Securing the Data Center

Overview

The data center is undergoing rapid transformation. This change is being inspired by many factors, including consolidation, virtualization, and “green” initiatives; the need to provide greater access to customers, employees, and partners; the proliferation of low-cost endpoints; the demand for rich, interactive media experiences; and the mass adoption of Internet-deployed applications. “Last-generation” data center designs are not sufficient to meet the current set of needs and technologies.

Securing the new data center is a significant challenge. Numerous applications are being deployed without proper testing or security safeguards in order to meet rapidly escalating business, performance, and scalability requirements. Telemetry critical to meeting auditing, compliance, and forensics requirements is also being neglected.

The Cisco® Self-Defending Network enables companies to create a trusted data center infrastructure based on a systems approach, using best-of-breed security solutions that protect against business disruption and enable your company to evolve and operate effectively while maintaining a secure, compliant environment.

Today’s Self-Defending Network provides expanded capabilities that enable endpoint, network, content, and application security services to work together to deliver solutions for the security challenges that are unique to the data center. IT groups can more rapidly deploy required data center technologies without compromising on the ability to identify and respond to evolving threats, enforce business policies, and protect critical assets. At the same time, these solutions help decrease network complexity, ease the IT administrative burden, and lower the total cost of ownership. Organizations can more effectively and efficiently address top-of-mind business concerns, including data loss prevention, corporate and regulatory compliance mandates, and malware and threat prevention.

Challenges

Data centers have become a primary target for theft and attack. Many data centers, especially those assembled quickly during the economic boom of the 1990s, were rarely built with an emphasis on security. The resulting application and storage “islands” are often vulnerable to attack and compromise. Internet worms and viruses proliferate in part because of inconsistent, inadequate security technologies and procedures in data centers worldwide.

In support of management goals to protect, optimize, and grow their business, many IT groups are consolidating data center resources, such as servers, storage, networks, and applications. IT and network managers must consider how these changes affect both security posture and application resilience. In the past, managers relied upon physical application isolation or perimeter defense for security. But as data centers evolve, these perimeters are disappearing. Applications need to access information from multiple sources and locations, and end users, customers, and partners are given greater access to the data and information stored in an organization’s data centers.

Threats from inside the enterprise can be even more damaging. When detailed knowledge of an organization is exploited, either inadvertently or deliberately, serious financial damage can result. Hackers can include employees, temporary workers, and consultants. To protect applications, data center managers must use technologies that limit user access to only those resources they need to do their job, and deploy technologies to prevent sensitive data loss prevention.

Vulnerabilities and threats can prevent users from accessing mission-critical applications, directly disrupt application operation, or compromise confidential and valuable information. Security and network managers must collaborate to understand the particular vulnerabilities and threats to data center resources so they can develop a robust network security architecture.

Data center security issues can include the following:

- Attacks on mission-critical applications, application servers, databases, database servers, and storage resources through buffer overflows, malicious worms, viruses, and administrative access breaches.
- Exploiting vulnerabilities in legacy and Web 2.0 applications for identity theft, data theft, application disruption, and fraud.
- Theft or accidental leakage of sensitive information from file servers, content management solutions, databases, and other data repositories.
- Meeting regulatory compliances related to protection of data in motion and data at rest.
- Distributed denial of service (DDoS) and SYN flood attacks.

Solution: A Defense-in-Depth Data Center Security Strategy

Cisco data center security strategies take into account that security is a continuous process that should be integrated with and complement data center operations, communicated to the user community, and incorporated into the organization's culture and way of doing business. Successful security strategies employ the concept of "defense in depth," using multiple layers and complementary functions to mitigate threats throughout the data center.

Security Policy

Any security strategy begins with a security policy that aligns business needs with security goals and defines how to implement them through processes and technologies. A first step must be to ensure that any existing security policy is updated to address the particular requirements of the data center: its specific application requirements, access permissions, protection of sensitive information, and compliance with regulatory requirements.

An effective security policy results from collaboration among all stakeholders in the data center, including various management teams, the executive board, and user groups throughout the organization. The policy determines security design, management processes, and technologies that enable policy implementation and enforcement. A security policy is not static; it should be refined and adjusted regularly, especially as the security posture of the data center changes.

Start with the Network

The network is the ideal place to begin to secure your data center environment. Every device you are concerned about is connected to it, and every application and bit of data you need to secure traverses it. The network provides a solid first layer of defense, complementing operating system and application-level security. The network creates a secure environment not only at the perimeter, but also in security zones throughout the data center. Separating the network into virtual

compartments allows security managers to consolidate resources in a cost-effective manner and control user access to each application.

The Cisco Enterprise Data Center Architecture achieves optimal end-to-end security, performance, and manageability by integrating security directly into the network infrastructure. It uses the advanced integrated security capabilities of the Cisco Catalyst® switching and Cisco MDS intelligent storage networking platforms. Integrated security software and service modules for the Cisco Catalyst 6500 Series offer firewall, intrusion detection, anomaly detection, and intelligent service acceleration services at the higher performance levels required for bandwidth-intensive data center environments. In the storage network, the Cisco MDS 9000 Series Multilayer Director Switch offers virtual storage area network (VSAN) and advanced security services.

Specific Solutions

Cisco complements these integrated security solutions with additional security technologies, including integrated security services, data center confidentiality, data loss prevention, and web application protection.

Integrated Security Services

Cisco's network protection solutions mitigate network and host attacks caused by viruses, worms, DDoS attacks, and other malicious network traffic. Deploying these solutions throughout the data center isolates and blocks intruders, rogue applications, and other unwanted traffic. Some of these products include:

- **Cisco Catalyst 6500 Series Firewall Services Module (FWSM) 4.0:** A high-speed, integrated firewall module for Cisco Catalyst 6500 Series switches and Cisco 7600 Series routers, the FWSM provides the fastest firewall data rates in the industry: 5 Gbps throughput; 100,000 CPS; and 1 million concurrent connections. Up to four FWSMs can be installed in a single chassis providing scalability to 20 Gbps per chassis. The FWSM provides large enterprises and service providers with unmatched security, reliability, and performance
- **Cisco ASA 5580 Adaptive Security Appliance:** The Cisco ASA 5580 is a high-performance security appliance ideally suited to the data center. It provides 10 Gbps of firewall protection, including Layer 7 application protocol inspection, integrated intrusion prevention, IPSec and SSL VPN for encrypted communications and data transfers, and an array of plug-in security modules to help meet the security demands of your unique data center requirements.
- **Cisco Catalyst 6500 Series Intrusion Detection System (IDSM-2) Services Module:** An essential intrusion prevention solution that safeguards organizations against costly and debilitating network breaches from Internet worms, DDoS attacks, and e-business application attacks.
- **Cisco Anomaly Detection and Mitigation Solution:** A family of anti DDoS solutions that protect large enterprises and service provider environments, either as stand-alone appliances or as modules for Catalyst 6500 Series switches and Cisco 7600 Series routers, against massive DDoS attacks. This family of DDoS mitigation solutions includes: Cisco Anomaly Guard Service Module, Cisco Traffic Anomaly Detector Service Module, Cisco Guard XT DDoS Mitigation Appliance, Traffic Anomaly Detector XT, and the Cisco DDoS Multi Device Management System.

- **Cisco Catalyst 6500 Supervisor Engine 32 Programmable Intelligent Services Accelerator (PISA):** PISA embeds deep packet inspection technology into the Cisco Catalyst 6500 Supervisor Engine 32. This provides a platform for hardware acceleration of intelligent services. One of these services is flexible packet matching (FPM). This service adds a superior level of protection against notable worms and viruses. After FPM has identified a threat, it can be dropped, redirected, or logged for further investigation.

Data Center Confidentiality

Due to governance, risk, and compliance requirements, enterprises must deploy technologies to prevent eavesdropping and the theft of sensitive information. The following products provide strong authentication and encryption solutions.

Cisco TrustSec

Cisco TrustSec changes how network security is implemented for data centers. It helps ensure that network access for data centers is allowed only for trusted network devices and trusted users. It delivers three critical security services.

- **Role-based access control:** Cisco TrustSec uses rich identity services for authentication. TrustSec is transparent for wired, wireless, and VPN connections. It authenticates users and devices regardless of role, device type, operating system, or access method. After successful authentication, TrustSec maps users and networking devices to specific roles based on criteria such as identity, job function, location, posture, device type, and so on. The role-based access control capability simplifies the scaling of security services and provides a more efficient approach to implementing compliance requirements and security policies.
- **Converged policy framework:** Cisco TrustSec can coordinate and converge multiple compliance requirements and access policies when a user or device requests access to a network. With TrustSec, security policies can be collapsed into a centralized policy engine that acts as a broker between the campus network infrastructure and back-end policy directories, such as Active Directory. The Cisco Secure Access Control System (ACS) is being extended to provide policy aggregation and control of this converged policy framework.
- **Pervasive integrity and confidentiality:** Cisco TrustSec adds data protection by securing every data path in the campus-switching environment using digital device certificates and strong encryption based on the IEEE 802.1AE standard. Data confidentiality and integrity is instantiated between devices on a hop-by-hop basis. This allows mission-critical applications such as firewalls, intrusion prevention systems, and content inspection systems to maintain visibility into the packet streams at each switch boundary without disrupting the requirements for data integrity and confidentiality.

Cisco Storage Media Encryption

The Cisco Storage Media Encryption (SME) solution protects data at rest on heterogeneous tape drives and virtual tape libraries in a SAN environment using secure IEEE Advanced Encryption Standard (AES) algorithms. Cisco SME hardware and software are fully integrated with the Cisco MDS 9000 family. Encryption is performed as a transparent Fibre Channel fabric service, which greatly simplifies deployment and management of sensitive data on SAN-attached storage devices. Requiring no downtime to deploy, Cisco SME is built upon the Federal Information Processing

Standards (FIPS) Level 3 system architecture and offers secure, comprehensive key management, with support for offline media recovery

Data Loss Prevention

Data loss is a serious business issue. In this climate of financially motivated malware attacks, businesses must deploy security measures to protect sensitive information and address corporate compliance mandates. They should carefully consider their choices to avoid deploying a complex, standalone solution solely focused on protecting against just one problem. A single-purpose data loss prevention solution can push an IT team to the limit by requiring dedicated resources to deploy and administer. The solutions mentioned below cover all three major components of a corporate network: the Internet edge, endpoints, and the data center.

Cisco Security Agent 6.0

Cisco Security Agent 6.0 is the first endpoint server security solution that integrates behavioral-based intrusion prevention, data loss prevention, and signature-based antivirus into a single manageable agent. This unique blend of capabilities defends servers and desktops against sophisticated zero-day attacks, enforces acceptable-use and compliance policies, simplifies management, and reduces TCO. Cisco Security Agent 6.0 provides:

- Real-time behavioral-based malware protection
- Device malware scanning and deletion
- Identification and control of sensitive information
- Easier, faster deployability
- Automatic, no-cost antivirus signature updates

Cisco Security Agent 6.0's new data loss prevention features provide visibility and control of sensitive data across all endpoints, protecting against data loss from both end-user actions and targeted malware. These new features include:

- **Sensitive data detection:** Newly added content scanning capabilities detect credit card numbers, Social Security numbers, and customer-defined sensitive data in local files.
- **Data transfer control:** Access to sensitive information is audited and policy controls can be implemented as needed to stop the malicious transfer of data to removable devices (e.g., USB) or through insecure network applications.
- **Access control:** Access to sensitive information can be limited to authorized users only; all other attempts can be blocked and logged.
- **Change control:** The integrity of critical files and logs can be protected for compliance and audit purposes by blocking and logging any change attempts.
- **Location control:** Location-based controls can enforce sensitive data access policies or restrict printing documents when out of the office.
- **IronPort collaboration:** Cisco Security Agent provides content scanning on the host, which complements the Cisco IronPort® appliance's content scanning and protection at the network perimeter. Cisco Security Agent can enforce the usage of corporate VPN access while users are out of the office, preventing bypass of Cisco IronPort mail and web security services.

Cisco IronPort Data Loss Prevention

IronPort data loss prevention technology gives corporate IT teams a fully integrated solution that combines traditional email security functions (such as spam and virus filtering) with workflow-based functions such as policy creation, content scanning, message encryption, quarantining, and archiving. Ironport's key data loss prevention functions include:

- **Compliance dictionaries:** These dictionaries enable customers to address Payment Card Industry (PCI), Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act, Sarbanes-Oxley, and other regulatory compliance requirements. IronPort's compliance lexicons provide administrators with a prepackaged set of keywords and strings that make it easy to defend against outbound content compliance violations
- **Smart identifiers:** Identifiers give administrators a simple way to configure and scan for sensitive patterns and strings that violate policy. With a simple point and click, administrators can configure filters that scan for credit card numbers, Social Security numbers, ABA bank routing numbers, and others.
- **Content filters and attachment scanning:** IronPort's scanning engine can process more than 300 different attachment types and can render the content for filtering purposes to ensure data loss prevention policy enforcement. This makes it easy to create policies that are unique to your organization.
- **Encryption:** Encryption is the cornerstone of an effective data loss prevention solution. Automatic encryption is imperative as a remediation option for situations where sensitive information needs to be transmitted outside the organization.

Web Application Protection

Web 2.0 and service-oriented architecture (SOA) applications have become critical assets in helping organizations reach more customers, provide more flexible services, increase employee productivity, and interact in real time with remote offices, mobile employees, and other businesses. Enabling and streamlining the flow of data across the Web allows such things as:

- Recognizing customer interactions with your business and managing, analyzing, and optimizing those interactions
- Streaming data from field sales representatives to upper management
- Real-time feedback on marketing campaigns or customer experiences, with the ability to immediately update a campaign or service based on that feedback
- Interactive one-to-one and group communications with customers or between employees
- Inventory control and management, order processing and fulfillment, account management, and other critical business functions available in real time

Web and Web 2.0 application and service vulnerabilities are increasingly being exploited to target critical data center networks, servers, and databases for the purposes of identity theft, data theft, application disruption, and fraud. New application-focused attacks include HTML (Layer 7), Extensible Markup Language (XML), Simple Object Access Protocol (SOAP), and Asynchronous Java and XML (AJAX) (Layer 5) application and protocol exploits, highly sophisticated malware attacks, the emergence of new tools to help attackers create more effective Web-based attacks, and new forms of spam designed to evade conventional filtering techniques and infect targeted systems with Trojans, spyware, and other malware.

Threats originating from inside an organization often use many of the same exploits used from the outside, but can be even more damaging because internal users have detailed knowledge of the organization and can often exploit less secured internal applications.

Cisco web application security tools are designed to address these emerging threats. These solutions include:

Cisco ACE Web Application Firewall

The Cisco ACE Web Application Firewall combines full-proxy application firewall, deep web application and HTML analysis, and high-performance XML inspection and management to truly address the full range of threats associated with new web application services. The result is a single-box solution designed to dramatically reduce business exposure to attacks on modern mission-critical applications, protect sensitive customer and corporate information, enhance availability, and comply with increasingly stringent regulatory requirements.

By combining deep web application analysis with high-performance XML inspection and management, the Cisco ACE Web Application Firewall addresses the full range of threats associated with web application services. The result is dramatically reduced business exposure to attacks on modern mission-critical applications, protection of sensitive customer and corporate information, and enhanced availability.

The Cisco ACE Web Application Firewall provides:

- Enhanced enforcement of requirements outlined in PCI sections 6.5 and 6.6
- Full-proxy firewall
- Application access enforcement
- HTML and XML traffic inspection
- Attack pattern recognition
- Human-assisted learning
- Policy-based provisioning

Cisco Security Agent

Cisco Security Agent is the first endpoint security solution that combines zero-update attack protection, data loss prevention, and signature-based antivirus in a single agent. This unique blend of capabilities protects web servers and application servers against attacks such as buffer overflows, malware, zero-day attacks, and Trojan intrusions, and enforces acceptable-use and compliance policies within a simple management infrastructure.

Cisco Security Agent provides numerous application security benefits, including:

- Zero-update protection reduces emergency patching in response to vulnerability announcements, minimizing patch-related downtime and IT expenses.
- Visibility and control of sensitive data protects against loss from both user actions and targeted malware.
- Predefined compliance and acceptable use policies allow for efficient management, reporting, and auditing of activities.
- "Always vigilant" security means that your system is always protected, even when users are not connected to the corporate network or lack the latest patches.

Cisco IronPort S-Series

The speed, variety, and potential damage of web-based malware attacks highlight the importance of a robust, secure platform to protect the enterprise network perimeter from such threats. In addition to the security risks introduced by web-based malware and spyware, web traffic also exposes an organization to compliance and productivity risks introduced by inappropriate Internet usage within an organization.

The IronPort S-Series Web Security Appliance is the industry's first and only web security appliance to combine traditional URL filtering, reputation filtering, and malware filtering on a single platform to address. By combining these innovative technologies, the IronPort S-Series helps organizations address the growing challenges of securing and controlling web traffic.

IronPort S-Series appliances offer multiple layers of malware defense on a single, integrated appliance. These layers of defense include IronPort Web Reputation Filters™; multiple antimalware scanning engines; the Layer 4 Traffic Monitor, which detects non-Port 80 malware activity; and IronPort's breakthrough Dynamic Vectoring and Streaming™ engine, a new scanning technology that enables signature-based spyware filtering.

IronPort designed and built the first solution to offer all of these features on a single appliance. With the IronPort S-Series, administrators enjoy low total cost of ownership, simplified maintenance and configuration, greater efficacy in malware protection, higher performance through engineering optimizations, and robust management and reporting tools that deliver ease of administration, flexibility and control, and complete visibility into threat-related activity.

Summary

Many data center environments are inadequately protected against today’s threats. Properly securing the data center requires the integration of a variety of specialized security solutions, each designed to address threats targeted at specific segments of the data center environment. Cisco’s Self Defending Network approach to securing the data center provides best-of-breed security solutions combined with the power of an integrated, adaptive, and collaborative framework, to provide maximum risk reduction across your entire data center infrastructure. Integrating these solutions into a comprehensive data center security policy is an essential component of rolling out any next-generation data center architecture plan and deployment.

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.

Printed in USA C22-482422-00 06/08