Cisco Security Control Framework (SCF) Model

Contents

Introduction

The IT infrastructure architecture must be designed and implemented with security at its core in order to enable key business activities, while ensuring the confidentiality, integrity, and availability of the IT infrastructure and critical business and customer data. An organization's security requirements are derived from many sources, including organization goals and objectives, industry and international standards, and industry and government regulations. The process of designing, implementing, and operating an infrastructure that meets these business and security requirements benefits from the application of a coherent model to view and organize the myriad security control requirements.

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

The *Cisco Security Control Framework (SCF) model* defines a structure of security objectives and supporting security actions to organize security controls. The Cisco SCF model is based on proven industry best practices and security architecture principles, and the vast practical experience of Cisco engineers in designing, implementing, assessing, and managing service provider, enterprise, and small and medium-sized business (SMB) infrastructures. Using the Cisco SCF model, organizations can align security requirements and controls into logical groups to facilitate the understanding and communication of the control architecture for their IT infrastructure.

The organization of the Cisco SCF model is designed to increase the focus on three primary goals related to the security of the IT infrastructure and assets. These goals are as follows:

- Protect the IT infrastructure
- Protect the IT assets using network-based controls
- Mitigate and respond to security incidents using network-based controls

The design of the Cisco SCF model brings together the regulation- and standards-based requirements with fundamental architectural principles, industry best practices, and a wide breadth of engineering experience from inside and outside of Cisco. The result is a vendor-agnostic model that supports the organization and definition of control sets to meet each organization's specific objectives.

Terms and Definitions

Table 1 defines the terms relevant to the Cisco SCF model.

Table 1 Terms and Definitions

Term	Definition
Architecture Principle	Expression of a fundamental, primary, or general law or truth that is expected to be time invariant and direct the fulfillment of a particular mission.
Cisco Security Control Framework	The combination of the model, methodology, control structure, and control sets that codify Cisco's security knowledge as it applies to vendor-agnostic assessments of IT infrastructure security architectures and implementations. **Note** This version of the Cisco SCF document only addresses the model portion of the overall framework.
Cisco Security Control Framework Model	The security objectives and security actions used to organize security controls into a model that supports assessments of security architectures and implementations across multiple aspects within an organization's infrastructure.
Control	A measurable standard or mechanism that defines a required attribute, capability, or function in an infrastructure that delivers one or more security actions to support a specific security objective. Controls are realized in the infrastructure through the implementation of techniques. A control might require one or more techniques to be fully realized.
Control Set	A logical grouping of controls aligned across security actions to support one or more infrastructure aspects. The aspects supported by the control set can be aligned by places in the network (PIN), control type, functional block, or a specific organizational (business) concern.
Control Type	An organizational concept used to describe the type of control and the nature of the techniques associated with its implementation. Typical control types include technical, policy, and procedural.

Table 1 Terms and Definitions (continued)

Term	Definition
Functional Block	A common infrastructure aspect used to subdivide the infrastructure primarily along functional boundaries. Examples of functional blocks include the following: • Data center • Interior • Perimeter • Physical security
Infrastructure Aspect	A logical, physical, functional, or organizational portion, section, area, place or view of network devices, applications, servers, or other network-attached endpoints of an infrastructure that facilitates discussions, analysis, or scoping of control sets, assessments, architectures, or designs. Common infrastructure aspects used in related documents include PINs, functional blocks, or control type.
IT Infrastructure	The collection of traditional network devices, network services, network-attached devices, and the associated infrastructure to protect the network and devices. Examples of IT infrastructure elements include the following: • Routing and switching devices • Security – Firewalls – Intrusion detection and prevention systems – Anomaly, analysis, correlation and response systems – Web application firewalls – Host intrusion detection software • Data center – Application server farms – Storage area networks – Web server farms – Load balancers • Unified Communication devices • Wireless controllers and access points • Physical security devices
Network Service	An application or capability made available by the infrastructure, application servers, or other network attached devices.
Organizational Objectives	Key drivers or mission for the organization. In the context of the Cisco SCF, these are the key objectives that must be supported and enabled by the security infrastructure.

Table 1 Terms and Definitions (continued)

Term	Definition
Place in the Network (PIN)	A common infrastructure aspect used to view the infrastructure in physical, logical, and functional groupings that map to common industry vocabulary. Examples of PINs include the following: • Branch • Campus • Core • Data center • E-Commerce • Internet edge • WAN edge
Policy	A definite course of action, put in place and adopted by an organization, considered to be expedient, prudent or advantageous in guiding and influencing decisions, actions, and other matters.
Process	A systematic series of actions or steps designed to consistently accomplish a specific end result.
Risk	The exposure to or chance of harmful consequences that might negatively impact the value of an asset. A typical expression of risk is the product of the probability of an incident occurring and the potential impact of the incident.
Security Action	An organizational grouping of related attributes, capabilities , and functionality required in a security architecture to support a security objective.
Security Architecture Assessment	The assessment of an infrastructure's topology, design, architecture, device configurations, hosts and endpoints, and physical and logical characteristics compared to a standard set of controls, industry best practices, and organization objectives to identify security gaps.
Security Objective	Targets defined to direct the efforts or actions of an organization to realize a desired security state. Security objectives are supported through security actions and associated controls.
Security Posture	A point in time measure of the security state of an IT infrastructure.
Service	The performance of a set of lifecycle tasks for a customer primarily driven by engineering or professional service efforts.
Solution	The combination of products and services.
Technique	A method or procedure implemented in the infrastructure or related operations used to deliver all or part of an attribute, capability, or function required by a control.
Threat	A real or potential circumstance, capability, action, or event that can potentially exploit a system's vulnerabilities to negatively affect the value of an asset.
Vulnerability	A flaw or weakness in an asset or systems architecture, design, implementation, or operation and management that is capable or susceptible to being exploited to negatively affect the value of the asset.

Cisco Security Control Framework

The Cisco SCF is composed of a model, methodology, control structure, and control sets designed to support the assessment of technical risk in an infrastructure architecture. The Cisco SCF integrates into an ongoing process of continuous improvement to incrementally improve the security posture of the infrastructure architecture to address current key threats and to identify, track, and defend against new and evolving threats. The Cisco SCF's ability to do this is its base of sound architectural principles rather than a focus on specific individual threats, technologies, vendor products, or implementation configurations.

The Cisco SCF is composed of the following three sections:

- *Model* (addressed in this document)

  The *model* defines the security objectives and their supporting security actions as a mechanism to organize individual controls and address the underlying architectural principles.

- *Control Structure* (not addressed in this document)

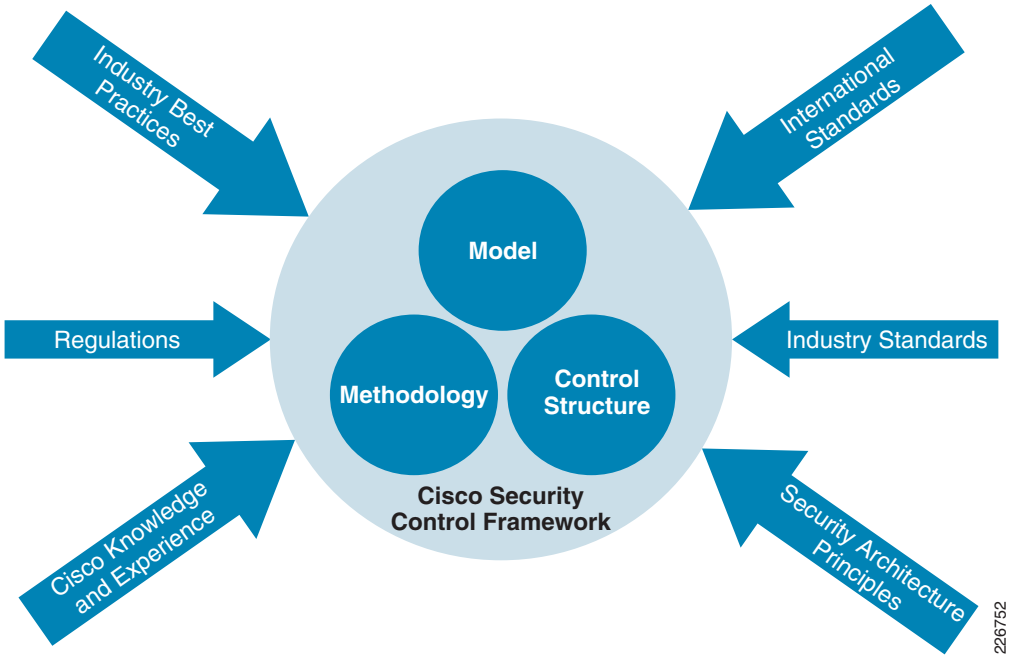
  The *control structure* defines the organization of individual controls and control sets and how they relate to the Cisco SCF model and methodology.

- *Methodology* (Not addressed in this document)

  The *methodology* defines the primary steps required to conduct a security architecture assessment using the Cisco SCF. The structure of controls, the scoring process, and the mechanism for aggregating these scores into meaningful results are also defined in the methodology.

The model and methodology sections provide the overall architecture for the Cisco SCF, including the various components, the interactions between the components, and the way in which components should be used to achieve the specific security objectives of an infrastructure security architecture assessment. As such, the Cisco SCF is not a design or implementation, but consist of guidelines—a set of rules or a playbook used to assess architectures in an orderly manner. Well-defined security infrastructure architectures, based on key foundational principles, have proven to be more robust and tolerant, surviving changes in technology, organizational boundaries, and external influences. The Cisco SCF is designed to be configurable and extensible through the definition and use of the appropriate control sets for a specific assessment's objectives and business environment. Figure 1 summarizes the components of the Cisco SCF and the major sources of influence on its design.

Figure 1 Cisco Security Control Framework



Cisco SCF Model

The Cisco SCF model is the application of foundational security principles to define the guidelines and rules for achieving a secure infrastructure. The security architecture does not define how to build or implement a secure infrastructure, but instead defines the properties, capabilities, processes, and controls that a secure infrastructure must possess to protect against a range of threats. The Cisco SCF model provides a useful organizational structure to capture the architectural aspects that the foundational principles require.

The definition of the Cisco SCF model starts with the fundamental security principles as summarized in Table 2. These fundamental principles are factored into the security objectives and security actions that define the Cisco SCF model.

Table 2 Underlying Security Architectural Principles

Security Architectural Principle	Description
Defense-in-Depth	Never assume that a single control can provide sufficient risk mitigation for a specific threat. Deploy multiple layers of controls to prevent, identify, and delay attacks in order to contain and minimize damage while an organization responds.
Service Availability and Resiliency	Ensure service availability through device hardening and by strengthening the resiliency of the network to adjust to and recover from abnormal circumstances.
Segregation and Modularity	Infrastructure is organized in functional blocks with distinct roles facilitating management, deployment, and securing of the devices and business assets within each block.
Regulatory Compliance and Industry Standards	Follow industry standards and best practices to facilitate the achievement of regulatory compliance.

Table 2 Underlying Security Architectural Principles (continued)

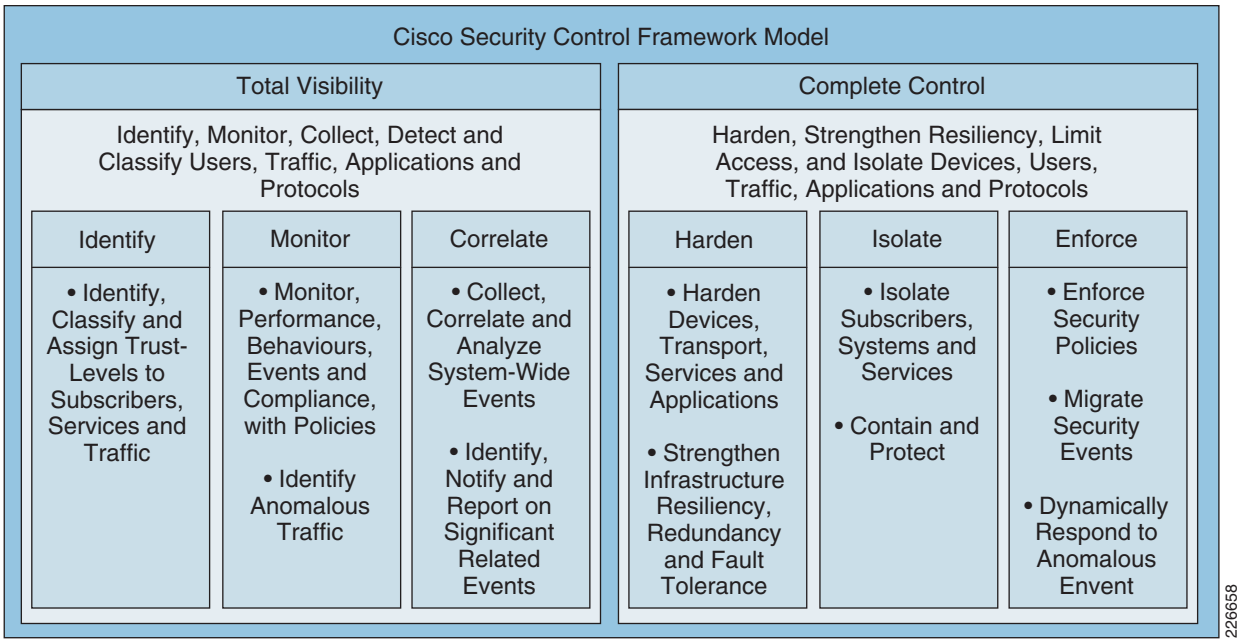
Security Architectural Principle	Description
Operational Efficiency	Simple and efficient configuration, deployment, and management of the infrastructure, throughout its entire lifecycle, increase control and visibility allowing for faster auditing, troubleshooting, problem isolation, and incident response.
Confidentiality, Integrity, and Availability	Security controls work to provide acceptable levels of confidentiality, integrity, and availability of data.
Auditable and Measurable Controls	Security controls must be auditable and measurable to be effective.
System-wide Collaboration and Correlation	Infrastructure security is not a set of independent point solutions. Effective security requires sharing, analysis, and correlation of information from all system-wide sources.

The Cisco SCF model defines the two fundamental security objectives of total visibility and complete control. The success of a security architecture and infrastructure implementation ultimately depends on the degree to which they enhance visibility and control. Without visibility there is no control and without control there is no security. Therefore, the Cisco SCF's main focus is on security actions and the underlying controls that enhance the fundamental principles of visibility and control. In practice, the Cisco SCF is used to drive the selection and deployment of platforms and capabilities to achieve a desirable degree of visibility and control. The definitions of visibility and control are elaborated in the following section.

Security Objectives

The Cisco SCF defines six security actions that support security objectives by improving visibility and control. The actions, three each for visibility and control, define logical groupings for organizing the more detailed security controls. Figure 2 depicts the six security actions and their relationships with the visibility and control objectives.

Figure 2 Cisco Security Control Framework Model



The following descriptions outline key considerations for total visibility and complete control.

Total Visibility

Total visibility consists of the following elements: identity, trust, compliance, event monitoring, and performance monitoring. Key considerations for total visibility include the following:

- Identifying and classifying users, traffic, applications, protocols, and usage behavior
- Monitoring and recording activity and patterns
- Collecting and correlating data from multiple sources to identify trends, and system-wide events
- Detecting and identifying anomalous traffic and threats

Complete Control

Complete control consists of hardening individual devices, increasing the resiliency of the network, isolating users, systems and services, security policy enforcement, and event mitigation. Key considerations for complete control include the following:

- Hardening IT infrastructure, including individual devices and increasing network resiliency
- Limiting access and usage per user, protocol, service, and application
- Isolating users, services, and applications
- Protecting against known threats and exploits
- Dynamically reacting in response to anomalous events

Security Actions

Security actions provide organizational groupings of related attributes, capabilities, and functionality required in a security architecture to support a security objective. These security actions are described in the following subsections.

Total Visibility

The total visibility security objective is supported by the *identify*, *monitor*, and *correlate* security actions described in the following subsections.

Identify

The identify controls deliver the capabilities for a system to identify and classify entities accessing a given resource and to then determine a trust level or state of trust for that entity. Usually, trust is established through mechanisms other than inspection of an IP address, including inspection of credentials. Identifying an entity applies to traffic from within the network and possibly external traffic entering a network.

Monitor

The monitor controls address the fundamental capabilities and instrumentation to facilitate security visibility, combined with the ability to monitor the behavior and usage of the infrastructure components, including resources, connected systems, users, applications, and IP traffic.

Correlate

The correlate controls focus on the ability of the system to derive and present intelligence related to the state of the infrastructure based on correlation and management of visibility data.

Correlation is the interpretation, dissemination, analysis, and classification of visibility data into meaningful operational information through the contextualization of seemingly unrelated events or changes. From a security operations perspective, it provides the foundation to apply policy enforcement and isolation controls.

Management is the ability to represent visually, in near real-time, the intelligence derived from various network elements including audit logs, event monitoring, fault knowledge, and health/status information.

Complete Control

The complete control security objective is supported by the *harden*, *isolate*, and *enforce* security actions described in the following subsections.

Harden

The harden controls address the ability of an infrastructure to withstand, adjust to and/or recover from adverse uncontrolled circumstances. Hardening includes both securing individual devices and the infrastructure as a whole through increased resilience, fault tolerance, route duplication and other means.

Isolate

The isolate controls focus on the ability of a system to limit the scope and minimize the impact upon users, services, and systems from known and unknown disturbances. Implementation of the isolate controls provides the ability to isolate logical and physical functional blocks of an infrastructure into security zones to control or to prevent access between the functional blocks in the infrastructure and to limit the scope of security breech exploitation.

Enforce

The enforce controls deliver the capabilities required to enforce the allowed behavior of connected systems, users, applications, and IP traffic. Policy enforcement may either be static (a control is applied on a permanent basis) or dynamic (a control is applied to specifically mitigate some discrete event or security incident).

Organizing Controls with the Cisco SCF

This section provides examples of the types of control techniques and technologies that are mapped to each of the security actions. This list is provided as an example to help describe the scope and intent of each of the security actions and to help define different specific controls that address the required attributes, capabilities, or functions of the security actions.

Example Controls, Techniques, and Technologies Mapping

Total Visibility

Identify

- Identity-based network solutions (802.1x, NAC, and so on)
- Authentication, Authorization, and Accounting (AAA)—Authentication
- Biometric recognition
- Routing authentication (MD5)
- Secure messaging (encrypted E-mail)
- VPN authentication
  - Digital certificates
  - Pre-shared keys
  - User authentication

Monitor

- AAA—Accounting
- Anomaly Detection System
- Intrusion Detection System (IDS) and Intrusion Prevention System (IPS)
- Network flow data collection

- Simple Network Management Protocol (SNMP)/Remote Monitoring (RMON)/Management Information Base (MIB)
  - CPU, memory threshold
- Syslog
  - Topologies: Cisco Discovery Protocol (CDP); routing protocols; multiprotocol label switching (MPLS) Label Distribution Protocol (LDP)
- Sinkholes

Correlate

- Analysis of network flow data (Arbor, Cisco Security Monitoring, Analysis, and Response System (CS-MARS), and so on)
- Host intrusion protection event correlation
- Security incident management system
- Event analysis and correlation
  - Syslog
  - SNMP
  - AAA
  - Antivirus
- Network Time Protocol (NTP) synchronization

Complete Control

Harden

- Control plane policing
- Device hardening
  - Disable unused services
  - Latest patch level
  - Restrict device accessibility
- Component redundancy
  - Power supply
  - Link and interface
- Device redundancy
- Topology redundancy

Isolate

- Firewall access control policies
- Network and segment isolation
- Out of band management
- VPN encryption

- Management traffic encryption—Secure Shell (SSH), SNMP, and so on
- Virtual LAN (VLAN)

Enforce

- Content filtering
- Distributed-denial-of-service (DDoS) protection
- Host intrusion prevention
- Port security
- Quality-of-Service (QoS) enforcement
- Network access control
  - Access control lists (ACL), filters
  - Unicast reverse path forwarding (uRFP)
  - Anti-spoofing
- Policy-based routing
- AAA authorization