How Cisco IT Upgraded Intrusion Detection to Improve Scalability and Performance

Migration to Cisco IDS 4250 Sensor improves intrusion detection performance and manageability.

Cisco IT Case Study / Security and VPN / Intrusion Detection Upgrade: This case study describes Cisco IT's internal solution deployment of an Intrusion Detection System (IDS) within the Cisco global network, a leading-edge enterprise environment that is one of the largest and most complex in the world. Cisco customers can draw on Cisco IT's real-world experience in this area to help support similar enterprise needs.

The Cisco Information Security team deployed Cisco IDS 4230 Sensors – in 2001. This deployment proved valuable for Cisco, and taught us much about effective intrusion detection. However, the IDS 4230 sensors had performance and management limitations that are being overcome by our current migration to Cisco IDS 4250 and IDS 4250-XL sensors.

> "Migrating to Cisco IDS Sensors improved intrusion detection performance and manageability."
>
> **John Stewart, Vice President and Chief Security Officer, Cisco**

BACKGROUND

Value of IDS to Cisco Information Security and to Cisco IT

In the network security world, firewalls are like strong locks on doors and bars on windows, blocking the casual intruder from breaking in. But a good security 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. In an environment where security incidents are rising sharply and costing millions of dollars at a time, it makes sense to plan ahead and to build formidable defenses to reduce the effects of these attacks. The Cisco internal Information Security (Infosec) group is responsible for planning and deploying these defenses within Cisco, and they support both firewalls and an IDS to protect the resources within the Cisco internal network.

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 Cisco Secure Architecture for E-Business (SAFE) security strategy for enterprise networks. An IDS provides added security: Infosec deployed more than 35 Cisco IDS 4230 sensors worldwide in 2001, and receives alerts to let them know when an intruder has gotten past the firewalls (or is coming from within the firewalls), and to help capture data that can identify the IP address of the intruder, which ports are being used in the exploit, and the pattern of when they had access to some systems within Cisco. This allows Infosec to respond quickly to an intrusion, to limit damage, and to secure the perimeter against a similar attack in the future.

For example, in 2001 (the same year Cisco deployed intrusion detection sensors) there were two devastating attacks on servers worldwide: Code Red 1 and 2 (July 2001) and NIMDA (September 2001). Both times the Cisco IDS 4230 sensors noticed an unusually sharp rise in suspicious traffic within the first few minutes, and within an hour Infosec and IT engineers were taking immediate steps:

- Identifying the type of threat based on the large number of alerts, customizing an IDS “signature” based on the worm/virus activity, and updating the IDS sensor signature file.
- Temporarily disconnecting network access to large and vulnerable targets, especially Cisco laboratories with large concentrations of Microsoft Internet Information Servers (IIS); Cisco has more than 1200 laboratories worldwide.
- Temporarily blocking possible worm/virus traffic (port 80/tcp) to vulnerable remote access users (more than 35,000 users worldwide).
- Using network based application recognition (NBAR), a Cisco IOS® Software feature on gateway routers to block traffic identified as worm or virus related (Cisco is now using Cisco CSS 11500 Series Content Services switches to do this while avoiding load on gateway routers).
- Deploying new cache engine rules on outbound traffic (to the Internet) to avoid spreading worm/virus traffic to others, and adding new Cisco 500 Series cache engines to handle the additional load (but without blocking outbound port 80/tcp access, so business was handled normally).
- Alerting Cisco employees of the problem and of the temporary blocks put in place.
- Gathering infected server IDs from IDS and other sources, and temporarily partitioning hosts and networks to isolate infected servers
- Developing tools to clean infected servers.
- Supporting other Cisco networking groups in developing workarounds (for example, proxy servers for remote access support, opening critical business systems that were cleaned or certified as safe).
- Helping develop tools to identify affected or vulnerable hosts, and automatically pushing upgrades and patches to vulnerable code.

Without the several hours advance notice that the IDS provided Cisco, it is likely that many of the affected servers within Cisco would have been overwhelmed, business would have been far more seriously affected, and Cisco would have been the source of far more infection for other Internet-connected businesses and users.

In January 2003, when SQL Slammer alerts were being sent throughout the industry, Infosec responded by shutting down a little-used port on the firewalls that blocked SQL Slammer. Our IDS system was able to tell us that this response was entirely successful, and Cisco remained unscathed by the attack.

IDS Within Cisco IT

Cisco Infosec, working with Cisco IT networking groups, had built a firewall-based security architecture to protect our Internet access points and our data centers. In 2001 Infosec deployed more than 35 Cisco IDS 4230 sensors (precursors to the IDS 4235 sensors) to perform critical monitoring of possible intrusions that penetrate this firewall protection. These IDS network sensors are standalone appliances near (but not on) the data stream they protect, owned and managed by the Infosec team with support from the IT corporate and global network teams.

Infosec has located these IDS network sensors at internal Internet access locations worldwide, wherever Internet links connect to the Cisco network. Major Internet access sites are at San Jose, California (with 620 Mbps of Internet access); Research Triangle Park, North Carolina (465 Mbps Internet access); Amsterdam, Netherlands (180 Mbps Internet access); Tokyo, Japan (20 Mbps Internet access); and Sydney, Australia (10 Mbps Internet access); smaller and more recent Internet access locations are in Richardson TX, Chelmsford MA, Israel, Hong Kong, Singapore, and Bangalore India. In addition, there are IDS network sensors located at each of the five Cisco production data centers: San Jose buildings 12 and K, Research Triangle Park, Amsterdam, and Sydney. Infosec has deployed these Cisco IDS 4230 sensors within the Internet access networks by placing sensors on both sides of the firewall, to view both the traffic that comes into Cisco and the traffic that comes through the firewalls (see Figure 1). Traffic from the Internet in San Jose, for example, comes through a pair of gateway routers, and is read by a pair of Cisco IDS 4230 sensors. This traffic is filtered at a pair of firewalls and a second pair of IDS 4230 sensors then reads this filtered

traffic to determine what is getting through the firewalls. The IDS 4230 sensors are deployed in pairs at larger Internet access sites for performance reasons (see “Challenge” below). Smaller Internet access sites would require only a single IDS sensor at each point because the switch can span all traffic to the sensor.

Figure 1. IDS in Internet DMZ

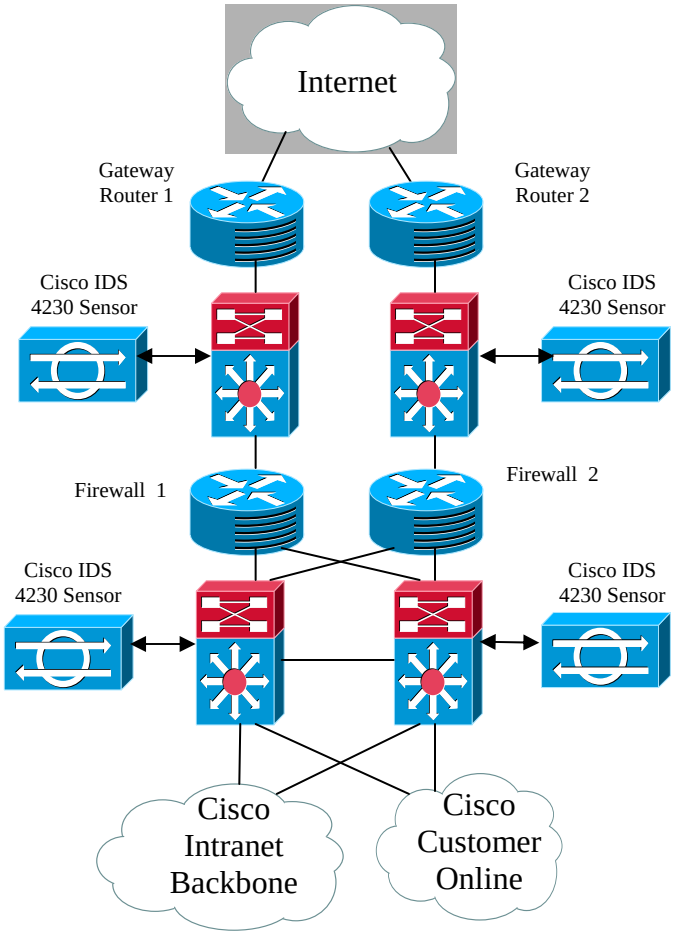
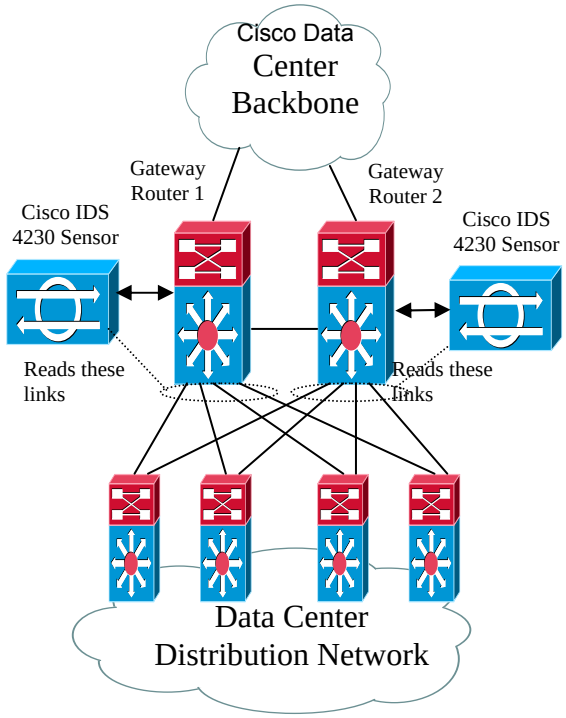


Figure 2. IDS in Data Center



In addition, Infosec has ringed the data centers with Cisco IDS 4230 sensors, installing one or more sensors outside every Cisco production data center gateway worldwide (see Figure 2). Each sensor is limited to scanning traffic only on the gateway router nearest it (which requires deploying them in pairs) because of performance issues with the IDS 4230 (see “Challenge” below). Again, smaller data centers would require only a single IDS 4230 because the switch can span all traffic to the sensor.

CHALLENGE

The Cisco network and data center backbones are composed of very high speed connections, mostly Gigabit Ethernet. Internet access is high speed, as well. Cisco IT has 4 155 Mbps OC-3s to handle Internet access in San Jose. Both the data centers and the Internet access points required an intrusion detection network sensor that could handle more than 150 to 250 Mbps throughput. However, in 2001 there were no credible high-speed intrusion detection devices, so the Infosec team selected the Cisco IDS 4230 Sensor, with a performance ceiling limited by its 100 Mbps Fast Ethernet interface.

Because of this performance limitation, Infosec initially considered subdividing the traffic coming into each of the Cisco IDS 4230 sensors by spanning portions of this traffic to a switch and allocating a separate IDS 4230 to each traffic subset. But even this awkward workaround had severe disadvantages, especially as it would have used one of the only two receive-span ports available on each gateway. Instead the Infosec team accepted the drawback of subdividing the traffic in a different way, by putting one IDS 4230 on each gateway, which limits the sensor to only scanning half the traffic coming in through the gateway pair. Although this does bring the average throughput per IDS down below its 100 Mbps ceiling, there are frequent spikes in traffic that simply cannot be read by the IDS. When traffic spikes beyond 100 Mbps, all information beyond the 100 Mbps limit is not read and no potential alerts from this traffic are captured.

This workaround had other limitations: using two sensors made the IDS architecture more complex, it made the DMZ and data center gateway architectures more inflexible, and it has increased our deployment and management costs. Worse, it limited the effectiveness of our IDS solution. In splitting the traffic and in allowing some of it (especially

during peak traffic conditions, which are occasionally associated with network attacks), we deprived the IDS of seeing the full traffic pattern. Not only did this limitation produce a higher rate of false positive alerts (and negative responses), but also the Infosec team was unable to deploy some of the intrusion signatures that could use the full duplex traffic pattern information.

Another part of the challenge was that the IDS 4230 came with little in the way of management tools. The Infosec team spent months developing tools to help automate many required management functions, including updating configurations and signature files, rebooting sensors, and more (see Appendix 1: Lessons Learned).

SOLUTION AND RESULTS

Cisco Infosec has begun replacing IDS 4230s with IDS 4250s, which can support traffic up to 500 Mbps, within the larger Internet DMZs. Infosec is starting in San Jose. The first IDS 4250 Sensor (in beta at the time) was installed in the San Jose DMZ in November 2002, replacing two IDS 4230s. This has allowed Infosec to remove the traffic sectionalization and switch spanning associated with those smaller IDS sensors, simplifying the architecture and allowing the IDS sensor to “read” all network traffic for the first time for more comprehensive threat response. We were able to add duplex alert signatures to the IDS. And we replaced two 4-rack unit devices with a single rack-unit device, and only had to use one span port instead of two. Future deployments of the IDS 4250 sensor with Cisco IDS Sensor Software Version 4.1 will allow Cisco IT to use these advantages, as well as replace larger numbers of IDS 4230 sensors in data centers with a single appliance configured as multiple “virtual sensors.” This again reduces the footprint in the data centers while decreasing management overhead costs.

NEXT STEPS

Cisco Infosec is planning to move ahead with a 3-step upgrade to their current ID S. The first step is upgrading the remainder of the 35+ Cisco IDS 4230 sensors in the Internet access points to IDS 4250 sensors. This follows the success of the upgrade in San Jose. The second step is to upgrade the IDS 4230s in the data centers to IDS 4250-XLs to use their Gigabit performance to handle the Gigabit Ethernet gateway interfaces leading into the data centers. Both these upgrades, when complete, will allow Infosec to eliminate all traffic sectionalization and switch spanning within the IDS. The third step will be to migrate these IDS 4250 sensors to the latest IDS Sensor Software, version 4.1, which promises greater ease of management and reduced false positives, issues which are critical to Infosec in the current deployment of IDS (see Appendix 1: Lessons Learned). The Infosec team is evaluating IDS Sensor Software Version 4.1 for this planned upgrade. The timeline for this effort will be determined by further human resource and budget review.

LESSONS LEARNED

The major lesson learned from building and using an Intrusion Detection System (IDS) is that an IDS is useless without a dedicated staff of network-knowledgeable engineers to manage the system, tune the signature sets, monitor the alerts every day for possible attacks, and make the call that an attack is taking place and respond quickly and appropriately. An alarm system is useless if no one responds to a real attack, or if the response is too slow or in the wrong direction.

Alert Collection System

Installing the IDS sensors is only a small part of the deployment. Infosec also installed several regional Unix (Solaris) local directors, servers connected to the IDS sensors in each region. These local directors connect to a pair of global directors at the Cisco headquarters site in San Jose, California. These local directors receive and store alerts from the IDS sensors (with alerts graded into six levels, from 0 to 5), and send the more urgent alerts (levels 3 to 5) to the global directors through a Cisco PIX® VPN link. We've installed an average of one local server for every 2 to 3 sensors, partly because of our regional security architecture (some remote sites like Hong Kong or Richardson, Texas have one Internet link and no data centers), and partly because during major crises like virus replications or denial-of-service attacks, the number of alerts from one sensor can overwhelm a single local director server. There is a pair of global directors in San Jose for this reason as well. One handles the majority of traffic and the other handles emergency loads from large-scale attacks. Infosec also uses these servers to replicate changes to the signature set.

Tuning the Signature Set

After the sensors and alert collection system are in place, the IDS sensors come with a set of 800+ default "signatures." These signatures are definitions of activity that suggest that an intrusion or attack is underway; for example, a sweep of open ports, repeated attempts to enter a restricted host, or attempts to ping and map network IP addresses). However, each network and user base is unique, and there are many legitimate business activities that will trigger these default signatures; for example, Cisco IT's internal Enterprise Management (EMAN) system (http://eman) pings large numbers of network equipment every 15 seconds, which looks like an attack. Infosec spent more than 3 weeks scanning the early alerts and refining the signature set (excluding alerts that relate to specific addresses, for example EMAN servers) to exclude normal business processes from the signature set. Based on this tuning they turned off about 50 of these default signatures for specific source or destination IP addresses.

The Infosec team continues to tune this signature set because the network continues to change and expand, new servers and LANs are added, and Infosec needs to make sure that the sensors include the new equipment in their traffic analysis. For some time the Infosec team would turn off tuning completely once per quarter, analyze the larger set of alerts that were collected by the IDS, and retune the system to make sure they weren't missing something that had changed from an earlier quarter. They would do this over the course of a month or more (tuning the IDS signature set at one site the first week, at another site the second week, and so on.) The Infosec team also adds signatures based on attacks that Cisco has experienced. Based on their experience, Infosec provided the VSEC Business Unit with more than 30 new signatures, which have been included in the product default signature set.

Reducing False Positives

Even after this initial tuning is done, the global IDS system will still generate numerous alerts—too many for anyone but a large dedicated staff of experts to handle. The Cisco IDS system is currently generating between 1000 and 3000 alerts per day (more than 100 events per hour) and this is considered to be a low figure by the rest of the industry. (During the peak of NIMDA virus attacks, however, we were getting about 1 million events per hour.) Because the alerts list the source IP, destination IP, and activity, this long list of alerts requires review by someone very familiar not only with the IP addresses of the relevant network entities, but also familiar with the normal business use on the network.

Infosec has developed scripts that transfer these alerts into an Oracle database, and then take a baseline average of normal activity on the network and compare the number of specific alerts to that baseline. Whenever the number of alerts registers as unusually high, those alerts are flagged for operator review. This reduces the Infosec burden to a list of about five issues per day to review. Each issue can take a few minutes to an hour to track down and resolve. The Infosec staff includes three people with this responsibility – in addition to working full time on other security projects.

Responding to Attacks

The IDS has flagged real attacks to the Infosec group. This allows them to do a postmortem on how the attacker got into the network (or where the internal attack originated), and shut down that entry point into the network. The IDS sensors do have the capability to break and reset connections that trigger alerts thereby blocking attackers, but the Infosec team points out that because almost all these connections are legitimate business events, they have not made use of this automated break/reset feature (although when an attack is determined to be legitimate, the Infosec team breaks connections, closes ports, adds new IP addresses to firewall blocks, and so on). The information gained from this analysis about the nature of the attack can provide valuable information about how best to defend against it and how to avoid such an attack in the future.

In addition, post-mortem analysis can sometimes disclose the IP address of the attacker, although frequently attackers will use DHCP or NAT addresses, which are hard to associate with the server used in the attack.

Managing the IDS Solution

Infosec spent 6 months studying the IDS 4230 management interfaces and writing more than 20 custom scripts to help them manage and monitor the sensors. Most customers use Cisco Secure Policy Manager; this product, designed to support mostly the IDS and PIX products, required different interfaces for different pieces of equipment, and at the time did not meet their needs. IDS Sensor Software Version 4.1 supports SSL and XML interfaces, which will make this sort of secure management and interface customization much easier and may influence third-party vendors to provide good management tools.

Some of the Infosec scripts use trusted SSH keys to send signature file updates out from the global director to the regional local directors and then out to the remote sensors. Others automate upgrades and other management functions.

Severity of Security Issues

CERT

The CERT Coordination Center (CERT/CC) research center funded by the U.S. government, found more than 82,000 security incidents reported in 2002, and the number of incidents appears to almost double every year.

http://www.cert.org/stats/cert_stats.html

FOR MORE INFORMATION

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

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.
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.**