Cisco SAFE: A Security Reference Architecture

The Changing Network and Security Landscape

The past several years have seen tremendous changes in the network, both in the kinds of devices being deployed and in the network services that are available. Innovations such as virtualization, cloud computing, and web-based access for employees, partners, and customers are bringing about a dramatic evolution in nearly every organization's infrastructure. Many organizations are also transitioning from physical-based collaboration processes to collaborating across geographies by building distributed networks to gain a time-to-market advantage.

The technology supporting these advances also continues to evolve. Bandwidth is ubiquitous. Workers are becoming more and more mobile because they have the devices and networks to do so. Web 2.0 technologies and service-oriented architectures (SOAs) are creating new ways to work and collaborate, and to reach out to customers and partners.

From a security standpoint, these changes have brought with them several new and complex challenges. Traditional point security tools are limited in their ability to support and secure this business transformation, either leaving critical new resources unprotected or preventing the deployment of new services because they do not secure new processes and protocols. At the same time, organizations are facing a host of new threats that target many of these new services and impact network and service availability; these include the theft of identity, data, and reputation, and the abuse of application and network resources.

Today's new threats share several characteristics. They are complex, targeted at specific networks, and increasingly focused on exploiting new applications and services. They include:

- Increasing botnet sophistication and effectiveness
- Emerging mobile phone threats
- Advanced identity theft
- Increasingly malicious spyware
- Web application security exploits
- Supply chain attacks infecting consumer devices

The increase in rigid security regulations further complicates securing the network, and has left many organizations wondering how to balance increased compliance requirements with expanding critical business services. A partial list of regulations includes Sarbanes-Oxley (SOX), Payment Card Industry Data Security Standard (PCI DSS), Graham-Leach-Bliley Act (GLBA), Health Insurance Portability and Accountability Act (HIPAA), Federal Information Security Management Act (FISMA), U.S. PATRIOT Act, Personal Information Protection and Electronic Document Act (PIPEDA), Japan Personal Information Protection Act (PIP), Australia Federal Privacy Act, Basel II, and EU Data Protection Directive (EU DPD).

Common Security Mistakes

Failure to address security in terms of securing and enabling specific business processes can leave organizations with serious security vulnerabilities. Some of the largest, yet most overlooked threats to organizations lie within their own networks. Here is a brief overview of some of the most common security mistakes organizations make:

Siloed Products and Design

This happens when an organization's security infrastructure is comprised of a host of legacy security products purchased over a period of time and loosely coupled together. The problems caused by this type of security architecture include:

- No central command and control
- Poor visibility into the network's health
- Inability to collect and share critical security event information
- Little to no collaboration between elements to address threats
- No real integration between security and network components
- High IT overhead for managing and maintaining siloed security elements

Fear-Based Security Decisions

Often, organizations fall into the trap of focusing on unlikely, high-profile threats rather than more common threats. While these organizations may be quite adept at thwarting a new Internet worm, for example, they often overlook more mundane security issues, such as turning off unused ports, preventing insider abuse and misuse, or detecting rogue wireless access points. Of course, addressing high-profile security events is important, but true risk management must be part of a comprehensive security strategy that sees the network, network services, and security elements as part of a greater whole.

Products vs. Risk Management

Another oversight many organizations make is selecting security products based solely on feature-to-feature comparisons. The reality is that all products are in a constant state of development, and any one product may have, at any moment in time, a particular feature that another product doesn't. In another six months, this sort of comparison is likely to yield completely different results. Instead, security products should all be evaluated on the criteria of risk management to ensure that the security element you acquire meets, as much as possible, the business risks and requirements of your unique environment, now and into the near future.

Inadequate Security Policy

The most essential foundation for any security strategy is an intelligent security policy. Unfortunately, for many organizations, a security policy either doesn't exist, or was an exercise completed some time ago that has been largely unused and perhaps ignored since its creation. Another common security policy error is that it is often focused on the placement of products in the network, paying little attention to supporting and securing the organization's network and business strategy. The result is a document that is not focused on the dual goals of business enablement and continuity, and maximum risk reduction, and that fails to provide guidelines for maintaining management, control, and visibility.

Risk Management

Risk management includes the assessment, mitigation, and monitoring of threats to keep risk at an acceptable level. Any risk management strategy needs to consider the following security priorities:

- **Protection of revenue sources:** Business disruptions caused by network outages and attacks may result in loss of revenue, both in terms of direct business conducted over the network and in the loss of consumer confidence due to publicized security breaches.
- **Addressing customer requirements:** Customers are increasingly concerned about the protection of their private and personal information. Threats to customer privacy, a loss of a sense of security or confidence, and reduced service levels can all adversely affect the corporate bottom line.
- **Safeguarding corporate identity and brands:** Security breaches and attacks, especially high-profile attacks, can have a significant impact on marketing campaigns, brand reputation, and confidence in the organization.
- **Compliance with regulations and standards:** Failure to comply with increasingly stringent legal and corporate regulations and standards can lead to stiff fines and penalties, loss of business, and legal action.

To address these issues, it is essential to make sure that current and future business processes are understood so that security implementations can be designed to support and defend them. Before evaluating any security product or creating or amending any security policy, a few simple questions need to be asked:

- Are business processes well-understood? Are there sufficient safeguards in place to protect data at rest, in transit, and in use?
- What business applications, services, and infrastructure changes are being deployed or may be deployed in the next several years?
- What are the risks associated with implementing those solutions?
- How do we reduce those specific risks as much as possible?
- What regulatory compliance mandates are required for the organization, and what is the plan for meeting them?

In answering these questions, organizations have traditionally been left on their own, largely because traditional security vendors only provide a narrow, “siloed” product to address a broad and integrated problem. Clearly, what is needed is specific guidance, based on best practices and validated designs, on how to discuss, design, and implement a coherent and consistent security solution.

Cisco SAFE Architecture

Cisco has updated its security reference architecture, called Cisco® SAFE, to provide detailed design and implementation guidelines for building secure and reliable network infrastructures and the policies that support them. These guides are based on security best practices combined with thousands of hours of design, testing, and documentation.

A network isn’t a single entity, but rather a collection of network elements, such as the data center, campus, or branch—each with specific functions and security requirements. The Cisco SAFE architecture takes a modular approach in order to best address the unique needs of different

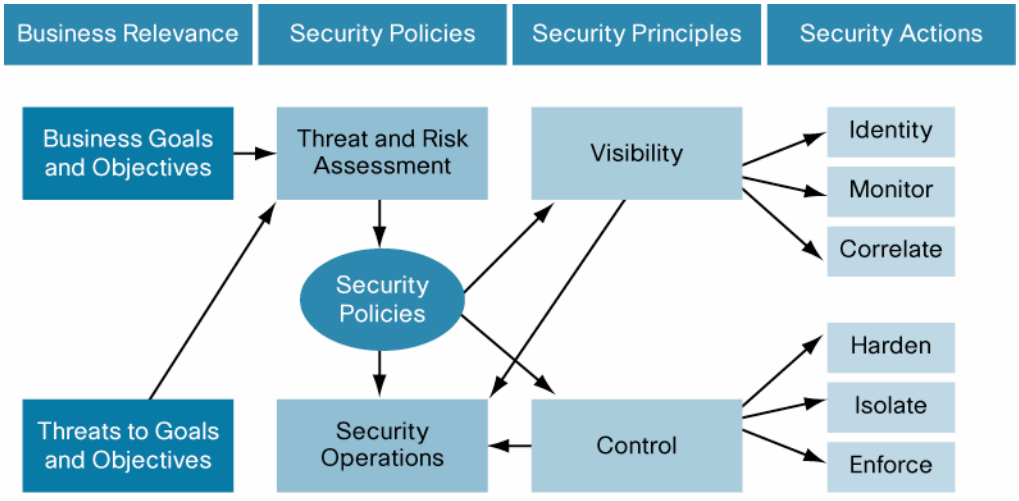
places in the network, as well as the critical interoperations between them. This modularity also extends the useful life of existing equipment, protecting previous capital investments. The designs also incorporate a set of tools to facilitate day-to-day operations, thereby reducing overall operational expenditures.

In today's threat environment, everything is a target. Because of this, Cisco SAFE takes a defense-in-depth approach to security. SAFE's systemwide intelligence approach addresses the security of the infrastructure; endpoints; network devices; applications and application servers; databases; web, email, and other servers; communications devices; and storage systems. It does this by emphasizing the integration of security into each of these components, so rather than being targets, each component contributes to the health of the network, the strategic placement of purpose-built security products, and the collaboration between these elements to create systemwide intelligence and improve visibility and control. Finally, SAFE's secure management and reporting design provides a unified strategy for enforcing policy and for monitoring, analyzing, and responding to threats.

Cisco SAFE design principles not only focus on providing deeper security within specific places in the network, but also between and among functional network zones, as data and transactions traverse the entire infrastructure. Event and posture information is shared among devices and across safeguards for greater visibility, with response actions coordinated under a common control strategy.

The Security Control Framework

SAFE's underlying strategy is the Security Control Framework, a standardized approach to security policy development and deployment. Security Control Framework principles and actions are used to identify the most appropriate technologies and best common practices to secure the unique environment of each place in a network. The result is that multiple security technologies and capabilities are used together throughout the network to gain visibility into network activity, enforce network policy, and address anomalous traffic. In addition, network infrastructure elements such as routers and switches are used as pervasive, proactive policy monitoring and enforcement agents.



Two fundamental principles of the Security Control Framework are maximizing visibility into the devices and events on the network, and control of the users, devices, and traffic moving across the network. Under the categories of visibility and control, the Security Control Framework defines six security actions to enforce security policies.

Visibility

1. Identify and classify users, services, traffic, and endpoints.
2. Monitor performance, behaviors, usage patterns, events, and policy compliance.
3. Collect, analyze, and correlate systemwide events.

Control

4. Harden endpoints, services, servers, applications, and infrastructure.
5. Isolate users, systems, and services when containment is needed.
6. Enforce access controls and security policies, and mitigate security events.

Planning, Review, and Improvement

Because business and security needs are always evolving, another key principle of the Security Control Framework is the ongoing review and adjustment of any security implementation to continually meet changing security and business requirements. There are five key steps in the Security Control Framework development and review process:

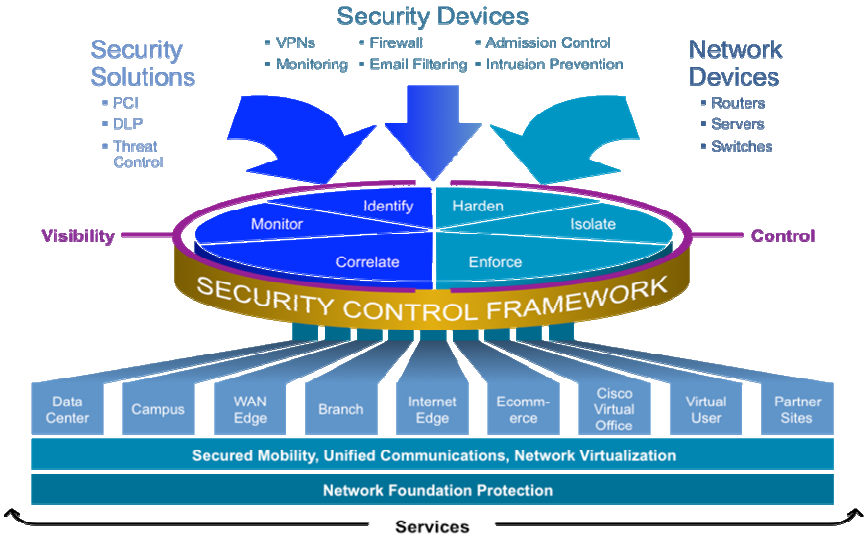
1. Plan. The planning stage must include a threat and risk assessment aimed at identifying assets and the current security posture. Planning should also include a gap analysis to unveil the strengths and weaknesses of the current architecture.
2. Design. Next is the creation of a detailed design that includes the selection of the platforms, capabilities, and best practices needed to close the gaps identified in the planning assessment, and to satisfy future business and technical requirements.
3. Implement. This includes the deployment and provisioning of platforms and capabilities, as well as hardening the underlying network infrastructure. Deployment is typically executed in separate phases, which requires plan sequencing.
4. Operate. Maintenance of the new security implementation includes the management and monitoring of the infrastructure, as well as gathering, reviewing, and responding to security intelligence for consistent and timely threat mitigation.
5. Maintain. Regular plan reviews need to be conducted to identify and address gaps resulting from changes or additions to the network environment. The information obtained from day-to-day operations and from ad-hoc assessments can be used for these purposes. A risk and threat reassessment needs to be periodically conducted. Results from this reassessment lead to restarting the solution cycle, to constantly improve the security architecture and better meet evolving business and security policy needs.

For many organizations, this process can be a daunting task, both in terms of the expertise required and the commitment of IT resources. To that end, Cisco Services has created a complementary suite of services designed to assist in each of the five steps recommended by the Security Control Framework, as well as in the ongoing lifecycle management of any SAFE deployment.

The SAFE Security Architecture

Cisco SAFE comprises a series of validated, end-to-end security design and technical implementation guides that are made available, free of charge, to any organization looking for guidance on developing or improving the security of their networked environment. Some of the key benefits of the Cisco SAFE design and implementation guides include:

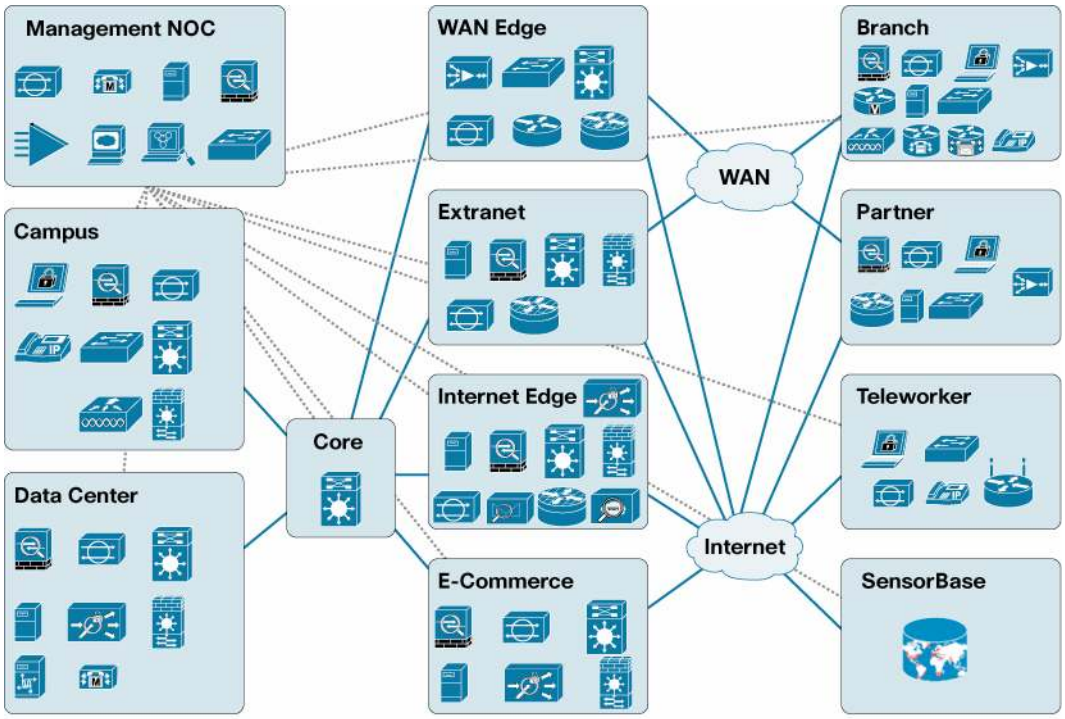
- Detailed designs, based on best practices and real-world testing and validation, help organizations move more quickly from concept to implementation. They also help frame discussions about how to create and improve security policy. By removing much of the guesswork that has traditionally gone into securing a network infrastructure, organizations can realize significant savings from the costs that can result from trial-and-error attempts to create a secure environment.
- Modular designs, based on securing the unique needs of specific places in the network, support incremental improvement over time. Most organizations are not in a position to overhaul their entire security infrastructure. Because of SAFE's modular approach, however, organizations can begin to improve their security profile by updating only that portion of the network most in need of improvement. And because the various components of SAFE are part of an integrated strategy, as each place in the network is improved, the overall visibility, control, and health of the network also improve incrementally and holistically.
- Defense-in-depth secures against more complex threats. With multiple vector attacks, many of the individual attacks either slip past security gaps or are identified as low-level concerns and ignored. Cisco's collaborative security design allows different devices to not only share threat information, but also to aggregate information to detect, report on, and thwart these more complex threats.
- Detailed, step-by-step architectural and platform-specific guidance reduces the IT costs associated with design, deployment, and implementation.
- Collaboration between security elements and the network infrastructure not only creates strong security, but also helps ensure network availability and support for key business applications and network services.



SAFE Network and Solution Modules

The SAFE architecture delivers defense-in-depth by strategically deploying Cisco products and capabilities across the network and by taking advantage of the collaborative nature between platforms. Multiple layers of security technologies are deployed under a common strategy and administration. Products and capabilities are positioned where they deliver most value and to best facilitate collaboration and operations.

Here is an overview diagram of the places in the network included in the Cisco SAFE architecture:



Design guidance is also provided for technologies or elements present across multiple places in the network, such as unified communications, network virtualization, mobility solutions, data loss prevention, identity management services, and network foundation protection.

Cisco Lifecycle Security Services for SAFE

Cisco offers services for the SAFE architecture that are based on an approach that considers the entire lifecycle of a SAFE security depoyment, from initial assessment to deployment to operations and optimization. These lifecycle support services address the following phases of a SAFE deployment:

- **Strategy and assessment:** Cisco offers a comprehensive set of assessment services based on a structured IT governance, risk management, and compliance approach to information security. These services help companies understand the needs of and gaps in their network security architecture. Recommendations are based on industry and international best practices. These services help companies to strategically plan the evolution of an information security program, including updates to security policy, processes, and technology.
- **Deployment and migration:** Cisco offers deployment services to support companies in planning, designing, and implementing Cisco security solutions. In addition, these services can help companies in evolving their security policy and process-based controls to make the security architecture more effective while supporting efforts to increase productivity and collaboration among network users.
- **Remote management:** Cisco Remote Management Services engineers become an extension of a company's IT staff, proactively monitoring the security technology infrastructure and providing incident, problem, change, configuration, and release management, as well as management reporting 24 hours a day, 365 days a year.

- **Security intelligence:** Cisco Security Intelligence Operations services provide early warning intelligence, analysis, and proven mitigation techniques to help security professionals respond to the latest threats. Cisco experts use in-depth knowledge and sophisticated tools to verify anomalies and develop techniques that help ensure timely, accurate, and quick resolution to potential vulnerabilities and attacks.
- **Security optimization:** The Cisco Security Optimization Service is an integrated service offering designed to assess, develop, and optimize a company's security infrastructure on an ongoing basis. Through quarterly site visits and continual analysis and tuning, the Cisco security team becomes an extension of the company's security staff, supporting them in long-term business security and risk management, as well as near-term tactical solutions to evolving security threats.

Conclusion

Cisco SAFE provides a much-needed holistic approach to securing the entire network environment. Its comprehensive security strategy improves an organization's ability to identify, prevent, and respond to threats. But just as important, SAFE enhances an organization's ability to securely deploy critical business applications and services that enable collaboration, increase productivity, and better address the increasing demands of customers, competitors, partners, and employees.

Cisco SAFE Resources

- Cisco SAFE: http://www.cisco.com/go/safe
- Cisco Validated Design Program: http://www.cisco.com/go/cvd
- Cisco Security Lifecycle Services for SAFE: http://www.cisco.com/go/services/security
- Cisco security products: http://www.cisco.com/go/security

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 C11-527476-00 04/09