

Why a Validated Network Architecture?

The network is undergoing tremendous change. Innovations such as virtualization, cloud computing, and web-based access are bringing about a dramatic evolution in nearly every organization's infrastructure.

From a security standpoint, these innovations have brought with them several new and complex challenges in the form of threats that attack network and service availability, exploit new applications and network resources, and focus on data and identity theft. Traditional point security solutions are largely unable to address these threats.

Organizations need reliable and proven guidance on how they can best secure these new, business-critical services while protecting against emerging threats.

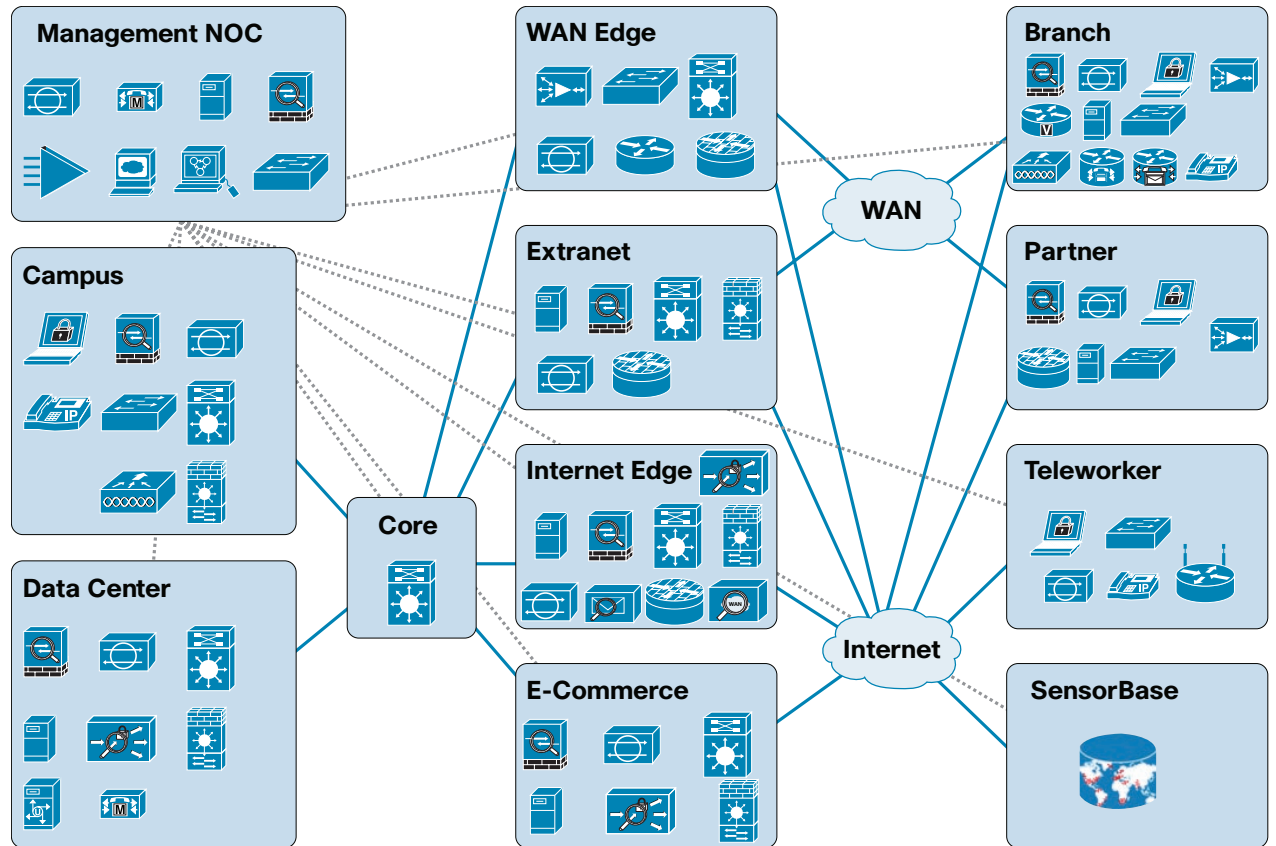
Complex Threat and Security Issues

Today's complex new threats are increasingly targeted at specific networks and new technologies and services. Some of these threats and issues include:

- Increasing botnet sophistication and effectiveness
- Emerging mobile phone threats
- Increasingly malicious spyware
- Web application exploits
- Supply chain attacks infecting consumer devices
- Increasingly rigid regulatory and compliance requirements

Cisco SAFE Validated Security Architectures

Cisco® SAFE is a security reference architecture that is part of the Cisco Validated Design program. SAFE provides prescriptive design guides, based on best practices, that address the planning, design, and deployment of security solutions. SAFE's modular design addresses the unique requirements of different places in the network, such as campuses, the Internet edge, branches, and data centers.



Cisco SAFE's defense-in-depth architectural blueprints provide best practices to help secure critical data and transactions across the network. Organizations can strategically position Cisco products and capabilities across the network, and can take advantage of the collaborative nature between security and network platforms.

Cisco SAFE designs focus on supporting critical business and network services by helping organizations develop and enhance network visibility and control.

Visibility

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

Control

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



The result is a validated security strategy that helps secure the interactions and transactions between and among places in the network to create a highly secure network environment.

What are the Benefits of SAFE?

The Cisco SAFE architecture can provide guidance on all aspects of a secure network so that organizations can create a thoughtful security deployment strategy based on available budget and critical need.

- Step-by-step network security design and implementation guidance shortens deployment.
- Solutions-based approach focuses on risk management rather than product placement.
- Layered security design helps prevent a network from being overwhelmed by a large or unexpected attack.
- Threat visibility and coordinated response reduces exposure and IT overhead.
- Integrated security and network architecture helps ensure business-critical services availability.
- Modular design enables a gradual improvement in security, based on organizational priority.
- Fully tested and validated designs

In addition, these best practices and functions can help organizations meet their compliance requirements.

Cisco Security Lifecycle Services

SAFE services delivered are based on a lifecycle approach and cover the entire lifecycle process:

Strategy and assessment: Cisco offers a comprehensive set of assessment services to help organizations understand their current security state and plan for the strategic deployment of SAFE security principles.

Deployment and migration: Cisco offers deployment services to support companies in planning, designing, and implementing Cisco SAFE validated designs.

Remote management: Cisco Remote Management Services offers engineers and tools to proactively monitor the SAFE security infrastructures and provide incident, problem, change, configuration, and reporting services 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.

Security optimization: The Cisco Security Optimization Service is an integrated service offering designed to assess, develop, and optimize a company's security infrastructure through quarterly site visits and continual analysis and tuning.

For More Information

For more information on Cisco SAFE, please contact your local account manager or security product sales specialist, or go to <http://www.cisco.com/go/safe>. You can also go to www.cisco.com/go/cvd to download the free SAFE design and implementation guides.

For information on Cisco's security products and services, go to <http://www.cisco.com/go/security>. For more information on Cisco Security Services, go to <http://www.cisco.com/go/services/security>.