Intrusion Detection Upgrade

How Cisco IT Upgraded Intrusion Detection to Improve Scalability and Performance

A Cisco on Cisco Case Study: Inside Cisco IT

Overview

- Challenge

  Firewalls are Cisco® IT's first line of network defense, guarding against most intrusions from outside the network at our Internet "demilitarized zone" (DMZ) areas and around our data centers. But firewalls make up only part of the Secure Architecture for E-Business (SAFE) security strategy for enterprise networks.

- Solution

  Cisco Intrusion Detection System (IDS) 4250 sensors

Overview (Contd.)

- Results

  Intrusion detection provides added security – InfoSec receives alerts when an intruder has gotten past the firewalls (or is coming from within the firewalls). This allows InfoSec to respond quickly to an intrusion, to limit damage, and to secure the perimeter against a similar attack.

- Next Steps

  Upgrade current Cisco IDS 4230 sensors with Cisco IDS 4250 sensors.

Challenge - Background

- The Cisco® internal Information Security (InfoSec) Group is responsible for planning and deploying defenses within Cisco to protect the resources within the Cisco internal network
- Cisco InfoSec and Cisco IT built a firewall-based security architecture to protect Cisco Internet access points and data centers

  Firewalls are like strong locks on doors and bars on windows, blocking the casual intruder from breaking in

Challenge - Intrusion Detection

- A good strategy also uses intrusion detection

  Like alarms and cameras at a secure building, an IDS alerts guards to the more determined and successful attacker, provides these guards with information about how the intruder entered and where they are, and supplies guards with the data necessary for determining how best to deal with the intruder in real time and how to prevent similar intrusions in the future.

Challenge - Cisco IDS 4230 Sensor

- In 2001 InfoSec deployed more than 35 Cisco® IDS 4230 sensors to perform critical monitoring of possible intrusions.

  These IDS network sensors are standalone appliances near (but not on) the data stream they protect.

- InfoSec deployed IDS sensors within the Internet DMZs by “sandwiching” the firewalls – placing sensors on both sides of the firewall, to view the traffic that comes into Cisco and the traffic that comes through the firewalls.

Challenge - Cisco IDS 4230 Sensor (Contd.)

- Each sensor is limited to scanning traffic only on the gateway nearest it, which required deploying them in pairs.

Challenge -
IDS 4230 Limitations

- Cisco® backbone network is mostly Gigabit Ethernet; Cisco IT also has four 155-Mbps OC-3s to handle Internet access in San Jose.

  Both required an Intrusion Detection network sensor that could handle more than 150–250 Mbps throughput.

- In 2001 no credible high-speed Intrusion Detection devices existed

Challenge – IDS 4230 Limitations (Contd.)

The InfoSec team selected the Cisco IDS 4230-FE, with a performance ceiling limited by its 100 Mbps Fast Ethernet interface.

InfoSec subdivided the traffic by putting one IDS 4230 on each gateway, limiting the sensor to scanning only half the traffic coming in through the gateway pair.

Subdividing the traffic brought the average throughput per IDS to below its 100-Mbps ceiling.

Challenge - Splitting the Traffic

- The workaround had several limitations
  - Made the IDS architecture more complex
  - Made the DMZ and data center gateway architectures more inflexible
  - Increased deployment and management costs
  - Limited the effectiveness of our IDS solution
- Splitting the traffic deprived the IDS of seeing the full traffic pattern.
  - This limitation produced a higher rate of false positive alerts (and negative responses) and the InfoSec team was unable to deploy some of the intrusion signatures that could use the full-duplex traffic pattern information.

Sample - IDS in Internet DMZ and Data Center

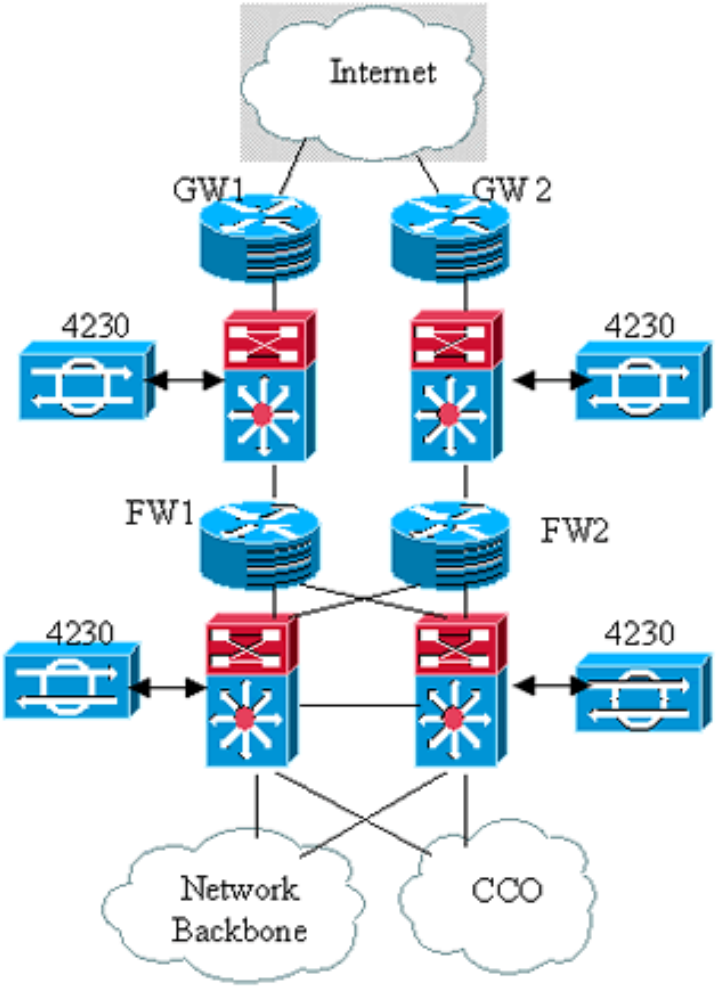

Figure 1: IDS in Internet DMZ

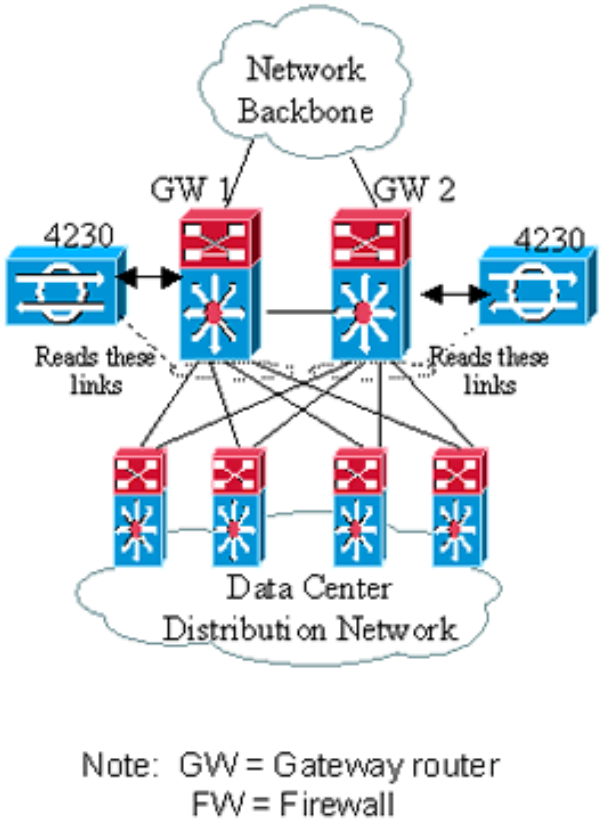

Figure 2: IDS in Data Center

Solution - Cisco IDS 4250 Sensors

- Starting in San Jose in the larger Internet DMZs, Cisco® InfoSec replaced Cisco IDS 4230s with IDS 4250s, which can support traffic up to 500 Mbps.

  The first Cisco IDS 4250 (in beta at the time) was installed in the San Jose DMZ in November 2002, replacing two Cisco IDS 4230s.

Results - Cisco IDS 4250 Deployment

- The Cisco® IDS 4250 has allowed InfoSec to remove the traffic sectioning and switch spanning associated with the smaller IDS sensors, simplifying the architecture and allowing the IDS sensor to “read” all network traffic for more comprehensive threat response.
- We were able to add duplex alert signatures to the IDS. We replaced two 4-rack-unit (RU) devices with a single RU device, and only had to use one span port.

Results - Cisco IDS 4250 Deployment (Contd.)

- Future deployments of the Cisco IDS 4250 with IDS Sensor Software Version 4.1 will allow Cisco IT to replace more IDS 4230s in data centers with a single appliance configured as multiple “virtual sensors”—again reducing the footprint in the data centers while decreasing management overhead.

Next Steps - 3-Step Upgrade

- Cisco® InfoSec is planning a 3-step upgrade to the current Intrusion Detection System
  1. Upgrade the remaining 35+ Cisco IDS 4230s in the Internet DMZs to Cisco IDS 4250s.
  2. Upgrade the Cisco IDS 4230s in the data centers to Cisco IDS 4250-XLs to use their gigabit performance to handle the Gigabit Ethernet gateway interfaces leading into the data centers.
  3. Migrate the Cisco IDS 4250s to Cisco IDS Sensor Software Version 4.1, the latest version.

IDS provides the next level of defense

- Cisco® intrusion protection is designed to efficiently protect data and information infrastructure. With the increased complexity of security threats, achieving efficient network intrusion security solutions is critical to maintaining a high level of protection.

Vigilant protection ensures business continuity and minimizes the effect of costly intrusions.

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.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

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.**