Securing a Diverse, Global Network

Cisco IT Insights

Introduction

The Cisco network, which is one of the largest and most complex in the world, must meet varied requirements for network security. Among these requirements are scalability to serve hundreds of thousands of users, as well as flexibility to accommodate country-specific security requirements and the differing security needs of certain applications and company organizations. To meet these requirements, Cisco IT uses Cisco ASA 5585-X Adaptive Security Appliances in both firewall and VPN concentrator deployments.

Challenge

The Cisco network must serve the company's operations in 400 locations in 90 countries, with a variety of facility types including offices, data centers and server rooms, labs, and co-location facilities. This variety of locations and facilities generates a comparable variety in security requirements, including:

- Protecting the Cisco network end-to-end from the Internet edge to the data center core while addressing specific security requirements as well as industry and government regulations.
- Providing secure remote access to the corporate network for Cisco employees and contractors, as well as users on the Cisco extranet.
- Supporting Cisco development labs and engineering organizations, which often need protected segmentation with the ability to manage their own firewalls when operating in the network demilitarized zone (DMZ).

  Cisco IT also wanted a security solution that would be scalable as the network continues to grow and could be implemented as a corporate standard across all network areas.

Solution

Cisco IT has deployed the Cisco ASA 5585-X Adaptive Security Appliance as its frontline network security solution. Cisco chose this appliance instead of using access control lists (ACLs) on the network routers for three primary reasons:

- Tighter control over network access policies. The Cisco ASA 5585-X appliances allow network managers to create dynamic rules, which are particularly important for securing voice and other complex network protocols.
- The ability to stop traffic spoofing. Router access lists are limited in their ability to address spoofing traffic. In contrast, the Cisco ASA 5585-X stateful firewall can recognize and stop spoofing traffic before it enters the network.
- Definitions for other malicious traffic types. Network managers can create firewall definitions for malicious traffic that targets certain applications or network uses, e.g., payment card data.

Cisco ASA 5585-X appliances are deployed in multiple places within the Cisco network, including:

- As the corporate firewall at the Internet edge, deployed in redundant pairs for stateful failover.
- As VPN termination devices, at Cisco IT's 13 Internet peering points worldwide, for allowing encrypted remote access by software VPN clients such as Cisco AnyConnect. The Cisco ASA 5585-X appliances offer the capacity to handle the high volume and dynamic nature of remote connections to the Cisco network.
- For Cisco's extranet VPN, the appliances give users differentiated network access across various tunnels.
- For special firewall deployments, such as the deployment of parallel Cisco ASA 5585-X appliances (using stateful failover mode) to protect data centers in the network DMZ and the company's public website, Cisco.com. Additional special deployments are made to meet the requirements of regulated environments. "The Cisco ASA appliances are good when you need to establish a clear network boundary," says Gerry Lian, a Cisco IT design engineer.
- As a network address translation (NAT) device in the network DMZ.
- For protecting highly sensitive environments, such as the public key infrastructure (PKI) used to track authenticity certificates as devices progress through the manufacturing process.

"Although it's possible to do some of these things with a separate platform, the Cisco ASA 5585-X appliance does a lot and does it well," says Tom Woodard, information security architect, Cisco Information Security.

Results

Cisco IT gains the following benefits from its deployment of the Cisco ASA 5585-X appliances:

- Stateful failover when the firewalls are deployed as a redundant pair, which improves network uptime while maintaining transparent user access.
- Deployment flexibility to meet the needs of different network areas and connectivity scenarios, but with integrated security functionality that simplifies Cisco ASA 5585-X implementation, operation, and maintenance.
- Greater performance, efficiency, and scalability through hardware-based encryption when the appliance is used as a VPN termination device and for processing lookups when used as a firewall.

"Operationally, the Cisco ASA 5585-X appliance is simpler for Cisco IT to manage and troubleshoot because we need to look at only one device, compared to multiple devices that handle separate security and access functions," says Rich West, information security architect, Cisco Information Security.

For More Information

For more information about the Cisco ASA 5585-X, visit: www.cisco.com/go/asa

To read 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.
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.**