CHAPTER 1

Introduction

Effective network security demands an integrated defense-in-depth approach. The first layer of a defense-in-depth approach is the enforcement of the fundamental elements of network security. These fundamental security elements form a security baseline, creating a strong foundation on which more advanced methods and techniques can subsequently be built.

Developing and deploying a security baseline can, however, be challenging due to the vast range of features available. The Network Security Baseline is designed to assist in this endeavour by outlining those key security elements that should be addressed in the first phase of implementing defense-in-depth. The main focus of Network Security Baseline is to secure the network infrastructure itself: the control and management planes.

This document outlines the key security elements identified for Network Security Baseline, along with implementation guidelines to assist in their design, integration, and deployment in production networks.

Security Baseline Overview

The Network Security Baseline presents the fundamental network security elements that are key to developing a strong network security baseline. The focus is primarily on securing the network infrastructure itself, as well as critical network services, and addresses the following key areas of baseline security:

- Infrastructure Device Access
- Routing Infrastructure
- Device Resiliency and Survivability
- Network Telemetry
- Network Policy Enforcement
- Switching Infrastructure

Unless these baseline security elements are addressed, additional security technologies and features are typically useless. For example, if a default access account and password are active on a network infrastructure device, it is not necessary to mount a sophisticated attack since attackers can simply log in to the device and perform whatever actions they choose.

In order to ensure a comprehensive solution, the Cisco Security Framework (CSF) is applied in the development of Network Security Baseline. CSF provides a comprehensive method of assessing and validating the security requirements of a system.

The CSF has been used in the creation of the Security Baseline to ensure that all the requirements have been considered for each particular contextual area. An overview of the CSF methodology is presented in the Cisco Security Framework Overview, page 1-2.

All sample configurations in this paper are based on Cisco IOS platforms and features. However, the general security objectives outlined in each section are equally applicable to non-IOS platforms.

Preliminary Network Design Assessment

The Network Security Baseline includes some security techniques that rely on the enforcement of IP address-based traffic filtering. These include ACLs to enforce policy on device management access, the ability to control route distribution and uRPF. More advanced security techniques, that can subsequently be added as an additional layer of security, also rely on IP address-based traffic filtering, such as firewall rule definition.

A rational, summarized, or compartmentalized IP address scheme, as well as the application of RFC1918 guidelines, makes the implementation of these IP address-based traffic filtering techniques simpler and more manageable on an ongoing basis.

In preparation for deploying a security baseline, it is recommended that a preliminary network design assessment be performed in order to facilitate its implementation. The key focus of this assessment is to review the current IP addressing scheme in terms of the following two key questions:

Q. Is the IP addressing scheme well structured and is it possible to easily summarize or compartmentalize the IP address space?

Q. Are RFC1918 IP addresses leveraged where appropriate?

An assessment of the current IP addressing scheme may identify areas where IP re-addressing may be desirable prior to implementation of a security baseline. Whilst this may demand some network changes, this will generally result in a more manageable and enforceable security policy, offering a significant benefit to overall network security.

For more information on RFC1918, see: http://www.ietf.org/rfc/rfc1918.txt

Cisco Security Framework Overview

The Cisco Security Framework (CSF) is a security operational process model aimed at ensuring network, and service, availability and business continuity. Security threats are an ever-moving target and the CSF is designed to identify current threat vectors, as well as track new and evolving threats, through the use of best common practices and comprehensive solutions.

The CSF is built upon two fundamental objectives, under the premise that one cannot control what one cannot see or measure:

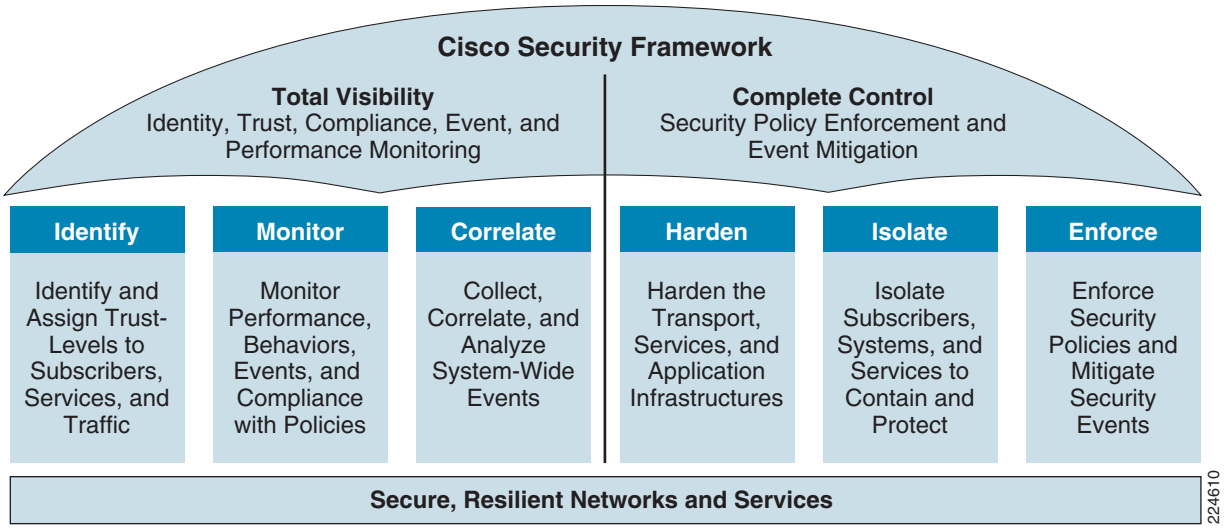
- Gain Total Visibility
- Identify, monitor, and correlate system-wide events
- Assure Complete Control

  Harden network infrastructure, isolate hosts and services, and enforce security policies

To achieve this total visibility and complete control, multiple technologies and capabilities are used throughout the network to gain visibility into network activity, enforce network policy, and address anomalous traffic. Network infrastructure elements such as routers and switches are leveraged as pervasive, proactive policy monitoring and enforcement agents.

The CSF focuses on six key actions, as illustrated in Figure 1-1.

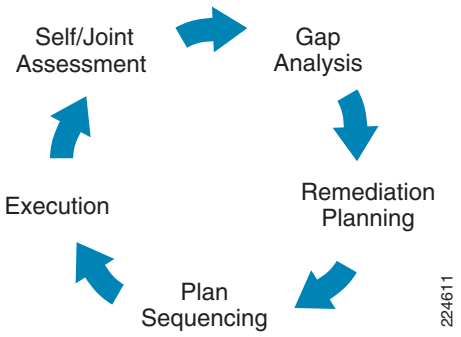
Figure 1-1 Cisco Security Framework Overview



The application of the CSF to a network results in the identification of technologies and best common practices to satisfy each one of the six key actions. However, the CSF is an ongoing process, involving review and modification of the implementation in accordance with changing business and security needs.

To that end, the CSF incorporates an evolutionary cycle, as illustrated in Figure 1-2.

Figure 1-2 CSF Evolution Cycle



The cycle starts with an initial assessment aimed at identifying current capabilities and security posture. It is followed by a gap analysis to unveil the strengths and weaknesses of the current architecture.

The Network Security Baseline presented may be used as a reference model during the initial assessment and gap analysis phases. It provides the minimum requirements for control and management protection. Strengths and weaknesses of real-world networks can be identified by comparing them against the baseline.

After the initial assessment and gap analysis, the cycle continues with remediation planning, which has the goal of closing the gap and satisfying future requirements by updating the overall network architecture. Plan sequencing follows to establish an implementation roadmap for the different components of the intended architecture. Each phase is then executed and results are evaluated as the cycle moves back into the assessment phase.

As Figure 1-2 illustrates, the process is iterative and each iteration results in the development of an architecture better designed to meet the evolving business and security policy needs.

The Network Security Baseline has been developed following the CSF. Each section includes a table showing how the proposed security features and best common practices help satisfy each one of the key actions of the CSF.