Cisco IT@Work Case Study:
Firewall Services Module (FWSM)

Cisco Information Technology

January 10, 2005

Overview

- **Challenge**

  Traditional stateless ACL firewalls bear significant weaknesses.

- **Solution**

  Migration to a stateful inspection firewall

  Migration: a three-stage process

- **Results**

  Dramatic increase in security of Network

  Dramatic increase in performance

- **Lessons learned**
- **Next Steps**

Challenge: Traditional stateless ACL firewalls bear significant weaknesses

- **Cisco needs to connect its intranets to the public Internet, without exposing the company to attacks.**

  The rising volume of denial of service (DoS) attacks and other threats has spurred organizations to investigate advanced firewall technology. The basic defense is a perimeter. In its best form the perimeter defense is a firewall.

- **People who design attacks mask their malicious traffic as legitimate traffic.**

  Non-stateful-inspection firewalls cannot accurately determine whether traffic is part of a legitimate session.

- **Traditional static firewalls remain vulnerable.**

  Non-stateful-inspection firewall routers with ACLs keep a large number of ports open, thus increasing vulnerability to attacks.

Solution: Migration to a stateful inspection firewall

- **Migration to FWSM: a stateful inspection firewalls solution.**

  FWSM was deployed at all Cisco sites for better security, manageability, and performance

- **FWSM allows the firewall to keep large numbers of ports closed.**

  FWSM keeps track of each application session, and dynamically adjusts the ports to be kept open based on the ports that are currently in use by legitimate application sessions.

- **Easy integration into the existing production network.**

  No complex design and operations changes were required.

Solution: A three-stage migration process

- **Preparation:**

  Conversion of ACLs from Cisco IOS® to FWSM and Cisco PIX formats. Took 8 hours per site, by 1 person. Plus 3 reviewers over each ACL

  Conversion of wildcard masks into appropriate subnet masks.

  Device configuration review and security audits for FWSM units.

- **Testing:**

  Creation of exact replica of Cisco production network, including all routers and switches surrounding the FWSM.

  Comprehensive testing included management, security, DoS attacks and failover. Main focus on Layer 2 transparency.

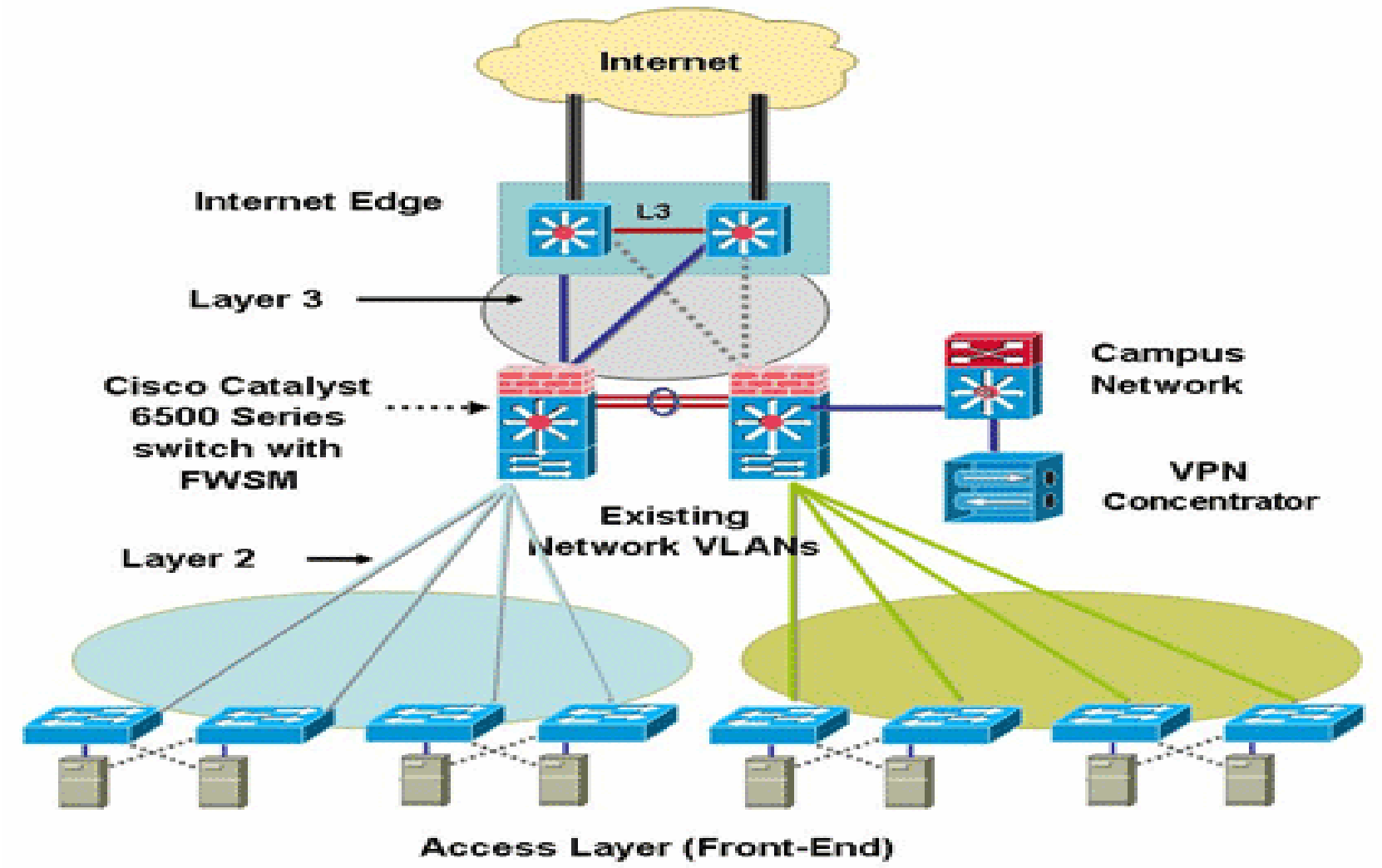
- **Deployment:**

  Preparation of network by converting point-to-point links to a bridged network

  Install and configuration of FWSMs

  Launch of FWSM security features

Solution: Cisco FWSM - Connecting the Internet edge to the existing topology



Results: Dramatic increase in security of Network

- **Greater security**
  - Mitigation of DoS attacks
  - Fewer holes in firewall
  - Reduction of network visibility from the outside
- **High availability**
  - Redundant deployment, with stateful failover, for an uninterrupted user experience
- **Easy integration thanks to Layer 2 transparency**

Results: Dramatic increase in performance

- **Ability to perform sophisticated traffic analysis**

  Cisco Catalyst 6500 and Catalyst 7600 accommodate also NAM-2. Combining NAM-2 and FWSM in the same switch enables traffic analysis both before and after firewall rules have been applied to inbound and outbound traffic.

- **High Performance**

  FWSM configuration in transparent mode provides a high performance, stateful inspection firewall that increases security posture without changing network infrastructure or topology.

Lessons learned

- **Careful planning and phased implementation**
- **Permanent communication with the application owners**
- **Activation of syslogs has little impact on CPU utilization.**

Next Steps

- **Definition of new policy changes to improve productivity**
  - **Allow outside voice and VideoConferencing through the firewall**
- **Object grouping to improve manageability**
  - **Decrease of ACLs size**
- **Introduction of FWSM's multiple-context feature into Cisco data center environment**
  - **Provide stateful inspection firewall capabilities for both inter- and intra-data center traffic**
  - **Virtualization feature will allow one physical FW to act like multiple virtual FWs**

For additional Cisco IT Case Studies on a variety of business solutions,
go to Cisco IT @ Work
www.cisco.com/go/ciscoitatwork

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.