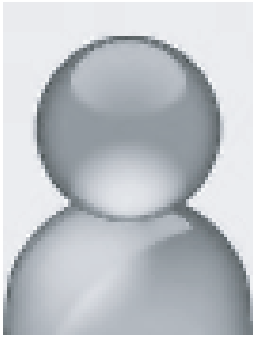
SAFE WebEx Node Integration Whitepaper

Last Updated: January 5, 2010

About the Author



Sherelle Farrington

Sherelle Farrington, Technical Leader, CMO Enterprise Solutions Engineering (ESE), Cisco Systems

Sherelle is a technical leader at Cisco Systems with over fifteen years experience in the networking industry, encompassing service provider and enterprise environments in the US and Europe.

During her more than ten years at Cisco, she has worked on a variety of service provider and enterprise solutions, and started her current focus on network security integration over four years ago. She has presented and published on a number of topics, most recently as one of the authors of the SAFE Reference Guide, the Wireless and Network Security Integration Solution design guide, and the Network Security Baseline paper.

CONTENTS

SAFE WebEx Node Integration Whitepaper

Introduction

The Cisco WebEx Node extends the Cisco WebEx Collaboration Cloud to the enterprise, providing significantly reduced Internet bandwidth consumption, along with improved response times, for internal WebEx client traffic. A SAFE WebEx Node integration ensures that these benefits are realized without impacting the overall security posture of the corporate network.

This document discusses how a SAFE WebEx Node integration can be achieved by applying the security principles of the Cisco SAFE security architecture to identify and address the specific security considerations for WebEx Node integration. These design and implementation guidelines enable a defense-in-depth approach to security that is critical for effective security and secure collaboration.

It is assumed that the reader is already familiar with the role and functionality of WebEx and the WebEx Node. The reader is also assumed to be familiar with the Cisco SAFE security architecture.

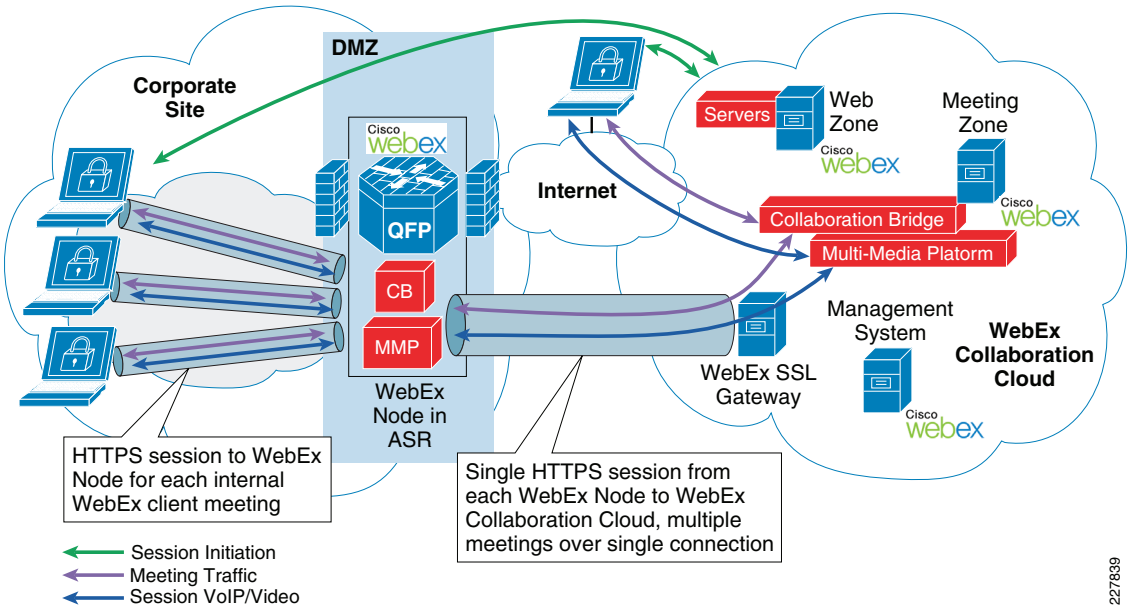
Cisco WebEx Node Overview

A WebEx Node achieves the Internet bandwidth and response time benefits it offers by deploying critical software components of the WebEx platform to the WebEx Node on a corporate site, offering a hybrid solution that blends the advantages of an onsite platform and a hosted solution. This reduces the number of WebEx streams to the WebEx Collaboration Cloud over corporate Internet connections that are, typically, costly and offer limited bandwidth, and provides local hosting and switching of WebEx streams to internal WebEx clients. This is achieved by a WebEx Node maintaining one stream per meeting to the WebEx Collaboration Cloud and sending a copy of that stream to each of the internal WebEx clients in that meeting. A WebEx Node can thus be thought of as a WebEx proxy and cache for internal WebEx client streams. This is true whether the internal WebEx clients are hosting or attending a meeting.

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

An illustration of a WebEx Node integration is shown in Figure 1.

Figure 1 WebEx Node Integration Architecture



A WebEx Node extends the WebEx Collaboration Cloud to a corporate site by initializing an HTTPS connection to the WebEx Collaboration Cloud. This secure extension of the WebEx Collaboration Cloud is established using strong, mutual authentication and features 256-bit Advanced Encryption Standard (AES) encryption for confidential communication over the Internet. It is over this single, secure HTTPS connection that all active WebEx meeting streams are transmitted to the WebEx Node for replication and transport to each of the internal WebEx clients.

Internal WebEx clients connect to a WebEx Node using HTTPS (128-bit AES encryption) in the same way as they connect directly to the WebEx Collaboration Cloud. The decision as to whether a WebEx client connects to a WebEx Node or directly to the WebEx Collaboration Cloud is performed automatically by the WebEx client and is transparent to the end-user. A WebEx Node hosts a HTTPS session for each internal WebEx client that has successfully chosen to connect to it, ensuring confidential communication over the corporate network.

WebEx client sessions via a WebEx Node benefit from a reduced Internet risk exposure since the WebEx Node, on behalf of the internal WebEx clients, establishes and maintains a single, secure connection to the WebEx Collaboration Cloud over the Internet and employs a strong encryption algorithm.

An internal WebEx client will select to connect to a WebEx Node, in preference to the WebEx Collaboration Cloud, based primarily on its responsiveness. A WebEx Node is configured with an internal hostname that will resolve to the WebEx Node IP address when clients are on the corporate network. Consequently, only internal WebEx clients are expected to connect to a WebEx Node.

The WebEx Node is currently available as a shared port adapter (SPA) for the Cisco ASR 1000 Series. The ASR provides network connectivity for the WebEx Node, logically acting as its network gateway. Traffic is passed between the ASR and the WebEx Node over the ASR backplane.

Cisco SAFE Overview

Cisco SAFE provides a security reference architecture and detailed design and implementation guidelines to effectively secure your network. The key security principles are as follows:

- *Network Foundation Protection*

  The baseline network infrastructure is critical to overall service availability. Consequently, it is critical to harden the network infrastructure itself by protecting the control and management planes, as well as preserving baseline service availability. This is achieved through secure device access, routing security, service resiliency, network policy enforcement, and switching security.

- *Threat Control and Containment*

  Incidents are a daily part of operations and appropriate tools and policies must be in place in order to handle them. These tools and techniques enable the accurate and timely detection and mitigation of anomalous activity across the end-to-end network. This is achieved through endpoint security, firewall integration, web security, E-mail security, IPS integration, and secure communications.

- *Monitoring, Analysis, and Correlation*

  Cross-network intelligence provides visibility into network activity that is critical to effective security. This is achieved through telemetry to gather system status, network status, and traffic monitoring information, along with intelligent systems to analyse the data and identify anomalies. This is provided by syslog, SNMP, centralized AAA, NTP and NetFlow, as well as Cisco ACS and CS-MARS.

These security guidelines should be reviewed and deployed on your network, in accordance with your security policies, in order to provide a secure network on which to integrate a WebEx Node. For more information on Cisco SAFE, refer to the *Cisco SAFE Reference Guide* listed in the "Reference Documents" section on page 14.

Security Considerations for WebEx Node Integration

A WebEx Node and the WebEx services it provides can be subject to a number of different attack vectors. We can group these into three key attack areas:

- WebEx Node as the target
  - Unauthorized access of a WebEx Node or its host platform
  - Denial-of-Service (DoS) attack against a WebEx Node or its host platform
- WebEx Node SSL sessions as the target
  - Attack against a WebEx Node SSL connection to the WebEx Collaboration Cloud
  - Attack against a WebEx client SSL connection to a WebEx Node
- WebEx Node as the launch pad for attacks
  - Compromised WebEx Node abuse to gain unauthorized access to the corporate network, launch a DoS attack or conduct any other malicious activity.

We apply the Cisco SAFE security principles and guidelines to WebEx Node integration in order to address all these security considerations.

Security Implementation for WebEx Node Integration

A SAFE WebEx Node integration involves the correct placement of a WebEx Node in the corporate network and extending the corporate security policies to this new hardware and new services. This is achieved through the application of each of the SAFE security principles to the WebEx Node and the services it provides. It is critical and assumed that the Cisco SAFE guidelines are already implemented on the corporate network.

Note that a WebEx Node is completely reliant on its host platform for availability. Consequently, the security of this host platform is critical to the security and availability of a WebEx Node and must be hardened according to the SAFE guidelines. In addition, if the host platform is hosting any other services, each must be assessed and secured accordingly.

Note that, as a general best practice, all network security controls should be complemented with ongoing end-user training and security awareness to be most effective.

WebEx Node Placement in an Enterprise

The configuration and operation of a WebEx Node is predominantly performed by Cisco WebEx. Consequently, since this device is partly managed and operated by an external third-party, the corporate DMZ is probably the most appropriate placement for it, though corporate policy will ultimately determine if this is the case.

Applying the SAFE guidelines for corporate DMZ design, WebEx Node integration will typically involve its placement behind an Internet-facing firewall and in front of corporate-facing firewalls, as illustrated in Figure 1 on page 6. This protects a WebEx Node from attacks launched from the Internet and also protects the corporate network from unauthorized access from a WebEx Node. The role of the firewalls is further discussed in the "Network Policy Enforcement for WebEx Node Integration" section on page 11.

For more information about SAFE DMZ guidelines, see the *Cisco SAFE Reference Guide* listed in the "Reference Documents" section on page 14.

Network Foundation Protection for WebEx Node Integration

Network Foundation Protection is focused on securing the network infrastructure and services themselves. In the case of a WebEx Node, this involves the WebEx Node itself, HTTPS from a WebEx Node to the WebEx Collaboration Cloud, and HTTPS from a WebEx client to a WebEx Node.

The security elements of Network Foundation Protection (NFP) are as follows:

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

Secure Device Access for WebEx Node Integration

Corporate management of a WebEx Node is performed either through the platform hosting the WebEx Node or via the WebEx Node Manager portal.

Secure device access to the host platform should be hardened according to SAFE guidelines, including the following:

- AAA to a centralized AAA server
- Strong password policy
- Restricted device accessibility
- Enforcement of SSH for CLI access
- Banners for legal notification
- SFTP or SCP for secure file transfer
- In-band management

WebEx proprietary management of a WebEx Node is performed over the SSL connection from a WebEx Node to the WebEx Collaboration Cloud and is under the stringent security control of WebEx. WebEx personnel do not have access to the host platform via its connection to the WebEx Node.

For more information on SAFE secure device access guidelines, see the *Cisco SAFE Reference Guide* listed in the "Reference Documents" section on page 14.

Routing Security for WebEx Node Integration

A WebEx Node itself does not participate in routing, relying on its host platform for network connectivity and advanced routing capabilities. If the platform hosting the WebEx Node participates in routing, then it should be secured according to the SAFE guidelines, including the following:

- Routing peer definition
- Neighbor authentication
- BGP TTL security
- Passive interfaces
- Route filtering
- Neighbor logging

For more information on SAFE routing security guidelines, see the *Cisco SAFE Reference Guide* listed in the "Reference Documents" section on page 14.

Service Resiliency for WebEx Node Integration

The resiliency and survivability of a WebEx Node and the overall WebEx services is ensured through a number of design features, including the following:

- Limited attack surface

  A WebEx Node only supports HTTPS connections and traffic.

- Protection from a SYN flooding DoS attack

  The number of client sessions permitted to connect to a WebEx Node are restricted and controlled by WebEx.

- Protection from SYN-flood DoS attacks

WebEx limits the number of embryonic connections permitted on both a WebEx Node and the WebEx Collaboration Cloud.

- WebEx Node VoIP/video stream preservation and optimization

  A WebEx Node deployed in Voice and Video Conferencing mode, by default, marks traffic with a DSCP value of Expedited Forwarding (EF). This enables an enterprise medianet to preserve and optimize these WebEx Node streams by leveraging the end-to-end QoS deployment to mitigate disruption from DoS attacks or simply network congestion. This provides greater resiliency and a higher quality of experience to internal WebEx clients connected to a WebEx Node.

- WebEx service resiliency

  A WebEx client connects to the most responsive connection point. WebEx Node redundancy is provided through alternate WebEx Nodes and the WebEx Collaboration Cloud, creating a highly resilient architecture.

A WebEx Node, as previously mentioned, is completely reliant on its host platform for availability. Therefore, the host platform itself, as well as any additional services it is hosting, must be assessed and secured according to the SAFE guidelines. These include the following:

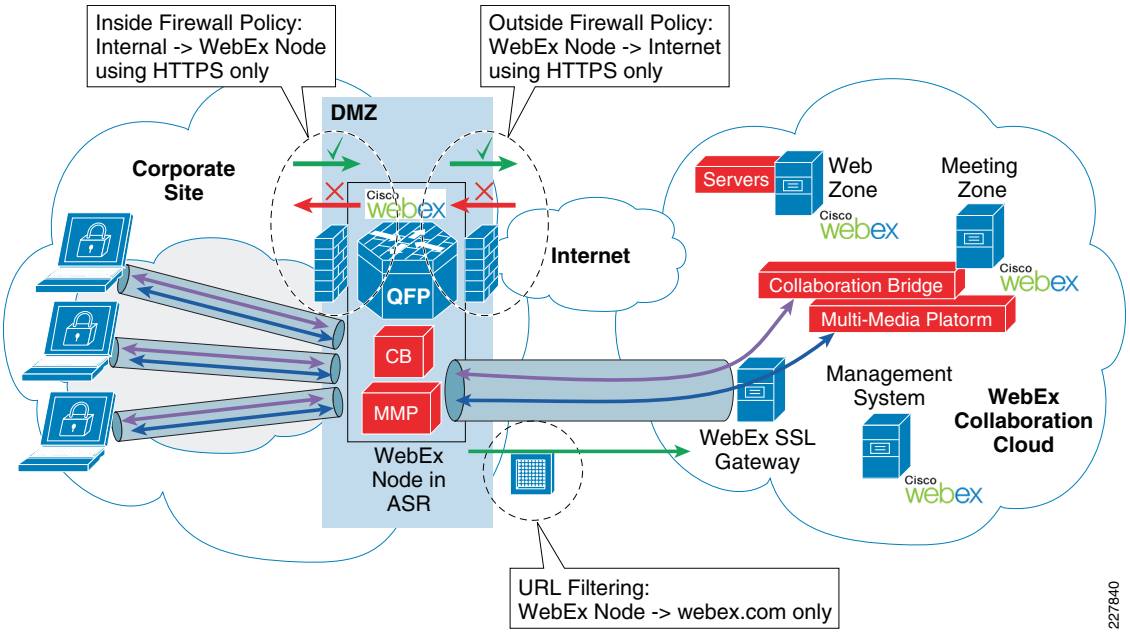
- Disable unnecessary services
- Control Plane Policing (CoPP)
- Service-specific resource exhaustion protection
- Preservation and optimization of services
- End-to-end QoS
- Redundancy

For more information on SAFE service resiliency guidelines, see the *Cisco SAFE Reference Guide* listed in the "Reference Documents" section on page 14.

Network Policy Enforcement for WebEx Node Integration

A WebEx Node only supports HTTPS connections on the corporate network. More precisely, it is only required to support outgoing HTTPS to the WebEx Collaboration Cloud and incoming HTTPS connections from internal WebEx clients. Consequently, network policy enforcement should be implemented accordingly in order to restrict risk exposure. Implementation is primarily through firewall integration but can be extended to include URL filtering, as illustrated in Figure 1.

Example 1 Network Policy Enforcement for WebEx Node Integration



Firewall policy enforcement and URL filtering enforcement is available on a range of different Cisco platforms, providing the enterprise with the flexibility, not only to select the platform that meets their particular deployment needs, but also with the ability to leverage this functionality on devices that are already deployed in the corporate DMZ. This enables optimized capital and operational overheads for the enterprise.

Cisco firewall functionality is available on the Cisco ASA 5500 Series appliances, IOS Firewall, and the Firewall Services Module (FWSM) for the Cisco Catalyst 6500. Cisco URL filtering functionality is available on the IronPort WSA appliance, IOS Content Filtering, or the Cisco ASA 5500 Series.

Enforcement of this network policy also ensures that, in the case of a compromised WebEx Node, the only permitted communication will be a HTTPS connection to the WebEx Collaboration Cloud. A compromised WebEx Node could not therefore be used to gain unauthorized access to the corporate network.

All general network activity related to corporate accessibility and availability of a WebEx Node is performed by the host platform. This includes IP routing, DNS, NTP, syslog, SNMP, etc. Consequently, network policy-enforcement on the host platform must be assessed and secured accordingly, including the following:

- Filter incoming traffic
- IP spoofing protection
- Segment and enforce policy domains

Network policy enforcement of a WebEx Node's connection, management, and activity within the Collaboration Cloud is under the stringent security control of WebEx.

For more information on SAFE network policy-enforcement guidelines, see the *Cisco SAFE Reference Guide* listed in the "Reference Documents" section on page 14.

Switching Security for WebEx Node Integration

A WebEx Node relies on its host platform for all network connectivity. If the host platform is connected to a DMZ switch, then that switch should be assessed and secured according to the SAFE guidelines, including the following:

- Restrict broadcast domains
- STP Security
- DHCP protection
- ARP spoofing protection
- IP spoofing protection
- MAC flooding protection
- VLAN best common practices

For more information on SAFE switching security guidelines, see the *Cisco SAFE Reference Guide* listed in the "Reference Documents" section on page 14.

Threat Control and Containment for WebEx Node Integration

Threat control and containment involves deploying the appropriate tools and techniques in order to detect and mitigate anomalous activities on the network. This typically includes, for example, IPS integration, application inspection, host-based IPS (HIPS), E-mail security and web security. These are complemented by cross-network intelligence, enabled through the features discussed in the "Monitoring, Analysis and Correlation for WebEx Node Integration" section on page 14.

The WebEx Node and the WebEx services rely on SSL sessions to enable secure collaboration. Consequently, these SSL sessions are an obvious attack vector and so we will look at some common SSL threats and the threat detection and mitigation measures to address them.

If analysis of traffic within the WebEx streams is required, such as to enable application inspection, intrusion prevention or data leakage prevention (DLP), then an SSL proxy can be used to decrypt and re-encrypt WebEx streams. The Application Control Engine (ACE) family provides high performance SSL proxy functionality, as well as HTTPS protocol anomaly detection, that make it ideal for this purpose.

The threat control and containment of anomalous activity within the WebEx Collaboration Cloud is under the stringent security control of WebEx.

For more information on SAFE threat control and containment guidelines, see the *Cisco SAFE Reference Guide* listed in the "Reference Documents" section on page 14.

SSL Threat Control and Containment

Threats against SSL sessions are generally related to:

- Eavesdropping or MITM (man-in-the-middle)

  Intercepting an SSL session in order to gain unauthorized access to the stream.

- Denial of Service (DoS)

  Preventing or interrupting an SSL session in order to disrupt service availability.

MITM attacks leverage a number of techniques in order to insert an attacker's device as an intermediary, but transparent, hop in the flow of an SSL session. Techniques include DNS poisoning, ARP spoofing, IP spoofing, DHCP server spoofing and SSL MITM attack tools that supply, for example, fake or intermediary certificates in order to decrypt and re-encrypt an SSL stream.

DoS attacks also leverage a number of techniques in order to disrupt a client's ability to establish and maintain an SSL session, or simply disrupt general network connectivity. Techniques include traffic flooding, route manipulation, DNS poisoning, resource exhaustion, and TCP and ICMP attacks.

The SAFE Network Foundation Protection guidelines mitigate the majority of the baseline MITM and DoS attack techniques through ARP, IP, and DHCP server spoofing protection, routing security, firewall policy enforcement, traffic flooding, CoPP and resource exhaustion protection, as well as secure device access to prevent unauthorized access to an intermediary network device. For more information, see "Network Foundation Protection for WebEx Node Integration" section on page 8.

In addition, Cisco IPS integration, in both the corporate DMZ and the corporate access edge, can detect and mitigate a range of possible attack vectors through its vulnerability and exploit-based signatures, protocol anomaly detection and behavioral-based anomaly detection, as well as reputation-based filtering using SensorBase.

These techniques are further complemented by implementing endpoint security. This provides clients with reduced risk exposure, as well as protection from a range of attacks, no matter which network they may be connected to. Endpoint security includes baseline best practices, such as operating system and application hardening and timely patching, as well as more advanced techniques such as host-based IPS (HIPS), as provided by Cisco Security Agent (CSA). CSA offers signature- and behavior-based threat detection and mitigation to address both known and zero-day attacks, as well as policy enforcement and data loss prevention.

The WebEx SSL sessions are SSLv3 and rely on digital certificates for authentication and the exchange of strong keys for encryption. A WebEx Node authenticates the WebEx Collaboration Cloud using its publicly-issued certificate signed by a trusted authority. The WebEx Collaboration Cloud authenticates a WebEx Node based on the strong credentials configured on the host platform. The SSL session is subsequently encrypted using 256-bit AES encryption to ensure confidential communication over the Internet.

A WebEx client connecting directly to the WebEx Collaboration Cloud also authenticates and validates the WebEx Collaboration Cloud using its publicly-issued certificate signed by a trusted authority. The WebEx Node does not currently provide a certificate signed by a trusted authority but mutual authentication occurs based on proprietary WebEx information. The SSL session is subsequently encrypted using 1286-bit AES encryption to ensure confidential communication either over the Internet or the corporate network.

Monitoring, Analysis and Correlation for WebEx Node Integration

Visibility is critical to security and cross-network telemetry must be extended to the WebEx Node.

Corporate monitoring of the status of a WebEx Node is available through telemetry from its host platform or via the WebEx Node Manager portal. The WebEx Node Manager portal provides basic status information, such as CPU and memory, as well as WebEx meeting information.

Visibility into WebEx Node and general WebEx traffic flows can be obtained through NetFlow data from devices within the DMZ, such as the host platform, Internet edge devices, and corporate edge devices. This can be used to detect anomalies in network traffic that may indicate a network incident.

As previously mentioned, since a WebEx Node is partly managed and operated by an external third-party, its host platform is typically in a DMZ and, consequently, management of the host platform should be conducted in-band. This ensures that a compromised device, be it the WebEx Node or the host platform, does not provide unauthorized access to the corporate network.

WebEx proprietary monitoring, analysis, and correlation of activity on a WebEx Node is performed over the SSL connection from a WebEx Node to the WebEx Collaboration Cloud and is under the stringent security control of WebEx.

For more information on SAFE monitoring, analysis and correlation guidelines, see the *Cisco SAFE Reference Guide* listed in the "Reference Documents" section on page 14.

Reference Documents

- Application Control Engine (ACE) Module
  http://www.cisco.com/en/US/products/ps6906/index.html
- Application Control Engine (ACE) Appliance
  http://www.cisco.com/en/US/products/ps8361/index.html
- ASA 5500 Series
  http://www.cisco.com/go/asa
- ASR 1000 Series
  http://www.cisco.com/en/US/products/ps9343/index.html
- Cisco SAFE
  http://www.cisco.com/go/safe
- Cisco Security Agent (CSA)
  http://www.cisco.com/go/csa
- IOS Content Filtering
  http://www.cisco.com/en/US/products/ps6643/index.html
- IOS Firewall
  http://www.cisco.com/en/US/products/sw/secursw/ps1018/index.html
- IOS NetFlow
  http://www.cisco.com/en/US/products/ps6601/products_ios_protocol_group_home.html
- IronPort Web Security Appliance (WSA)
  http://www.ironport.com/web

- Medianet
  http://www.cisco.com/web/solutions/medianet/index.html
- QoS Design Recommendations for Medianet
  http://www.cisco.com/en/US/docs/solutions/Enterprise/Video/qosmrn.html
- WebEx
  http://www.cisco.com/en/US/products/ps10352/index.html
- WebEx Node for ASR 1000 Series
  http://www.cisco.com/en/US/products/ps10353/index.html
- WebEx Security Overview
  http://www.cisco.com/en/US/prod/collateral/ps10352/cisco_webex_security_overview.pdf