



Network-Based Intrusion Prevention System (IPS)

Cisco Protects Data Center Assets



A Cisco on Cisco Case Study: Inside Cisco IT

Overview

- Challenge

 - Protect data center assets

- Solution

 - Deploy network-based Intrusion Prevention System (IPS)

 - Augment existing perimeter-based IPS

- Results

 - Early detection and mitigation of data center threats

Challenge

Protect Data Center Assets

- Monitor Cisco network for threats
 - Insider threat, unauthorized access to data center assets, policy violations, botnets, more
 - Malicious activity can originate outside or inside the company
- Perimeter-based IPS detects threats traveling across the network perimeter
 - Deployed in the Cisco DMZ and at service provider points of presence
- But perimeter-based IPS does not provide visibility into events **inside** Cisco data centers
 - And that is where the company's most valuable assets reside

“In 2002, a typical threat involved 1000 computers launching a concerted attack on one server. Today, a larger concern is preventing a hacker from quietly gaining access to our data.”

Member of the CSIRT Team
Cisco

Solution

Network-Based IPS Deployment

- CSIRT deployed IPS sensors in Cisco data centers, engineering server rooms, and offshore development centers

Augmented perimeter-based IPS

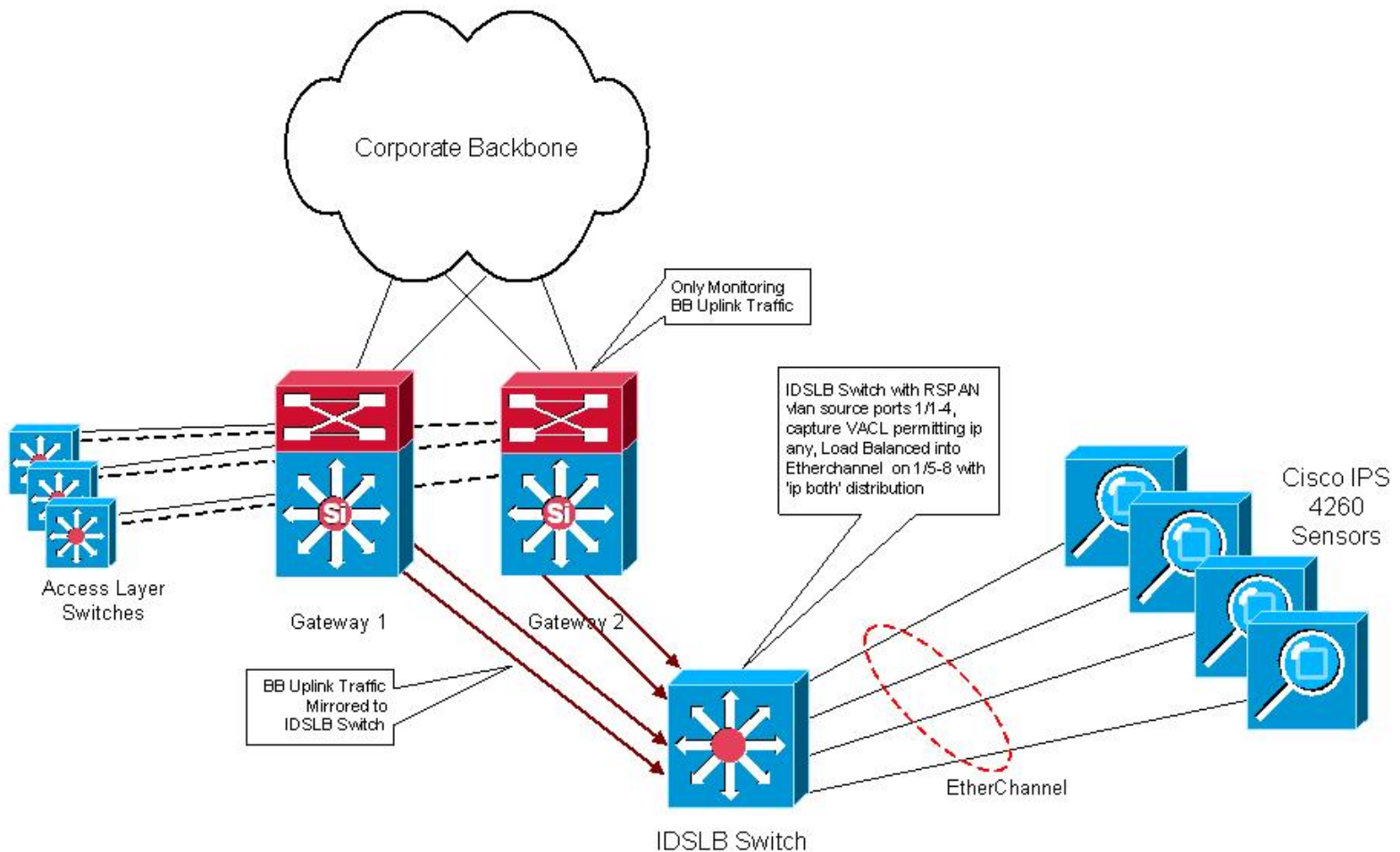
- Solution involves monitoring and analysis, investigation, tuning and custom signatures, and deployment

Tuning reduces false positives while not generating false negatives

CSIRT continually develops custom signatures for threats specific to the Cisco network

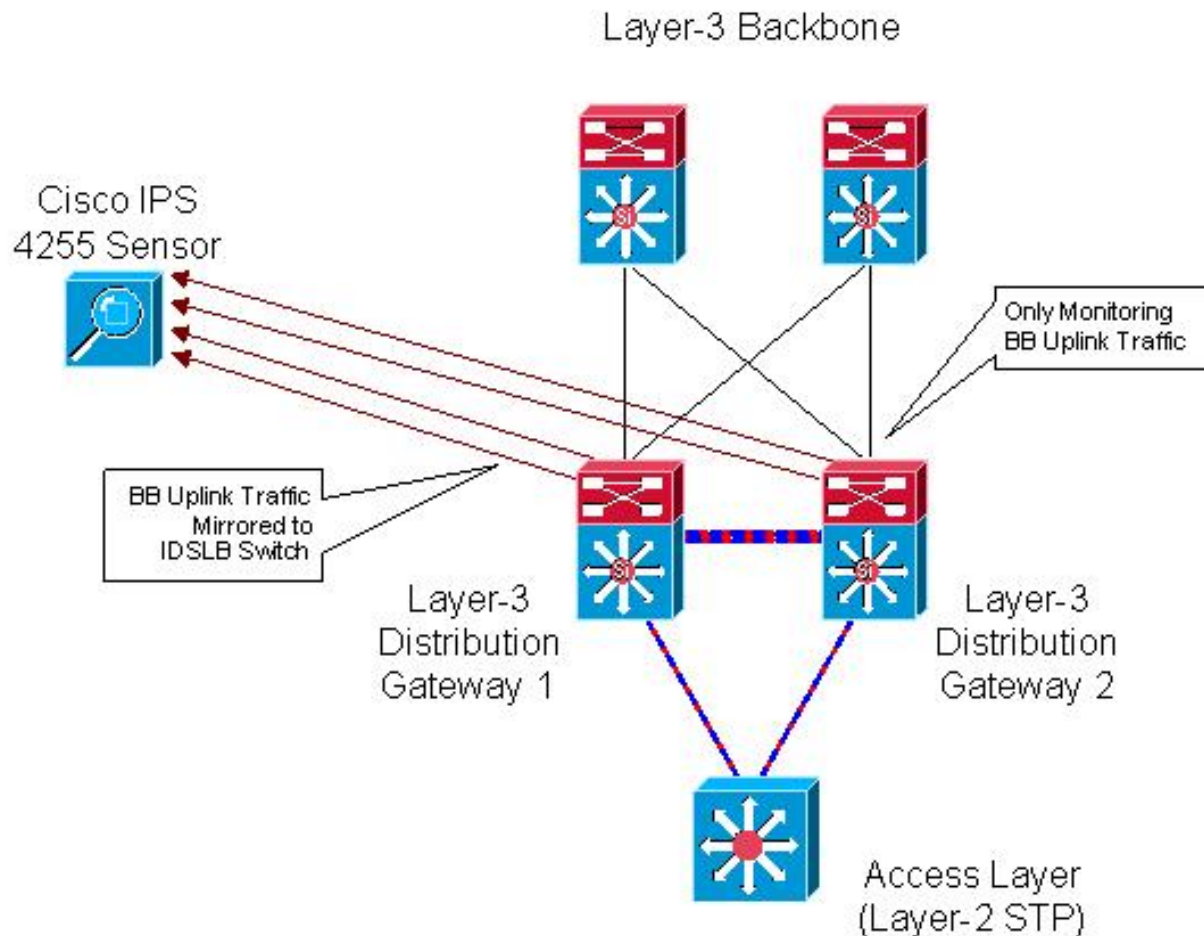
Solution

Design for Large Data Centers: >600Mbps Bandwidth



Solution

Design for Small Data Centers: <600 Mbps Bandwidth



Results

Early Detection and Mitigation of Data Center Threats

- Prevention of data loss or service interruption
- Rinbot virus was detected on day zero
 - Cisco CSIRT deployed a custom signature on the IPS that identified affected lab systems, which were then remediated
- Every week between March and June 2007, CSIRT identified and mitigated ten new botnet command-and-control servers

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



CISCO



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 (USA) Pte. Ltd.
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.

©2007 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0710R)