CHAPTER 5

Medianet Security Design Considerations

A medianet is the foundation for media-rich collaboration across borderless networks. The availability and overall security of a medianet is thus critical to global business operations.

The security challenge is enabling an enterprise to confidently embrace and deliver these rich global collaboration services without compromising the overall security posture of the company.

The chapter illustrates the key strategies for enabling secure collaboration by employing a defense-in-depth approach that extends and integrates consistent, end-to-end security policy enforcement, and system-wide intelligence, across an enterprise medianet.

An Introduction to Securing a Medianet

The security of a medianet is addressed as two broad categories:

- Medianet foundation infrastructure

  This consists of the end-to-end network infrastructure and services that are fundamental to a medianet, including switches, routers, wireless infrastructure, network clients, servers, baseline network services, as well as the WAN and other elements that enable pervasive access to medianet services.

- Medianet collaboration services

  This consists of the media-rich collaboration and communication services that a medianet may support, such as TelePresence, Digital Media Systems (DMS), IP Video surveillance (IPVS), Unified Communications, desktop video and WebEx conferencing, along with their associated infrastructure and clients.

In order to secure a medianet, Cisco SAFE guidelines are applied to these two broad categories of a medianet. The security of both being critical to the delivery of pervasive secure collaboration.

Medianet Foundation Infrastructure

The network infrastructure and clients of a medianet are its fundamental elements. Security of these medianet clients and infrastructure thus provides the secure foundation for all the collaboration services that a medianet enables. Without the security of this foundational element, secure collaboration is impossible to deliver and any additional security measures are futile.

The Cisco SAFE guidelines must be applied to this fundamental area and each of its elements in order to provide a secure medianet foundation.

Medianet Collaboration Services

Each of the collaboration and communication services deployed on a medianet must each be assessed and secured in accordance with security policy and by applying the Cisco SAFE guidelines. This requires detailed analysis of the platforms and protocols used, the traffic flows and communication points, as well as possible attack vectors. The extension and integration of current, and possibly new, security techniques to each of these services can then be developed and deployed.

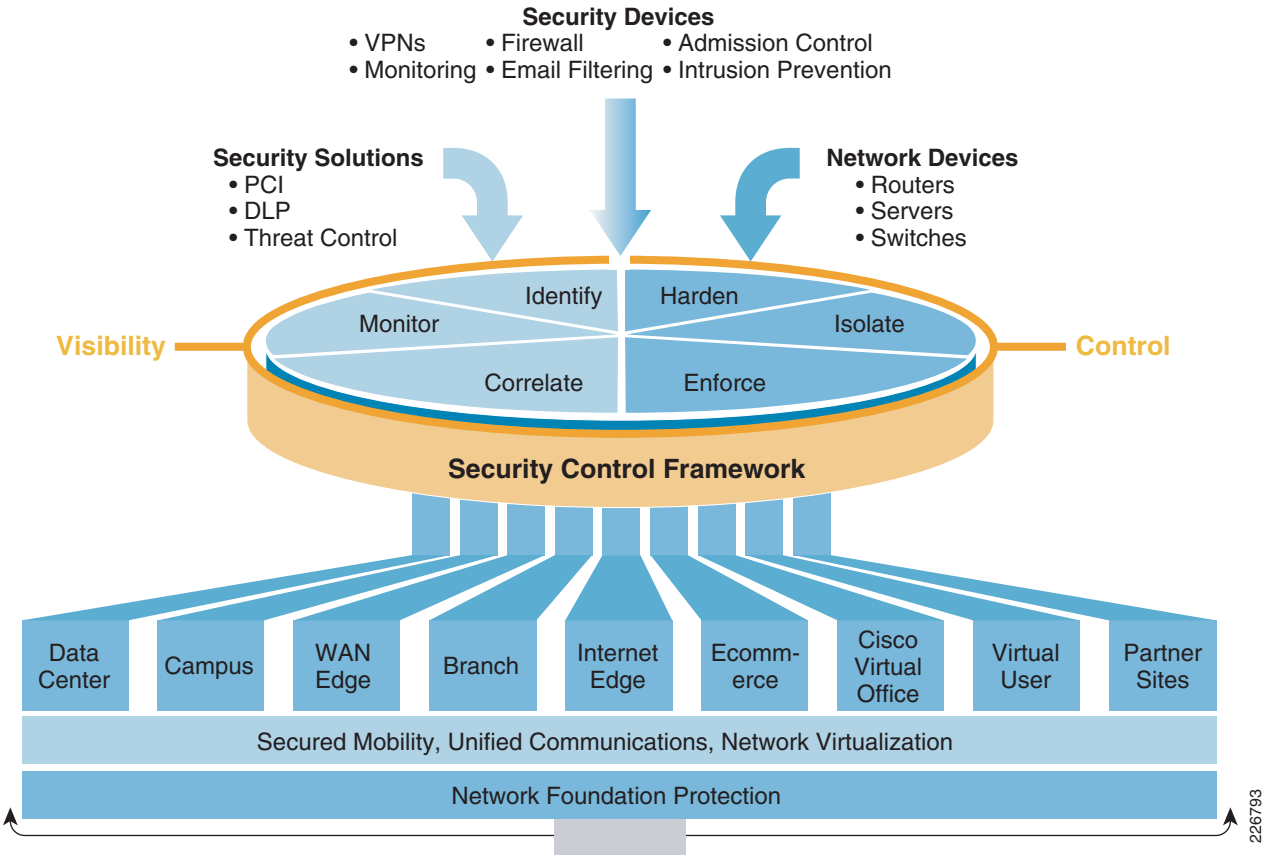
The implementation details may vary but the Cisco SAFE guidelines provide a consistent blueprint of the security considerations that need to be addressed.

Cisco SAFE Approach

Cisco SAFE provides a reference guide, an architecture and design blueprints for consistent, end-to-end security policy enforcement and system-wide intelligence. We will apply Cisco SAFE to a medianet in order to extend this approach to all elements of a medianet.

The Cisco SAFE approach includes proactive techniques to provide protection from initial compromise. This includes Network Foundation Protection, endpoint security, web and E-mail security, virtualization and network access control, as well as secure communications. These are complemented by reactive techniques that provide the ability to identify anomalous activity on the network and, where necessary, mitigate their impact. This includes telemetry, event correlation, firewall, IPS, data loss prevention and switching security.

Figure 5-1 Cisco SAFE



For more information about Cisco SAFE, see the link referenced in Medianet Security Reference Documents, page 5-12.

Security Policy and Procedures

Every organization should have defined security policies and procedures that form the basis of a strong security framework. These policies concisely define the required security actions and may, in turn, specify associated standards and guidelines. Procedures define how these policy goals are to be accomplished.

Security policies and procedures must be in place in order to achieve consistent, effective network security. The security guidelines provided in this chapter can be leveraged to enforce these policies, according to the specific policy requirements.

For more information on developing and implementing a security policy, the SANS Technology Institute offers some excellent resources including training, guidelines and sample security policies, see Medianet Security Reference Documents, page 5-12.

Security of Medianet Foundation Infrastructure

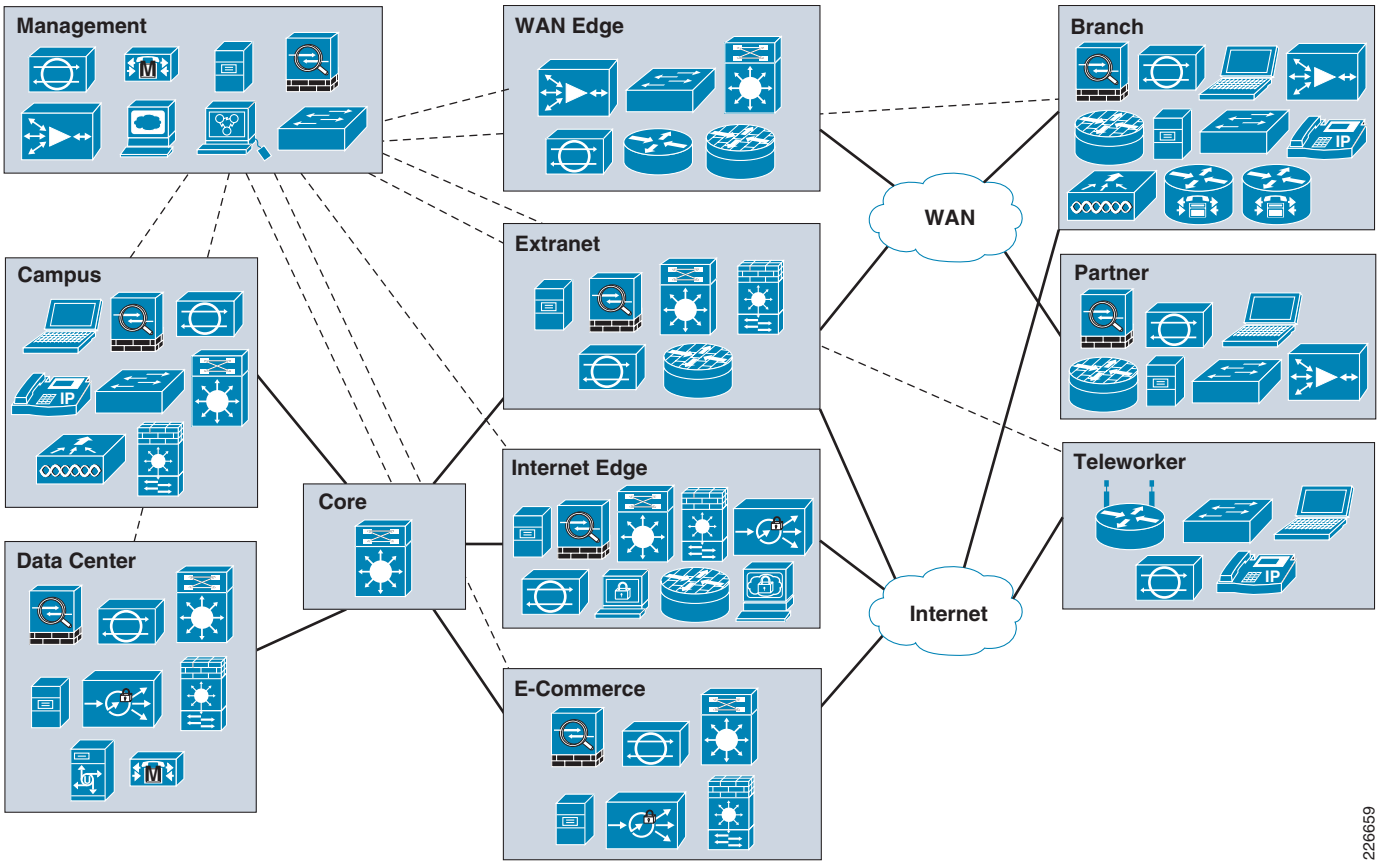
The security of this foundational element of a medianet is critical to the security of all services that a medianet enables. If the medianet itself is vulnerable, fundamental network services are vulnerable and thus, all additional services are vulnerable. If the clients that access a medianet are vulnerable, any hosts, devices or services they have access to are vulnerable.

To address this area, we can leverage the Cisco SAFE reference guide to provide the fundamental security guidelines. This chapters provides a brief overview of the key elements of Cisco SAFE; for the complete *Cisco SAFE Reference Guide* and additional Cisco SAFE collateral, see the link referenced in Medianet Security Reference Documents, page 5-12.

Security Architecture

The Cisco SAFE architecture features a modular design with the overall network represented by functional modules, including campus, branch, data center, Internet edge, WAN edge, and core. This enables the overall security design, as well as the security guidelines for each individual module to be leveraged, applied, and integrated into a medianet architecture.

Figure 5-2 Cisco SAFE Architecture



The Cisco SAFE architecture features virtualization and segmentation to enable different functional and security domains, secure communications for data in transit, centralized management and control for ease of operations and consistent policy enforcement, along with fundamental design principles such as the Cisco Security Control Framework and the architecture lifecycle.

Network Foundation Protection

The focus of Network Foundation Protection (NFP) is security of the network infrastructure itself, primarily protecting the control and management planes of a medianet. NFP mitigates unauthorized access, denial-of-service (DoS) and local attacks such as man-in-the-middle (MITM) attacks that can be used to perform eavesdropping, sniffing, and data steam manipulation.

The key areas NFP addresses include the following:

- Secure Device Access
- Service Resiliency
- Network Policy Enforcement
- Routing Security
- Switching Security

Integration of these elements is critical to medianet security and, unless implemented, renders any more advanced techniques futile. For instance, if a malicious user can access the local LAN switch using a simple password, they will have access to all traffic flowing through that switch, can reconfigure the device and mount a vast array of attacks.

Endpoint Security

Endpoints are exposed to a wide range of threats, including malware, botnets, worms, viruses, trojans, spyware, theft of information, and unauthorized access. Hardening these endpoints is thus critical to overall network security, protecting both the endpoint itself, the data they host and any network to which they connect.

Endpoint security includes the following:

- Operating system and application hardening

  It is critical that the operating system and applications running on an endpoint are hardened and secured in order to reduce the attack surface and render the endpoint as resilient as possible to attacks. This involves implementing a secure initial configuration, as well as the regular review of vulnerabilities and the timely application of any necessary updates and security patches.

- User education and training

  End-users should receive ongoing education and training to make them aware of the critical role they play in mitigating existing and emerging threats, including security awareness, protection of corporate data, acceptable use policy and minimizing risk exposure. This should be presented in a simple, collaborative way to reinforce corporate policies.

- Host-based IPS (HIPS)

  HIPS provides endpoints with protection against both known and zero-day or unpatched attacks, whichever network they may be connected to. This is achieved through both signature- and behavior-based threat detection and mitigation that are key features of HIPS. This functionality is offered by the Cisco Security Agent (CSA), along with the ability to enforce policy and perform data loss prevention on the endpoint itself. Some of this functionality may also be available in the host operating system.

- Cisco Security Services Client (CSSC)

  The CSSC is a software supplicant that enables identity-based access and policy enforcement on a client, across both wired and wireless networks. This includes the ability to enforce secure network access controls, such as requiring the use of WPA2 for wireless access and automatically starting a VPN connection when the endpoint is connected to a non-corporate network.

For more information about Cisco CSA and CSSC, see Medianet Security Reference Documents, page 5-12.

Web Security

The web is increasingly being used to distribute malware and, whilst malicious sites continue to operate as one key delivery method, the majority of today's web-based threats are delivered through legitimate websites that have been compromised. Add to this the threats posed by spyware, traffic tunneling, client usage of unauthorized sites and services, and the sharing of unauthorized data, and it is easy to see why web security is critical to any organization.

Cisco offers four web security options:

- Cisco Ironport S-Series Web Security Appliance (WSA)

  An on-premise, dedicated appliance offering high performance web-based threat mitigation and security policy enforcement. The WSA provides web usage controls, known and unknown malware protection through multiple scanning engines and reputation filtering, data loss prevention, URL filtering, protocol tunneling protection and malware activity monitoring.

- Cisco ScanSafe

  Hosted web security (SaaS) offering web-based malware protection in the cloud. ScanSafe provides real-time scanning of inbound and outbound web traffic for known and unknown malware, as well as monitoring of malware activity.

- Cisco ASA 5500 Series Content Security and Control Security Services Module (CSC-SSM)

  Service module for the Cisco ASA 5500 Series providing comprehensive antivirus, anti-spyware, file blocking, anti-spam, anti-phishing, URL blocking and filtering, and content filtering.

- Cisco IOS Content Filtering

  Integrated web security in Cisco IOS platforms offering whitelist and blacklist URL filtering, keyword blocking, security rating, and category filtering

For more information about Cisco Ironport WSA, ScanSafe, and Cisco IOS security, see Medianet Security Reference Documents, page 5-12.

E-mail Security

E-mail is one of the primary malware distribution methods, be it through broad phishing attacks, malware in attachments or more sophisticated, targeted E-mail attacks. E-mail spam is a major revenue generator for the miscreant community, and E-mail is one of the most common methods for unauthorized data exchange. Consequently, E-mail security is critical to an enterprise.

Cisco offers E-mail security through the Ironport C-Series E-mail Security Appliance (ESA), providing spam filtering, malware filtering, reputation filtering, data loss prevention (DLP) and E-mail encryption. This is available in three deployment options:

- On-premise appliance enforcing both inbound and outbound policy controls.
- Hybrid Hosted service offering an optimal design that features inbound filtering in the cloud for spam and malware filtering, and an on-premise appliance performing outbound control for DLP and encryption.
- Dedicated hosted E-mail security service (SaaS) offering the same rich E-mail security features but with inbound and outbound policy enforcement being performed entirely in the cloud.

For more information on Cisco Ironport ESA, see Medianet Security Reference Documents, page 5-12.

Network Access Control

With the pervasiveness of networks, controlling who has access and what they are subsequently permitted to do are critical to network and data security. Consequently, identity, authentication and network policy enforcement are key elements of network access control.

Cisco Trusted Security (TrustSec) is a comprehensive solution that offers policy-based access control, identity-aware networking, and data confidentiality and integrity protection in the network. Key Cisco technologies integrated in this solution include:

- Cisco Catalyst switches providing rich infrastructure security features such as 802.1X, web authentication, MAC authentication bypass, MACSec, Security Group Tags (SGT), and a selection of dynamic policy enforcement mechanisms and deployment modes.
- Cisco Secure Access Control System (ACS) as a powerful policy server for centralized network identity and access control.
- Cisco Network Access Control (NAC) offering appliance-based network access control and security policy enforcement, as well as posture assessment.

For more information about Cisco TrustSec, see Medianet Security Reference Documents, page 5-12.

User Policy Enforcement

User policy enforcement is a broad topic and, based on the defined security policy, may include:

- Acceptable Use Policy (AUP) Enforcement

  For example, restricting web access and application usage, such as P2P applications and adult content. This can be achieved through Cisco IOS Content Filtering and Ironport WSA Web Usage Controls (WUC).

- Data Loss Prevention (DLP)

  DLP is often required for regulatory purposes and refers to the ability to control the flow of certain data, as defined by security policy. For example, this may include credit card numbers or medical records. DLP can be enforced at multiple levels, including on a host, through the use of Cisco Security Agent (CSA), in E-mail through integration of the Ironport ESA and via web traffic through integration of the Ironport WSA.

Secure Communications

The confidentiality, integrity, and availability of data in transit is critical to business operations and is thus a key element of network security. This encompasses the control and management, as well as data planes. The actual policy requirements will typically vary depending on the type of data being transferred and the network and security domains being transited. This is a reflection of the risk and vulnerabilities to which data may be subject, including unauthorized access, and data loss and manipulation from sniffing or man-in-the-middle (MITM) attacks.

For example, credit card processing over the Internet is governed by regulatory requirements that require it to be in an isolated security domain and encrypted. A corporate WLAN may require the use of WPA2 for internal users and segmented wireless access for guests.

Secure communications is typically targeted at securing data in transit over WAN and Internet links that are exposed to external threats, but the threats posed by compromised internal hosts is not to be overlooked. Similarly, sensitive data or control and management traffic transiting internal networks may also demand additional security measures.

Cisco offers a range of VPN technology options for securing WAN access, either site-to-site or for remote access, along with PKI for secure, scalable, and manageable authentication. Cisco VPN technologies include MPLS, IPSec VPN, SSL VPN, GRE, GETVPN, DMVPN.

For more information about Cisco VPN technologies, see Medianet Security Reference Documents, page 5-12.

Firewall Integration

Firewall integration enables extended segmentation and network policy enforcement of different security policy domains. For example, to isolate and secure servers that store highly sensitive data or segment users with different access privileges.

In addition, firewall integration offers more advanced, granular services, such as stateful inspection and application inspection and control on Layer 2 through Layer 7. These advanced firewall services are highly effective of detecting and mitigating TCP attacks and application abuse in HTTP, SMTP, IM/P2P, voice, and other protocols.

Cisco offers the following two key firewall integration options:

- Adaptive Security Appliance (ASA) 5500 Series

  Dedicated firewall enabling a highly scalable, high performance, high availability and fully featured deployment that is available on a range of platforms. The ASA 5500 Series also features the Cisco ASA Botnet Traffic Filter, providing real-time traffic monitoring, anomalous traffic detection, and reputation-based control that enables the mitigation of botnets and other malware that shares phone-home communication patterns.

- Cisco IOS Firewall

  Cost-effective, integrated firewall offered as a classic, interface-based firewall or as a zone-based firewall (ZBFW) that enables the application of policies to defined security zones.

For more information about the Cisco ASA 5500 Series and Cisco IOS Firewall, see Medianet Security Reference Documents, page 5-12.

IPS Integration

The integration of network IPS provides the ability to accurately identify, classify, and stop malicious traffic on the network, including worms, spyware, adware, attacks, exploits, network viruses, and application abuse. Cisco IPS offers dynamic and flexible signature, vulnerability, exploit, behavioral and reputation-based threat detection and mitigation, as well as protocol anomaly detection.

In addition, the collaboration of Cisco IPS with other Cisco devices provides enhanced visibility and control through system-wide intelligence. This includes host-based IPS collaboration with Cisco Security Agent (CSA), reputation-based filtering and global correlation using SensorBase, automated threat mitigation with the WLAN controller (WLC), multi-vendor event correlation and attack path identification using Cisco Security Monitoring, Analysis, and Response System (CS-MARS), and common policy management using Cisco Security Manager (CSM).

Cisco IPS is available in a wide range of network IPS deployment options, including:

- Cisco IPS 4200 Series Appliances

  Dedicated high scalability, high availability hardware appliances.

- Integrated modules for ISR, ASA and Catalyst 6500

  Offering flexible deployment options but consistent rich signature set and policy enforcement

- Cisco IOS IPS

  Cost-effective integrated IPS with sub-set of common signatures.

For more information about the Cisco IPS offerings, see Medianet Security Reference Documents, page 5-12.

Telemetry

Visibility into the status of a medianet and the identification of any anomalous activity is critical to overall network security. Security monitoring, analysis & correlation is thus essential to the timely and accurate detection and mitigation of anomalies.

The baseline elements of telemetry are very simple and inexpensive to implement, and include:

- Time Synchronization

  Synchronize all network devices to the same network clock by using Network Time Protocol (NTP) to enable accurate and effective event correlation.

- Monitoring of System Status Information

  Maintain visibility into overall device health by monitoring CPU, memory and processes.

- Implementation of CDP Best Common Practices

  Enable CDP on all infrastructure interfaces for operational purposes but disable CDP on any interfaces where CDP may pose a risk, such as external-facing interfaces.

- Remote Monitoring

  Leverage syslog, SNMP and additional telemetry techniques, such as Netflow, to a centralized server, such as CS-MARS, for cross-network data aggregation. This enables detailed and behavioral analysis of the data which is key to traffic profiling, anomaly-detection and attack forensics, as well as general network visibility and routine troubleshooting.

For more information about management and visibility in a medianet, see Chapter 6, “Medianet Management and Visibility Design Considerations.”

Security of Medianet Collaboration Services

Once the foundational elements of a medianet are secured, the next step is to address the security of each of the collaboration and communication services that a medianet is being used to deliver, whether it is TelePresence, DMS, IPVS, Unified Communications, desktop video, WebEx conferencing, or any other collaboration and communication service.

As each collaboration service is deployed, the service must be well-researched and understood, security policy must be reviewed and applied, and network security measures extended to encompass it. To achieve this, the same Cisco SAFE guidelines are applied to each medianet collaboration service and their associated infrastructure, enabling consistent, end-to-end, security policy enforcement.

Security Policy Review

Prior to deployment of a new service, it is critical to review it in relation to security policy. This will initially require detailed analysis of the service itself, including the protocols it uses, the traffic flows and traffic profile, the type of data involved, as well as its associated infrastructure devices and platforms. This enables a security threat and risk assessment to be generated that identifies possible attack vectors and their associated risk. In addition, there may be regulatory requirements to take into consideration.

The service can then be reviewed in relation to security policy in order to determine how to enforce the security policy and, if necessary, what changes are required to the policy. This is generally referred to as a policy impact assessment.

Reviewing a new service in relation to the security policy enables consistent enforcement that is critical to overall network security.

Architecture Integration

Integration of a new service into a medianet requires an assessment of the traffic flows, the roles of its associated infrastructure and the communications that take place, as well as an understanding of the current corporate network design. This enables the most appropriate deployment model to be adopted, including the appropriate segmentation of security domains.

For example, a WebEx Node resides on the corporate network, but communicates with the external WebEx cloud as well as internal clients. Consequently, the logical placement for this device, performing an intermediary role between internal clients and an external service, is the DMZ. For more information about WebEx Node integration, see Medianet Security Reference Documents, page 5-12.

Application of Cisco SAFE Guidelines

For each medianet collaboration service, we will apply the Cisco SAFE guidelines to enable the consistent enforcement of security policy. Taking each of the Cisco SAFE security areas, we will assess if and how they apply to this service and its associated infrastructure, and what additions or changes may need to be made to the current security measures. The Cisco SAFE security areas we will apply include:

- Network Foundation Protection (NFP)

  Hardening of each of the service infrastructure components and services, including secure device access and service resiliency. QoS and Call Admission Control (CAC) being two key features of service resiliency for media-rich communication services.

- Endpoint Security

  Hardening of each of the service endpoints and a review of current endpoint security policies. For instance, if the CSA Trusted QoS feature is currently employed, this may need to be modified to reflect the requirements of a new desktop video deployment.

- Web Security

  Extension of web security policies to the service, including perhaps the modification of web usage controls, DLP policies, and URL filtering. For instance, a WebEx Node should only connect to the WebEx Cloud and so corporate URL filtering policies may be modified to enforce this.

- E-mail Security

  A review of E-mail security policies may be required if the service involves the use of E-mail, either as an integral part of the service itself or as part of its monitoring and management.

- Network Access Control (NAC)

  Extension of network access control to the service, including identification, authentication and network policy enforcement of users and devices. This may involve the extension of policies to include service-specific policy enforcement, such as to restrict the authorized users, devices, protocols and flows of a particular service, thereby only granting minimum access privileges and reducing the risk exposure of the service endpoints.

- User Policy Enforcement

  A review of user policies may be required to reflect the new service offerings. For instance, to define the data sharing policy for external Cisco WebEx Connect Spaces.

- Secure Communications

  The path and risk exposure of data in transit must be assessed in order to deploy the most appropriate security solution. This may include the security of control and management planes, as well as the data plane. For example, the encryption of TelePresence media flows may be required if data traverses an insecure security domain or the media content is sensitive.

- Firewall Integration

  Firewall policies may need to be modified to allow firewall traversal for the service. For instance, if you wish to provide secure access to your UC infrastructure from external softphones, you may enable the ASA Phone Proxy feature.

- IPS Integration

  IPS integration and signature tuning may be required to ensure the accurate and timely detection and mitigation of anomalies in these new services. For instance, to identify SIP attacks or DoS attacks against UC servers.

- Telemetry

  Extension of monitoring to the new service in order to provide visibility into its operational status, to enable the detection of anomalous activity that may be indicative of an incident, as well as to record activity for detailed analysis and forensics.

Implementation involves leveraging the available security features on the service infrastructure devices themselves and those offered within the service, as well as extending existing or new network security techniques to these new services.

Since the actual implementation of security for each service is very specific and often very different, it should be addressed as an integral part of the overall design and deployment of each service. For more information on securing each of the collaboration services, see Medianet Security Reference Documents, page 5-12 for additional collateral.

Medianet Security Reference Documents

- ASA 5500 Series
  http://www.cisco.com/go/asa
- Cisco Data Center Security
  http://www.cisco.com/en/US/netsol/ns750/networking_solutions_sub_program_home.html
- Cisco IOS Content Filtering
  http://www.cisco.com/en/US/products/ps6643/index.html
- Cisco IOS Firewall
  http://www.cisco.com/en/US/products/sw/secursw/ps1018/index.html
- Cisco IOS NetFlow
  http://www.cisco.com/en/US/products/ps6601/products_ios_protocol_group_home.html
- Cisco IP Video Surveillance (IPVS)
  http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns819/landing_vid_surveillance.html
- Cisco IronPort C-Series E-mail Security Appliance (ESA)
  http://www.ironport.com/products/email_security_appliances.html
- Cisco IronPort S-Series Web Security Appliance (WSA)
  http://www.ironport.com/products/web_security_appliances.html
- Cisco Medianet
  http://www.cisco.com/web/solutions/medianet/index.html
- Cisco Network Admission Control (NAC)
  http://cisco.com/en/US/netsol/ns466/networking_solutions_package.html
- Cisco SAFE
  http://www.cisco.com/go/safe
- Cisco SAFE WebEx Node Integration
  http://www.cisco.com/en/US/docs/solutions/Enterprise/Video/WebEx_wpf.html
- Cisco ScanSafe Web Security
  http://www.scansafe.com/
- Cisco Secure Services Client (CSSC)
  http://cisco.com/en/US/products/ps7034/index.html
- Cisco Security Portfolio
  http://www.cisco.com/go/security
- Cisco Security Agent (CSA)
  http://www.cisco.com/go/csa
- Cisco Trust and Identity Management Solutions
  http://cisco.com/en/US/netsol/ns463/networking_solutions_sub_solution_home.html
- Cisco Trusted Security (TrustSec)
  http://www.cisco.com/en/US/netsol/ns774/networking_solutions_package.html

- Cisco Unified Communications (UC) Security

  http://www.cisco.com/en/US/netsol/ns340/ns394/ns165/ns391/networking_solutions_package.html
- Cisco VPN

  http://cisco.com/en/US/products/ps5743/Products_Sub_Category_Home.html
- Cisco WebEx Security Overview

  http://www.cisco.com/en/US/prod/collateral/ps10352/cisco_webex_security_overview.pdf
- SANS Policy Resources

  http://www.sans.org/security-resources/policies/