IPS Deployments in Enterprise Data Centers

Introduction

Enterprises consolidate all their applications and servers into data centers. The services hosted by the data center are crucial; the data center offers key functions for day-to-day business and e-commerce transactions. The concentration of services, confidential information, and resources make these centralized locations attractive for exploit. Attacks against these server farms can result in losses in business and productivity, which enterprises cannot afford.

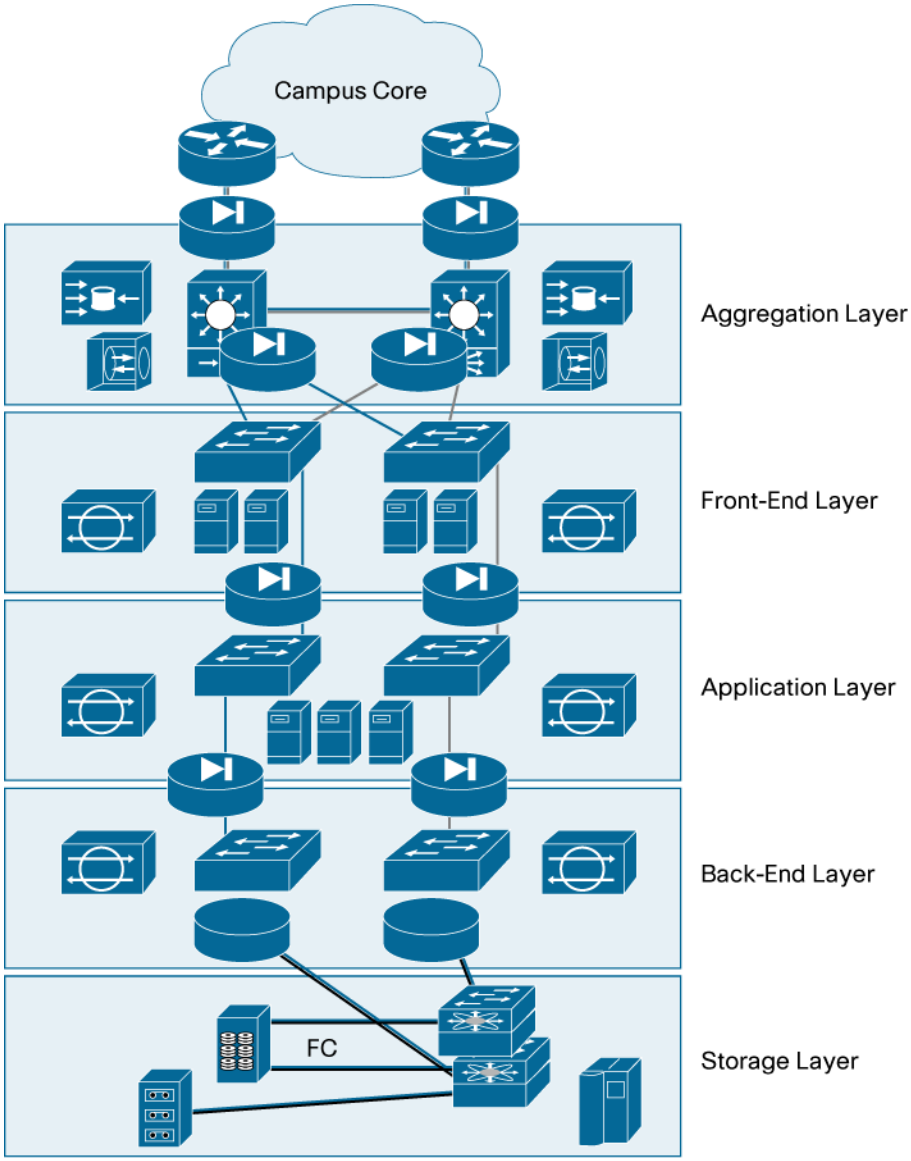
Overview

Business applications in the data center are typically built around a multitiered architecture. Separating functions on different servers (and on different layers) allows for better performance, better scalability, and a more secure design. The front-end layer typically hosts services that an external client can access from outside the campus. The application and back-end layers run Web and database services for the enterprise. The aggregation layer typically offers networking services such as load balancing and SSL offloading.

Connectivity between these different layers is provided through access switches and routers (Figure 1). The workflow and connectivity could be between servers, between client and server, or even between the server and its storage elements. All these influence the choice of security measures and products.

All contents are Copyright © 1992–2007 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Figure 1. Typical multitiered architecture



Several security services are available to protect the content within a data center and to control and secure the access to the business applications in a server farm. A secure design can help ensure that attacks are not carried out by external client machines from over the Internet, or by internal server machines that become infected and try and become agents for other attacks.

Access control lists, firewalls, and host-based intrusion prevention systems (IPSs) should be implemented in combination with NetFlow detection systems to mitigate vulnerabilities and assure resilience against external and internal threats.

Cisco IPS 4270 Sensor Appliance

The Cisco IPS 4270 Sensor is at the high end of the Cisco IPS 4200 Series of sensor appliances. Using Cisco IPS Sensor Software, the Cisco IPS 4270 can accurately detect and stop malicious traffic, providing enterprise data centers the business continuity they need.

All contents are Copyright © 1992–2007 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

The Cisco IPS 4270:

- Delivers performance of up to 4 Gbps that is best-suited for the high-speed requirements of today's data centers.
- Supports a large number of copper and fiber interfaces; with this flexibility, it can be used in a number of deployments.
- Uses logical VLAN interfaces along with the option of either provisioning inline or promiscuous together with support for virtualization, giving you the design flexibility to address different deployment requirements.
- Supports mechanisms such as EtherChannel load-balancing, enabling multiple Cisco IPS 4270 devices to be grouped and function as a cluster. This adds resiliency and allows for higher throughput. As many as eight Cisco IPS 4270 Sensors can be grouped as such.
- Provides built-in resiliency with the inclusion of two hot-swappable power supplies; features such as bypass mechanisms (both hardware and software) help ensure that traffic continues to flow in case of failure in the power supply, interfaces, or sensor application engines.

The Cisco IPS 4270 Sensor analyzes data by either inserting itself into the flow of traffic (configured via inline or VLAN pairing) or by way of SPAN or VACL redirect mechanisms (IDS or promiscuous mode). The Cisco IPS 4270 processes the packet against an extensive internal database of signatures for known attacks. Upon identifying a threat, the Cisco IPS 4270 can log, alarm, shun, or drop the offending connection. A single Cisco IPS 4270 performs at 4 Gbps in media-rich environments such as file transfers and video, and up to 2 Gbps in transactional environments where there are numerous connections.

For larger security deployments, the Cisco Security Management Suite unifies security configuration and policy management for Cisco IPSs, firewalls, and VPNs. The Cisco Security Monitoring, Analysis, and Response System (MARS) unifies security incident management, with an end-to-end network view, extensive correlation and analysis tools, and more than 150 ready-to-use customizable reports.

Each Cisco IPS 4270 Sensor comes equipped with integrated command-line and Web management as well as intelligent correlation. Policies can be defined and events can be managed immediately upon setting up the sensor.

IPS Deployments in the Data Center

The Cisco IPS 4270 Sensor is ideal for data center deployments, with its multigigabit IDS performance and its capability to support up to 16 physical ports and 8000 VLANs. These sensors can identify real-time malicious attacks based on protocol or traffic anomalies and can detect any exploits from a signature base of well-known vulnerabilities.

The deployment and placement of intrusion prevention techniques in the data center are influenced by several factors. In a multitiered data center environment, servers for these different tiers may be connected to different, physically separate access switches. In a more consolidated infrastructure, Web, application, and database servers may all reside on the same access switch. VLANs provide segmentation between these servers. Segmentation of the design using different routers, switches, firewalls, or VLANs allows traffic to be split across multiple IPS sensors.

All contents are Copyright © 1992–2007 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

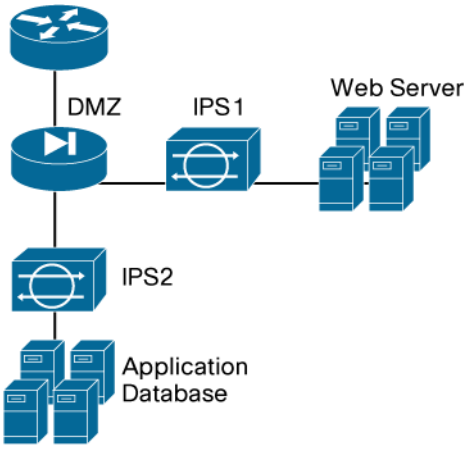
Cisco IPS Sensor Software 5.0 added the capability of bridging interfaces (VLAN pairing came in Version 5.1) through the IPS sensor. This inline capability enhanced the sensor's ability to process packets and detect and mitigate an attack before it reached its destination. From a data center perspective, it also allowed for easier deployments, where a sensor could be added to a subnet without changing any of the network parameters. This mode of deployment is referred to as IPS mode. In IDS mode or promiscuous mode, however, traffic mirroring techniques such as Switched Port Analyzer (SPAN), Remote SPAN (RSPAN), or virtual ACL (VACL) capture are used to redirect to ports that connect to the IPS sensor without modifying the packet contents. Both methods are useful for hybrid environments that require both promiscuous IDS and inline IPS.

Deployment of IPS

As discussed earlier, data center deployments should be designed to protect against external Internet attacks as well as attacks from internal client machines or compromised servers. Also discussed were the benefits of segmentation in the server farm, where either Layer 2 domains or VLANs are used to separate the server machines that provide the different functions of applications, services, or databases. Cisco IPS 4270 Sensors can be deployed in these scenarios.

Figure 2 shows a multitier design where a virtual firewall is used to separate the Web and application servers. Different mechanisms could have been used to separate these tiers, such as a Layer 3 mechanism with routers and firewalls, or Layer 2 techniques such as VLAN segregation. Firewalls provide the highest security among these methods as they only open specific ports that the applications uses.

Figure 2. A multitier design

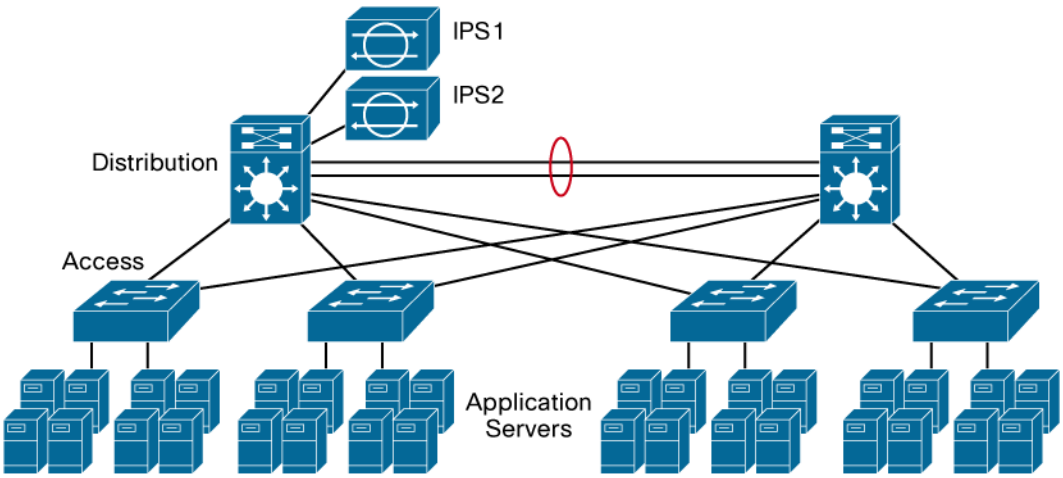


In Figure 2, IPS1 monitors external client-to-Web traffic and IPS2 monitors Web and application server-to-database traffic. When an attack compromises the Web/application tier, IPS1 can trigger the event, whereas IPS2 could drop offending packets and report alarms when the compromised Web/server attacks the database.

Figure 3 shows a redundant data center topology with access and distribution layers. The design has a pair of Cisco Catalyst® 6500 Series switches at the distribution layer and application servers connected to redundant Layer 2 access switches. Segmentation between these servers is ensured with the use of either VLANs or routers and switches. Both IPS devices are attached to trunk ports, and the VLANs they need to inspect are bridged through the IPS devices. The user must establish policies on what traffic IPS1 and IPS2 need to monitor. For example, IPS1 could monitor HTTP traffic and IPS2 could monitor DNS traffic.

All contents are Copyright © 1992–2007 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Figure 3. A redundant data center topology

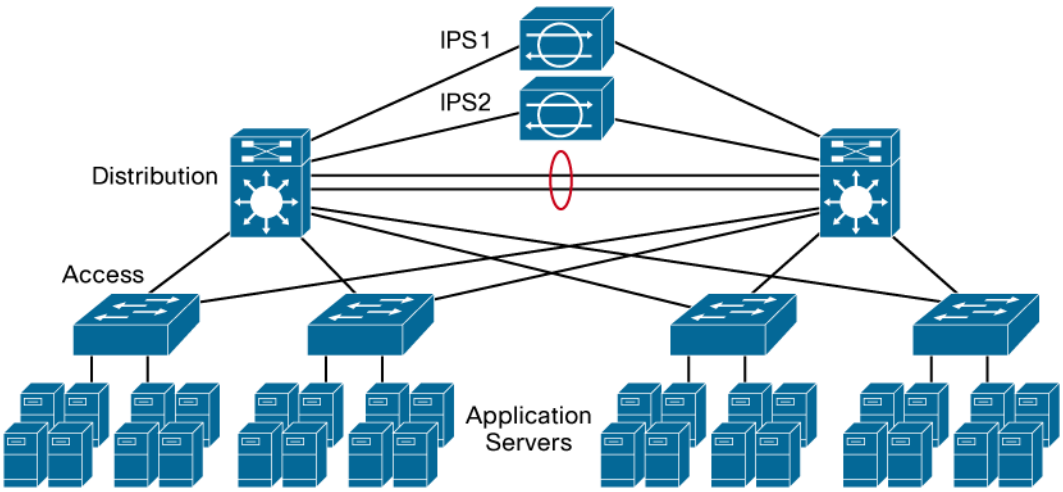


In data centers like these, redundant routers, switches, and even power supplies help ensure business continuity during an outbreak. The IPS appliances, however, do not support stateful failover. IPS devices maintain state with traffic flows and may drop traffic from an asymmetrical traffic flow. It is therefore important to factor this into the design.

Some other factors to consider in the design are whether the IPS appliances are attached to Layer 2 access devices or to Layer 3 aggregation devices. Techniques to ensure that traffic does get redirected to the primary aggregation switch that the IPS sensors are attached to are spanning tree and RSPAN with VACL capture.

Figure 4 shows another design option, where the IPS devices are attached to each aggregation switch and have mirror configurations and capture flows that take asymmetric paths. An EtherChannel that carries VLANS associated with the IPS devices helps ensure that traffic maintains session stickiness to get to the right IPS device.

Figure 4. Asymmetric path deployment option



All contents are Copyright © 1992–2007 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.

Conclusion

IPSs are critical to the enterprise data center. The Cisco IPS 4270 Sensor provides high performance and deployment flexibility to suit data center environments. For more information, review the IPS Sensor Software 6.0 Design Guide, and the IPS Product information . .

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.**

©2007 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and the Cisco Square Bridge logo 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, 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. (0708R)

Printed in USA C17-436978-00 10/07

All contents are Copyright © 1992–2007 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.