CHAPTER 1

Solution Overview

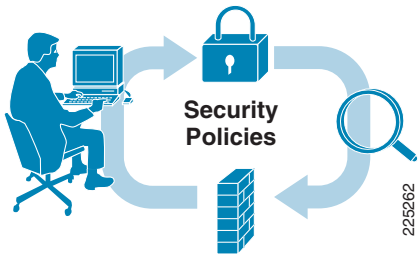
Design Overview

The purpose of this design guide is to describe the integration and collaboration of network security technology and the Cisco Unified Wireless Network. The Cisco Unified Wireless Network features comprehensive wireless security functionality but the goal of this solution is to explain how wired-side network security complements these wireless-specific security features and how it can be integrated into a network-wide security plan—enabling an enterprise to apply a common network security policy that is inclusive of both wired and wireless network access methods.

Network Security

Network Security is an ongoing process of defining security policies, implementing proactive security measures to enforce them, monitoring the network to obtain visibility into activity, identifying and correlating anomalies, mitigating threats and reviewing what occurred in order to modify and improve the security posture, as illustrated in Figure 1-1.

Figure 1-1 The Security Process



The Cisco Unified Wireless Network features a comprehensive architecture of security tools and technologies to secure the WLAN environment, clients, and infrastructure, which are summarized in Chapter 4, “Cisco Unified Wireless Network Architecture— Base Security Features.” In a comprehensive, network-wide layered security solution, the Cisco Unified Wireless Network plays an important role in securing wireless access, but there are opportunities to create a superset of layered network security via collaboration with the network infrastructure.

A wireless network is only one of the attack vectors against a network. While a WLAN network must be secure and able to protect itself from attack, a network-wide security solution that only addresses WLAN-related attacks is dangerously unbalanced. Mobile network clients need to be protected on all interfaces at all locations, enterprise networks need to be protected on all their perimeters, and

monitoring and anomaly detection are required regardless of the source of network traffic. Ideally the same sets of tools and interfaces should be used to provide these baseline security functions as it reduces operational costs, reduces the risk of misconfiguration, and avoids the creation of a unbalanced security architecture that can be simply bypassed.

Table 1-1 illustrates the role of the Cisco Unified Wireless Network security and the roles of other components in a network security architecture. The Cisco Unified Wireless Network provides solutions and WLAN standards-based proactive and operational security, and components such as Cisco Security Agent (CSA), Cisco Network Access Control (NAC) Appliance, Cisco Intrusion Prevention System (IPS), Cisco Security Monitoring, Analysis and Response System (CS-MARS), and Cisco firewalls build on this to provide an overall network security architecture. This provides a layered security system where the Cisco Unified Wireless Network provides security particular to the access layer technology and integration into the overall network security system.

Table 1-1 WLAN Security Elements and General Network Security Elements

Proactive Security	WLAN Specific Elements	General Network Security Elements
Harden the network infrastructure	Cisco Unified Wireless Network, LWAPP, Management Frame Protection, 802.1X	Infrastructure Hardening
Protect the endpoints	Wi-Fi Protected Access/Wi-Fi Protected Access2	CSA and Cisco Secure Services Client
Identify and enforce policy on users	Wi-Fi Protected Access/Wi-Fi Protected Access2, Client Exclusion on the Wireless LAN Controller	CSA, Cisco Secure Services Client, NAC, and Cisco Firewall
Secure communication	Wi-Fi Protected Access/Wi-Fi Protected Access2	
Access control	Access Control Lists on Wireless LAN Controller	Cisco Firewall
Operational Security		
Monitor the network	Wireless LAN Controller, Wireless Control System, Adaptive wireless IPS	AAA, SNMP, Platform Management, and CS-MARS
Detect and correlate anomalies, mitigate threats	Wireless LAN Controller, Wireless Control System, adaptive wireless IPS	CS-MARS, CSA, and IPS

Solution Components

The Secure Wireless architecture is built on the core Cisco architectures for the branch and campus networks. The Secure Wireless Architecture describes the integration and collaboration of Cisco security solutions with the Cisco Unified Wireless Network to provide a common security framework for networks regardless of the client access mechanism. The core components of the Secure Wireless Architecture are:

- Cisco Unified Wireless Network
  - Wireless intrusion prevention
  - Rogue detection and mitigation

  - Access control
  - Traffic encryption
  - User authentication
  - RF interference and DoS monitoring
  - Wireless security vulnerability monitoring and auditing
  - Infrastructure hardening—MFP, infrastructure device authentication
- CSA
- Cisco NAC appliance
- Cisco firewalls
- Cisco IPS
- CS-MARS

Cisco Unified Wireless Network

The Cisco Unified Wireless Network is a unified wireless network solution that cost-effectively addresses the wireless network security, deployment, management, and control issues your enterprise faces. It combines the best elements of wireless networking to deliver secure, scalable wireless networks with a low total cost of ownership.

The Cisco Unified Wireless Network helps you maintain your competitive advantage through the freedom and flexibility of a secure, scalable, cost-effective solution. Wireless networks offer:

- Anytime, anywhere access to information, promoting collaboration with colleagues, business partners, and customers
- Real-time access to instant messaging, e-mail, and network resources, boosting productivity and speeding business decision making
- Mobility services, such as voice, guest access, advanced security, and location, that help you transform business operations
- Modular architecture that supports 802.11n, 802.11a/b/g, and enterprise wireless mesh for indoor and outdoor locations, while ensuring a smooth migration path to future technologies and services

Cisco Security Agent (CSA)

CSA 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 defends servers and desktops against sophisticated day-zero attacks, and enforces acceptable-use and compliance policies within a simple management infrastructure.

CSA provides numerous 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
- Signature-based anti-virus protection to identify and remove known malware

- Predefined compliance and acceptable use policies allow for efficient management, reporting, and auditing of activities
- Industry-leading network and endpoint security integration and collaboration, including Cisco NAC, Cisco network IPS devices, and CS-MARS
- Centralized policy management offering behavioral policies, data loss prevention, and antivirus protection fully integrated into a single configuration and reporting interface

Cisco NAC Appliance

The Cisco Network Admission Control (NAC) appliance is a powerful, easy-to-use admission control and compliance enforcement solution. Cisco NAC provides comprehensive security features:

- In-band or out-of-band deployment options
- User authentication tools
- Bandwidth and traffic filtering controls
- Vulnerability assessment and remediation (also referred to as posture assessment)

As the central access management point for your network, the Cisco NAC appliance enables you to implement security, access, and compliance policies in one place instead of having to propagate the policies throughout the network on many devices. With remote or local system checking, Cisco NAC appliance blocks user devices from accessing your network, unless they meet the requirements you establish.

These same Cisco NAC appliance features can be integrated with a Cisco UWN to provide consistent policy enforcement across both the wired and wireless network.

Cisco Firewall

Firewalls protect networks from attacks and unauthorized access, both externally and internally. For secure wireless, firewalls protect the wireless network from unauthorized access from other networks, both wired and wireless. It also restricts users from gaining access to the wireless network without authorization. Cisco integrates firewall into several product lines, including the ASA 5500 series, IOS secure routers, and services modules for the Catalyst 6500 series switches.

Cisco IPS

Cisco IPS are network-based platforms designed to accurately identify, classify, and stop malicious traffic, including worms, spyware, adware, network viruses, reconnaissance and application abuse, and policy violations. This is achieved through detailed traffic inspection at Layers 2 through 7.

Cisco offers a range of network IPS platforms, including the Cisco IPS 4200 Series dedicated appliances and IOS IPS, as well as integrated modules for the Cisco ASA 5500 series, Cisco Integrated Security Routers (ISR), and Catalyst 6500 series.

CS-MARS

CS-MARS provides security monitoring across the network, including network devices and host applications, wired and wireless, Cisco and other vendors. CS-MARS greatly reduces false positives by providing an end-to-end topological view of the network, threat identification, correlation, and aggregation to identify top alerts. It creates mitigation responses options, provides strong forensics analysis intelligence, and creates reports for incident response and compliance regulations.