# Outsourcing Intrusion Prevention System Management

## How Scientific Atlanta Outsourced IPS Management to Cisco Remote Operations Services

**A Cisco on Cisco Case Study: Inside Cisco IT**

Bob Scarbrough

# Overview

- Challenge

  Monitor and manage IPS sensors

- Solution

  Managed IPS Service from Cisco ROS

- Results

  Early awareness of security events

- Next Steps

  Active prevention by stopping traffic on routers and firewalls

# Challenge

## Monitor and Manage IPS Sensors

- Scientific Atlanta lacked IT staff to provide:
  - 24-hour monitoring of sensor data
  - Continually update signatures
  - Ongoing tuning to reduce false positives
- Selection criteria for a managed service provider were:
  - Commitment to communication
  - SLAs for response times
  - In-depth knowledge of Cisco IPS Sensors

# Solution

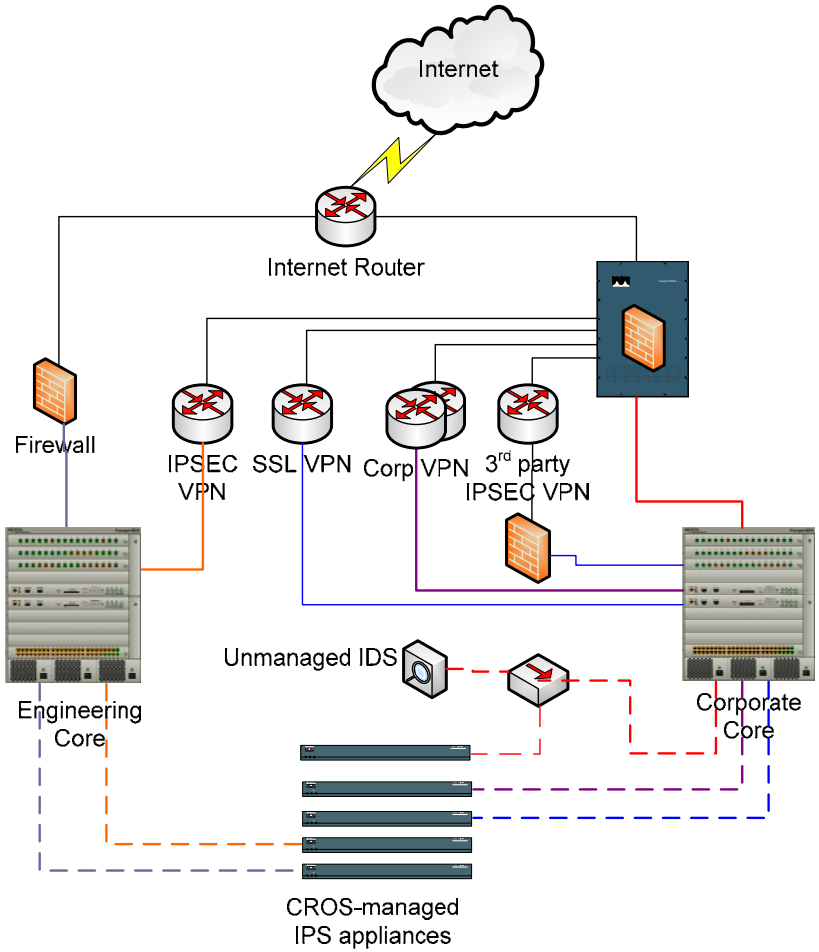
## Managed IPS Service from Cisco ROS

- Pre-implementation meeting
  - Types of attacks requiring notification
  - Places in the network to monitor
  - Asset values
  - Contact methods
  - Sensor model recommendations
- Two-step deployment
  - Perimeter sensors
  - Internal sensors
- 24-hour monitoring
- Notification by e-mail or phone
  - Scientific Atlanta can view more information about threats reported in e-mail trouble tickets using an online portal

# Solution

## Perimeter IPS Implementation

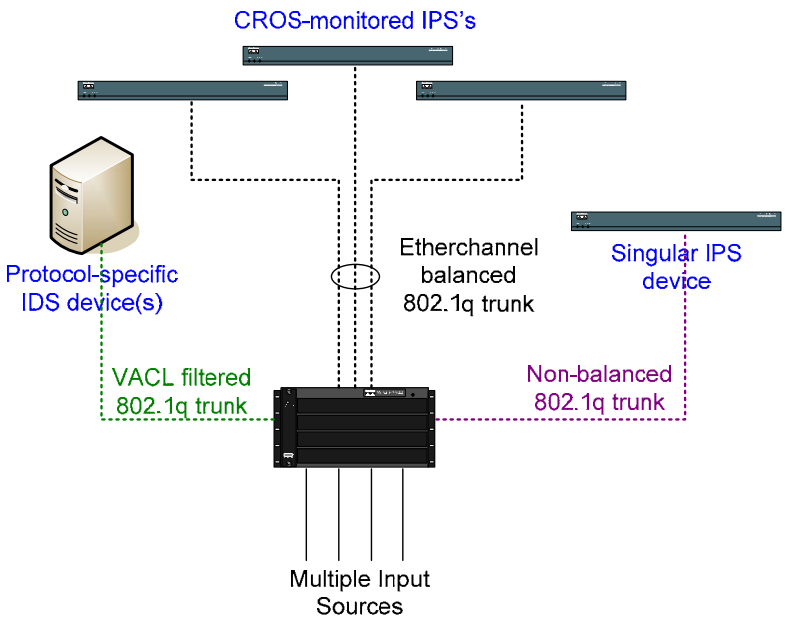



Dotted lines indicate SPAN or Monitor outputs to IPS appliances. In some cases, a single IPS will receive multiple SPAN inputs.

# Solution

## Internal IPS Implementation




6504 configuration uses RSPAN to mirror inputs to a target VLAN. This VLAN is trunked via 802.1q to the IPS devices. VACLs may be used to filter IP's or src/dst ports.

# Results

## Early Awareness of Security Events

- Reduced false positives
- Visibility into security events and performance, using online portal
- Easy access to experienced staff

“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.”

Scott Stanton
Information Security Architect
Scientific Atlanta, a Cisco Company

# Next Steps

## Active Prevention

- In the future, Cisco ROS will block malicious traffic on Cisco routers and firewalls
  - After Scientific Atlanta confirms the threat is real

To read the entire case study, or for additional Cisco IT case studies on a variety of business solutions, visit Cisco on Cisco: Inside Cisco IT
www.cisco.com/go/ciscoit


**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.**