Wireless and Network Security Integration Solution Overview

Solution Overview

Introduction

Enterprise businesses are being transformed to meet the evolving challenges of today's global business economy. New innovations and new business models are enabling new kinds of productivity, competitive advantage, revenue growth, and efficiency that drive the top line and the bottom line. Employee and customer expectations are rising, demanding real-time information anytime and anywhere, and collaboration beyond traditional borders.

Security is fundamental to the ability to leverage, with confidence, these rich services that are critical to business success. A Cisco unified network, featuring both wired and wireless access, is the platform that enables the Enterprise to meet these challenging business needs while maintaining operational reliability, scalability and efficiency, and without compromising security. The comprehensive and diverse Cisco security portfolio enables the complex security challenges faced in this environment to be addressed through an integrated, defense-in-depth approach to security that is embedded in end-to-end solution architectures.

The Wireless and Network Security Integration solution illustrates how to extend this integrated, defense-in-depth approach to security to encompass the mobility services offered by a wireless LAN. Mobility is a critical service for enterprises, offering employees greater flexibility, and enabling increased productivity, through pervasive access to network resources and applications. However, this service offering must comply with the defined network security policies and integrate with the end-to-end network security strategies in order to be compliant, effective and efficient.

The *Wireless and Network Security Integration Solution Design Guide* provides architectural, design and implementation guidelines on how to extend and integrate wired-side network security to the Cisco Unified Wireless Network and mobile clients. It uses the comprehensive wireless security features of the Cisco Unified Wireless Network but its primary focus is on the complementary wired-side network security features of the Cisco security portfolio and how they can be integrated to provide a more comprehensive security solution. This enables an enterprise to deploy and enforce a common network security policy that is inclusive of both wired and wireless network access methods, enabling consistent, end-to-end policy enforcement and more effective threat detection and mitigation.

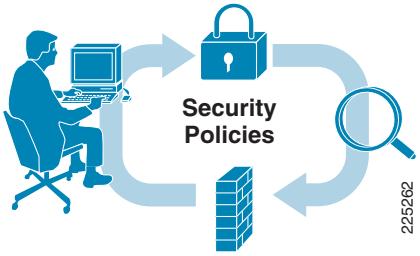
Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

The Wireless and Network Security Integration solution illustrates how to extend an integrated, defense-in-depth approach to security to encompass the Cisco Unified Wireless Network and mobile clients. It leverages the rich and diverse elements of the Cisco security portfolio to complement the wireless security features of the Cisco Unified Wireless Network, delivering a comprehensive solution that enables consistent, end-to-end policy enforcement and effective threat detection and mitigation across both wired and wireless networks.

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.

Figure 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” of the *Wireless and Network Security Integration Design Guide*. 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 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 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, 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.

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.

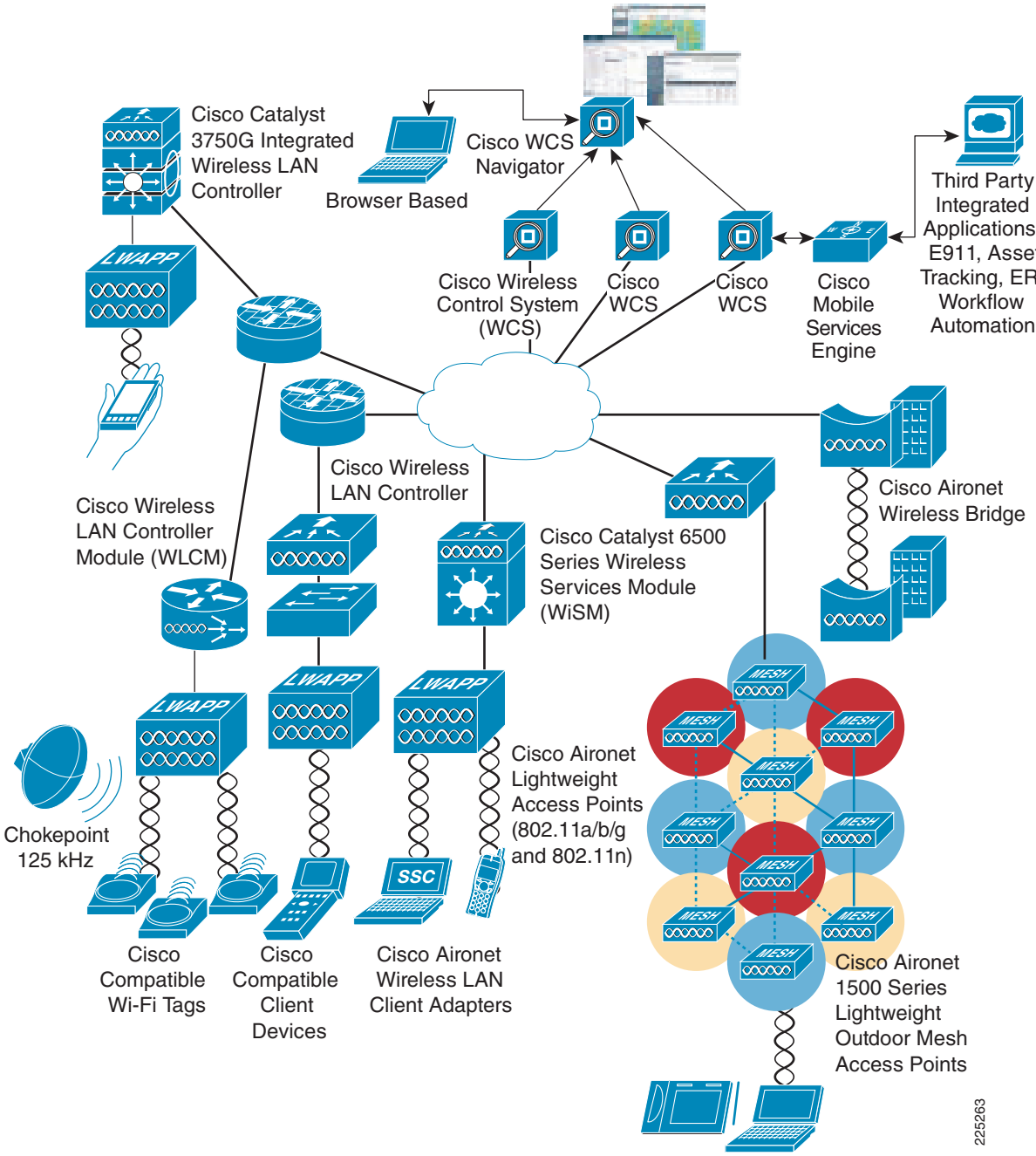
Cisco Unified Wireless Network

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 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
- World-class network management
- Mobility services

Figure 2 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 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.

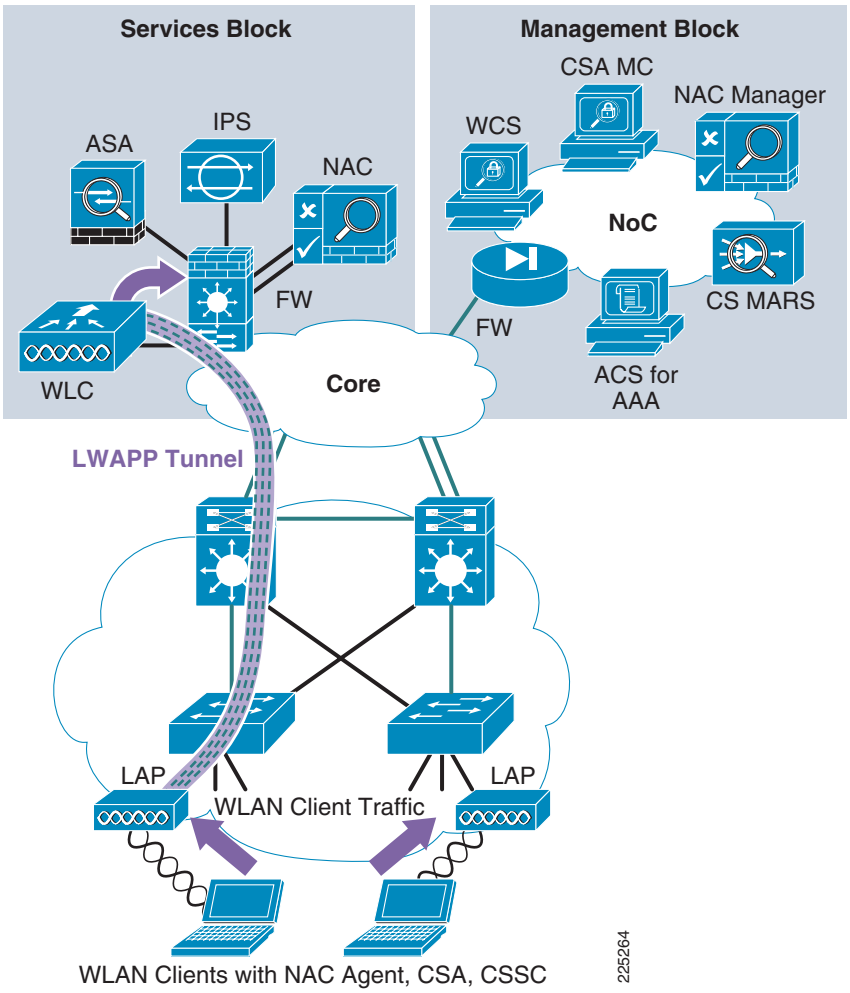
As mentioned earlier, Cisco can further supplement the built-in wireless security with technologies from the Cisco network security portfolio, thus providing a layered approach to wireless security. Leveraging network security platforms, such as Cisco wired intrusion prevention, Network Admission Control 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 (see Figure 3) . 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 3 Secure Wireless Architecture Overview

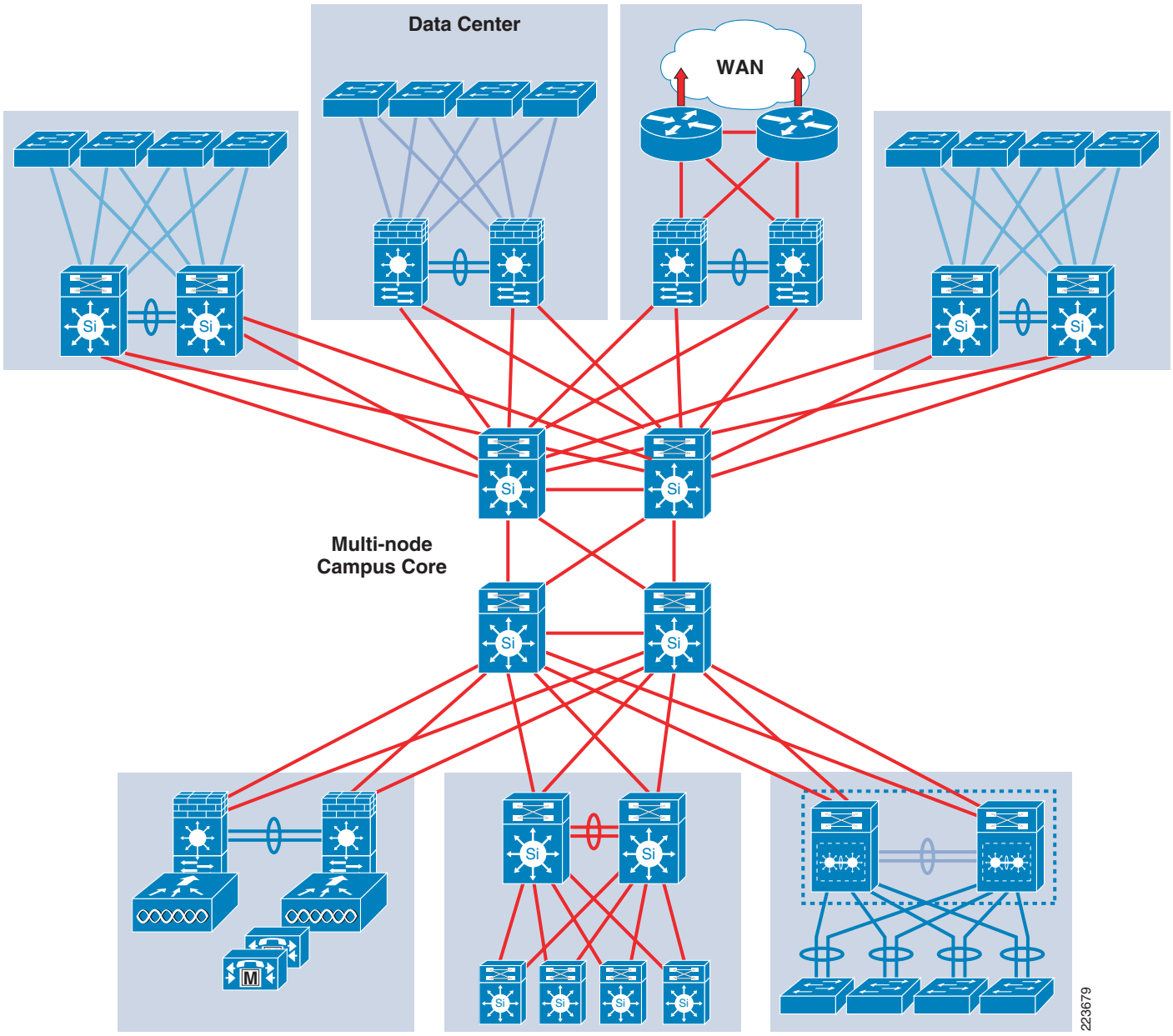


Campus Architecture

The overall campus architecture, as shown in Figure 4, 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 4 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 5.

Figure 5 Branch Architecture