning of the engagement, dedicate IT resources to work with Cisco ROS engineers to help them understand the network and the importance of its information assets to the business. "Scientific Atlanta recognized the importance of this step, which enabled us to assign accurate risk levels and filter out less important information," says Haugen.

PRODUCT LIST

Routing and Switching
- Cisco Catalyst 6504 Switches

Security and VPN
- Cisco IPS 4240 Sensors (perimeter)
- Cisco IPS 4255 Sensors (internal)
- Cisco Security MARS

- Respond promptly to requests for information from Cisco ROS. "The Scientific Atlanta team responds to our e-mail queries quickly and makes themselves available to answer questions, nearly always within the hour," says Mahon. "This helps us provide the best possible service."
- Be aware that Cisco ROS needs to understand the network in order to recommend the optimal placement for internal IPS sensors. Scientific Atlanta provided the necessary information during the pre-implementation meeting.
- Realize that the sensor is just a data-generation device, and that a complete solution also requires interpretation of the data. "The most important part of the Cisco ROS managed security service is converting raw sensor data into actionable information," says Stanton. "Trouble tickets explain the significance of sensor data and recommend corrective actions, which helps our security team be more effective while spending less time."

Next Steps

Scientific Atlanta is making plans for active prevention of malicious traffic. In the future, when Cisco ROS detects a security event and Scientific Atlanta confirms that it is a real threat, Cisco ROS will block traffic carrying the signature on Cisco routers and firewalls.

.

For More Information

For additional Cisco IT case studies on a variety of business solutions, visit Cisco on Cisco: Inside Cisco IT
www.cisco.com/go/ciscoit

Note

This publication describes how Cisco has benefited from the deployment of its own products. Many factors may have contributed to the results and benefits described; Cisco does not guarantee comparable results elsewhere.

CISCO PROVIDES THIS PUBLICATION AS IS WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some jurisdictions do not allow disclaimer of express or implied warranties, therefore this disclaimer may not apply to you.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA

C00-000000-00 08/07