CHAPTER 2

Solution Architecture

Introduction

The purpose of the Secure Wireless Solution Architecture is to provide common security services across the network for wireless and wired users and enable collaboration between wireless and network security infrastructure for a layered security architecture. This architecture is equally applicable in both campus and branch deployments. The core components of this architecture are:

- Cisco Unified Wireless Network Architecture
- Cisco Campus Architecture
- Cisco Branch Architecture

The Cisco Unified Wireless Network Architecture provides the core mobility services platform securing the wireless environment as well as all the functions required to secure the wireless deployment itself. The underlying campus and branch architectures provide a secure high performance, high availability network platform for mobility services. This provides a common wired and wireless platform for the integration of security services, allowing a common security architecture to be developed for all network clients and traffic types.

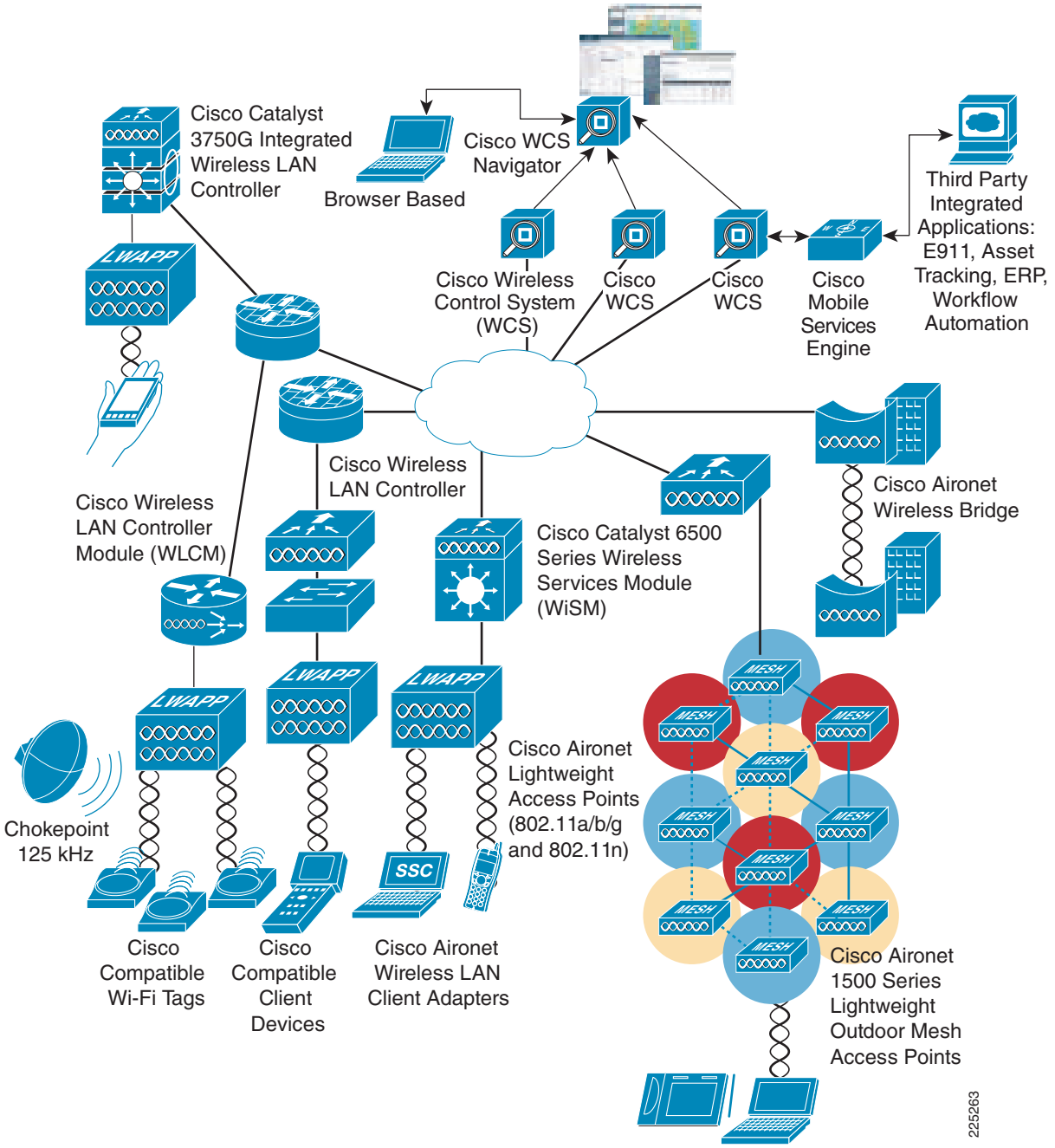
Cisco Unified Wireless Network

WLANs in the enterprise have emerged as one of the most effective means for connecting to a network. The Cisco Unified Wireless Network is a unified wired and wireless network solution that addresses the wireless network security, deployment, management, and control aspects of deploying a wireless network. It combines the best elements of wireless and wired networking to deliver secure, scalable wireless networks with a low total cost of ownership. Figure 2-1 shows the elements of the Cisco Unified Wireless Network.

The following five interconnected elements work together to deliver a unified enterprise-class wireless solution:

- Client devices
- Access points
- Wireless controllers
- Network management
- Mobility services

Figure 2-1 Cisco Unified Wireless Architecture Overview



Beginning with a base of client devices, each element adds capabilities as the network needs evolve and grow to create a comprehensive, secure WLAN solution. The Cisco Unified Wireless Network cost-effectively addresses the WLAN security, deployment, management, and control issues facing enterprises. This framework integrates and extends wired and wireless networks to deliver scalable, manageable, and secure WLANs with the lowest total cost of ownership. The Cisco Unified Wireless Network provides the same level of security, scalability, reliability, ease of deployment, and management for wireless LANs that organizations expect from their wired LANs.

For more information about the Cisco Unified Wireless Network, refer to the following URL: http://www.cisco.com/go/unifiedwireless

The components required for secure deployment and operations of a wireless network are built into the Cisco Unified Wireless Network infrastructure. Leveraging Wireless LAN controllers, access points and wireless management system provide comprehensive wireless security, reducing capital costs while streamlining security operations. Cisco has the benefit of being both a wireless company as well as a network security company. As such, Cisco brings many advanced network security technologies to bear on securing wireless networks. Leveraging the features and functions of our network security portfolio delivers a greater degree of control over wireless networks, users, and their traffic. Furthermore, supplementing wireless security with wired network security provides layered defenses which deliver more thorough protection, with greater accuracy and operational efficiency for both network operations and security operations teams within IT departments.

Wireless, due to its over the air transmission, has unique security requirements. The primary security concerns for a wireless network are:

- Rogue access points and clients that can create backdoor access to the company's network.
- Hacker access points, such as evil twins and honeypots, that try to lure your users into connecting to them for purposes of network profiling or stealing proprietary information.
- Denial of service that disrupts or disables the wireless network.
- Over the air network reconnaissance, eavesdropping, and traffic cracking. This is now primarily a legacy issue as the wireless industry has done a good job creating standard approaches to user authentication and traffic encryption via 802.11i and WPA.
- Controlling the networks wireless users connect to, especially when they are outside of the office.
- Wireless security for guest users.

Security event management and reporting on all of these functions, complete with physical location tracking of where the security event took place on the network, is key to any robust wireless security solution.

All of these concerns are addressed by security technologies built-in to the wireless controllers, access points and WCS management system that comprise the Cisco Unified Wireless Network infrastructure. The same wireless gear that provides connectivity to users also provides security for the entire deployment. A built-in wireless intrusion prevention system detects and mitigates rogue access points and clients, as well as DoS attacks, hacker access points, network reconnaissance, eavesdropping, and attempted authentication and encryption cracking. Furthermore, Cisco can provide wireless IPS monitoring from the same access points that service user traffic, as well as provide full-time dedicated wireless IPS monitoring. Providing both approaches enables site-specific flexibility based on network security policies, which reduces the high infrastructure costs associated with stand-alone wireless intrusion prevention systems.

At Cisco, we believe networks should be self-defending. Providing a hardened network core that is impenetrable to attacks is better than simply detecting an attack after the damage is done. To this end Cisco's Management Frame Protection renders most wireless attacks ineffective, providing a proactive layer of attack prevention in addition to the wireless intrusion prevention system.

Secure guest access management is also integrated in the Cisco Unified Wireless Network infrastructure, providing captive guest user portal, network segmentation, and full guest management functionality. Finally, wrapping all this together is the WCS management system that provides full configuration management, security event aggregation, and security reporting for all of the embedded security solutions outlined.

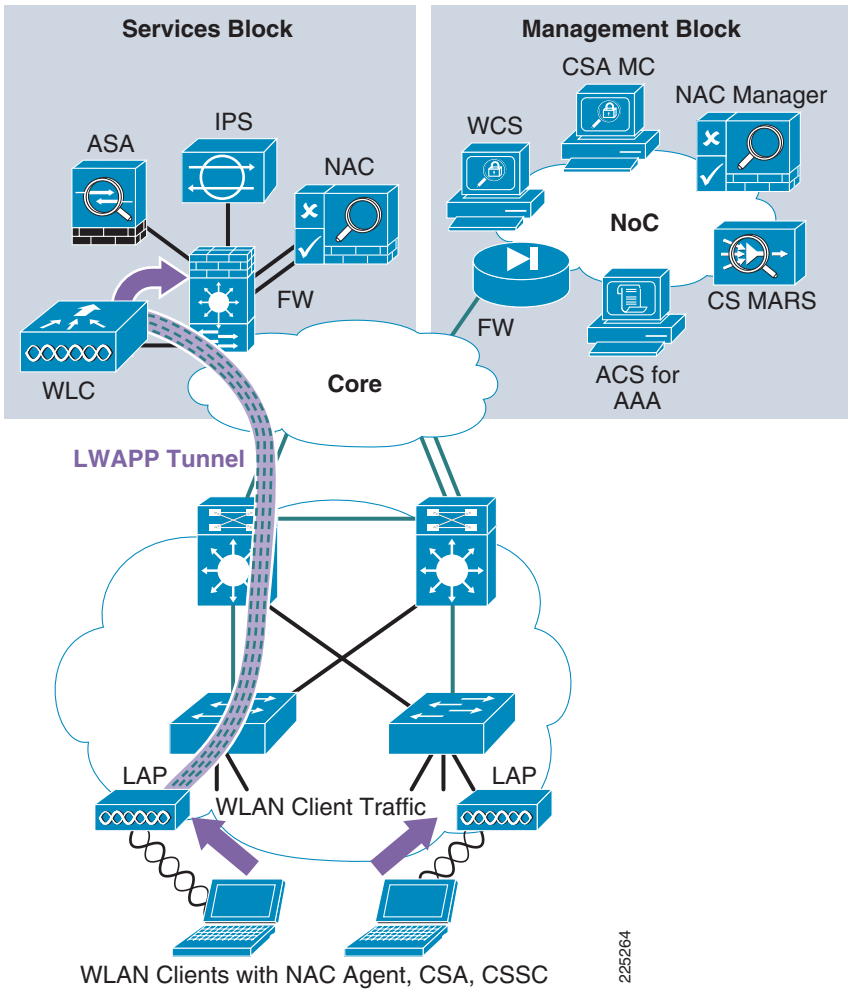
As mentioned earlier, Cisco can further supplement the built-in wireless security with technologies from the Cisco network security portfolio, thus providing a layered approach to wireless security. Leveraging network security platforms, such as Cisco wired intrusion prevention, Network Admission Control Appliance, the Cisco MARS security information management system, and Cisco Security Agent for advanced client security, delivers wired/wireless security collaboration that increases and extends network protection against malware, such as worms and viruses, enforces client security posture, and provides network-wide security event aggregation, analysis, and reporting.

Secure Wireless Architecture

The Secure Wireless Solution Architecture consists of a WLAN security component and network security components. The Cisco Unified Wireless Network provides the WLAN security core that integrates with other Cisco network security components to provide a complete solution. The Cisco Unified Wireless Network Architecture provides a mechanism to tunnel client traffic to the wireless LAN controller in a campus service block. The services block provides a centralized location for applying network security services and policies such as NAC, IPS, or firewall. In addition to the components protecting the network in the services block, the Cisco Security Agent provides addition protection network, as well as protecting the mobile client.

At Cisco, wired/wireless collaboration does not just mean putting more boxes in the network. It is the purpose-built linkages that have been built between Cisco's wired and wireless security technologies to deliver a superset of security functionality and protection.

Figure 2-2 Secure Wireless Architecture Overview

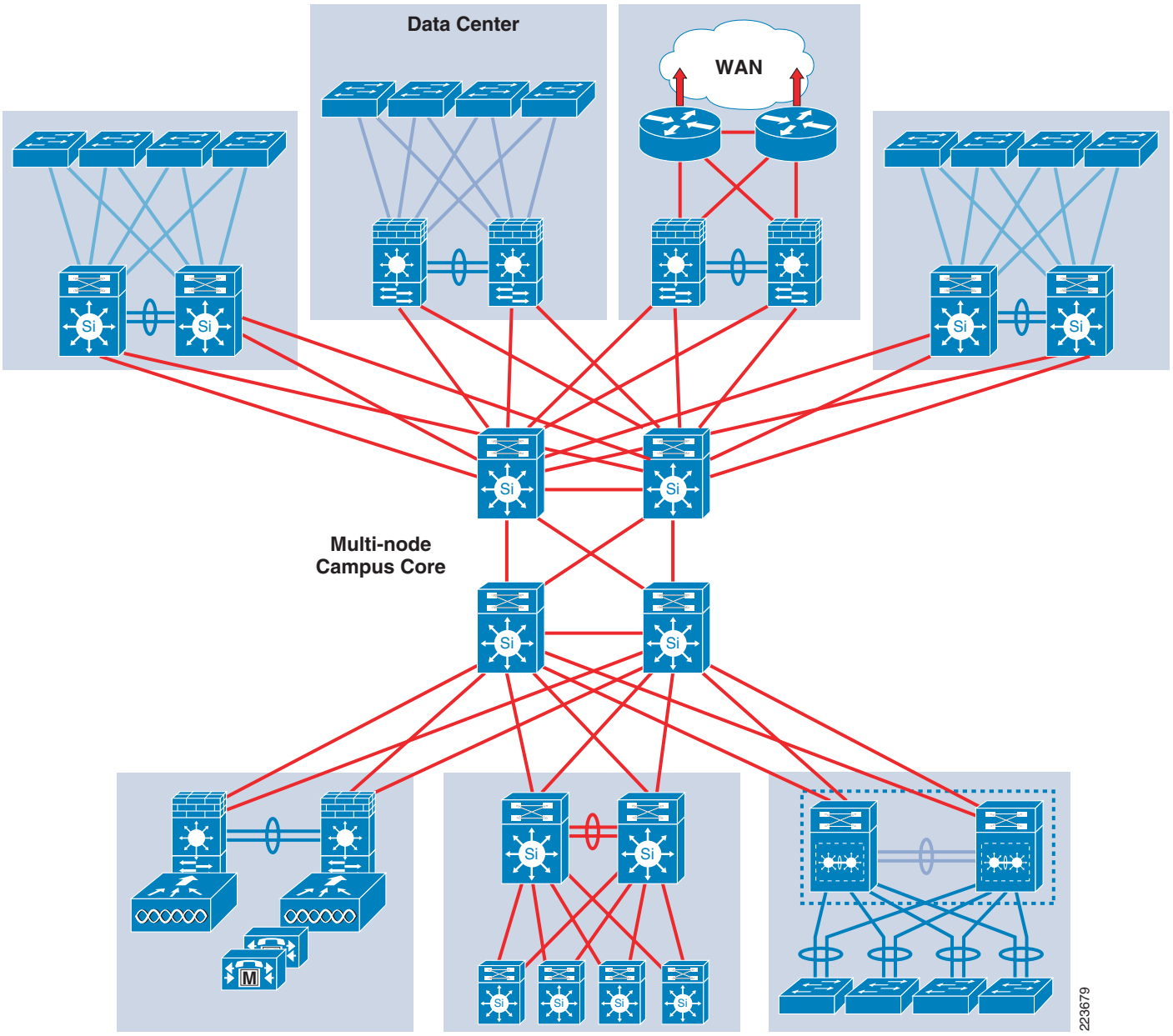


Campus Architecture

The overall campus architecture, as shown in Figure 2-3, is more than the fundamental hierarchical router and switch design. While hierarchies such as access, distribution, and core are fundamental to how to design and build campus networks, they do not address the underlying questions about what a campus network does. The campus network provides services that are used to build the secure wireless solutions. Services such as these provide the foundations for the Secure Wireless Solution:

- High availability
- Access services
- Application optimization and protection services
- Virtualization services
- Security services
- Operational and management services

Figure 2-3 Campus Architecture



Branch Architecture

The full service branch provides the same solutions and services to a branch as are available for the campus. This includes security and wireless, and the Secure Wireless solution is equally applicable for branch deployments as it is for the campus.

There are a number of WLAN, firewall, and NAC options for a branch, including either an H-REAP, WLAN Controller Module (WLCM), 21XX WLC, or larger WLCs, PIX, ASA, or IOS Firewalls, NAC appliances or NAC modules, and IPS appliances or IPS Modules. It is not possible to include all the different permutations in this design guide, so the branch design focuses on using products that are more

typical for branch deployments and deployments and products that are substantially different from those in campus examples. Therefore, this design guide uses H-REAP and the 2106 WLC, IOS firewall, and the IPS and NAC modules. A schematic of the architecture is shown in Figure 2-4.

Figure 2-4 Branch Architecture