



Deployment of Cisco Enterprise Class Teleworker Solution

The Cisco® Enterprise Class Teleworker solution is a highly scalable Cisco IOS® Software-based solution that securely integrates the network infrastructure, management infrastructure, managed services, and applications across the entire enterprise, including LAN, WAN, branch, and teleworker locations.

The solution is an integral part of the Cisco Service-Oriented Network Architecture (SONA), a framework that enables enterprise customers to build integrated systems across a fully converged, intelligent network. Using the Cisco SONA framework, the enterprise network can evolve into an Intelligent Information Network—one that offers the kind of end-to-end functions and centralized, unified control that promote true business transparency and agility.

Cisco Systems® has successfully deployed the Enterprise Class Teleworker (ECT) solution within its own organization, increasing productivity and improving efficiency while enabling “zero-touch” deployment, manageability, and low-to-negative total cost of ownership (TCO). Enterprises and service providers can use the Cisco ECT solution to offer the benefits of network services to their end users and customers, while maintaining an effective Return of Investment (ROI).

For the Cisco ECT/SONA Solution Overview, refer to:

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6660/prod_brochure0900aecd803fc7ec.html

For Cisco ECT/SONA solution, services, and applications support, refer to:

<http://cisco.com/go/ect/>

PURPOSE AND SCOPE

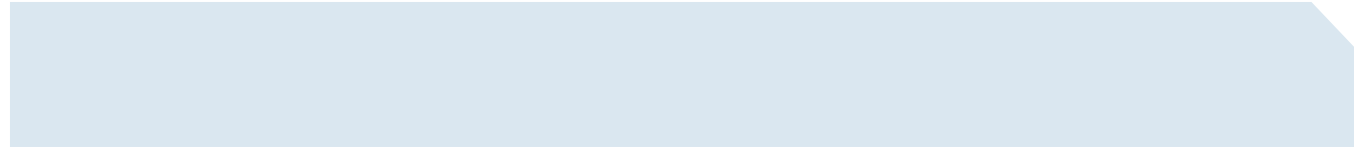
This document describes the various solutions and managed services available in the Cisco ECT solution. However, actual configurations and image platform recommendations are not provided as part of this guide. Links to Cisco ECT deployment guides are included in the document.

TARGET MARKET SEGMENTS

The Cisco ECT solution is targeted toward commercial, enterprise, and service provider networks.

As a business grows to new locations (national and international), its IP network growth should be consistent. The network infrastructure needs to be standardized to provide a consistent security architecture for all sites, including corporate headquarters, data center locations, remote sites and branches, extranet partners, and remote teleworkers. The VPN architecture needs to provide customer premises equipment (CPE)-based access, VPN client-based access, and clientless access. A zero-touch deployment model is required to seamlessly integrate CPE and remote users into the network, and to help customers achieve a lower TCO. Continuous central network management and auditing, using push technology, is needed to simplify administration.

Data center and campus networks need to be virtualized in order to use all network, computing, and storage resources to maximum potential. Customers require a solution that protects their investments, keeps network expansion costs down, and provides easy network manageability. It is essential to make the network easily expandable without incurring extra costs for resources for deploying and managing new nodes.



Overall, customers are trying to achieve low to negative total cost of network ownership. They want to see their network infrastructure becoming so efficient that it starts managing itself; pays for itself; keeps ongoing costs comparatively low; and maximizes the use of network and server resources. The Cisco ECT solution addresses all these customer issues.

CISCO ECT SOLUTION

The Cisco ECT solution provides IOS Software-based large-scale, secure, end-to-end managed IP network with integrated managed services and applications support. The solution helps increase network and IT efficiency and provides a standard solution for facilitating an equal level of secure network integration to suppliers, partners, employees, and customers. It supports global deployment and provides a management model which provides low to negative TCO.

The Cisco ECT solution and services are an integral part of the SONA framework and are fully aligned with the framework's multilayer strategy (network layer, services layer, and application layer). The SONA framework guides LAN and WAN integration for all sites, including branch sites and teleworkers. The ECT conversion of SONA and IIN layered model into actual solutions and services results in fully deployable, cook-book, end-to-end solutions.

Using the Cisco ECT solution, the network can become so efficient that it starts managing itself, lowering ongoing costs and maximizing the utilization of network resources. Cisco IOS Software, managed services, and applications can be integrated on the same CPE. The ECT solution consists of a baseline solution, along with managed services, applications, threat defense solutions, and a management solution.

The baseline solutions provide various VPN solutions that cover all requirements from any location away from the corporate headquarters. The technologies range from legacy IP Security (IPsec) VPN to advanced VPN technologies such as Dynamic Multipoint VPN (DMVPN), Enhanced Easy VPN, and Secure Sockets Layer VPN (SSLVPN). All VPN technologies can be integrated on the same Cisco IOS Software-based concentrator, enabling enterprises to provide a global business view of their entire network for suppliers, partners, employees, and customers.

The Cisco ECT solution supports many different managed services for enterprises and service providers; these value-added services can then be made available to end customers. The services can be incrementally enabled on the CPE without having to reinvest or upgrade the entire network.

Applications provide support for secure voice, video, and wireless solutions; secure IP multicast support; and IP services like quality of service (QoS) and Network Address Translation (NAT).

The threat defense solution provides proactive and reactive security services, which enable network devices to achieve secure LANs and WANs.

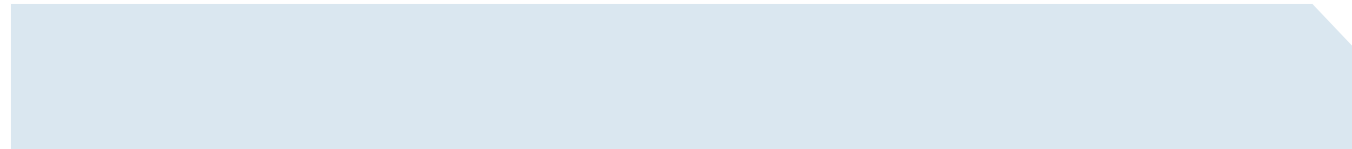
The management solution is used for achieving zero-touch deployment, ongoing management, and "virtualization" for efficient use of server resources. The solution helps increase network manageability and corporate control, and reduces the complexity of support.

Baseline Solution

Converged VPN Solution

The converged VPN solution standardizes and scales the network by facilitating seamless integration of VPN technologies. DMVPN, Easy VPN, and SSLVPN can be integrated to provide a single consolidated hub for the VPN deployment. This provides standardized and scalable support for all types of end users, including telecommuters, road warriors, and branch sites.

DMVPN optimizes performance, reduces latency for real-time applications, and enables dynamic configuration. It reduces the maintenance and configuration on the hubs and uses QoS to provide the priority to the marked network and real-time sensitive applications.



Easy VPN provides access to both software and hardware clients, complementing the other VPN deployments. Easy VPN deployments can be easily migrated to DMVPN deployments. And with the availability of IPsec Dynamic Virtual Tunnel Interface (DVTI), Enhanced Easy VPN now supports IP Multicast and QoS as well.

SSLVPN provides clientless, thin-client, or full client-based secure access to corporate network and resources, from any device with an SSL-enabled browser, like laptops and PDAs. SSLVPN also enables users to download Cisco Secure Desktop, which provides a secure desktop on top of the guest desktop. Mobile users, retail brokers, and extranet partners can benefit from SSLVPN when the allowable SSL VPN client, Cisco Secure Desktop, or clientless access depends on corporate policy. SSLVPN can integrate and share a hub with both Easy VPN and DMVPN.

More information about the deployment of a converged VPN solution can be found at:

http://www.cisco.com/en/US/products/ps6808/products_ios_protocol_option_home.html

GDOI DMVPN Solution

Group Domain of Interpretation (GDOI) is a group key protocol whereby all group members register with a key server. It defines a method of sharing a common group key among devices that can be used for encryption and decryption. GDOI has been integrated with the DMVPN solution to take advantages of its group keying concept. With this integration, each spoke maintains a GDOI session only with the key server and there is no permanent tunnel between the hub and spoke.

The major benefit of this integration is that spokes and hubs are group members and a common group key is distributed to them, eliminating the need for point-to-point IPsec sessions between them. Any group member can talk to any other group member using the same key. This reduces the delay when setting up spoke-to-spoke connections by eliminating creation of dynamic IPsec tunnels between them. There is minimal or no delay in setting up voice calls between spokes. As with IPsec-based DMVPN, both unicast and multicast data are still secured.

More information about the GDOI-based DMVPN solution can be found at:

http://www.cisco.com/en/US/products/ps6811/products_ios_protocol_option_home.html

Easy VPN and DMVPN Convergence Solution

Easy VPN can be combined with DMVPN for the deployment of the Cisco ECT solution. Easy VPN provides access to both software and hardware clients, complementing the regular DMVPN deployment.

When an existing Easy VPN deployment is based on Cisco IOS Software and the customer wants to add DMVPN to the same hub, DMVPN configuration can be added to the same hub without affecting the existing Easy VPN setup. The converse is also true.

A converged Easy VPN and DMVPN ECT solution is beneficial when a customer wants to provide full-scale integrated access to both small office or home office (SOHO) teleworkers and mobile users using the same end-to-end secure solution setup. For SOHO users, Easy VPN or DMVPN can run on a home router, providing corporate access to the computers and IP phones connected to the home network. For mobile users, the Easy VPN client (software VPN client) installed on a laptop provides the desired connectivity, because that client can work from any location and will integrate well with the same solution.

With the addition of IPsec DVTI, Easy VPN now supports IP Multicast and QoS as well.

More information about Easy VPN and DMVPN convergence solutions can be found at:

http://www.cisco.com/en/US/products/ps6808/products_ios_protocol_option_home.html

SSLVPN and DMVPN Convergence Solution

Cisco IOS® SSLVPN provides remote secure corporate network (intranet) access over the standard public Internet using only a Web browser and its native SSL encryption. SSL authentication and encryption/decryption operates at the application level, which eliminates the need for any special-purpose software installation at the client side. An SSL-enabled Web browser and e-mail client can be used to access e-mail, intranet, and various applications and resources inside the corporate network.

SSLVPN can be integrated with DMVPN and deployed as a complement to the DMVPN solution for the mobile users that sometimes need to have access to the corporate intranet from a public Internet access location. There is no need to install any software on the end host; only an SSL-enabled Web browser is needed.

The SSLVPN and DMVPN configurations can be combined in the same hub; however, the two technologies are completely independent from each other.

More information about a SSLVPN and DMVPN convergence solution can be found at:

http://www.cisco.com/en/US/products/ps6808/products_ios_protocol_option_home.html

DMVPN Dial-Backup Solution

The Cisco IOS Software dial backup feature uses dialup service over a regular telephone wire to provide backup Internet connectivity if the primary ISP connection fails. In an ECT-based DMVPN solution, the dial backup feature provides connectivity to the data gateway using the dialup network if the primary ISP connection fails. The primary ISP connection is usually a broadband connection. The bandwidth and speed provided by a dialup network are low and should be used mainly to provide secondary connectivity. Whenever connection to the ISP is restored, the tunnel to the data gateway using dialup connectivity is torn down, and the tunnel using the ISP is restored.

More information about the DMVPN dial backup solution can be found at:

http://www.cisco.com/en/US/products/ps6660/prod_white_papers_list.html

High-Concentration Hub Solution

In a Cisco ECT solution, high-concentration hub services are recommended for larger networks (at least 3000 spokes) or for networks that require high bandwidth. If customers are interested in maintaining a single large network that allows spokes to belong to one DMVPN domain rather than splitting the network into multiple small segments, Cisco recommends server load balancing (SLB)-enabled hub stack support.

When customers want to incorporate hierarchical network design (for example, banking services in which certain branch offices terminate at a regional office and the regional offices terminate at the national office), a hub that has less capacity (in terms of the number of spokes it can handle) and that provides greater bandwidth is suitable. In this situation, a Cisco Catalyst 6500/7600 Series router with a VPN shared port adapter for encryption is advised, along with a Cisco 7301 server farm for routing, Next Hop Resolution Protocol (NHRP), and multicast.

When high-end routers, such as Cisco Catalyst 6500/7600 Series router, are used for basic secure connectivity, the slots in the chassis can enhance the provided services. Modules such as the Firewall Services Module (FWSM) and Intrusion Detection System Services Module 2 (IDSM-2) can enhance security with firewall and intrusion prevention (IPS) capabilities.

More information about the high-concentration hub solution can be found at:

http://www.cisco.com/en/US/products/ps6816/products_ios_protocol_option_home.html

Managed Services

PKI Solution

Cisco IOS PKI provides certificate management to support security protocols such as IPsec, Secure Shell (SSH), and Secure Sockets Layer (SSL). As defined in the IPsec protocol, the peers must be authenticated during Internet Key Exchange (IKE) phase 1 to identify the validity before establishing the secure communication.

When a pair of Cisco IOS routers is configured for IPsec peers, the routers can use preshared keys (PSKs) to authenticate each other as part of security establishment. Using preshared keys can be a better choice for customers deploying a small to medium-sized network containing few routers. As networks become larger in size and scale, PSK configuration increases in complexity and it becomes difficult to manage multiple keys. PKI offers a much more secure and scalable method for medium-sized and large enterprise deployments, whether it is a full mesh of security connections for DMVPN or newly supported xVPN technology; where spoke-to-spoke communication is desired; or for enterprise deploying site-to-site VPN for hundreds of remote branch offices needing to communicate with each other. PKI reduces management overhead and simplifies the deployment of the network infrastructure by using digital certificates exchange in place of preshared keys for device authentication.

More information about the PKI solution can be found at:

http://www.cisco.com/en/US/products/ps6807/products_ios_protocol_option_home.html

802.1x Convergence Solution

802.1x and its Layer 2 and Layer 3 extensions provide IP device-level security for both the switch-port and routed-port CPE.

Using this feature, all the IP devices are classified as trusted or nontrusted, based on the 802.1x authentication status. When a new device becomes active on the network, the router initiates an 802.1x exchange. Depending on the 802.1x client running on the user device, the user will be prompted for credentials. They are then passed on to the router. The router uses the credentials to get authenticated from a RADIUS server. If the authentication is passed, it is considered a trusted device and is given more privileges, such as access to the corporate network.

If the device fails the authentication or is a clientless device, it is considered a nontrusted device. This can be given less privileges, such as IP addresses from a separate DHCP pool.

More information about the 802.1x convergence solution can be found at:

http://www.cisco.com/en/US/products/ps6807/products_ios_protocol_option_home.html

NAC Solution

Computers and networks are under constant attack. Antivirus programs are usually installed on computers to protect them. The software version and data files of these programs need to be updated continuously. The Network Admission Control (NAC) feature in Cisco IOS Software ensure that only computers with up-to-date antivirus programs and operating system updates can access the corporate network, thereby preventing (possibly) infected computers from infecting other machines on the network. This also helps to prevent vulnerable machines from getting infected by the viruses that are present in the network.

The router talks to the Cisco Trust Agent installed on the computer. The Cisco Trust Agent then collects important parameters about the computer (for example, OS type, OS version, antivirus version, or antivirus data files version) and passes it on to the router. The router forwards this information to a RADIUS server, which validates the data. This process is called posture validation. Depending on the outcome of the validation, the machine can be given complete access, limited access, or no access.

More information about the NAC solution can be found at:

http://www.cisco.com/en/US/products/ps6807/products_ios_protocol_option_home.html

Cisco Secure ACS Solution

A RADIUS server is required for different components of the Cisco ECT solution, namely NAC, 802.1x, Authentication Proxy (AuthProxy), and PKI-AAA authentication of routers. NAC and 802.1x have been discussed in the preceding section.

The AuthProxy feature is used for end-user authentication. The user is allowed access to the corporate site only if valid credentials are provided. The credentials need to be verified by a RADIUS server. Upon verification of the credentials, appropriate permit access control entries (ACEs) are downloaded and applied on the remote spoke, giving the user the appropriate level of access. PKI-AAA authentication can be used for device authentication to check the validity of ECT routers as part of secure session setup.

The Cisco Secure Access Control Server (ACS) can be configured to support all these applications. More information about the Cisco Secure ACS solution can be found at:

http://www.cisco.com/en/US/products/ps6807/products_ios_protocol_option_home.html

Mobile IP Solution

Cisco IOS IP Mobility technology can be integrated into the Cisco ECT solution framework to enable users to roam between networks while enjoying secure connectivity to the corporate intranet without service interruption.

Cisco Mobile Client, installed on laptops and PDAs, maintains a mobile IP session between the device and home agent (residing on the corporate network). Mobile users with Internet connections that are provided by Mobile IP often use data tunnels (IP or generic routing encapsulation [GRE] in IP tunnels) to handle endpoint addresses that change frequently. The data within the mobile IP tunnel is not encrypted.

Running an Easy VPN or SSLVPN session over the Mobile IP session helps ensure that sensitive data coming to the corporate network is encrypted and protected. By encapsulating this tunnel securely using Easy VPN or SSLVPN, users can enhance the level of security provided to the end user, while providing voice capabilities and the ability to use multiple devices.

This Mobile IP solution offers a secure connection while enabling users to freely move from one location to another and to switch between networks without worrying about application sessions being dropped. This solution provides secure access to employees even from roaming locations; for example, commuting employees or sales personnel can maintain connectivity to their corporate network without having to re-establish sessions while moving from place to place.

More information about the Mobile IP solution can be found at:

http://www.cisco.com/en/US/products/ps6820/products_ios_protocol_option_home.html

Branch Voice Solution

Integrated secure voice managed services enable various voice and video applications behind CPE (such as a remote router) within a secured network. While a firewall ACL in a Cisco ECT-enabled CPE will block anything needed for these voice services (except the control messages), other security features (such as NAC, 802.1x, AuthProxy) should also bypass authentication confirmation from VoIP phones. Firewall inspection will open necessary ports to permit voice traffic after a call has been initiated. QoS must be initially enabled for voice traffic, based on uplink bandwidth available from the ISP. The bandwidth usage depends on the codec; the most popular codecs are G.729 and G.711.

The above services are common for any Cisco ECT spoke, usually a SOHO site.

From a branch perspective, the Cisco ECT solution includes Cisco Unified CallManager Express and Cisco Unity Express, providing an IP telephony system that offers a comprehensive set of telephony features, as well as integrated routing, security, and Ethernet switching on a single platform. After installation and configuration, users registered at the site's Cisco Unified CallManager Express shall be able to place and receive calls within that system; place and receive calls to other sites (like other Cisco Unified CallManager Express installments); and place and receive calls from/to the public switched telephone network (PSTN).

A Cisco ECT branch site can be deployed using a Cisco 2800 Series or 3800 Series Integrated Services Routers, which combines all the other ECT services plus Cisco Unified CallManager Express and Cisco Unity Express.

More information about the branch voice solution can be found here:

http://www.cisco.com/en/US/products/ps6812/products_ios_protocol_option_home.html

IPsec High-Availability Solution

The Cisco IOS IPsec High Availability (IPsec HA) feature provides an infrastructure for reliable and secure networks to provide transparent availability of the VPN gateways—that is, Cisco IOS Software-based routers. This feature works well for all IPsec-based networks.

In a Cisco ECT solution, which encompasses a DMVPN architecture for data gateway infrastructure and plain IPsec for management gateway infrastructure, IPsec HA can be used to provide redundancy. Stateful failover and rollback of the gateways can be used to provide uninterrupted management connectivity to the spokes.

More information about the IPsec high availability solution can be found here:

http://www.cisco.com/en/US/products/ps6816/products_ios_protocol_option_home.html

Applications

Application and IP Services

Application and IP services provide support for secure voice, wireless, and video solutions, as well as QoS, NAT, Optimized Edge Routing (OER), and Cisco IOS IP Service Level Agreement (IP SLA).

Voice and video capability are extended to remote sites through a secure network. This supports wired and wireless VoIP phones as well as Cisco IP Communicator softphones, wireless access points, and the Cisco VT Camera. Secure wireless is supported through integrated wired or wireless LAN network solutions, connecting the wireless nodes in the network.

QoS offers prioritization of real-time and latency-sensitive traffic (such as voice). NAT allows Cisco ECT spokes and hubs to reside behind existing NAT devices and also allows the spokes and hubs to support split tunneling. OER chooses the best path when two or more physical or logical paths are available. IP SLAs provide support for performing network performance measurements.

More information about application and IP services can be found at:

http://www.cisco.com/en/US/products/ps6810/products_ios_protocol_option_home.html

IP Multicast Solution

IP Multicast services provide solutions for the secure support of IP Multicast applications over VPN technologies. Initial support for securing multicast combines GRE over site-to-site IPsec VPNs; however, scalability is an issue when additional devices are included within a domain.

With the advent of new technologies, including DMVPN and Enhanced Easy VPN, users can enjoy the benefits of improved IP Multicast performance and scalability, and easy deployment.

In DMVPN, multicast packets are encapsulated within the GRE header and then encrypted when sent over the tunnel. This supports routing protocols and multicast data forwarding, and simplifies configuration management and scalability. However, the packets are replicated and then encrypted, which limits the number of multicast receivers in a multipoint GRE (mGRE) interface based on the router platform and stream bandwidth.

Enhanced Easy VPN (DVTI) dynamically creates a virtual interface, similar to a point-to-point GRE tunnel, when the session is established. Multicast forwarding is possible using this virtual interface. All that is needed is enabling configuration for the VTI server as multicast in the template configuration.

Group Domain of Interpretation (GDOI) is a group-key-based VPN, where a group of systems share the same group key for encryption and decryption, making multicast forwarding possible without GRE-type tunnels. Secure multicast, which relies solely on GDOI, is mainly deployed for enterprise networks running across a Multiprotocol Label Switching (MPLS) core. Benefits include reduced multicast packet replications at the GDOI group members by using packet replication done by the multicast VPN in provider edge routers.

More information about the IP Multicast solution can be found at:

http://www.cisco.com/en/US/products/ps6811/products_ios_protocol_option_home.html

Secure Voice and Wireless Solution

Integrated secure voice managed services extend the voice and video capability available in users' offices to their homes. Support is provided for Skinny Client Control Protocol (SCCP) and Session Initiation Protocol (SIP) based on Cisco Unified IP phones, which are ready to be plugged in behind the CPE. Support is also provided for Cisco IP Communicator, a PC-based Cisco IP softphone solution, which supports only SCCP. Cisco Wireless IP is supported using a wireless access point, which is then connected to a voice VLAN in the Cisco ECT solution-enabled CPE.

Integrated secure wireless managed services focus on enabling wireless applications behind the Cisco ECT-enabled CPE within a secure network. Strong security policies, which protect the company from rogue access points, intruders, unauthorized users, and unauthorized viewing of transmitted data, are required for enterprise wireless LANs. Cisco supports IEEE 802.1x authentication and numerous Extensible Authentication Protocol (EAP) types, providing a centrally managed, standards-based, open wireless network security scheme in addition to some of the earlier 802.11 Wired Equivalent Privacy (WEP) implementations.

Integrated secure wireless managed services provides support for Temporal Key Integrity Protocol (TKIP), which provides enhancements to 128-bit encryption such as per-packet key hashing, digital certificates on every frame, and rotate broadcast keys in wireless access points to encrypt both unicast and broadcast packets. Several EAP types are supported, including Cisco LEAP, EAP-Flexible Authentication via Secure Tunneling (EAP-FAST), EAP-Transport Layer Security (EAP-TLS), EAP-Tunneled TLS (EAP-TTLS), Protected EAP (PEAP), and EAP-Subscriber Identity Module (EAP-SIM). The Wi-Fi Protected Access (WPA) standards-based solution addresses wireless LAN vulnerabilities and provides enhanced protection from targeted attacks. WPA uses TKIP for encryption.

More information about secure voice and wireless solutions can be found at:

- http://www.cisco.com/en/US/products/ps6812/products_ios_protocol_option_home.html
- http://www.cisco.com/en/US/products/ps6814/products_ios_protocol_option_home.html

Threat Defense Solution

Layered Security Solution (Proactive Security Services)

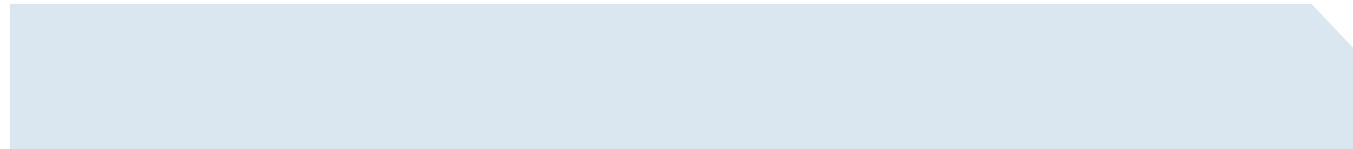
Layered security and perimeter security managed services provide support for secure LAN and WAN infrastructures for the Cisco ECT solution. These security services help secure the remote CPE, IP devices, IP-based applications, and end users, vendors, and customers.

The layered security concept provides various CPE-, device-, and user-level security mechanisms, while perimeter security provides the edge-level security for the CPE, which helps define the securely integrated ECT Solution framework.

Layered security and perimeter security include:

PKI enables CPE-level authentication as part of VPN tunnel establishment. RSA keys and digital certificates are used to authenticate and authorize each CPE before it becomes part of the trusted network.

802.1x and its Layer 2 and Layer 3 extensions provide IP device-level security for both the switch-port and routed-port CPE.



NAC validates the posture of the IP device to ensure it is running the latest antivirus software and OS patches before permitting access to corporate networks. This prevents infected devices from spreading viruses across other machines in the network.

Authentication Proxy (AuthProxy) provides end-user security by authenticating users with Cisco Secure ACS before they are allowed to access corporate networks.

USB-based eTokens provide CPE security by providing a location to store critical information like digital certificates, RSA keys, and secondary configurations. This information can be enabled on the CPE by the eToken login. This safeguards against the “stolen box” scenario and prevents unauthorized users from setting up VPN access back to corporate headquarters.

Cisco IOS Firewall provides perimeter security by blocking unauthorized access to the end devices sitting behind the spoke router, thereby protecting the internal networks from security attacks.

Together, the Cisco IOS Software-based firewall and IPS features further strengthen perimeter security by monitoring permitted traffic for any malicious signatures in real time, and taking appropriate action.

Cisco Secure ACS supports RADIUS and TACACS+ and provides the authentication, authorization, and accounting (AAA) capabilities that a secure network requires. Cisco Secure ACS maintains a central database to validate the user and device authentication and authorization required by PKI, 802.1x, NAC, and AuthProxy.

More information about the layered security solution can be found at:

http://www.cisco.com/en/US/products/ps6807/products_ios_protocol_option_home.html

Threat Defense Solution (Reactive Security Services)

The Cisco IOS Software-based threat defense solution delivered in the Cisco ECT solution, addresses the reactive security services. This solution uses the service of some network monitoring tools (as listed below) to maintain constant network security, recognize internal and external threats, and respond to any threats while alerting users to the issues.

Tools such as Cisco Security Monitoring, Analysis and Response System (Cisco Security MARS), and Cisco Guard/Detector (or Peakflow X/SP) facilitate the monitoring, detection, and classification of threats. Threat Information Distribution Protocol (TIDP) controllers and TIDP Mitigation Services (TMS) consumers work together to provide the transport and rules distribution mechanism for threat mitigation services using dynamic ACLs, IPSs, and OER redirection.

The Cisco ECT solution-enabled CPE (the remote router) can be configured to upload syslog messages and NetFlow entries to Cisco Security MARS for threat detection and classification. Cisco Guard can also be used for packet inspection, or Arbor Peakflow X/SP device can be used for NetFlow data analysis.

Mitigation action can be provided using the TIDP/TMS XML-based threat file or using the Cisco Flexible Packet Matching (FPM) feature. Also, Cisco Security MARS can poll the CPE to detect any triggered IPS signatures and provide threat mitigation by pushing the IPS signatures dynamically onto other routers within the network to prevent further attacks on the network.

More information about a threat defense solution can be found at:

http://www.cisco.com/en/US/products/ps6813/products_ios_protocol_option_home.html

Management Solution

The Cisco ECT management solution is used for achieving zero-touch deployment, ongoing management, and “virtualization” for efficient use of server resources.

Cisco SDM Solution

Cisco Router and Security Device Manager (SDM) is a Web-based graphical user interface (GUI) tool that can be used to configure and manage Cisco IOS routers. It usually comes with a router's factory default configuration and can be invoked from any Java-enabled browser that has connectivity to the Cisco IOS router to be configured.

When Cisco ECT is deployed for a small number of VPN spokes, the network can be provisioned by configuring all hubs and spokes using Cisco SDM. The configuration can be downloaded from Cisco SDM directly to the routers, or it can be saved to a file.

Cisco SDM can be used to manage devices that are online, as it allows the user to remotely access a router using SSL and change the configuration.

Cisco SDM is a good choice for deploying a Cisco ECT solution for a small number of routers. In this scenario, the VPN routers are usually provisioned locally at the central office and then shipped or hand-delivered to the end user, or sent to a small office.

More information about the Cisco SDM solution can be found at:

http://www.cisco.com/en/US/products/ps6809/products_ios_protocol_option_home.html

Secure Device Provisioning Solution

Secure Device Provisioning is a critical component for achieving zero-touch deployment in the Cisco ECT solution. It permits the end user to initiate the device provisioning from a remote site, without any ECT admin touching the spoke, just starting with factory default configuration in the router.

Secure Device Provisioning can be used to securely push the initial bootstrap configuration to the remote-site router, install a new certificate, configure PKI trustpoint enrollment and IPsec VPN connectivity, and provision system attributes and other desired information to a new spoke router.

Secure Device Provisioning reduces the time and cost of deploying a secure network infrastructure by using a simple Web-based enrollment and configuration-bootstrap interface. It involves less user intervention, thereby shortening provision time and lowering TCO.

More information about Secure Device Provisioning can be found at:

http://www.cisco.com/en/US/products/ps6809/products_ios_protocol_option_home.html

Cisco Security Manager/Cisco Configuration Engine Solution

For medium-sized and large deployments, the Cisco ECT solution can be provisioned using the Cisco Security Manager. This enterprise VPN tool centrally provisions all aspects of device configurations and security policies for Cisco firewalls, VPNs, IPSs, and virtually any Cisco IOS Software feature through the use of flexible configuration templates.

Cisco Security Manager automatically configures ECT spokes and hubs based on predefined global or individual policies. It audits device configuration for unallowed policy changes. It also allows the provisioning of thousands of devices. It has the ability to do deferred provisioning, meaning that it can prepare all policies for Cisco ECT routers and be set in listening mode so that it automatically pushes policies when a spoke connects to the hub for the first time.

The Cisco Configuration Engine provides an automated and event-driven way to push predefined configuration files (or updates) to remote devices. It understands the Cisco Networking Services language and communicates with the spoke routers. It keeps track of all spokes connected to the corporate network, informing Cisco Security Manager of all events. It can also run tasks to automatically upgrade images for groups of devices.

More information about the Cisco Security Manager/Cisco Configuration Engine solution can be found at:

http://www.cisco.com/en/US/products/ps6809/products_ios_protocol_option_home.html

eToken Solution

A USB eToken can be used to securely store files. The eToken can store X.509 digital certificates, configuration files, and RSA keys for PKI support. USB eToken files are securely encrypted and a PIN is necessary to unlock access the configuration, keys, and credentials.

For the Cisco ECT solution, eTokens can be used with Cisco integrated services routers to securely store the full router's configuration, just one piece of it, or just RSA keys for PKI support. eToken can also hold the initial bootstrap configuration of an integrated services router. This can be transferred to the router using Cisco SDM, which optionally ships with new routers.

By removing the eToken from an integrated services router, the secure VPN tunnels can be dropped right away, or after a timed value if RSA keys are stored in the eToken. This is the most common use of eToken with ECT.

More information about the eToken solution can be found at:

http://www.cisco.com/en/US/products/ps6809/products_ios_protocol_option_home.html

REFERENCES

For more information about the Cisco ECT solution, visit:

<http://www.cisco.com/go/ect/>



Corporate Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters

Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters

Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco.com Website at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus • Czech Republic
Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy
Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal
Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2006 Cisco Systems, Inc. All rights reserved. CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, ScriptShare, SlideCast, SMARTnet, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0601R)

Printed in USA

C11-362315-00 08/06