Cisco IOS Software Release 12.4T Features and Hardware Support

PB3002

Last Updated: October 2008

1) Introduction: Cisco IOS Software Release 12.4T

Cisco IOS Software is the world's premiere network infrastructure software, delivering seamless integration of technology innovation, business-critical services, and hardware support. Currently operating on millions of active systems, from small home office routers to the core systems of the world's largest service provider networks, Cisco IOS Software is the most widely leveraged network infrastructure software in the world.

Cisco IOS® Software Release 12.4T integrates a comprehensive portfolio of new capabilities, including security, voice, and IP services, with powerful hardware support to deliver advanced services for Enterprise and access customers.

Release 12.4(22)T delivers QoS support for IPSec tunnels, Trusted Relay Point (TRP) IOS firewall security for unified communications, flexible NetFlow enhancements, and support for the Cisco 880 SRST and 880G Integrated Services Routers.

Release 12.4(20)T added significant embedded management enhancements, category-based productivity and security ratings support, multi-level Quality of Service (QoS) scheduling, and support for the Cisco 860, 880, and 1861 Routers.

Release 12.4(15)T streamlined the Cisco IOS Software upgrade process, provided sub-second link failure detection and faster convergence, delivered next-generation Layer 2-7 flexible packet classification, enhanced Intrusion Protection (IPS) and SSLVPN capabilities, and support for the new Cisco 7201 Router.

Release 12.4(11)T delivered new Layer 2 VPN transport over MPLS capabilities, enhanced MPLS management, mobile IPv6 authorization and identity support, and support for the high performance Network Processing Engine G2 (NPE-G2) and VPN Service Adapter (VSA) for the Cisco 7200 Series Router.

Release 12.4(9)T delivered improved manageability, integrated IP communications capability, enhanced HTTP and P2P security, and faster routing protocol convergence.

Release 12.4(6)T delivered highly available firewalls, comprehensive endpoint and network security for SSL VPN environments, and optimized bandwidth management for improved VoIP call quality.

Release 12.4(4)T enhanced threat protection against malicious worm and virus attacks, improved performance monitoring of VoIP networks, and extended support for secure concurrent services on the Cisco 1800 Series router.

1.1) Migration Guide

Cisco recommends that customers running Release 12.3T, 12.3, or prior releases upgrade to Release 12.4T or 12.4. Customers should determine their functionality needs and choose the appropriate release.

Note: Release 12.3 reached End of Software Maintenance on March 15, 2008. For additional information please visit: http://www.cisco.com/en/US/prod/collateral/iosswrel/ps8802/ps6947/ps5187/prod_end-of-life_notice0900aecd8052e110.html

Release 12.4(15)T will receive extended bug fix support through December 2010. Cisco is taking this action to indicate that Release 12.4(15)T maintenance releases are treated in a similar manner as Release 12.4. Both undergo comprehensive testing and review cycles to continuously improve and increase reliability, quality, and stability. As per Cisco policies, no new technologies or features are to be added to either Release 12.4 or maintenance rebuild releases of Release 12.4(15)T. For more information please visit: http://www.cisco.com/en/US/prod/collateral/iosswrel/ps8802/ps6968/ps6441/ps8258/product_bulletin_c25-496283.html

Release 12.4(15)T provides significant software feature benefits and hardware support over Release 12.4. For additional details please visit:

http://www.cisco.com/en/US/products/ps8258/index.html

http://www.cisco.com/en/US/products/ps6441/prod_release_notes_list.html

Figure 1 illustrates the current migration path from Cisco IOS Release 12.3T and 12.3 (or prior) into Releases 12.4T or 12.4.

Figure 1. Release 12.4T Migration Plan

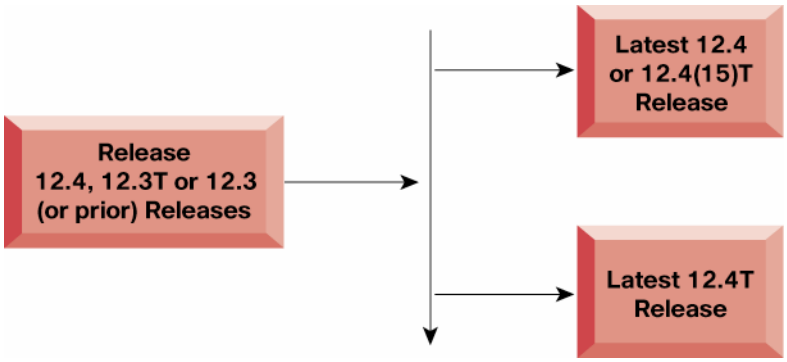


Figure 2 below illustrates the relationship between Release 12.4T and Release 12.4.

Figure 2. Release 12.4T and Release 12.4 Relationship

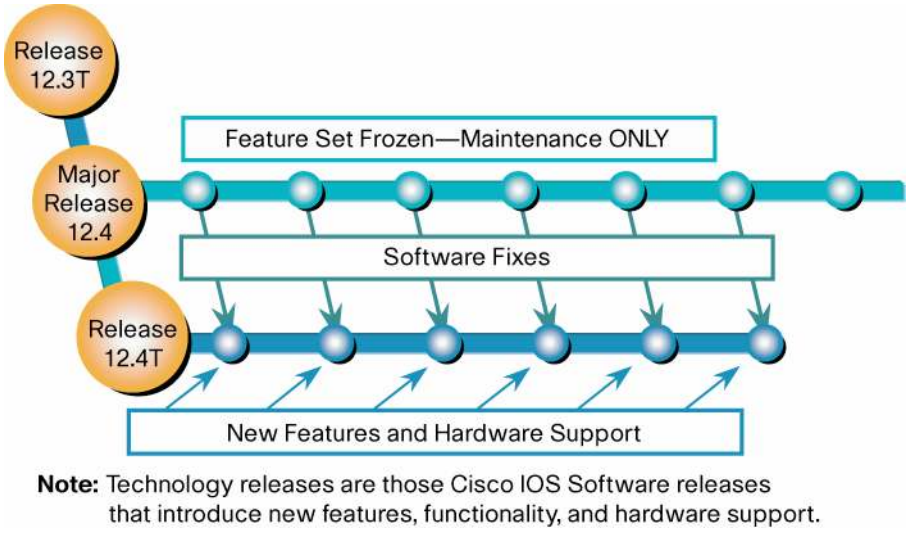
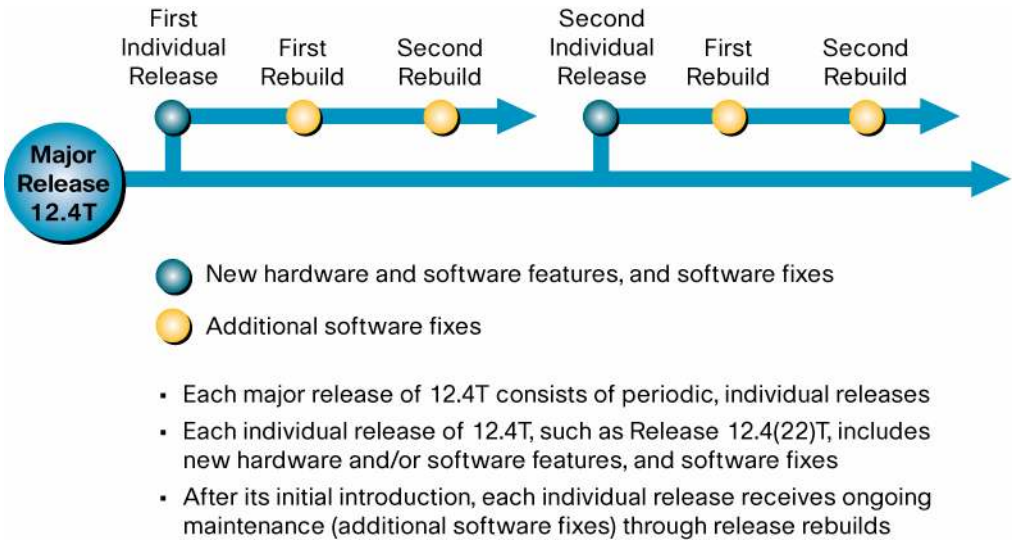


Figure 3 below shows the relationship between Release 12.4T and individual 12.4(n)T new feature releases.

Figure 3. Release 12.4T and Individual 12.4(n)T Release Relationship



Note: Cisco IOS Software Release 12.4(20)T, Release 12.4(22)T, and later releases do not support several Cisco hardware platforms that were supported in Release 12.4(15)T and prior releases. These platforms will be supported by Release 12.4(15)T via regularly scheduled software maintenance rebuilds and bug fix support until the end of software maintenance date for the respective platform is reached.

- Cisco SOHO 90 Series
- Cisco 831, 836, 837, and 850 Series
- Cisco 1701, 1711, 1712, 1721, 1751, 1751-V, and 1760 Series
- Cisco 2610XM-2611XM, 2620XM-2621XM, 2650XM-2651XM, and 2691 Series
- Cisco 3631 and 3660 Series
- Cisco 3725 and 3745 Series
- Cisco 7400 Series

- Cisco AS5850 Universal Gateway

For more information refer to the following product bulletin: Cisco IOS Software Release 12.4(15)T: Last Cisco IOS T Release for Select Cisco Hardware Platforms http://www.cisco.com/en/US/prod/collateral/iosswrel/ps8802/ps6968/ps6441/product_bulletin_c25_466578.html

The Cisco release delivery process, rigorous software testing, and regularly scheduled software maintenance results in significant incremental enhancements and improvement to the quality, stability, and resiliency of Cisco IOS Software Release 12.4T and 12.4.

1.2) Release 12.4T Additional Information

- **Cisco IOS Software Release 12.4T**

  Cisco IOS Software Releases 12.4 T—Products & Services—Cisco Systems

- **Cisco IOS Software Product Lifecycle Dates & Milestones, Product Bulletin No. 2214**

  http://www.cisco.com/en/US/prod/collateral/iosswrel/ps8802/ps6969/ps1835/prod_bulletin0900aecd801eda8a_ps6441_Products_Bulletin.html

- **Changes to Cisco IOS Software Product Support in Release 12.4T, Product Bulletin No. 3000**

  http://www.cisco.com/go/124thardware/

- **Cisco IOS Software Download Center**

  Download Cisco IOS Software releases and access software upgrade planners.

  http://www.cisco.com/public/sw-center/sw-ios.shtml

- **Cisco Feature Navigator**

  A web-based application that allows you to quickly match Cisco IOS Software releases to features, to hardware.

  http://www.cisco.com/go/fn/

- **Cisco Software Advisor**

  Determine the minimum supported software for selected hardware.

  http://tools.cisco.com/Support/Fusion/FusionHome.do

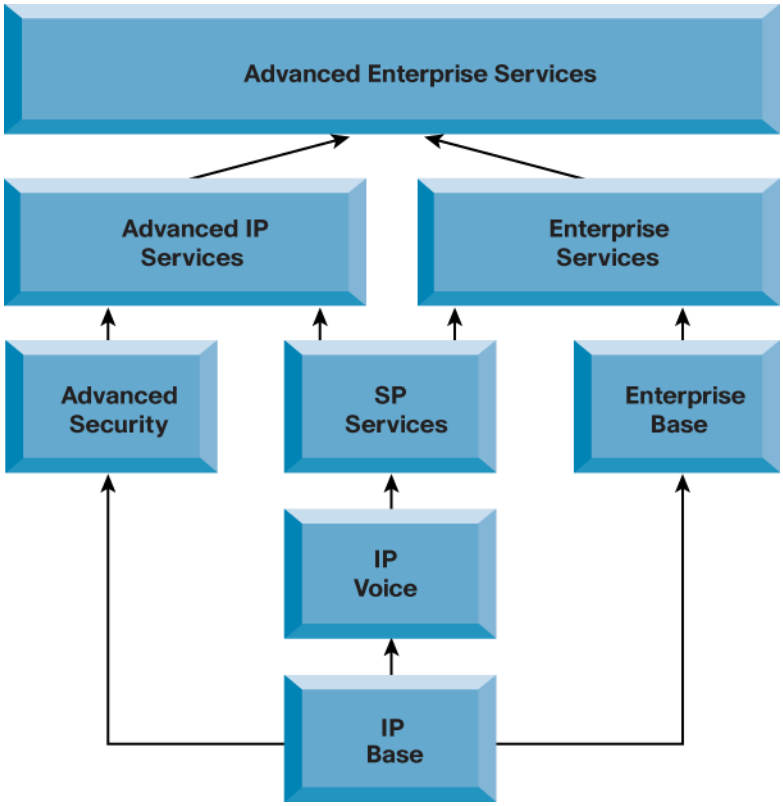
- **Cisco IOS Upgrade Planner**

  View all major releases, hardware, and software features from a single interface.

  http://www.cisco.com/pcgi-bin/Software/Iosplanner/Planner-tool/iosplanner.cgi

1.3) Cisco IOS Packaging

Figure 4. Cisco IOS Packaging for Cisco Routers



2) Release 12.4(22)T Highlights

Table 1. Release 12.4(20)T Feature Highlights

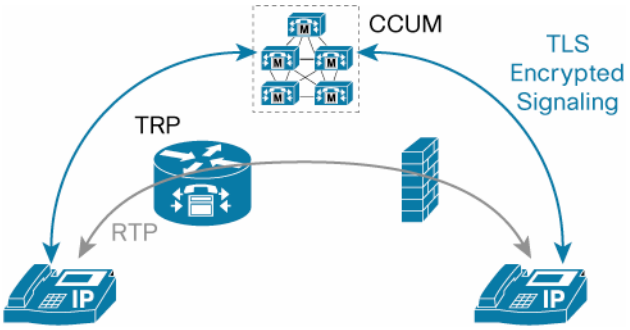
2.1) Cisco IOS Security
2.1.1) IOS Firewall Support for Trusted Relay Point (TRP)
2.1.2) Access Control List (ACL) Syslog Correlation
2.1.3) Per (DMVPN) Tunnel Quality of Service (QoS)
2.1.4) Certificate IP Address Extension Support
2.1.5) Time-based Anti-replay on VPN Services Adapter (VSA)
2.1.6) Group Encrypted Transport VPN (GET VPN) Enhancements
2.1.7) IOS SSL VPN Internationalization
2.1.8) IOS Support for Lawful Intercept

2.1) Cisco IOS Security

2.1.1) IOS Firewall Support for Trusted Relay Point

Cisco IOS firewall enhances security for Unified Communications (UC) by supporting Trusted Relay Point (TRP). This solution provides a trusted anchor within the network for seamless UC related services including media recording, QoS enforcement, and intelligent firewall traversal.

Figure 5. IOS Firewall Trusted Relay Point Use Case Scenario



Trusted Relay Point is a multi-functional architecture covering Quality of Service (QoS), Optimized Edge Routing (OER), and virtual network traversal. It eliminates the deep packet inspection and overhead associated with firewalling by signaling the firewall to permit traffic.

Benefits of UC-Trusted Firewall Control

- Provides authentication required to open port requests on the firewall
- Supports asymmetric signaling/media paths control, cases where signaling and media may not traverse the same paths in the network (such as internal “firewalling”) and might ordinarily be blocked
- Provides encrypted signaling between voice entities, cases where the firewall has the group key to look at the signaling and allow pinholes for media
- Ports for media and signaling remain open for session length only, providing more secure sessions

Hardware

Routers	• Cisco 871, 1800, 2800, 3700, 3800, 7200, and 7301 Series Routers

Product Management Contact: ask-stg-ios-pm@cisco.com

2.1.2) Access Control List (ACL) Syslog Correlation

Cisco IOS ACL Syslog Correlation feature provides a correlation mechanism for ACLs that can be used by Network Management System (NMS) tools to correlate the triggered syslog with the specific Access Control Entry (ACE) within the ACL that triggered the syslog. The ACL Syslog Correlation feature utilizes a 'tag' which is appended to the ACE generated syslog. The 'tag' can either be a user-configured alpha-numeric cookie or an IOS generated 32-bit hash. If the user does not configure the cookie, IOS will create the hash for ACEs configured with the 'log' keyword.

Figure 6. Define a tag to be used for ACE generated syslogs

```
! Define an ACE cookie to monitor access to "red-server" and "blue-server"
ip access-list extended access-control
 permit ip any host 10.10.10.100 log red-server
 permit ip any host 10.10.10.200 log blue-server
 permit ip any any
```

Figure 7. Configured tags are appended to ACE generated syslogs

```
Sep  3 16:31:18.958: %SEC-6-IPACCESSLOGDP: list access-control permitted icmp
192.168.1.100 -> 10.10.10.100 (0/0), 11 packets  [red-server]

Sep  3 16:32:18.953: %SEC-6-IPACCESSLOGDP: list access-control permitted icmp
192.168.1.100 -> 10.10.10.200 (0/0), 3 packets  [blue-server]
```

Benefits

- Provides a consistent monitoring solution for IOS ACLs, allowing network management tools to easily correlate the triggered syslog with the specific Access Control Entry (ACE) within the ACL that triggered the syslog
- Reduces complexity of managing and monitoring ACL rules for access and control by simplifying the correlation of ACE rules with their corresponding syslog events
- Assists network administrators in troubleshooting issues that occur as a result of ACE rules and allows them to monitor ACE rules' effectiveness

Hardware

Routers	• Cisco 800, 1800, 2800, 3700, 3800, and 7200 Series Routers

Additional Information: http://www.cisco.com/go/iossecurity

Product Management Contact: ask-stg-ios-pm@cisco.com

2.1.3) Per Dynamic Multipoint VPN (DMVPN) Tunnel Quality of Service (QoS)

This feature enables the DMVPN hub to dynamically allocate a QoS service policy for each spoke. The DMVPN hub can have multiple QoS policies for all the remote spokes. If QoS is configured, each spoke requests a QoS policy from the hub during Next Hop Resolution Protocol (NHRP) registration. This QoS service policy is applied on the hub in the outbound direction. A typical QoS policy provides multiple classes of service, including a priority queue for voice, and traffic shaping for the total bandwidth of all classes.

Table 2. Detailed Capabilities of DMVPN Per Tunnel QoS Functionality

Feature	Benefit
Dynamic QoS policy allocation for spokes during the NHRP registration with hub	Simplifies QoS configuration on the hub router for dynamically addressed spokes
Cisco Modular QoS CLI (MQC) support configuration in every spoke policy	Allows prioritization to VoIP/delay sensitive data traffic
Protect critical control traffic before and after encryption	Enhances network stability
Dynamic QoS on the hub ensures optimal traffic flow when a spoke connects to the hub	Simplifies QoS enablement in VPN networks
Protect the crypto engine by supporting full tunnel queuing hierarchy in hierarchical queuing format; QoS queuing and shaping happens before encryption	Avoids anti-replay error reporting with IPSec
Shaping and queuing happens at the physical interface	Centralizes QoS policy in the router and simplifies configuration
Protection for critical control traffic before and after encryption	Enhances network stability
Dynamic QoS allocation on the hub router protects the spoke from traffic bursts	Protects small spokes from becoming overwhelmed from large hub sites

Hardware

Routers	• Cisco 800, 1800, 2800, 3700, 3800, and 7200 Series Routers

Additional Information: http://www.cisco.com/go/iossecurity

Product Management Contact: ask-stg-ios-pm@cisco.com

2.1.4) Certificate IP Address Extension Support

This feature enables support for RFC3779, X.509 Extensions for IP addresses. One of the first protocols to use this feature will be the SEcure Neighbor Discovery Protocol (SEND). IPv6 hosts run Neighbor Discovery Protocol (NDP) to discover other devices on a link. If this link is not secured, NDP is vulnerable to various attacks such as neighbor solicitation/advertisement spoofing and duplicate address detection DoS attacks. SEND is designed to counter the threats to NDP and can use X.509 IP extensions to provide a stronger control on prefix advertisements.

Note that with SEND, RFC3779 (X.509 Extensions for IP addresses) is an optional feature. While SEND will provide its full capabilities with this version of PKI, it could still be deployed with older PKI versions that don't support IP extensions.

Benefits

- Generates certificates with IP extensions
- Counters threats to NDP
- Allows for stronger control on prefix advertisements

Hardware

Routers	• Cisco 87x, 88x, 1800, 2800, 3700, 3800, 7200, and 7301 Series Routers

Additional Information:
http://www.cisco.com/en/US/products/ps6638/products_ios_protocol_group_home.html

Product Management Contact: ask-stg-ios-pm@cisco.com

2.1.5) Time-Based Anti-Replay on The VPN Services Adapter (VSA)

This feature enables Time-Based Anti-Replay (TBAR) support on the VPN Services Adapter (VSA) of the 7200 NPE-G2 platform. TBAR is used in the Group Encrypted Transport VPN (GETVPN) solution to detect replay attacks since standard sequence-based anti-replay attack detection is not supported. This feature prevents ‘man in the middle’ attacks.

The Cisco GETVPN solution allows organizations to have branch-to-branch secure connectivity without having to incur the cost of establishing and maintaining full-mesh connections.

Benefits

- Supports anti-replay in the Cisco GET VPN solution
- Allows protection against ‘man in the middle’ attacks, bolstering overall GET VPN security

Hardware

Routers	• Cisco 7200 with Network Processing Engine (NPE) G2

Additional Information: http://www.cisco.com/go/vsa

Product Management Contact: ask-stg-ios-pm@cisco.com

2.1.6) Group Encrypted Transport VPN (GET VPN) Enhancements

Several new GET VPN feature enhancements are introduced in Release 12.4(22)T:

- **Passive Security Association (SA)**

  This feature enables a new mode of IPSec Security Association (SA) with GET VPN. In this mode, the SA will accept unencrypted traffic and encrypted traffic on the inbound, while it will always encrypt traffic on the outbound. Passive SA mode is configured on the Group Member (GM), and is persistent over router restarts: this allows the Group Member to modify the SAs downloaded from the Key Server (KS). Passive SA can be used similar to the SA receive-only to enable transitions in large scale deployment.

- **Fail-Close**

  This feature enables GET VPN traffic forwarding to follow the “fail-close” model, wherein an unregistered Group Member (GM) stops forwarding data packets rather than send them out unencrypted.

  The fail-close command sets up an implicit “permit ip any any” at the end of the crypto map during the pre-registration phase. Post successful GDOI registration, the “permit ip any any” is removed from the crypto map.

  You can specify exceptions that need to be forwarded in the clear, through a deny entry in the ACL. This is useful to allow routing packets and management packets from a particular host to get through. However, note that the deny ACL in the GDOI crypto map still takes precedence. After the registration is successful, the deny entry in the ACL goes away while the deny entry in the GDOI crypto map is persistent.

  Once the GM is successfully registered to all its groups, the policies downloaded from the KS take over, governing the GMs behavior and the fail-close ACL and implicit “permit ip any any” are taken out. GMs keep the policies downloaded from the KS even if the re-registration fails and IPSec SA has expired.

  When fail-close is activated, unencrypted packets are prevented prior to and during registration. Once the GM is successfully registered to all its groups however, the policies

downloaded from the KS take over, governing the GMs behavior and the fail-close ACL and implicit “permit ip any any” are dropped. GMs keep the policies downloaded from the KS even if the re-registration fails and IPSec SA has expired.

Note: GET VPN supported fail-close previously, using an interface ACL. With the above feature, interface ACL may not be required. Fail-close with interface ACL might still be useful to customers looking to enforce a policy that certain packets must always be encrypted, regardless of the downloaded key server policy.

- **Change Key Server Role**

  This feature allows you to switch the primary Key Server (KS)by forcing an election. Issuing the new **clear crypto gdoi ks coop role** command on the primary Key Server makes it relinquish the primary role and initiate an election. If the priorities have changed, a new primary will be declared elected. Note: This command does not clear any policies—it merely facilitates switching the primary KS.

- **Co-operative Key Server: Sharing Keys**

  This feature optimizes the number of rekeys that are sent out in the event of a network split, thereby allowing the network to stabilize rapidly. When there is a network split, a secondary KS takes the partition that cannot reach the primary; with this new feature, the new primary reuses the existing policies where possible. At split, the rekey is sent only if there are keys that are due to expire within the lifetime threshold (150 seconds). Unless this threshold is met, the current keys and policies are retained on the KS separated from the primary. This new ability to share the keys created by another KS reduces the number of policies to manage, thereby improving the cooperation between the KS’es.

- **Re-key From Secondary on Merge**

  This feature distributes rekeying when a partitioned network merges back. When the merge occurs, the newly-demoted secondary KS takes responsibility to send out rekeys to the group members in its database. The primary KS is freed from having to send out all rekeys, and is able to focus on sending rekeys to only the members in its own database.

Benefits

- Enables controlled deployments in phases
- Provides ability to eliminate flow of unencrypted data packets
- Allows primary key server to be changed midstream ie: for scheduled maintenance
- Optimizes cooperative key server communications during split and merge, providing better stability

Hardware

Routers	• **Group Member (GM):** Cisco 870, 88, 1800, 2800, 3800 and 7200 Series and Cisco 7301 • **Key Server (KS):** Cisco 1840, 2800, 3800 and 7200 Series and Cisco 7301

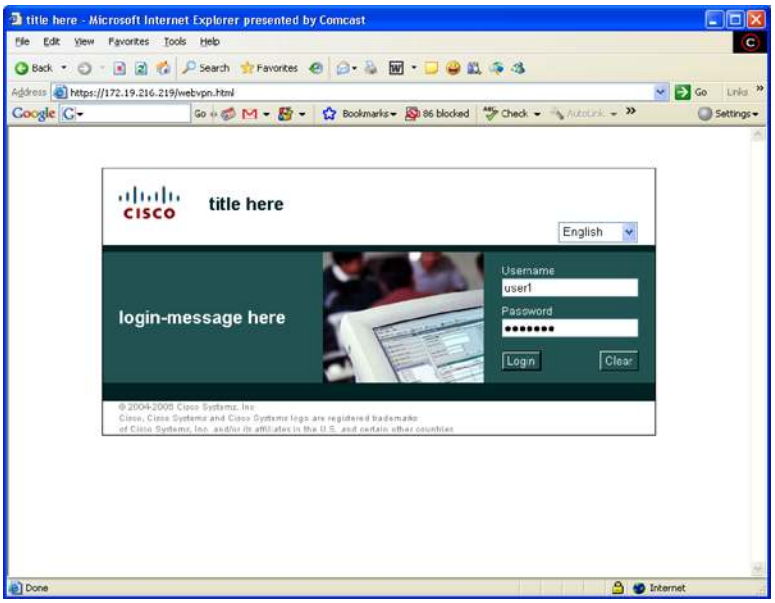
Additional Information: http://www.cisco.com/go/getvpn

Product Management Contact: ask-stg-ios-pm@cisco.com

2.1.7) IOS SSL VPN Internationalization

Cisco IOS SSL VPN Internationalization lays the framework to support multiple languages in the login and portal pages. Users will be able to select their language preference for their session from a drop down menu at the time of login.

Figure 8. IOS SSL VPN Internationalization Support



Benefits

- Allows content to be presented in the local language.

Hardware

Routers	• Cisco 87x, 88x, 1800, 2800, 3700, 3800, 7200, and 7301 Series Routers

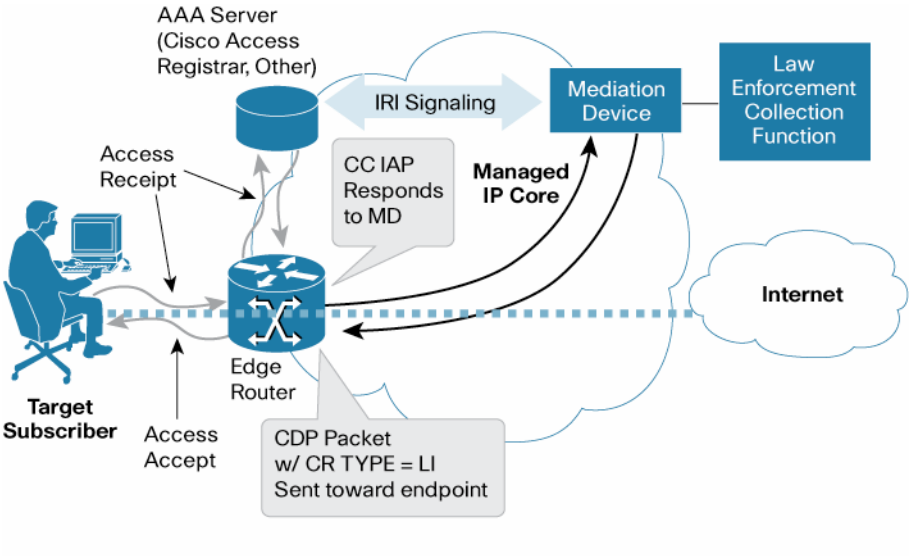
Additional Information: http://www.cisco.com/go/iossslvpn

Product Management Contact: ask-stg-ios-pm@cisco.com

2.1.8) IOS Support for Lawful Intercept

Cisco IOS provides a cost effective, yet powerful Communications Assistance for Law Enforcement Act (CALEA) compliant solution with the ability to monitor digital communications. The Cisco Service Independent Intercept (SII), Control Point Discovery (CPD) and Packet Cable 2.0 support Dynamic Discovery of Intercept Access Point (IAP). Cisco Lawful Intercept provides an out-of-band control mechanism when using a third-party mediation device to request intercepts on the network elements within the organizations trust boundaries. When performing captures for Lawful Intercept, this activity is transparent to everything else going on in the network, providing access only to authorized personnel.

Figure 9. IOS Control Point Discovery (CPD) Lawful Intercept - Use Case Scenario



1. The Cisco IOS Router will act as a platform for lawful intercept, offering a complete end-to-end solution for the network with all communication sessions and intercept details preserved.
2. The Cisco Lawful Intercept solution offers scalable packet captures and an effective, powerful solution for organizations looking to comply with CALEA requirements.

Benefits

- Cost effective way to leverage existing infrastructure to meet LI regulatory obligations
- Provides easy, proactive compliance and offers quick deployment

Hardware

Routers	• Cisco 7200 Routers

Product Management Contact: ask-stg-ios-pm@cisco.com

3) Release 12.4(20)T Highlights

Table 3. Release 12.4(20)T Feature Highlights

3.1) Cisco IOS Security
3.1.1) Group Encrypted Transport VPN (GET VPN) Support for the Cisco VPN Services Adapter (VSA) for Cisco 7200 NPE-G2 Series Routers
3.1.2) Cisco IOS Content Filtering
3.1.3) VRF-Aware Cisco IOS Intrusion Prevention System (IPS)
3.1.4) User-based Cisco IOS Firewall
3.1.5) Application Inspection and Control for Simple Mail Transfer Protocol (SMTP)
3.1.6) Cisco IOS Firewall Support for Skinny Local Traffic
3.1.7) Cisco IOS Firewall Session Initiation Protocol (SIP) Application Layer Gateway (ALG) Enhancements
3.1.8) Cisco IOS Firewall H.323 Version 3 (v3) and Version 4 (v4) Support
3.1.9) Instant Messaging Blocking Support in Cisco IOS Firewall for “I Seek You” (ICQ) and Windows Messenger
3.1.10) Object Groups for Access Control Lists (ACLs)
3.1.11) Cisco IOS SSL VPN Access Control Enhancements
3.1.12) Cisco IOS SSL VPN AnyConnect Client Support
3.1.13) Cisco IOS SSL VPN Back End HTTP Proxy
3.1.14) Cisco IOS SSL VPN Full-Tunnel Performance Enhancements
3.1.15) Cisco IOS SSL VPN URL Split Rewrite Support
3.1.16) Next Hop Resolution Protocol (NHRP) MIB for Dynamic Multipoint VPN (DMVPN)
3.1.17) IPv6 Over Dynamic Multipoint VPN (DMVPN) Support
3.1.18) Group Encrypted Transport (GET) VPN Support for VRF-Lite
3.1.19) Cisco Tunnel Control Protocol (cTCP) Support on Easy VPN Hardware Clients
3.1.20) IPSec Usability Enhancements
3.1.21) Secure Shell Protocol Version 2 (SSHv2) Feature Enhancements
3.1.22) Command Line Interface (CLI) for Displaying Certificates
3.1.23) CLI to Control Certification Revocation List (CRL) Cache
3.1.24) Secure Device Provisioning (SDP) Connect Template

3.1) Cisco IOS Security

3.1.1) Group Encrypted Transport VPN (GET VPN) Support for the Cisco VPN Services Adapter (VSA) for Cisco 7200 NPE-G2 Series Routers

Cisco IOS Release 12.4(20)T adds GET VPN support for the Cisco VSA, the latest high-performance encryption and key-generation services module for IPSec VPN applications on Cisco 7200 NPE-G2 Series Routers.

GET VPN offers a new standards-based IP Security (IPSec) security model that is based on the concept of "trusted" group members. Trusted member routers use a common security methodology that is independent of any point-to-point IPSec tunnel relationship. GET VPN simplifies securing large Layer 2 or MPLS networks requiring partial or full-mesh connectivity.

Benefits

The VSA offers increased IPSec performance over the Cisco VPN Acceleration Module 2+ (VAM2+) module.

Hardware

Routers	• Cisco 7200 NPE-G2 Series Routers

Additional Information:

http://www.cisco.com/go/vsa

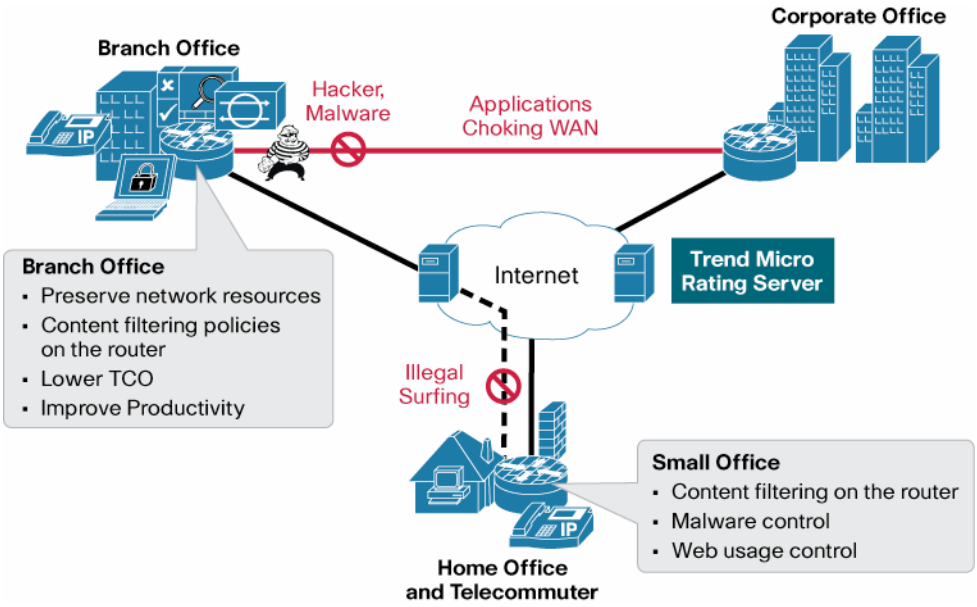
http://www.cisco.com/go/getvpn

Product Management Contact: ask-stg-ios-pm@cisco.com

3.1.2) Cisco IOS Content Filtering

Cisco IOS Content Filtering offers category-based productivity and security ratings. Content-aware security ratings protect against malware, malicious code, phishing attacks, and spyware. URL and keyword blocking help to ensure that employees are productive when accessing the Internet. This is a subscription-based hosted solution that leverages Trend Micro's global TrendLabs™ threat database, and is closely integrated with Cisco IOS Software. It is supported on routers running the Advanced Security image. Feature licenses can be purchased directly from the Cisco.com ordering tool or through your Cisco partner/account team.

Figure 10. IOS Content Filtering Use Case Scenario



Benefits

- Secures Internet access to branch, without the need for additional devices
- Controls spyware and malware at the remote site; conserves WAN bandwidth
- Improves employee productivity and protects network resources by enabling content filtering

Hardware

Routers	• Cisco 800, 1800, 2800, and 3800 Series Routers

Additional Information: http://www.cisco.com/go/ioscontentfiltering

Product Management Contact: ask-stg-ios-pm@cisco.com

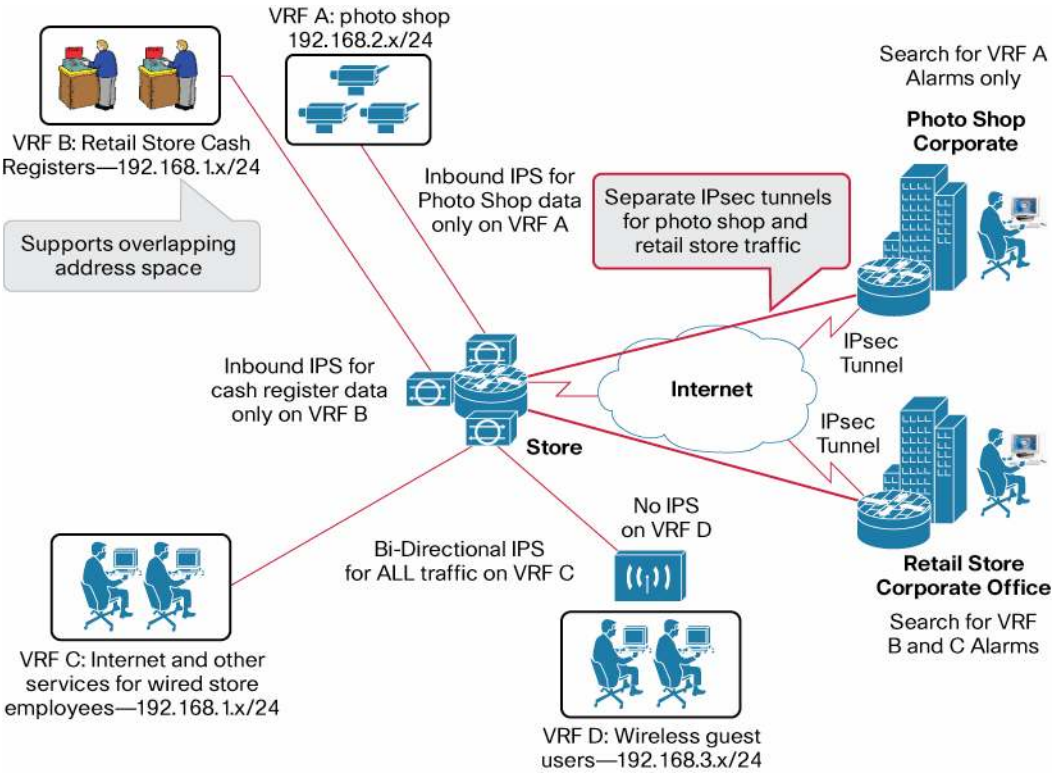
3.1.3) VRF-Aware Cisco IOS Intrusion Prevention System (IPS)

VRF-Aware Cisco IOS IPS allows Enterprises or service providers to put different groups of users or network segments into separate Virtual Routing and Forwarding (VRF) groups and to configure IPS on only certain VRFs or to configure IPS differently on each VRF. Divisions or functional groups separated by VRF segments may have different threat protection needs. Examples include:

- Vendor-provided applications vs. native applications
- Administrative users vs. regular employees vs. contractors/guests
- Vendor (photo shop, deli, pharmacy, etc.) network vs. point-of-sale network
- Students vs. faculty members vs. school administration

VRF-aware Cisco IOS IPS will also enable network security operators to distinguish between the IPS event alarms generated within each user group or network segment based on their VRF ID.

Figure 11. Typical Use Case for VRF Aware Cisco IOS IPS



Benefits

- Allows the configuration of IPS on only certain virtual network segments (VRFs) or in a different way on each VRF
- Distinguishes between IPS alarms/events generated within each group (VRF segment) based on VRF ID
- Supports IPS on VRF interfaces in addition to physical interfaces with or without overlapping IP addresses

Hardware

Routers	• Cisco 800, 1800, 2800, 3800, and 7200 Series Routers

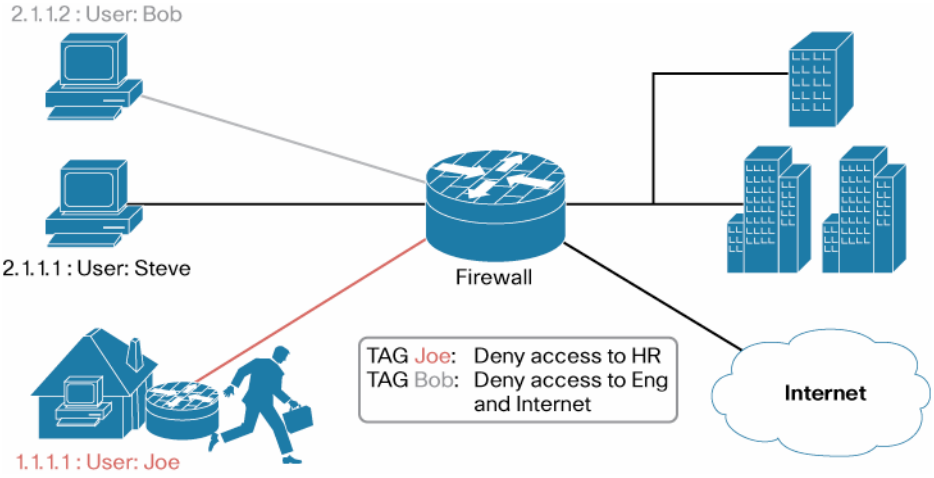
Additional Information: http://www.cisco.com/go/iosips

Product Management Contact: ask-stg-ios-pm@cisco.com

3.1.4) User-based Cisco IOS Firewall

Cisco IOS Firewall offers the ability to deploy secure access policies at all network interfaces: Internet perimeter, remote-site connectivity, business-partner access, and telecommuter connections. User-based Cisco IOS Firewall dynamically binds unique zone-based firewall policies to a group where members, regardless of IP address entry point, are authorized using authentication proxy or Network Admission Control (NAC).

Figure 12. User based Cisco IOS Firewall Example



Benefits

- Facilitates the support of Enterprise mobile workers where user access is dynamic, while maintaining source IP address and user group associations
- Secures granular access to the branch, without the need for additional devices
- Enforces non-intrusive, per-user security policies

Hardware

Routers	• Cisco 800, 1800, 2800, 3800, 7200 Series, 7301 Routers

Additional Information: http://www.cisco.com/go/iosfw

Product Management Contact: ask-stg-ios-pm@cisco.com

3.1.5) Application Inspection and Control for Simple Mail Transfer Protocol (SMTP)

Cisco IOS Firewall Application Inspection and Control (AIC) has expanded the SMTP capability to support a more detailed inspection, providing more control over how SMTP inspection is performed.

Benefits

- Inspects SMTP at a more granular level
- Scans actual e-mail data like attachment types and encoding types

- Detects a limited number of attack signatures
- Ability to use signatures in SYSLOG message alerts to warn of a possible attack, such as the detection of illegal SMTP commands in a packet

Hardware

Routers	• Cisco 800, 1800, 2800, 3800, 7200, and 7301 Series Routers

Additional Information: http://www.cisco.com/go/iosfw

Product Management Contact: ask-stg-ios-pm@cisco.com

3.1.6) Cisco IOS Firewall Support for Skinny Local Traffic

Cisco IOS Firewall enhances Skinny Local Traffic support. This feature offers inspection for locally generated and locally terminated SKINNY protocol data in two main deployment scenarios:

1. Cisco Call Manager Express (CME) is enabled on the Cisco IOS Firewall and manages the VoIP phones using SCCP over intranet or Internet.
2. Analog and VoIP phones are connected and managed by the Cisco IOS Firewall-enabled CME router.

Benefits

- Improves user groups SCCP locally generated traffic support
- Provides inspection of CME using SCCP over the intranet/Internet

Hardware

Routers	• Cisco 800, 1800, 2800, 3800, 7200, and 7301 Series Routers

Additional Information: http://www.cisco.com/go/iosfw

Product Management Contact: ask-stg-ios-pm@cisco.com

3.1.7) Cisco IOS Firewall Session Initiation Protocol (SIP) Application Layer Gateway (ALG) Enhancements

Cisco IOS Firewall SIP ALG and protocol inspection feature prevents unauthorized calls, call hijacking, SIP protocol exploits, and related DoS attacks. It supports both pass-through and local traffic.

Benefits

- Removes malformed packets from reaching Cisco Unified Communications Manager at the head office

Hardware

Routers	• Cisco 800, 1800, 2800, 3800, 7200, and 7301 Series Routers

Additional Information: http://www.cisco.com/go/iosfw

Product Management Contact: ask-stg-ios-pm@cisco.com

3.1.8) Cisco IOS Firewall H.323 Version 3 (v3) and Version 4 (v4) Support
Cisco IOS Firewall adds support for H.323 v3 and v4 to maintain high availability of mission-critical IP telephony calls while upholding high level call experience.

Benefits

- Includes H.323 v3 and v4 Annex E, Annex G, and Annex D support
- Supports H.323 v3 and v4 fax and call transfer capabilities

Hardware

Routers	• Cisco 800, 1800, 2800, 3800, 7200, and 7301 Series Routers

Additional Information: http://www.cisco.com/go/iosfw

Product Management Contact: ask-stg-ios-pm@cisco.com

3.1.9) Instant Messaging Blocking Support in Cisco IOS Firewall for “I Seek You” (ICQ) and Windows Messenger
Cisco IOS Firewall Application Inspection and Control (AIC) adds comprehensive management and control of Instant Messaging (IM) applications such as ICQ and Windows Messenger.

Benefits

- Detects, blocks or throttles ICQ and Windows Messenger services
- Enforces associated policy of “I Seek You” (ICQ) Instant Messenger Version 2001b and above as well as Windows Instant Messenger Version 5.1
- Provides granular control when managing things such as file transfers and attachments, application sharing, games, video/audio conferencing, and pop-ups
- Offers the ability to send syslog information of the event

Hardware

Routers	• Cisco 800, 1800, 2800, 3800, 7200, 7301 Series Routers

Additional Information: http://www.cisco.com/go/iosfw

Product Management Contact: ask-stg-ios-pm@cisco.com

3.1.10) Object Groups for Access Control Lists (ACL)
ACL Object Groups allow network administrators to classify users, devices, and protocols into groups allowing them to apply policies based on group classification. IP hosts and networks, protocols and ports are defined in object groups. Once configured, object groups can then be used in the place of IP addresses, protocols or ports within Access Control Lists (ACLs).

The two steps required to configure object groups for ACLs is shown below:

Step 1. Define the Object Group:

```
! Define network type object-groups to group IP hosts and networks
object-group network Engineering
```

```
  10.240.12.0 255.255.255.0
  10.245.10.0 255255.255.0
object-group network Web-Servers
  10.1.1.0 255.255.255.0
   host 10.10.10.100
object-group network Mail-Servers
  10.32.1.0 255.255.255.0

! Define a service type object group to group you protocols and ports
object-group service Web-ports
  tcp www
  tcp 8080
object-group service Mail-ports
  tcp smtp
  tcp pop3
  tcp 587
  tcp 143
```

Step 2. Use Object Groups in ACL Configurations:

```
ip access-list extended access-policy
  10 permit object-group Web-ports object-group Engineering object-group
Web-Servers
  20 permit object-group Mail-ports object-group Engineering object-group
Mail-Servers
```

Benefits

- Provides a simple and intuitive mechanism for configuring and managing large ACLs, especially ones that frequently change
- Reduces ACL configuration size and make ACLs more readable and easier to manage

Hardware

Routers	• Cisco 800, 1800, 2800, 3800, 7200, and 7301 Series Routers

Additional Information: http://www.cisco.com/go/iosfw

Product Management Contact: ask-stg-ios-pm@cisco.com

3.1.11) Cisco IOS SSL VPN Access Control Enhancements

Depending on the network security design, the need to repeatedly provide user credentials to gain secure access may be redundant. This is especially true for cellular providers that authenticate users as they join the network. Using Cisco IOS SSL VPN Access Control Enhancements, login credentials can be embedded in the URL used by the client machine to connect to the SSL VPN gateway. Users would not be challenged for credentials but would instead immediately start their secure SSL VPN session.

Benefits

- Simplifies the user login procedures
- Reduces intrusive and repetitive login prompts

Hardware

Routers	• Cisco 800, 1800, 2800, 3800, 7200, and 7301 Series Routers

Additional Information: http://www.cisco.com/go/iossslvpn

Product Management Contact: ask-stg-ios-pm@cisco.com

3.1.12) Cisco IOS SSL VPN AnyConnect Client Support

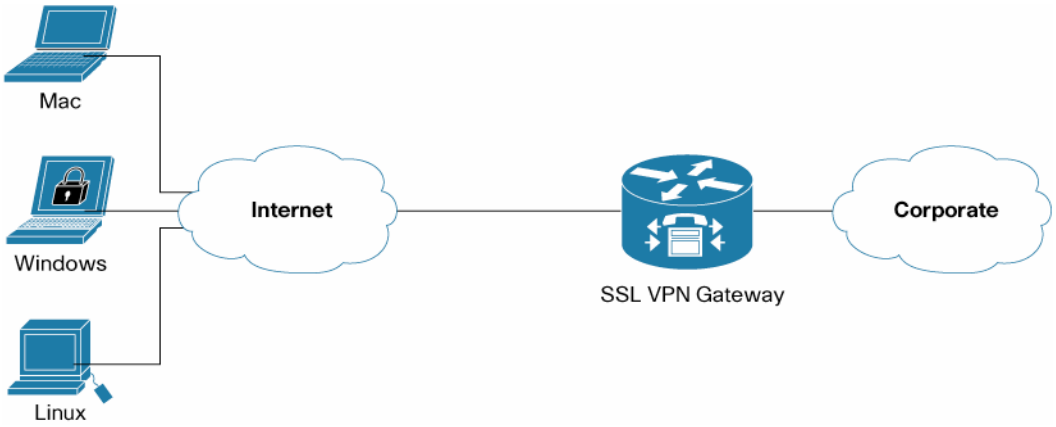
AnyConnect is the Cisco next generation SSL VPN client. It replaces the current Cisco SSL VPN Client (SVC), and requires no pre-installation or pre-configuration on the client machine.

The Cisco IOS SSL VPN AnyConnect Client is pushed from the secure gateway to the client machine when needed. Traffic is encrypted and authenticated using a Layer 2 tunneling functionality that is similar to traditional IPSec, and is agnostic to traffic type. Performance is greatly improved because there is no need to apply URL mangling on the secure traffic as is required with clientless connections.

AnyConnect provides added functionality beyond the current SVC client with support for multiple operating systems including Windows Vista, Apple Mac OS X, and Linux. Administrators can now support a mixed operating system network environment.

Once pushed down to the user, the Cisco AnyConnect client can be configured to stay installed so that subsequent connections do not require repeated downloads and installations. Standalone mode allows users to initiate new SSL VPN tunnel sessions without the need of a web browser, simplifying the login procedure.

Figure 13. Cisco IOS SSL VPN AnyConnect Client Support



Benefits

- Avoids pre-configuration and pre-installation requirements
- Improves performance over clientless only traffic

- Offers support for multiple operating systems
- Reduces bandwidth requirements in Standalone mode

Hardware

Routers	• Cisco 800, 1800, 2800, 3800, 7200, and 7301 Series Routers

Additional Information: http://www.cisco.com/go/iossslvpn

Product Management Contact: ask-stg-ios-pm@cisco.com

3.1.13) Cisco IOS SSL VPN Back End HTTP Proxy

In the past, all clientless mode user requests were sent to internal servers directly. This meant that the internal servers had to be directly addressable by the SSL VPN gateway for connectivity to succeed. This feature enhancement adds HTTP proxy client functionality to the Cisco IOS SSL VPN gateway so requests can now be passed through to an internal proxy server in the protected network.

Benefits

- Provides increased flexibility and control in supporting more diverse internal network architectures

Hardware

Routers	• Cisco 800, 1800, 2800, 3800, 7200, and 7301 Series Routers

Additional Information: http://www.cisco.com/go/iossslvpn

Product Management Contact: ask-stg-ios-pm@cisco.com

3.1.14) Cisco IOS SSL VPN Full-Tunnel Performance Enhancements

Cisco Express Forwarding (CEF) Scalability and Selective Rewrite (CSSR) technology for IP has been added to full-tunnel mode as well as clientless SSL VPN deployments. Combining CSSR with SSL VPN full-tunnel traffic provides greater throughput and reduces router CPU utilization.

Note: CSSR, supported in Cisco IOS Release 12.4(20)T onward, is a scalable, distributed, Layer 3 switching technology designed to meet the future performance requirements of Enterprise networks. Refer to the Cisco IOS Infrastructure section for more information on CSSR support.

Benefits

- Increases scalability and performance

Hardware

Routers	• Cisco 800, 1800, 2800, 3800, 7200, and 7301 Series Routers

Additional Information: http://www.cisco.com/go/iossslvpn

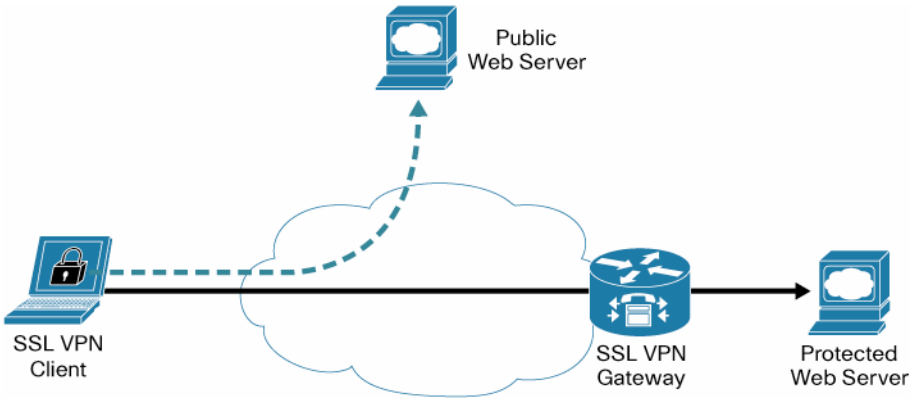
Product Management Contact: ask-stg-ios-pm@cisco.com

3.1.15) Cisco IOS SSL VPN URL Split Rewrite Support

In SSL VPN clientless operation, the SSL VPN gateway acts as a proxy between client and server, inspecting all web-based traffic and rewriting URLs in the content. This process is very CPU intensive and time consuming, affecting performance and scalability.

Conceptually similar to split tunneling in IPSec, the URL Split Rewrite for Cisco IOS SSL VPN feature enables the administrator to select which URLs are processed through the SSL VPN gateway, and which URLs the client can reach directly. Internal web-based connections to protected resources are still processed normally through the SSL VPN gateway, while external traffic can be allowed a direct connection.

Figure 14. Cisco IOS SSL VPN URL Split Rewrite Support



Benefits

- Provides flexibility to selectively define what traffic needs SSL VPN protection
- Improves scalability and performance by not having to process all of a remote users traffic

Hardware

Routers	• Cisco 800, 1800, 2800, 3800, 7200, and 7301 Series Routers

Additional Information: http://www.cisco.com/go/iossslvpn

Product Management Contact: ask-stg-ios-pm@cisco.com

3.1.16) Next Hop Resolution Protocol (NHRP) MIB for Dynamic Multipoint VPN (DMVPN)

To manage DMVPN deployments most effectively, administrators are not only interested in knowing about individual IPSec and tunnel protected Multipoint GRE (mGRE) tunnels, but also the control plane (ie: NHRP) statistics associated with corresponding tunnels.

The NHRP MIB for DMVPN feature addresses this by providing information on NHRP usage, routes, sessions, NHRP supported hub maximum throughput, and memory in a DMVPN network.

Benefits

- Improves manageability of DMVPN networks.

Hardware

Routers	• Cisco 800, 1800, 2800, 3800, 7200, and 7301 Series Routers

Additional Information: http://www.cisco.com/go/dmvpn

Product Management Contact: ask-stg-ios-pm@cisco.com

3.1.17) IPv6 Over Dynamic Multipoint VPN (DMVPN) Support

DMVPN has added support for IPv6 in combined IPv4 and IPv6 network environments. Where secure connectivity is required, DMVPN can now be used to connect IPv4 and IPv6 networks.

Benefits

- Supports standards-based IPv6
- Supports IPSec native mode

Hardware

Routers	• Cisco 800, 1800, 2800, 3800, 7200, and 7301 Series Routers

Additional Information: http://www.cisco.com/go/dmvpn

Product Management Contact: ask-stg-ios-pm@cisco.com

3.1.18) Group Encrypted Transport (GET) VPN Support for VRF-Lite

GET VPN support for VRF-Lite allows Enterprises or service providers to support multiple VPN Routing and Forwarding (VRF) instances on Customer Edge (CE) devices. VRF-Lite extends limited Provider Edge (PE) functionality to a CE device, giving it the ability to maintain separate VRF tables and extending the privacy and security of a VPN to the branch office. This also allows the capability of sharing the same CE device for various internal departments while maintaining separate VRF tables for each department.

The GET VPN key server is not VRF aware. As a result, there can be 2 possible scenarios (cases) for deployment depending on whether single or multiple MPLS VPNs (PE VRFs) are used on the PE router for each GETVPN group:

- **Case 1:** PE uses a single MPLS VPN (PE VRF) for all group member VRFs (CE VRFs). For this, group members can use the same certificate for authentication, for all the crypto maps applied on VRF interfaces. No overlapping addresses can be supported in the group member VRFs because the PE has all the group member addresses in a single VRF. However, traffic excluded from any of the encryption policies are subject to be routed across group member VRFs.
- **Case 2:** To use overlapping addresses between group member VRFs, the PE router should use a unique MPLS VPN (PE VRFs) for each group member VRFs. In addition, a separate key server must be dedicated to each VRF because the key server is not VRF-aware. Group members should also use a separate certificate to authenticate each crypto map.

Benefits

- Allows customers to share the same CE router for various internal departments while maintaining separate VRF tables for each department

Hardware

Routers	• Cisco 800, 1800, 2800, 3800, 7200, and 7301 Series Routers

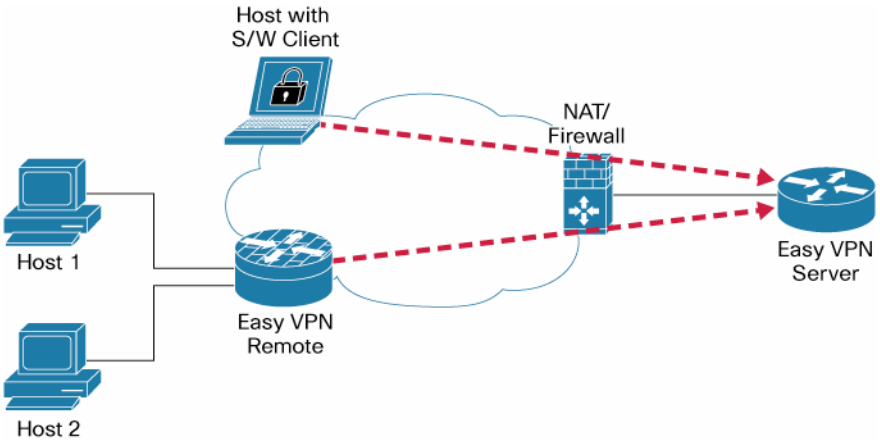
Additional Information: http://www.cisco.com/go/getvpn

Product Management Contact: ask-stg-ios-pm@cisco.com

3.1.19) Cisco Tunnel Control Protocol (cTCP) Support on Easy VPN Hardware Clients

There are many situations where customers require a VPN client to operate in an environment where standard ESP (Protocol 50) or UDP 500 (IKE) can either not work, or not function transparently without modifications to existing firewall rules. With Cisco Tunnel Control Protocol (cTCP), users can establish VPN tunnels from the client to an Easy VPN Server through a third-party Network Address Translation (NAT) device or firewall.

Figure 15. Cisco Tunnel Control Protocol (cTCP) Support on Easy VPN Hardware Clients



Benefits

- Requires no modification of firewall rules
- Creates fewer limitations from where clients can connect
- Offers transparent interoperability with third party firewalls

Hardware

Routers	• Cisco 800, 1800, 2800, 3800, 7200, and 7301 Series Routers

Additional Information: http://www.cisco.com/go/easyvpn

Product Management Contact: ask-stg-ios-pm@cisco.com

3.1.20) IPSec Usability Enhancements

A variety of IPSec usability enhancements are being introduced in Release 12.4(20)T:

Intelligent Defaults

Support for eight Internet Key Exchange (IKE) default policies and IPSec transform set policies. By default, the IKE option is turned on. The default IPSec transform set will be used only if no other transform set is configured for a crypto map.

To display the default IKE policy, the following CLI command has been created:

```
show crypto isakmp default policy
```

If the default policies are turned off, then show crypto isakmp default policy will not display the default policies. If the user configures the isakmp policy then the default policy will not be used during negotiation. This command is not available in the K8 images.

To display the default IPSec transform set policy, the following CLI command has been created:

```
show crypto ipsec default  transform-set
```

The default transform-sets is not available in the K8 images.

IPSec Show Command Enhancements

Using IOS `show` commands to display MIB agent maintained data helps monitor CPE devices. The following show commands are some examples (MIB table information is for a specific VRF if the VRF-name is provided; otherwise, the information for all vrfs is displayed):

```
show crypto mib isakmp flowmib failure { vrf <vrf-name> }
show crypto mib isakmp flowmib global  { vrf <vrf-name> }
show crypto mib isakmp flowmib history  { vrf <vrf-name>}
```

Show Tech Support IPSEC

Often to resolve technical issues, multiple `show` commands need to be executed and the output needs to be collected. To simplify this process, the show `tech-support IPSEC  [vrf <vrf>] [peer-ip <address>]` has been created to collect the same output in one show command.

Benefits

- Improves administration
- Simplifies configuration with default policies
- Improves problem reporting

Hardware

Routers	• Cisco 800, 1800, 2800, 3800, 7200, and 7301 Series Routers

Additional Information: http://www.cisco.com/go/ipsec

Product Management Contact: ask-stg-ios-pm@cisco.com

3.1.21) Secure Shell Protocol Version 2 (SSHv2) Feature Enhancements
A number of SSHv2 enhancements have been added including additional debugging functionality, VRF-aware SSH support, SSH keyboard mode, and Diffie-Hellman group exchange key support for mods 2048 and 4096.

Benefits

- Simplifies debugging
- Supports larger Diffie-Hellman key sizes
- Provides VRF-aware SSH client-side functionality

Hardware

Routers	• Cisco 800, 1800, 2800, 3800, 7200, 7301 Series Routers

Additional Information:
http://www.cisco.com/en/US/products/ps6665/products_ios_protocol_option_home.html

Product Management Contact: ask-stg-ios-pm@cisco.com

3.1.22) Command Line Interface (CLI) for Displaying Certificates
Cisco IOS CLI introduces a new command to allow administrators to easily display all certificates in the Cisco IOS Certificate Server database.

Benefits

- Improves manageability by allowing all certificates in the Cisco IOS Certificate Store (CS) database to be displayed

Hardware

Routers	• Cisco 800, 1800, 2800, 3800, 7200, and 7301 Series Routers

Additional Information:
http://www.cisco.com/en/US/products/ps6638/products_ios_protocol_group_home.html

Product Management Contact: ask-stg-ios-pm@cisco.com

3.1.23) CLI to Control Certification Revocation List (CRL) Cache
When processing X.509 certificates, the Certificate Revocation List (CRL) is consulted. To improve performance of certificate validation, IOS keeps a cache of the downloaded CRL in volatile storage on the router. Instead of using a fixed amount of volatile memory, administrators can reduce the cache size for low memory conditions or increase it for better performance when dealing with a large number of CRLs.

Benefits

- Helps to optimize router memory allocation

Hardware

Routers	• Cisco 800, 1800, 2800, 3800, 7200, and 7301 Series Routers

Additional Information:
http://www.cisco.com/en/US/products/ps6638/products_ios_protocol_group_home.html

Product Management Contact: ask-stg-ios-pm@cisco.com

3.1.24) Secure Device Provisioning (SDP) Connect Template
SDP Connect Template increases the usability and range of applications for configuring the device for Internet connectivity. This eases the deployment process for routers, particularly routers that do not already have Internet connectivity.

Benefits

- Eases deployment burden on administrators
- Reduces deployment costs

Hardware

Routers	• Cisco 800, 1800, 2800, 3800, 7200, and 7301 Series Routers

Additional Information:
http://www.cisco.com/en/US/products/ps6638/products_ios_protocol_group_home.html

Product Management Contact: ask-stg-ios-pm@cisco.com

4) Release 12.4(15)T Highlights

Table 4. Release 12.4(15)T Feature Highlights

4.1) Cisco IOS Security
4.1.1) Cisco IOS Intrusion Prevention System (IPS) Support for Microsoft Vulnerabilities *
4.1.2) Flexible Packet Matching (FPM) Full Packet Filtering *
4.1.3) Cisco IOS SSL VPN Enhancements
4.1.4) Cisco IOS Software Support for AnyConnect VPN Client
4.1.5) Reverse Route Injection Distance Metric Enhancements

* Indicates Key Highlight

4.1) Cisco IOS Security

4.1.1) Cisco IOS Intrusion Prevention System (IPS) Support for Microsoft Vulnerabilities

Cisco IOS Intrusion Prevention System (IPS) is an inline, deep-packet inspection-based feature that enables Cisco IOS Software to effectively mitigate a wide range of network attacks. As a core facet of the self-defending network, Cisco IOS IPS enables the network to defend itself with the intelligence to accurately identify, classify, and stop or block malicious or damaging traffic in real time.

While it is common practice to defend against attacks by inspecting traffic at the data centers and corporate headquarters, distributing the defense to stop malicious traffic close to its entry point at the branch offices is also critical. Deploying inline Cisco IOS IPS at the branch enables gateways to drop offending traffic, send an alarm, block an attacker or reset a potentially malicious client-server connection as needed to stop attacking traffic at its point of origin.

Key **Benefits** of Cisco IOS IPS features include:

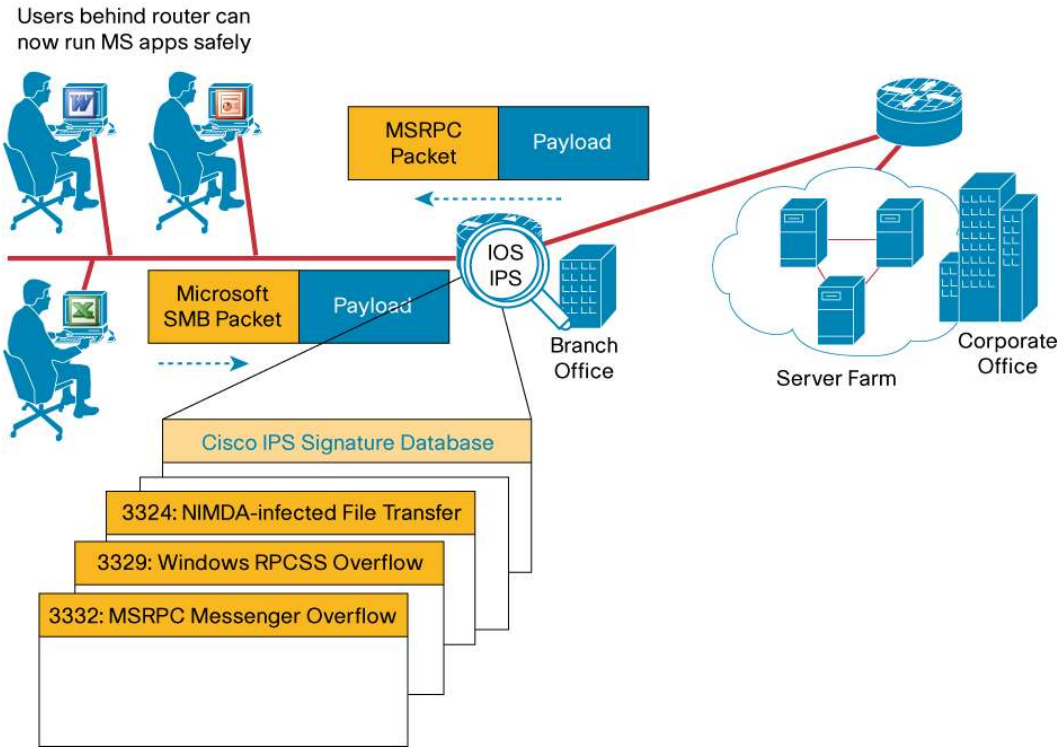
- Provides network-wide, distributed protection from many worms, viruses, and attacks exploiting vulnerabilities in operating systems and applications
- Eliminates the need for a standalone IPS device at branch and telecommuter offices as well as in small and medium-sized business networks
- Offers field-customizable worm and attack signature set and event actions
- Offers inline inspection of traffic passing through any combination of router LAN and WAN interfaces in both directions
- Works with Cisco IOS® Firewall, control-plane policing, and other Cisco IOS Software security features to protect the router and networks behind the router
- Supports same signature database available for Cisco Intrusion Prevention System (IPS) appliances

In Cisco IOS Software Release 12.4(15)T, Cisco IOS Intrusion Prevention System (IPS) provides support for the Cisco IPS Software Version 5.x/6.0 signature format, which is also used by the latest Cisco appliance-based IPS products. The Cisco IPS version 5.x signature format is improved to support encrypted signature parameters and other features such as signature Risk Rating. In this release, Cisco IOS IPS feature will also support signatures for many vulnerabilities found in Microsoft Server Message Block (SMB) and Microsoft Remote Procedure Call (MSRPC) protocols. Both of those protocols are widely and frequently used by most of Microsoft's computer applications and software packages.

New Cisco IOS IPS features in Cisco IOS Release 12.4(15)T provides:

- Signatures for vulnerabilities in Microsoft SMB and MSRPC protocols
- Support for encrypted signatures provided by vendors under NDA (such as Microsoft)
- Risk Rating value in IPS alarms for efficient event filtering, monitoring and correlation
- Supports Signature Event Action Processor (SEAP) for automated adjustment of signature event actions based on Risk Rating
- Support for the same signature format as the latest Cisco IPS appliance/module software version
- Individual and category based signature provisioning capabilities via Cisco IOS CLI
- XML-based IDCONF signature provisioning mechanism
- Automated signature updates (at periodic intervals) from a local TFTP or HTTP/HTTPS server

Figure 16. IPS Now Supports Microsoft SMB and MSRPC Signatures Natively



Benefits of IPS Features in Cisco IOS Software Release 12.4(15)T

- **Enhanced Microsoft Signature Support (MSRPC and SMB):**

Cisco IOS IPS adds support for ~95 signatures for vulnerabilities in Microsoft Remote Procedure Call (MSRPC) and Microsoft Small Message Block (SMB) protocols.

- **Support for Encrypted Signatures Released Under NDA:**

  Cisco IOS IPS can now scan for encrypted signatures for certain vulnerabilities as provided by vendors under NDA (such as Microsoft) sometimes even before their public release.

- **More Accurate and Efficient Event Monitoring with Reduced False Positives:**

  Event Risk Rating value provided in IPS alarms are calculated based on signature severity, signature fidelity (high fidelity signatures have a lower rate of false positives) and a "target value rating" defined by users. Event monitoring/correlation applications or devices such as CS-MARS may use the Risk Rating (RR) value in IPS alarms to filter out events below a certain RR threshold and/or trigger event correlation/action rules based on relative importance of IPS events indicated by their Risk Rating value.

- **Quick and Automated Adjustment of Signature Event Actions Based on Calculated Risk:**

  The Signature Event Action Processor (SEAP) feature allows overriding of default signature actions based on calculated Risk Rating value. For instance, signatures generating events with a Risk Rating value of 90 or higher (on a scale of 1 to 100) may be configured to drop offending packets and/or deny traffic from the attacker's address in addition to the default action of simply sending an alarm.

- **Common Operational Model for Cisco IPS Appliances, Modules and Cisco IOS IPS:**

  In this release, Cisco IOS IPS starts using the same signature format and deployment/update/provisioning mechanism as all other Cisco IPS devices allowing Cisco Security Manager 3.1 to apply the same policy changes (signature tunings) to all Cisco IOS routers, IPS appliances and modules in a customer network.

- **Secure and Scalable Management of Signature Policies for Any Kind of Deployment:**

  Security Device Manager 2.4 and Cisco Security Manager 3.1 provides complete IPS provisioning capabilities for a single router and multiple routers and IPS devices, respectively. Both management applications use IDCONF protocol running securely over HTTPS. Granular customization and tuning of signatures is also possible via CLI and custom CLI scripts. For large scale deployments, it is possible to distribute signature selection and action tunings applied to a single router to a large number of routers using Cisco Configuration Engine.

- **Timely Protection from the Latest Threats with Minimal User Intervention:**

  Automated and periodic signature updates from a local TFTP or HTTP(S) server.

Hardware

Routers	• Cisco 87x, 1800, 2800, 3700, 3800, 7200 Series Routers

Additional Information: http://www.cisco.com/go/iosips

Product Management Contact: Kemal Akozer (kemal@cisco.com)

4.1.2) Flexible Packet Matching (FPM) Full Packet Filtering

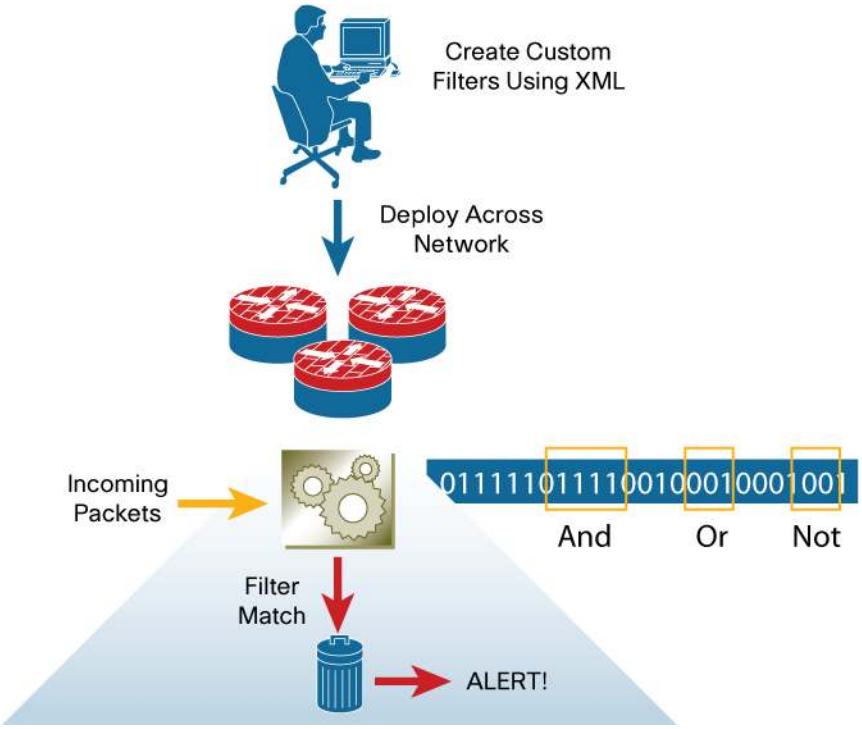
Flexible Packet Matching (FPM) is the next-generation Access Control List (ACL) technology that provides a flexible and rapid first line of defense against malicious traffic at the entry point into the network. It features powerful custom pattern matching deep within the packet header or payload, minimizing inadvertent blocking of legitimate business traffic.

FPM is a packet classification feature that allows users to define one or more classes of network traffic by pairing a rich set of standard matching operators with user-defined protocol header fields. FPM further extends the network traffic class definition capability to include new CLI syntax to offset into a user-defined protocol header and, furthermore, into the data portion of the packet.

FPM provides network security administrators with powerful tools to identify miscreant traffic as it enters the network, and to immediately drop and/or keep a log for audit purposes. Administrators can specify custom match patterns at multiple offsets within the packet. FPM includes ready-made definitions for standard protocols via Protocol Header Definition Files (PHDF), which simplify deployment. Customers can also customize and add extensions to PHDFs at device run time.

FPM was first introduced in Cisco IOS Release 12.4(4)T. In the initial release, FPM was limited to searching for patterns 32 bytes long within the first 256 bytes of a packet. Release 12.4(15)T extends the FPM matching capability by allowing network security administrators the ability to search for strings up to 256 bytes long anywhere within the entire packet. This provides greater flexibility for defining filters for miscreant traffic targeting your network.

Figure 17. Flexible Packet Matching Process



Benefits

- FPM enables users to create their own stateless packet classification criteria and to define policies with multiple actions (ie: drop, log or send ICMP unreachable) to immediately block new viruses, worms, and attacks

- FPM provides a flexible, granular Layer 2-7 matching capability providing the ability to inspect packets for characteristics regardless of the header fields involved
- FPM goes beyond static attributes allowing you to specify arbitrary bits/bytes at any offset within the entire packet (header or payload), minimizing inadvertent blocking of legitimate business traffic
- Allows network security administrators to rapidly set up custom filters using CLI or XML-based policy language
- Useful for Security Incident Response Teams for reacting to threats targeting their networks

Hardware

Routers	• Cisco 800, 1700, 1800, 2600, 2800, 3700, 3800, 7200 and 7301 Series

Considerations

The Flexible Packet Matching feature is only available in Cisco IOS Software Release 12.4(15)T (and higher) Advanced Security, Advanced IP Services, and Advanced Enterprise Software packages.

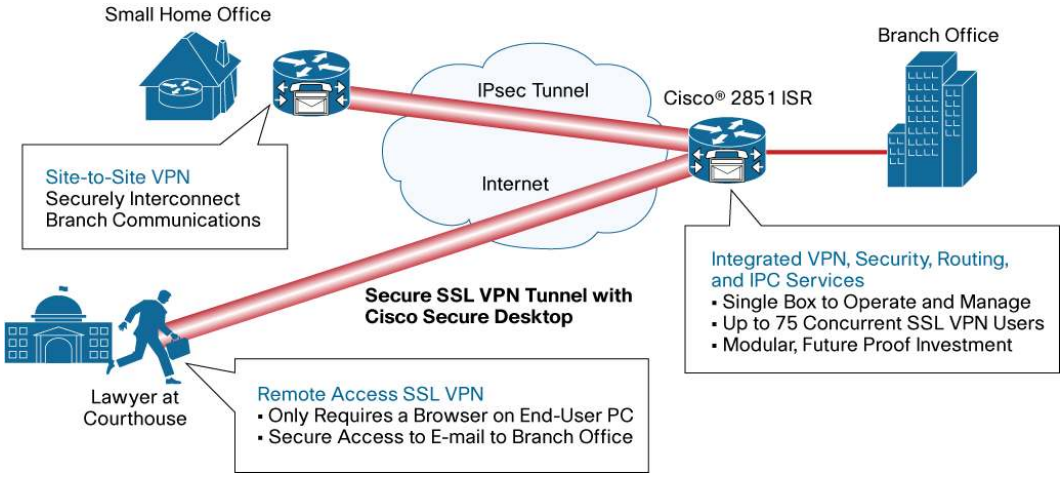
Additional Information: http://www.cisco.com/go/fpm

Product Management Contact: ask-stg-ios-pm@cisco.com

4.1.3) Cisco IOS SSL VPN Enhancements

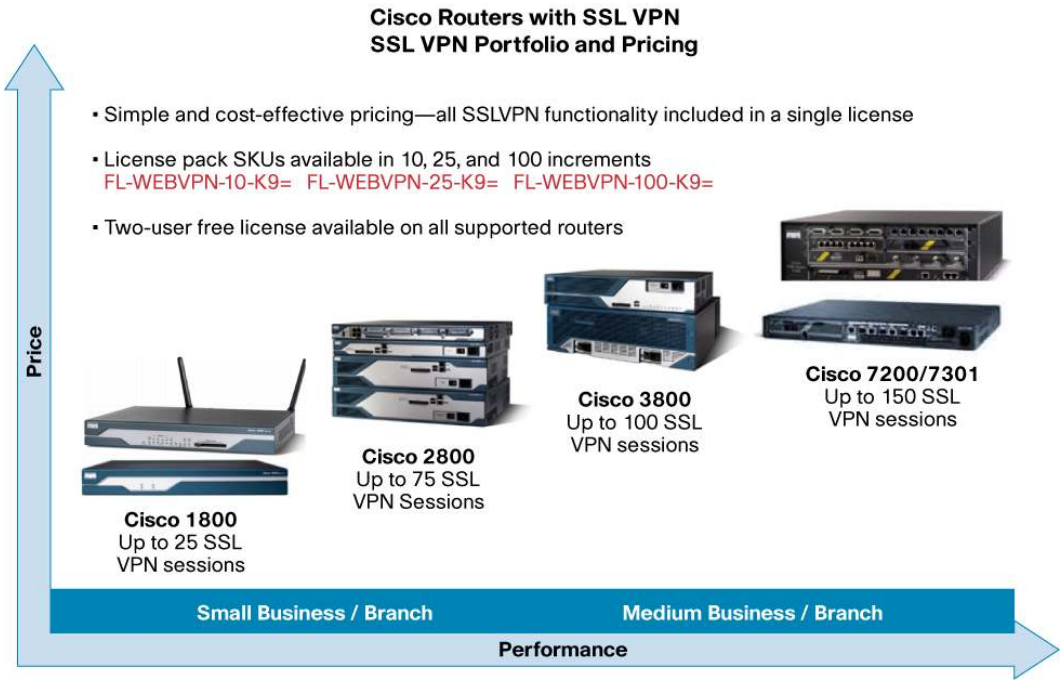
Unlike IPsec-VPN, SSL VPN in clientless mode is an application-aware technology. Using SSL VPN on the routers, companies can securely and transparently extend their companies' networks to any Internet-enabled location. SSL VPN is compelling because the security is transparent to the end user and easy for IT to administer. Using only a Web browser, companies can extend their secure Enterprise networks to any Internet-enabled location, including home computers, Internet kiosks, and wireless hotspots-thereby enabling higher employee productivity and protecting corporate data. Cisco IOS SSL VPN supports clientless access to applications such as HTML-based intranet content, email, network file shares, and Citrix. While this allows for a great end-user experience, it must be balanced with proper access-control so end-users have access to only those resources dictated by corporate policy. Figure 29 provides a use-case scenario for customers to implement Cisco IOS SSL VPN effectively at the branch.

Figure 18. IOS SSL VPN Use Case Scenario



Cisco IOS® SSL VPN is a licensed feature supported on Cisco® 871, 1800, 2800, 3700, 3800, 7200, and 7301 routers running the Advanced Security image since Cisco IOS Software Release 12.4(6)T (and higher). You can purchase the feature license in packs of 10, 25, or 100 simultaneous users directly from the Cisco.com ordering tool or through your Cisco partner/account team. Figure 30 provides more portfolio and license pricing details.

Figure 19. Cisco IOS SSL VPN Portfolio and Pricing



New SSL VPN features in Cisco IOS Software Release 12.4(15)T include the following:

1. SSL VPN Clientless Performance Enhancements
2. SSL VPN GUI Enhancements
3. SSL VPN User-level Bookmarking
4. Front Door-VRF Support

4.1.3.1) SSL VPN Clientless Performance Enhancements

Prior to this feature, traffic from clientless SSL VPN users was processed switched. Clientless performance enhancements bring CEF support to clientless SSL VPN traffic through this Cisco IOS SSL VPN gateway. Cisco Express Forwarding (CEF) technology for IP is a scalable, distributed, layer 3 switching solution designed to meet the future performance requirements of the Internet and Enterprise networks. Hardware acceleration is also now supported, offloading the processor from extensive cryptographic computations.

Reduction of the overall load of the processor allows for greater scalability and throughput providing for an improved user experience and user density per router. Reducing the CPU load also allows for configuration of other concurrent features on the router. CEF and hardware support are enabled by default.

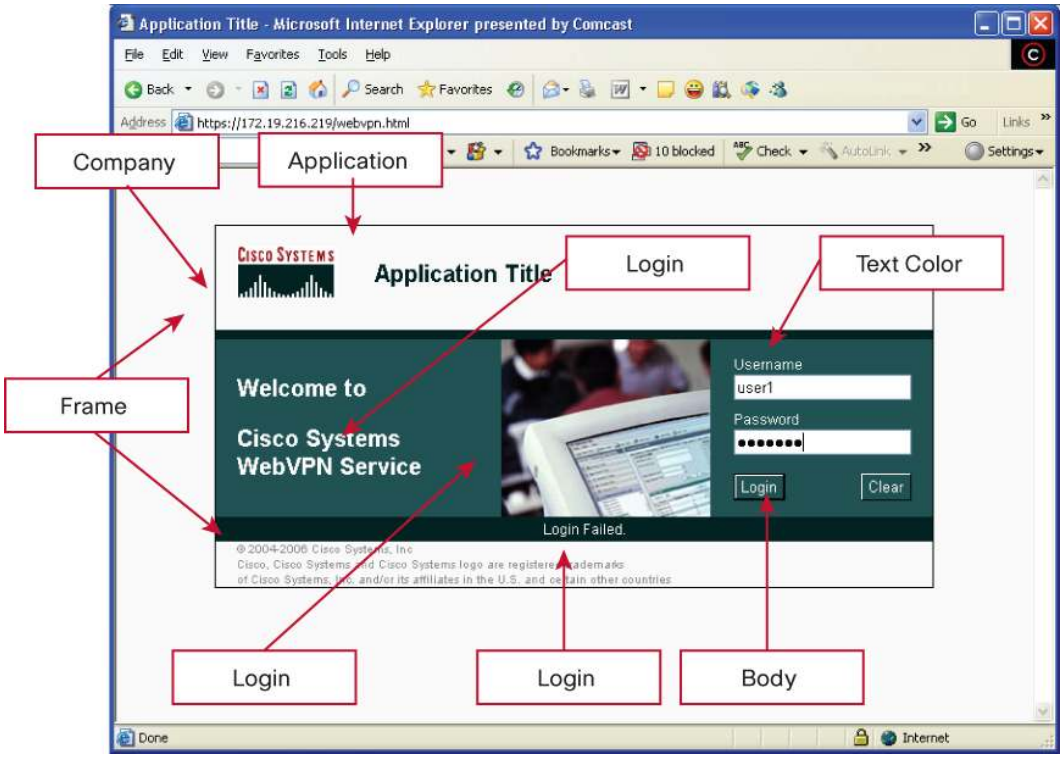
Benefits

- **Increased Scalability and Performance:** Increased number of concurrent users and throughput.

4.1.3.2) SSL VPN GUI Enhancements

Ergonomic improvements of the GUI user interface of the Cisco IOS SSL VPN gateway have been added. Improved customization of the user interface provide for greater flexibility and ability to tailor the portal pages for an individualized look and feel. Features are more clearly delineated, making for a more intuitive and less cluttered interface. The portal page now spawns new pages for mangled links or URLs, eliminating any need to navigate back to the portal page. The separate toolbar window has been replaced with an integrated floating toolbar that floats in either the upper left or right (dynamically configurable) of pages spawned from the portal page. Previous interface configurations are still available.

Figure 20. SSL VPN GUI Enhancements

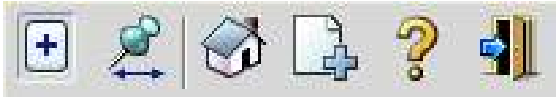


User Configurable Enhancements:

- Login Banner message
- Login Picture

GUI Improvements:

- GUI layout
- Toolbar integrated directly into spawned pages:



Previous Configurable Elements:

- Login message
- Color accents
- Logo
- Secondary browser color
- Secondary text color

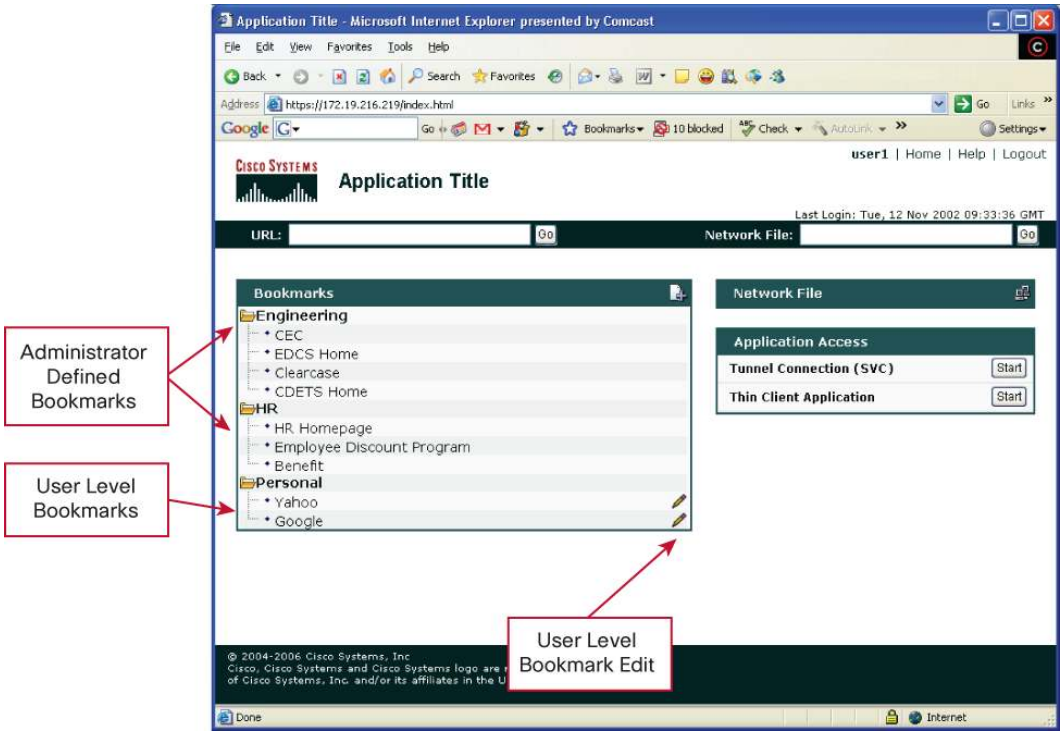
Benefits

- **Ease of use/Customization:** The improved GUI takes into account the latest Cisco IOS SSL VPN features and presents them in a layout that is more intuitive and aesthetic. Integration of the toolbar reduces clutter of the desktop by removing an extra window.

4.1.3.3) SSL VPN User-Level Bookmarking

User level bookmarking allows individual users to customize the portal page with their own bookmarks. Bookmarks are stored on the router and are linked to the individual user id's so the user's bookmarks are location/machine independent. The user profile location can be stored on any of the file systems on the router as well as externally such as a Trivial File Transfer Protocol (TFTP) server. In addition to administrator defined bookmarks, Cisco IOS SSL VPN users can create, edit, and delete their own individual bookmark list and have access to them on any computer at any location.

Figure 21. SSLVPN User-Level Bookmarking



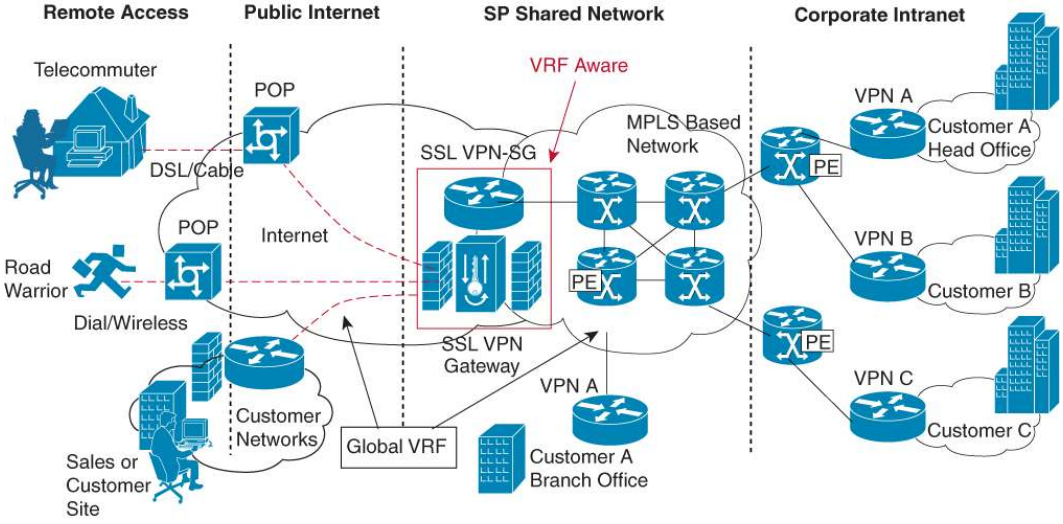
Benefits

- **Increased Usability:** The user level bookmarking feature gives flexibility to users to customize the portal page to suit their individual needs. In addition to predefined links configured by the administrator, users can create a list of bookmarks that are most useful for them.

4.1.3.4) Front door-VRF (fVRF) Support

Front door-VRF (fVRF) support, coupled with the already supported internal VRF (iVRF) capability in Cisco IOS Software Release 12.4T, allows the Cisco IOS SSL VPN gateway to be fully integrated into an MPLS network. The virtual gateway can be placed into a VRF, separate from the Internet to avoid internal MPLS/IP network exposure. This reduces the vulnerability of the router by separating the Internet routes and/or the global routing table. Clients can now reach the gateway via the fVRF which can be separate from the global VRF. The backend or iVRF functionality remains the same.

Figure 22. Front door-VRF Support



Benefits

- **Increased Security:** Cisco IOS SSL VPN virtual gateway can be placed and accessed on a separate VRF to reduce network exposure and provide support for overlapping IP addresses.

Hardware

Routers	• Cisco 871, 1800, 2800, 3700, 3800, 7200, 7301 Series Routers

Additional Information: http://www.cisco.com/go/iossslvpn

Product Management Contact: ask-stg-ios-pm@cisco.com

4.1.4) Cisco IOS Software Support for AnyConnect VPN Client

The Cisco AnyConnect VPN Client is the Cisco next generation VPN client providing secure remote access through an SSL VPN tunnel. It provides similar functionality and features as traditional IPsec clients. As with clientless access, no provisioning on the client machine is required. The AnyConnect client is pushed from the Cisco IOS SSL VPN gateway to the client

where it is installed and a secure tunnel is established. Initial installation requires admin rights, but upgrading an existing install does not.

AnyConnect supports 32-bit Microsoft Windows 2000, Windows XP, Windows Vista (64-bit platforms to follow as well as Windows Mobile 5), Mac, and Linux platforms.

Figure 23. Cisco IOS Software Support for AnyConnect VPN Client

Benefits

- **Increased Functionality and Flexibility:** The Cisco AnyConnect VPN Client provides a secure remote access alternative for non-Web based traffic. It compliments clientless operations, allowing for traditional IPsec like connectivity between clients and the secure Cisco IOS Software gateway.

Hardware

Routers	• Cisco 871, 1800, 2800, 3700, 3800, 7200, 7301 Series Routers

Additional Information: http://www.cisco.com/go/iossslvpn

Product Management Contact: ask-stg-ios-pm@cisco.com

4.1.5) Reverse Route Injection Distance Metric Enhancements

Reverse Route Injection (RRI) is the ability for static routes to be automatically inserted into the routing process for those networks and hosts that are protected by a remote tunnel endpoint. The RRI Distance Metric Enhancement defines a distance metric for each static route created by RRI.

RRI is supported on both ipsec-profile and crypto map configuration (CLI) profiles:

- Configuration example on crypto map:

```
crypto map mymap 1 ipsec-isakmp
   set reverse-route distance 20
```

- Configuration example on ipsec-profiles:

```
crypto ipsec profile myprof
   set reverse-route distance 20
```

Benefits

- **Increased Flexibility:** Improves RRI flexibility when used in dynamic routing scenarios. Static routes can be tailored so dynamic routes can have priority in the routing table.

Hardware

Routers	• Cisco 871, 1800, 2800, 3700, 3800, 7200, 7301 Series Routers

Additional Information: http://www.cisco.com/go/iossecurity

Product Management Contact: ask-stg-ios-pm@cisco.com

5) Release 12.4(11)T Highlights

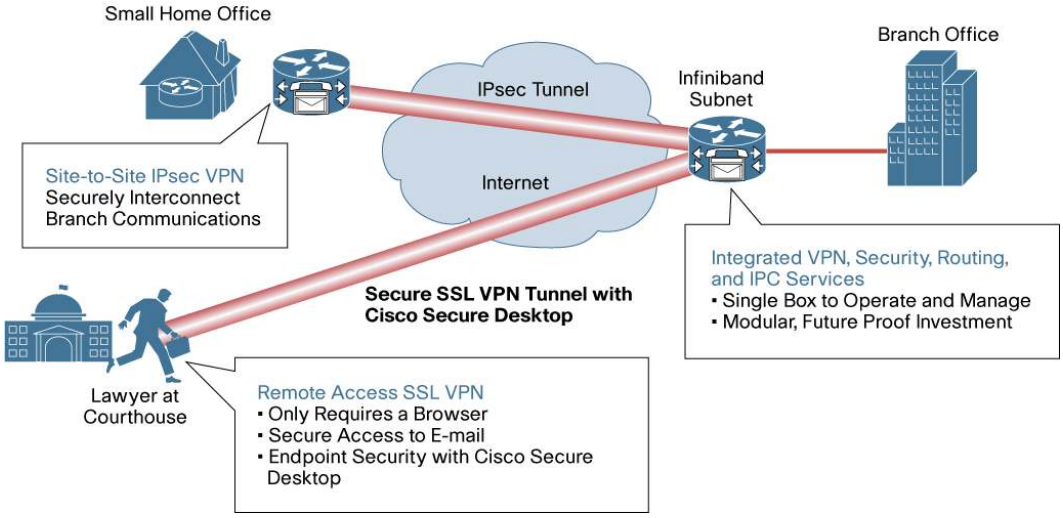
Table 5. Release 12.4(11)T Feature Highlights

5.1) Cisco IOS Security

5.1.1) Cisco IOS SSL VPN Enhancements

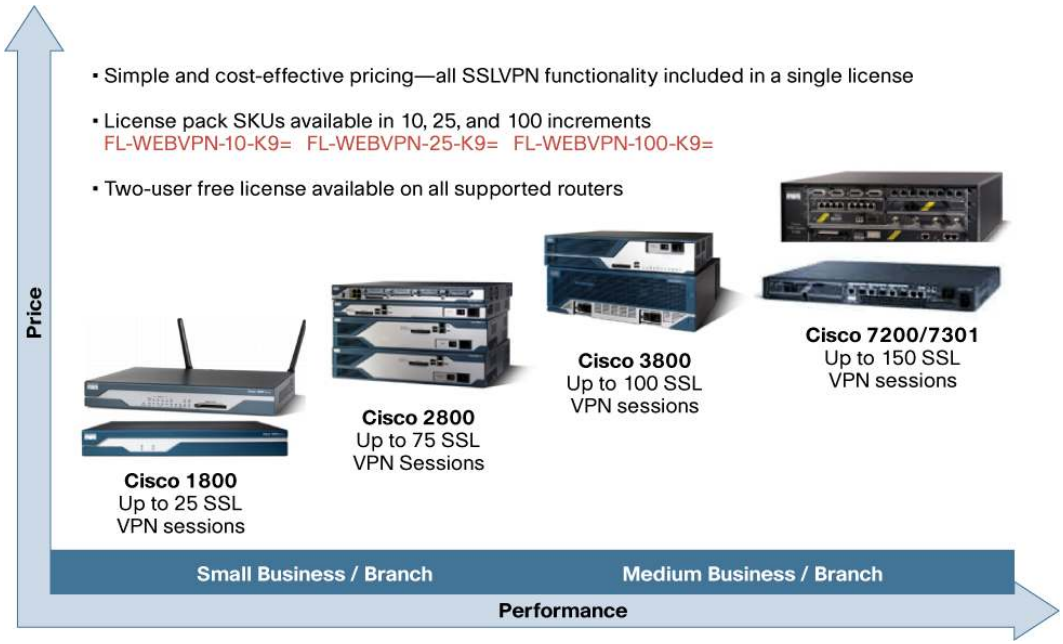
SSL VPN in clientless mode is an application aware technology. Using SSL VPN on the routers, companies can securely and transparently extend their companies' networks to any Internet-enabled location. SSL VPN is compelling because the security is transparent to the end user and is easy for an IT staff to administer and maintain. Using only a Web browser, companies can extend their secure Enterprise networks to any Internet-enabled location, including home computers, Internet kiosks, and wireless hotspots, enabling higher employee productivity and protecting corporate data. Cisco IOS SSL VPN supports full tunnel client access and clientless access to applications such as HTML-based intranet content, email, network file shares, and Citrix. While this allows for a great end-user experience, it has to be balanced with proper access-control for the end-user to only get access to the corporate resources that are allowed by the corporate policy. Figure 49 illustrates a user case scenario for customers implementing Cisco IOS SSL VPN effectively at the branch router.

Figure 24. Cisco IOS SSL VPN Use Case Scenario



Cisco IOS SSL VPN is a licensed feature supported on Cisco 871, 1800, 2800, 3700, 3800, 7200, and 7301 routers running the Advanced Security image on Cisco IOS Software Release 12.4(6)T or higher. The feature license can be purchased in packs of 10, 25, or 100 simultaneous users directly from the Cisco.com ordering tool or through your Cisco partner/account team. Figure 50 provides more portfolio and license pricing details.

Figure 25. Cisco Routers with SSL VPN
SSL VPN Portfolio and Pricing



SSL VPN functionality added in Release 12.4(11)T includes the following features:

- SSL VPN Netegrity Single Sign-on (SSO) Support
- SSL VPN Application ACL Support
- SSL VPN Port-forwarding Enhancement

- SSL VPN Debug Infrastructure
- SSL VPN URL Obfuscation Support

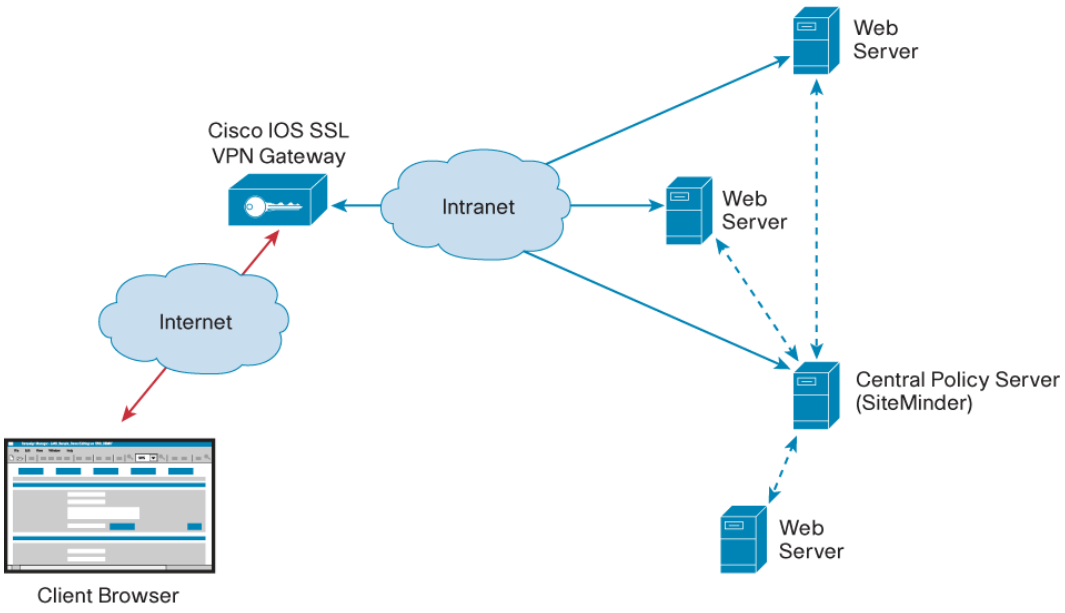
5.1.2) SSL VPN Netegrity Single Sign-on (SSO) Support

When users attempt to access web (HTTP/HTTPS) resources of a corporation or a partner, they may be prompted to authenticate in order to validate access to the particular information. Generally these credentials are specific to a particular application and access control information must be located on each individual web server. Basic centralized authentication options offered do not allow for granular access control. This may mean that a user needs to remember multiple passwords or to enter the same username/password multiple times.

Netegrity SiteMinder allows corporations to provide seamless access to many web resources, using almost any possible authentication option, and eliminates the need to authenticate to each individual server. This solution simplifies the authentication process for network resources by eliminating the need to constantly re-authenticate and removes the requirement for multiple distinct access control databases.

Netegrity SiteMinder functions by supplying an encrypted cookie back to the user's Web browser after authenticating to the first SiteMinder Agent-enabled web server. Other enabled servers use this cookie to identify this particular user and validate access to any available resources. Each web server must have a SiteMinder Agent installed, which performs verification of the cookie and access rights by communicating with a centrally controlled policy database (SiteMinder Policy Server). Figure 51 illustrates what the implementation would look like in a customer network.

Figure 26. SSL VPN Netegrity SiteMinder Single Sign-on implementation



Benefits

- **Seamless end-user access:** SSL VPN Netegrity SiteMinder Single Sign-on feature enables users to avoid redundant and tedious logins to different web servers/applications.
- **Flexible Intranet access:** This feature support provides the convenience of single unified login to all applications for the users logging in through the SSL VPN gateway.

5.1.3) SSL VPN Application ACL Support

The SSL VPN Application ACL feature provides administrators the ability to control end-user access to corporate applications, by filtering the connection requests based on URL and user/group policy. While developing this functionality, a balanced approach was adopted by keeping configuration as simple as possible while providing administrators the detail/flexibility they need to secure their corporate applications through applying corporate security application usage policy to each user.

The SSL VPN Application ACL functionality includes both Network-level and Application-level ACL support. In the application layer, the gateway may have a better idea regarding how to filter the traffic than it does in network layer; hence this feature provides great flexibility for customers to filter the traffic going through their SSL VPN tunnel. SSL VPN Application ACL enhances the already rich Cisco IOS SSL VPN feature-set, providing the necessary control on the traffic that traverses the SSL VPN tunnel to the inside network.

Network-level ACL, the SSL VPN gateway (router) will allow access control based on network protocols, source IP address and destination IP address.

Application-level ACL, the SSL VPN gateway (router) will allow matches based on the application filter URL string. The URL may include a wildcard for the server names, may be a partial URL, or may include a port number or server IP address/net mask.

Benefits

- **Flexibility in access methods:** Using SSL VPN, companies can securely and transparently extend their companies network to any Internet-enabled location, while using Application ACL to control what these end-users can access.
- **Broad Range of Filtering Options:** The administrator is allowed to match based on the application filter URL string. The URL may include a wildcard for the server names, may be a partial URL, or may include a port number or server IP address/net mask.

5.1.4) SSL VPN Port-forwarding Enhancement

The Port forwarding applet is started when the user clicks the “Start Application Access” link on the SSL VPN portal page. A new browser window will be launched with the applet. This Java-based Port forwarding applet is also known as the SSL VPN Thin-client mode. The Java-based application helper provides support for additional TCP-based applications that are not Web-enabled and supplements clientless access by providing connectivity to applications such as e-mail, instant messaging, Telnet, SSH etc.

The Port-forwarding enhancements were added to improve the existing thin-client support (application helper). As part of this enhancement, HTTP proxy functionality was added, like the one that might be found on the network (ie: an Internet Proxy). The HTTP proxy code modifies the browser’s proxy configuration on demand to redirect all browser HTTP/S requests to the new proxy configuration. This allows the Java Applet to take over as the proxy for the browser. For additional security, the applet needs to be digitally signed, since this allows for file modification, and port opening rights. It supports both HTTP and HTTPS connections.

Another possible use case for this functionality is to provide access to Web pages for which the mangling code isn’t supported. This occasionally occurs with sites that use Java, ActiveX and Flash. By auto-installing an HTTP proxy on the user’s workstation, the mangling code can be bypassed, while allowing connection to pass through the secure gateway.

The table below provides a quick comparison between the old and new port-forwarding enhancement.

Table 6. SSL VPN Port Forwarding Comparison by Cisco IOS Release

Feature	hosts file update	Ports <= 1024	Registry Modification
Original Port forwarding applet in Cisco IOS Release 12.4(6)T	Optional	Optional	Not needed
Enhanced Port forwarding using HTTP Proxy in Cisco IOS Release 12.4(11)T	Not needed	Not needed	

Note: It is recommended that Cisco Secure Desktop be used with the HTTP Proxy feature when used on a public terminal or a non-corporate owned workstation.

Benefits

- **Improved Performance:** The enhanced port-forwarding applet uses HTTP proxy which provides much better performance due to client side caching as compared to the older implementation.
- **Support for Virtually all client-side Web technologies:** No mangling is required at the SSL VPN Gateway which provides seamless support for all web content that cannot be mangled using the SSL VPN clientless functionality including embedded ActiveX and Flash content.

5.1.5) SSL VPN Debug Infrastructure

The SSL VPN Debug Infrastructure introduced in Release 12.4(11)T aims to provide an easy to use methodology to debug SSL VPN problems more efficiently. This release adds an extensive debug infrastructure to help customers and Cisco Technical Assistance Center engineers better identify and filter the activity on the network.

Benefits

- **Increased Visibility and Troubleshooting Capabilities:** Using the SSL VPN Debug Infrastructure, customers and Cisco Technical Assistance Center engineers can easily identify and resolve problems by filtering data based on client information such as username, source IP address, and context name.
- **Timely resolution:** The Debug Infrastructure provides a better way to filter all the messages and resolve the problem in a timely manner.

5.1.6) SSL VPN URL Obfuscation Support

Employees or partners accessing internal resources via SSL VPN have visibility in to internal IP addressing and DNS names. This unnecessarily exposes internal host information to remote users accessing web resources. This feature would ensure that the directory path being accessed on the internal network is hidden from the remote user. The functionality provides the ability to hide (ie: obfuscate) the internal hostnames, IP addresses in the URL links presented at the client browser.

The benefit is the security of hiding/masquerading internal hosts for over-the-shoulder viewers at an Internet kiosk etc. If enabled, sites accessed become converted into masqueraded URLs containing randomly generated strings (cookies) instead of actual host names/IPs. This includes all bookmarks and sites accessed by entering in the URL in the appropriate location on the web page.

Example:

Accessing http://somesite.cisco.com/index.html which presently becomes something like:

https://testvpn.cisco.com/http/0/somesite.cisco.com/index.html

Would become a randomly generated URL:

https://testvpn.cisco.com/http/0/342FDSFDSCS0AFA5A1DSA/index.html

Benefits

- **Increased Security:** URL obfuscation provides the ability to hide the internal hostnames, IP addresses, directory path in the URL links presented at the client browser.

Considerations

The SSL VPN URL obfuscation feature is disabled by default.

Hardware

Routers	• Cisco 871, 1800, 2800, 3700, 3800, 7200, 7301 Series Routers

Additional Information: http://www.cisco.com/go/iossslvpn

Product Management Contact: Aamir Waheed, (awaheed@cisco.com) or ask-stg-ios-pm@cisco.com

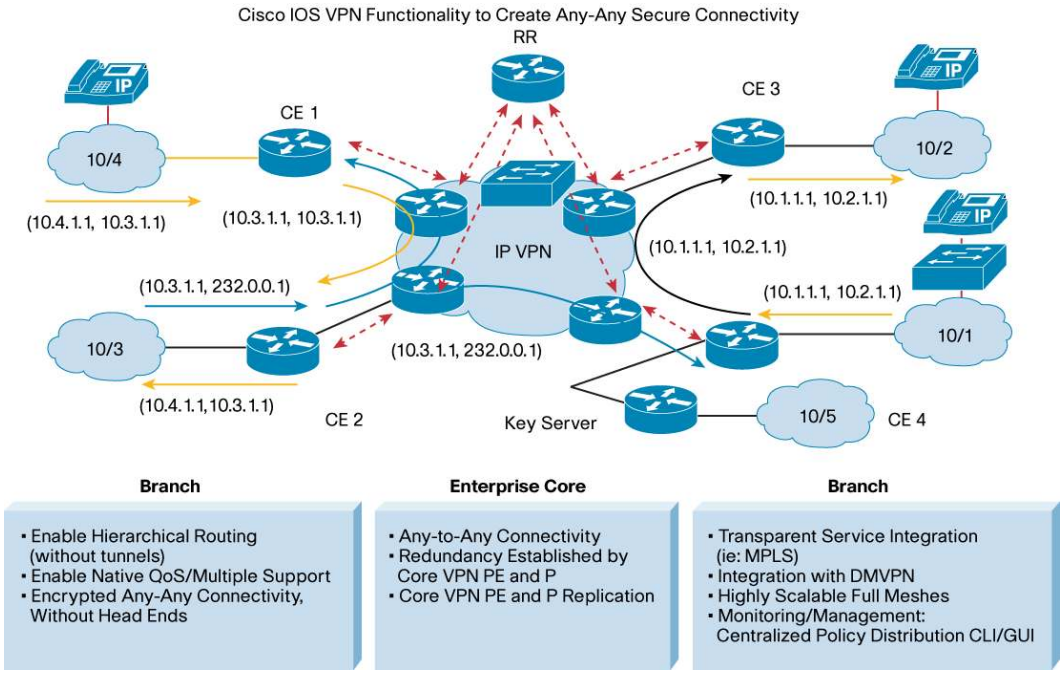
5.1.7) Group Encrypted Transport (GET) VPN

Today's networked applications such as voice and video drive the need for instantaneous, branch interconnected, and QoS-enabled WANs. The distributed nature of these applications results in increased demands for scale. At the same time, Enterprise WAN technologies force businesses to make a trade-off between QoS-enabled branch interconnectivity and transport security. As network security risks increase and regulatory compliance becomes paramount, Group Encrypted Transport (GET) VPN, a next-generation WAN encryption technology, eliminates the need to compromise between network intelligence and keeping data private.

GET introduces a new IPsec-based security model that is based on the concept of "trusted" group members. Trusted member routers use a common security methodology that is independent of any point-to-point IPsec tunnel relationship. By utilizing trusted groups instead of point-to-point tunnels, meshed networks are able to scale higher while maintaining network intelligence features critical to voice and video quality—such as QoS, routing and multicast.

Group Encrypted Transport networks can be used in a variety of WAN environments, including IP/MPLS. GET-enabled MPLS VPNs are highly scalable, manageable and cost-effective, and meet government mandated encryption requirements. The flexible nature of GET allows security-conscious Enterprises to manage their own network security over a service provider WAN service or to off load encryption services to their providers. GET simplifies securing large Layer 2 or MPLS networks requiring partial or full mesh connectivity.

Figure 27. Group Encrypted Transport



Features

GET is built on standards based technologies and integrates routing and security seamlessly together in the network fabric. Secure group members are managed through an IETF standard, Group Domain of Interpretation (GDOI).

Table 7. Summary of key GET features

Group Domain of Interpretation	GDOI (RFC 3547) is the key management protocol that establishes security associations among authorized group member routers.
IP Header Preservation	The original IP header in IPsec packets is preserved.
Centralized Key and Policy Management	A centrally available key server, typically a head-end router, is responsible for pushing keys and re-key messages as well as security policies to authorized group member routers. Both local and global policies—applicable to all members in a group– are supported, such as “Permit any any,” a policy to encrypt all traffic.
Key Server High Availability	The key server, responsible for pushing keys and policies, supports high availability by synchronizing keys and the policy database with a secondary key server.
Support for Anti-replay	Anti-replay support protects against Man-in-the-Middle attacks.
Encryption Support	DES, 3DES and AES

Benefits

In extending GDOI by encrypting and authenticating both multicast and unicast traffic, GET provides benefits to a variety of applications:

- Provides data security and transport authentication, helping to meet security compliance and internal regulation by encrypting all WAN traffic
- Enables high-scale network meshes and eliminates complex peer-to-peer key management with group encryption keys
- For MPLS networks, maintains the network intelligence such as full-mesh connectivity, natural routing path, and Quality of Service (QoS)
- Grants easy membership control with a centralized key server

- Ensures low latency and jitter by enabling full-time direct communications between sites—no inefficient central hub site traversal required
- Reduces traffic loads on CPE/PE encryption devices by leveraging core for replication for multicast traffic—no packet replication for each individual peer site

Hardware

Routers	• Cisco 870, 1800, 2800, 3800, 7200, 7301 Series Routers
Key Servers	• Cisco AIM-VPN/SSL module for Cisco Integrated Services Routers • Cisco VAM2+ for Cisco 7200 Series and 7301 Routers
Group Members	• Cisco Integrated Services Router (ISR) Series, Cisco 870, 1800, 2800, 3800

Product Management Contact: Siva Natarajan (sinatara@cisco.com) or ask-stg-ios-pm@cisco.com

5.1.8) MPLS VPN (RFC 2547) over Dynamic Multipoint VPN (DMVPN)

Enterprise customers increasingly require segmentation for a number of different reasons. Those reasons include:

- Closed User Groups (CUG)
- Virtualization
- Enterprises acting as an internal service providers
- Protection for critical applications

Enterprises require VPNs to be created and segmented based on practical considerations that conform to the business needs of the organization. For example, a company-wide multicast stream would need to be accessible by all the employees irrespective of their group association.

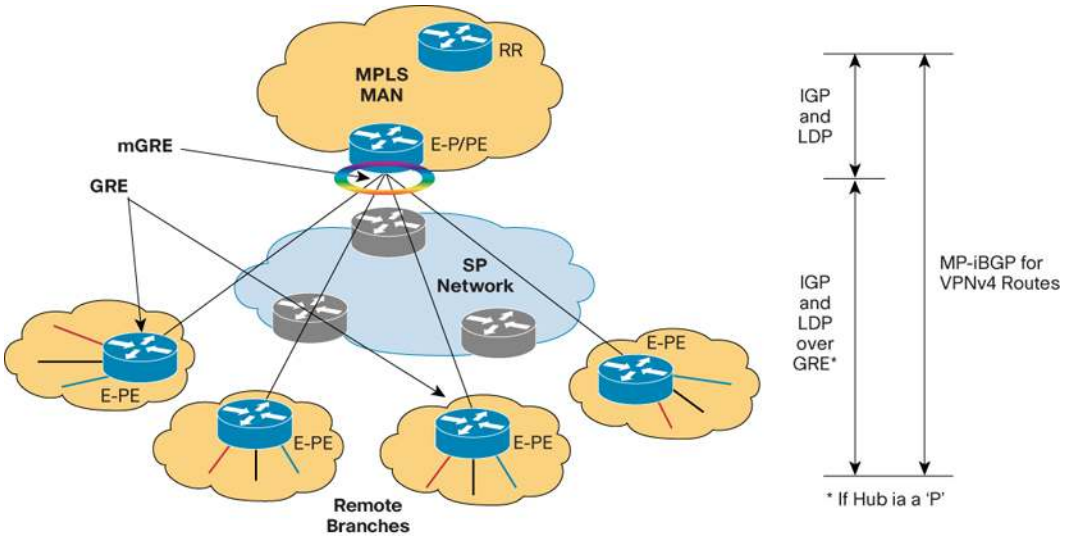
Segmentation to the end-user desktop is driving virtualization in the application server space. This means that even existing employees can be segmented into different Closed User Groups where they are provided access to internal services based on their group membership. For certain Enterprises, in addition to users, the applications themselves are driving the needs for virtualization. For example, an organization that feels that its critical applications need to be separated from everyday network users can create VPNs for each application or group of applications.

Initially, the solutions focused for virtualization requirements focused on the Enterprise core networks. Lately, the concept of virtualization has been expanded across the WAN edge to their remote branches. MPLS VPN (RFC 2547) over DMVPN is a deployment model for these Enterprises that have requirements for virtualizing their Enterprise branches.

DMVPN provides two key advantages—bulk encryption, and scalable overlay model--for extending MPLS VPNs to the branches. The large number of existing DMVPN deployments makes this an attractive deployment option. Since the branches are connected to the hub through a Layer 3 SP service, a tunneled model using GRE is needed to extend MPLS to the branches. DMVPN allows the hub to have a single multipoint GRE tunnel interface to support large numbers of spokes. The spokes can be point-to-point or multipoint GRE tunnels depending on the requirement of direct spoke-to-spoke communication.

The DMVPN model does not have some of the scale limitations of the Multi-VRF based solutions because the GRE tunnels are created outside the VRFs and a single tunnel can be shared for transporting many VRFs. The hub is configured with a single mGRE tunnel while spokes have a single GRE tunnel. It is important to note that the model is to be used for hub and spoke communication only.

Figure 28. MPLS VPN (RFC 2547) over DMVPN (Hub & Spoke Only)



As shown in Figure 53, in the control plane the following protocols exist:

- Routing protocol with the provider to learn the branch and head end router physical interface addresses (tunnel source address). Static routes could be used as well if they could be easily summarized.
- Static GRE tunnel between the branch PE and the head end P.
- IGP running in the Enterprise global space over the GRE tunnel to learn remote PE's and RR's loop back address (only if the head end is a P).
- LDP session over the GRE tunnel with label allocation/advertisement for the GRE tunnel address by the branch router (only if the head end is a P).
- MP-iBGP session with Route Reflector, where the branch router's BGP source address is the tunnel interface address—this forces the BGP next-hop lookup for the VPN route to be associated with the tunnel interface.

Additionally, IPsec can be used to encrypt the GRE tunnels; encryption happens after the GRE encapsulation.

Benefits

Key benefits and applications of MPLS VPN (RFC 2547) over DMVPN include:

- **Bulk Encryption:** Customers can use the MPLS VPN (RFC 2547) over DMVPN to do bulk encryption, satisfying security requirements.
- **Scalable overlay model:** Customers can use the MPLS VPN (RFC 2547) over DMVPN to build a scalable overlay model.

Hardware

Routers	• Cisco 1800, 2800, 3800, 7200, 7301 Series Routers
Hub Devices	• Cisco 7200VXR with NPE-G1 or higher
Spoke Devices	• Cisco Integrated Services Router (ISR) Series 1800, 2800, 3700, 3800, 7200, 7301

Product Management Contact: Siva Natarajan (sinatara@cisco.com) or ask-stg-ios-pm@cisco.com

5.1.9) EasyVPN Phase 8.0 Enhancements

EasyVPN Manageability Enhancements

These enhancements include new filters for existing show, clear, and debug commands. It also includes new commands for group and individual session viewing and debugging.

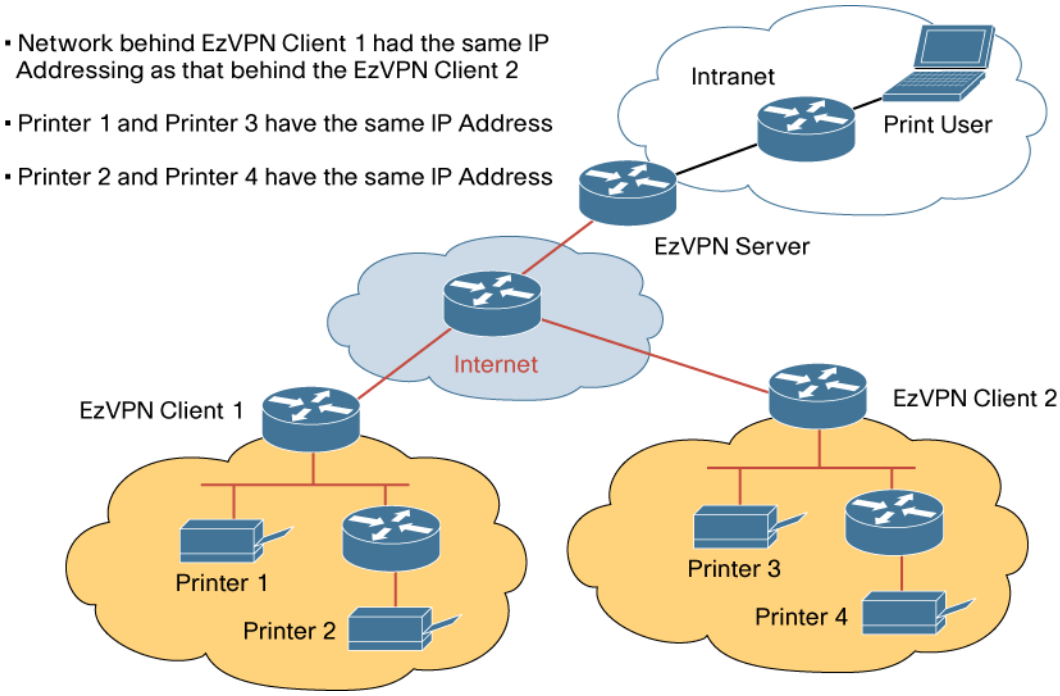
The specific enhancements include:

- New filters for the “show crypto session” command. The filters include username, isakmp-profile, group, local-address, and interface.
- Extending the “show crypto session” and “show crypto session detail” displays to include username, isakmp-profile, group, assigned-address, fvrf, and ivrf.
- Providing one line session information using “brief” extension to “show crypto session” commands or any of the other “show crypto session” command variants such as “show crypto session isakmp group <group> brief.”
- New filters for the “clear crypto session” command. The new filters include username and isakmp-group. The username filter is only valid when Extended Authentication (XAuth) is used.
- New filters for the “debug crypto session” command. The new filters include username, profile-name, and local-address.

EasyVPN Remote Identical Addressing Support

This feature supports having identically addressed LANs on EasyVPN Remotes. Network resources such as printers and Web servers on the LAN side of the EasyVPN Remote that have overlapping addressing with other EasyVPN remotes can now be reachable. The EasyVPN Remote feature was enhanced to work with NAT to provide this functionality. The EasyVPN Server requires no changes to support this functionality. This feature is supported in network extension modes only (network-extension and network-plus).

Figure 29. Easy VPN Remote Identical Addressing Support



Notes

- This is an EasyVPN Remote functionality enhancement and involves no change on the existing EasyVPN Server configuration.
- The restriction to use this feature is that it is supported on Enhanced EasyVPN with Network-Extension mode only.

Hardware

Routers	• Cisco 800, 1800, 2800, 3700, 3800, 7200 Series, and 7301, Routers

Product Management Contact: ask-stg-ios-pm@cisco.com

5.1.10) Cisco IOS Firewall H.323 Registration, Admission, and Status (RAS) Message Inspection Support

The Registration, Admission and Status (RAS) signaling protocol is part of the H.323 protocol suite and is generally used between voice gateways and gatekeepers. The H.323 RAS message inspection support feature provides users/customers a secure way to allow RAS messages between zones without having to enable entire UDP protocol inspection for the H.323 RAS port (1719 by default). H.323 RAS messages between peers are tracked to establish their request-response relationship and accordingly, only RAS messages from known peers are accepted for inter-zone traffic. This feature is only supported in the new zone based firewall policy configuration model. This feature is also supported for messages originated from the router or terminating on the router.

Please note that the ports registered by an endpoint are NOT opened automatically for H.225 connection acceptance through the Cisco IOS Firewall. The user has to include H.323 inspection separately to allow connections to an endpoint.

Benefits

Customers who previously had to enable “inspect UDP” for RAS messages on port 1719 can now only enable “inspect h.323-ras” and achieve better performance and security because not all UDP messages on port 1719 are allowed through/inspected.

Hardware

Routers	• Cisco 871, 1800, 2800, 3700, 3800, 7200, 7301 Series Router

Additional Information: http://www.cisco.com/go/iosfirewall

Product Management Contact: Darshant Bhagat (dabhagat@cisco.com) or ask-stg-ios-pm@cisco.com

5.1.11) Cisco IOS Intrusion Prevention System (IPS) Version 5.0 Signature Format Support
The Intrusion Prevention System (IPS) feature now supports using the same signature format as Cisco IPS appliances/modules (also known as Cisco Intrusion Prevention System version 5.x signature format). This enhancement allows the Cisco IOS IPS feature to support more signatures. It also provides a “Risk Rating” value (calculated based on signature severity and fidelity) within the IPS alarms sent to event monitoring applications for easier and more effective event correlation.

Due to this change in IPS signature format in Release 12.4(11)T, existing users of the Cisco IOS IPS feature will have to follow the update procedure to migrate to the new format while upgrading their routers to this new release. More information on can be found at http://www.cisco.com/go/iosips.

To configure and manage Cisco IOS IPS features in Release 12.4(11)T, Cisco highly recommends using one of the two management applications: The next release of Cisco Security Manager Software and Cisco Router and Security Device Manager (SDM) will support Cisco IOS IPS 5.x. SDM will also include a IPS migration wizard to assist existing Cisco IOS IPS users to migrate their configuration and signature files from previous Cisco IOS Software Releases to Release 12.4(11)T.

Hardware

Routers	• Cisco 800, 1700, 1800, 2600, 2800, 3700, 3800, 7200, 7300 Series Routers

Product Management Contact: Kemal Akozer (kemal@cisco.com) or ask-stg-ios-pm@cisco.com

6) Release 12.4(9)T Highlights

Table 8. Release 12.4(9)T Feature Highlights

6.1) Cisco IOS Security
6.1.1) Cisco IOS Firewall Enhancements —HTTP Application Inspection and Control Enhancements, Session Policing and Ingress Rate Policing based on Firewall Policies, P2P Application Filtering*
6.1.2) Cisco EasyVPN 7.1
6.1.3) DMVPN Manageability Enhancements
6.1.4) Virtual Private Network (VPN) Advanced Integration Module (AIM) for Cisco 1841/2800/3800 Integrated Services Routers (ISRs)
6.1.5) Cisco IOS WebVPN—Auto-Applet Port Forwarding Download
6.1.6) Cisco IOS WebVPN—HTTP Authentication
6.1.7) Cisco IOS WebVPN—RADIUS Accounting

* Indicates Key Highlight

6.1) Cisco IOS Security

6.1.1) Cisco IOS Firewall Enhancements

Cisco IOS Firewall integrates stateful firewall and application inspection functionality as part of a complete set of threat defense features offered on Cisco routers. Routers with integrated firewalls enable cost-effective and easy-to-deploy security solutions at every access point in the network. A firewall combined with other integrated router security capabilities allows new classes of solutions to connect mobile workers, branch offices, telecommuters, partners and customers into the network.

Release 12.4(9)T introduces the following functionality to Cisco IOS Firewall:

- HTTP Application Inspection and Control Enhancements
- Session Policing and Ingress Rate Policing based on Cisco IOS Firewall Policies
- P2P Application Filtering

HTTP Application Inspection and Control Enhancements

HTTP is the most commonly used application-layer protocol on the Internet. HTTP offers a flexible, extensible mechanism to support numerous networked applications. Businesses, educational institutions, and government offices that rely on the Internet must allow HTTP traffic through their firewalls to accommodate most Web-based applications. Unfortunately, the pervasive nature of HTTP support has contributed to TCP port 80 being a transmission vector for malicious software such as worms and viruses, as well as offering an effective conduit for concealing other traffic generated by undesirable software such as Instant Messaging (IM) applications and Peer-to-Peer (P2P) file-sharing tools.

Cisco IOS Software HTTP Application Inspection (AI) offers flexible application-layer inspection to examine network traffic to detect and take action against malicious or unwanted HTTP traffic. This release offers the following enhancements in this area:

1. User Definable and Extensible Policies—Policies may be defined based upon various HTTP Protocol objects like HTTP methods, URLs, header names and values such as maximum URL length, maximum header length, maximum number of headers, maximum header-line length, non-ascii headers, or duplicate header fields. This allows the ability to limit buffer overflows, HTTP header vulnerabilities, binary or non-ascii character injections, exploits like SQL injection, cross site scripting and worms attacks.
2. Flexible CPL Based Configuration—Configuration and application is done using the Class-based Policy Language (CPL) to allow user defined patterns for policy definitions. This enables a very flexible, powerful and granular approach to prevent against HTTP attacks and vulnerabilities. This support comes in addition to the existing HTTP application inspection that allows for extensive RFC (2616 and 2068) conformance checking to prevent malicious HTTP traffic.

Session Policing and Ingress Rate Policing based on Firewall Policies

Denial of Service (DoS) attacks designed to cripple network routers and corporate computing resources by flooding networks with packets are an important security threat that needs to be defended against to maintain network integrity and availability for designated users. Additionally, controlling the allocation of network resources based on protocol is critical to engineering high

performance networks. Preventing DoS attacks and controlling network resource utilization, both require the ability to designate which users and/or applications can use the network and how much bandwidth they can consume.

To address this topic, Cisco introduces two new innovations for Cisco IOS Firewall policies:

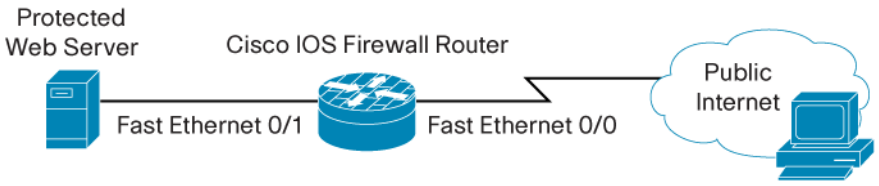
1. **Session Policing:** Session Policing is the ability to control the number of sessions for a particular protocol or user group allowed through a Cisco IOS Firewall. This session control limits the amount of resources a DoS attack can use on the router and offers a method to prevent and minimize DoS attacks.
2. **Ingress Rate Policing:** Ingress Rate Policing is the ability to control the bandwidth that is used by an application or a set of traffic through the firewall. This serves as a limiting factor to DoS attacks by preventing excessive bandwidth from being consumed by the packets from the DoS attack.

Although the above descriptions focus on the issue of preventing malicious users from gaining control of the network in DoS attacks, it is straightforward to see how these mechanisms can also be used to control the usage pattern of users and/or applications. This control allows network administrators to have a means of controlling network resource utilization.

P2P Application Filtering

Peer-to-Peer (P2P) Applications, like eDonkey, Kazaa, and Gnutella, are becoming an increasingly common form of network traffic that consumes valuable network bandwidth and can potentially become a security threat by carrying malicious traffic and applications. In order to address this issue, Cisco is introducing P2P Application Filtering as part of its firewall policies to help customers defend and protect their networks from P2P threats. A key differentiator of Cisco's offering is the ability for customers to load a protocol definition file, called a Packet Description Language Module (PDLM), for new P2P protocols; the Cisco IOS Firewall can then start dynamically recognizing the protocol and apply firewall policies on the protocol without requiring an update of the software image.

Figure 30. HTTP Application Inspection on Firewall Router for a Web Server



Benefits

- **Increased Security against HTTP Attacks and Vulnerabilities:** User definable and extendable HTTP inspection policies allows many methods to increase security of HTTP traffic and prevent attacks and vulnerabilities based upon HTTP.
- **Increased Security against P2P Attacks and Vulnerabilities:** PDLMs allow Firewall policy functionality to be used in the context of P2P Application Filtering to prevent security breaches and control network bandwidth usage from this traffic type.
- **Simplified Configuration:** HTTP Application Inspection policies defined and applied through CPL to simplify configuration process.

- **Prevents DoS Attacks:** Session Limiting and Ingress Rate Policing on Cisco IOS Firewall policies prevents DoS attacks from consuming bandwidth on firewall interfaces to minimize the effects of these attacks. This functionality also offers greater control for network resource utilization.

Hardware

Routers	• Cisco 800, 1700, 1800, 2600, 2800, 3600, 3700, 3800, and 7200 Series Routers • Cisco 7301 Routers

Additional Information:
http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_data_sheet09186a0080117962.html

Product Management Contact: Darshant Bhagat (dabhagat@cisco.com)

6.1.2) Cisco EasyVPN 7.1

Cisco EasyVPN, a software enhancement for existing Cisco routers and security appliances, greatly simplifies VPN deployment for site to site, remote offices and tele-workers. Cisco EasyVPN centralizes VPN management across all Cisco VPN devices thus reducing the complexity of VPN deployments. Cisco EasyVPN enables integration of VPN remote devices, Cisco routers, Cisco Adaptive Security Appliances (ASA), PIX Firewalls, and Cisco VPN concentrators or software clients; it allows a consistent policy and key management method within a single deployment to enable simplified remote site administration.

Release 12.4(9)T introduces the following key functionality to Cisco EasyVPN:

- Cisco Tunnelling Control Protocol (CTCP) in Cisco IOS Software
- Split DNS
- DHCP Client Proxy support for EasyVPN

Cisco Tunnelling Control Protocol

In many situations, customers require a VPN client to operate in an environment where standard Encapsulating Security Protocol (ESP with protocol or next header field value 50) or UDP Port 500 (Internet Key Exchange - IKE) can either not function, or not function transparently (without modification to existing firewall rules). TCP tunnelling of IPsec packets is often requested by road warriors, operating out of hotels rooms, airports etc. to pass through third party firewall devices in their environments.

Situations where standard ESP or UDP 500 is often not acceptable/permitted include:

- Small/home office router performing Port Address Translation (PAT). This router usually supports both TCP & UDP translation by default.
- Network Address Translation (NAT) provided IP address behind a large corporate router. A hotel providing private address space to guests could fall under this category, or the previous PAT scenario.
- Non-NAT Firewall (packet filtering or stateful). This scenario is common at companies that wish to use routable address space on their internal networks. Particular TCP applications will function, but UDP outbound is not permitted as it is often considered a security hole.

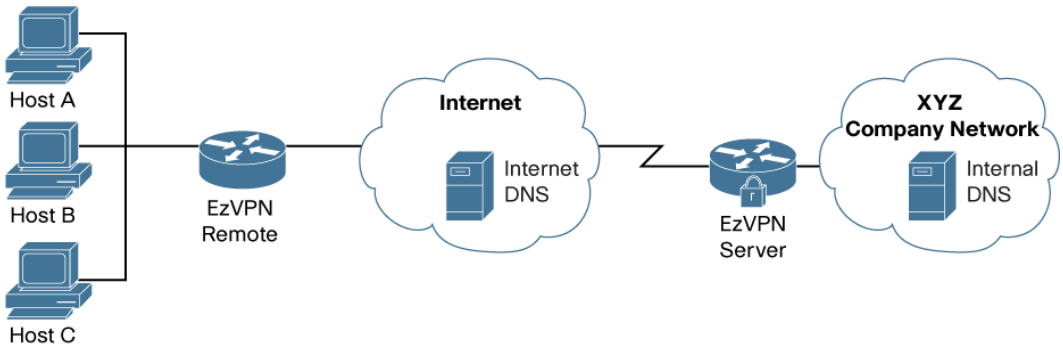
- Proxy server. If a proxy server is smart enough to actually look at each packet to confirm that the activity occurring is the defined activity, native IPsec flows will not be able to work in this situation.

To solve this problem in the above situations, without modifying the rules configured in the firewall, Cisco has come up with a protocol called Cisco Tunneling Control Protocol (CTCP). When CTCP is enabled on client and head-end devices, IKE and ESP traffic will be encapsulated in TCP header, so that the firewalls in between the client and the head-end device would simply permit this traffic (considering it as TCP traffic).

Split DNS in EasyVPN

The Split-DNS functionality enables EasyVPN client to act as a “DNS proxy”, directing Internet queries to the DNS Server of the ISP and directing corporate DNS requests to the corporate DNS servers. Without Split DNS, enterprises typically must point their CPEs to the corporate DNS servers for all DNS queries, because only their internal servers can resolve all their internal domains. This means that the internal servers will also have to carry the load of resolving or proxying all the queries for Internet URLs. This puts an unnecessary extra load on this key corporate resource. If the Internet queries can be sent to the ISP, the load on the corporate DNS server will reduced. This feature accomplishes that functionality.

Figure 31. Topology for Split DNS



In the diagram above, DNS requests coming from hosts behind the router (EzVPN Remote), need to be sent out to the correct DNS server (ISP’s DNS or corporate DNS) based on domain name being queried for. For example, if a request is made to the Internet, this request will be sent to the ISP’s DNS server.

DHCP Client Proxy Support in EasyVPN

This functionality allows the EasyVPN server to assign a DHCP address to a client from the corporate DHCP Server rather than the local pool.

The Cisco IOS EzVPN server currently assigns an ip address to a client using either a local pool configured on the router or using the framed-IP-address attribute defined in radius. With this functionality, the EzVPN server will support DHCP for assigning ip address. The EzVPN server will act as a proxy DHCP client and acquire an ip address from the corporate DHCP server. The ip address will be pushed to the client.

The client supplies its hostname, in a mode configuration request. This should be forwarded to the DHCP server, so that DHCP servers that support Dynamic DNS (DDNS) registration will be able to

register the hostname with the ip address assigned with the DDNS server. This will allow anyone in the corporate network to reach the client by its DNS hostname rather than an ip address.

Benefits

- **Increased Flexibility in Tunnelling IPsec Flows through Firewalls:** With cTCP, road warriors, operating out of hotels rooms, airports etc. can pass IPsec through third party firewall devices in their environments.
- **Reduced Load on Corporate DNS Servers:** With Split DNS, Internet queries can be sent to the ISP and the load on the corporate DNS server is drastically reduced. In some situations this reduction may be substantial such as home broadband connections used for home and telecommuting applications.
- **EasyVPN Client Reachability:** With DHCP Proxy functionality, it is now possible for branches to host servers behind the EasyVPN Clients. These servers will be assigned addresses from the corporate pool and will be reachable from any other host in the network. Further, if Dynamic DNS is enabled on the DHCP Proxy Server, these hosts would be reachable by their hostname. It is also useful for debugging purposes by system administrators trying to monitor VPN connections.

Hardware

Routers	• Cisco 800, 1700, 1800, 2600, 2800, 3600, 3700, 3800, and 7200 Series Routers • Cisco 7301 Router

Additional Information: http://www.cisco.com/go/easyvpn

Product Management Contact: Jai Balasubramaniyan (jsundar@cisco.com)

6.1.3) DMVPN Manageability Enhancements

DMVPN provides an easy and scalable way to create large and small IPsec VPNs by combining GRE tunnels, IPsec encryption, and Next Hop Resolution Protocol (NHRP). Dynamic Multipoint VPN (DMVPN) enables zero-touch deployment of IPsec networks. DMVPN Spoke-to-Spoke Functionality is an enhancement that enables the secure exchange of data between two branch offices without traversing the head office. This improves network performance by reducing latency and jitter, while optimizing head office bandwidth utilization.

DMVPN functionality has been enhanced to allow easier manageability by including the following key features:

- Show commands dealing with DMVPN as a single entity
- Debug commands for debugging DMVPN session and NHRP
- Syslog commands to support DMVPN session, Crypto Socket and NHRP
- Traps to support DMVPN session, Crypto sockets, and NHRP

Benefits

- **Rapid Troubleshooting:** The combination of show/debug commands and Syslog and Traps information help to troubleshoot networking devices in DMVPN environments.
- **Ease of Management:** Syslog and Traps offer an easy method to identify critical network events for network operations as well as overall network management/operations.

Hardware

Routers	• Cisco 800, 1700, 1800, 2600, 2800, 3600, 3700, 3800, and 7200 Series Routers • Cisco 7301 Router

Product Management Contact: ask-stg-ios-pm@cisco.com

6.1.4) Virtual Private Network (VPN) Advanced Integration Module (AIM) for Cisco 1841/2800/3800 Integrated Services Routers (ISRs)

Description

The Cisco VPN AIM optimizes the ISR platforms for virtual private networks in both IPsec and SSL WebVPN Deployments

This module is now designed to perform hardware based SSL Encryption for Cisco IOS WebVPN; the module also still supports VPN IPsec Encryption, Data Encryption Standard (DES&3DES) and Advanced Encryption Standard (AES 128, 192, 256), with the added hardware compression support of the IP Payload Compression Protocol (IPPCP). The ISR Router with AIM-VPN/SSL is ideal for use in small-to-medium sized businesses and small-to-large enterprise branch offices for connecting remote offices, mobile users, and partner extranets. The ISR VPN router is designed for both service provider managed-services Customer Premises Equipment (CPE) and Managed Security Service Providers (MSSPs). The ISR router together with the AIM-VPN/SSL module and Cisco IOS Advanced Security Feature set offers a rich, integrated package of routing, firewall, intrusion-protection system, and VPN functions. As an integral component of Cisco VPN solutions and the Cisco self defending network, the Cisco series VPN modules provide industry-standard encryption (IPsec), application-aware Quality of Service (QoS) and bandwidth management, together with robust perimeter security options.

Figure 32. AIM-VPN/SSL for Cisco 1841/2800/3800 ISRs

Benefits

Feature	Benefit
Offloads High Overhead IPsec Processing from the Main Processor	Reserves critical processing resources for other services such as routing, firewall, and voice.
IPsec MIB	The IPsec MIBs allow Cisco IPsec configuration monitoring and can be integrated in a variety of VPN management solutions.
Certificate Support Enables Automatic Authentication using Digital Certificates	Scales encryption use for large networks requiring secure connections between multiple sites.
VPN modules Easily Integrated into existing Cisco 1841, 2800, 3700 and 3800 Series Routers	Significantly reduces the system costs, management complexity, and deployment effort over multiple box solutions.
IPsec Provides Confidentiality, Data Integrity, and Data Origin Authentication	Enables the secure use of public-switched networks and the Internet for WANs.
Cisco IOS® WebVPN	WebVPN allows the ISR to be a single-box solution, unlike other vendor products that require multiple devices and management systems. WebVPN combined with the consolidated technology platform of the ISR, provides customers with unparalleled cost savings and competitive per-user pricing

Hardware

Routers	• Cisco 1841, 2800, 3700, 3800 Routers

Router	Part #	Description
1841	AIM-VPN/SSL-1	1841 DES/3DES/AES/SSL VPN Encryptions/Compression Module
2800	AIM-VPN/SSL-2	2800 DES/3DES/AES/SSL VPN Encryptions/Compression Module
3700	AIM-VPN/SSL-3	3700 DES/3DES/AES/SSL VPN Encryptions/Compression Module
3800	AIM-VPN/SSL-3	3800 DES/3DES/AES/SSL VPN Encryptions/Compression Module

Considerations

Requires Cisco IOS® Software with the Advance Security, Advance IP or Advanced Enterprise Feature Set

Additional Information:

http://www.cisco.com/en/US/products/hw/routers/products_promotion0900aecd8017150a.html

Product Management Contact: Kevin Sullivan (sullivan@cisco.com)

6.1.5) Cisco IOS WebVPN—Auto-Applet Port Forwarding Download

Description

The Cisco IOS WebVPN implementation has been enhanced to provide the ability to automatically download the Port Forwarding Applet at login time. Previously the user was required to click on “Start Application Access” on the portal page. This feature is configurable on the gateway under the group policy, as well as on the AAA server.

In the gateway, here is an example of the command line syntax:

```
policy group my_policy
  port-forward “email” auto-download
```

On the AAA server, administrator can define the following Cisco Attribute-Value (AV) pair under “Cisco IOS/PIX” section:

```
  port-forward-name=email
  port-forward-auto=1
```

Hardware

Routers	• Cisco 870, 1800, 2800, 3700, 3800, and 7200 Series Routers • Cisco 7301 Router

Additional Information: http://www.cisco.com/go/ioswebvpn

Product Management Contact: Aamir Waheed (ask-stg-ios-pm@cisco.com)

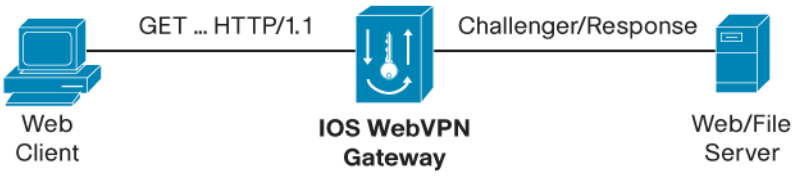
6.1.6) Cisco IOS WebVPN—HTTP Authentication

Description

The Cisco IOS WebVPN implementation has been enhanced to support HTTP Basic and NT LAN Manager (NTLM) authentication with password caching functionality. HTTP basic authentication

uses a simple username/password scheme. NTLM employs a challenge-response mechanism for authentication which is used by various Microsoft network servers. The Cisco IOS WebVPN gateway behaves as a proxy for the web client for HTTP authentication.

Figure 33. Cisco IOS WebVPN Authentication



Hardware

Routers	• Cisco 870, 1800, 2800, 3700, 3800, and 7200 Series Routers • Cisco 7301 Router

Additional Information: http://www.cisco.com/go/ioswebvpn

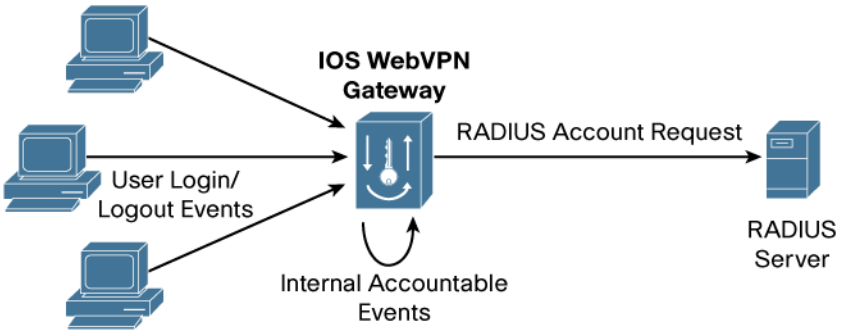
Product Management Contact: Aamir Waheed (ask-stg-ios-pm@cisco.com)

6.1.7) Cisco IOS WebVPN—RADIUS Accounting

Description

The Cisco IOS WebVPN implementation has been enhanced to record user based session activity to a RADIUS server for auditing purposes. The user session start and stop accounting events are supported.

Figure 34. Cisco IOS WebVPN RADIUS Accounting



Hardware

Routers	• Cisco 870, 1800, 2800, 3700, 3800, and 7200 Series Routers • Cisco 7301 Router

Additional Information: http://www.cisco.com/go/ioswebvpn

Product Management Contact: Aamir Waheed (ask-stg-ios-pm@cisco.com)

7) Release 12.4(6)T Highlights

Table 9. Release 12.4(6)T Feature Highlights

7.1) Cisco IOS Security
7.1.1) Cisco IOS Firewall Enhancements
7.1.2) Cisco IOS Web VPN
7.1.3) Scalability Enhancements for Dynamic Multipoint VPN with Next Hop Resolution Protocol-Cisco Express Forwarding
7.1.4) Complete Certificate Chain Validation in Cisco IOS Public Key Infrastructure
7.1.5) Enhanced Online Certificate Status Protocol in Cisco IOS Public Key Infrastructure
7.1.6) EasyVPN Password Aging via Authentication, Authorization and Accounting
7.1.7) EasyVPN Dynamic Firewall/Access Control List Policy Push to Cisco VPN Software Client
7.1.8) Secure Multicast
7.1.9) Control Plane Logging
7.1.10) Management Plane Protection
7.1.11) Network Address Translation ARP Ping

7.1) Cisco IOS Security

7.1.1) Cisco IOS Firewall Enhancements

Cisco IOS Firewall integrates stateful firewall and application inspection functionality as part of a complete set of threat defense features offered on Cisco routers. Routers with integrated firewalls enable cost-effective and easy-to-deploy security solutions at every access point in the network. A firewall combined with other integrated router security capabilities allows new classes of solutions to connect mobile workers, branch offices, telecommuters, partners and customers into the network.

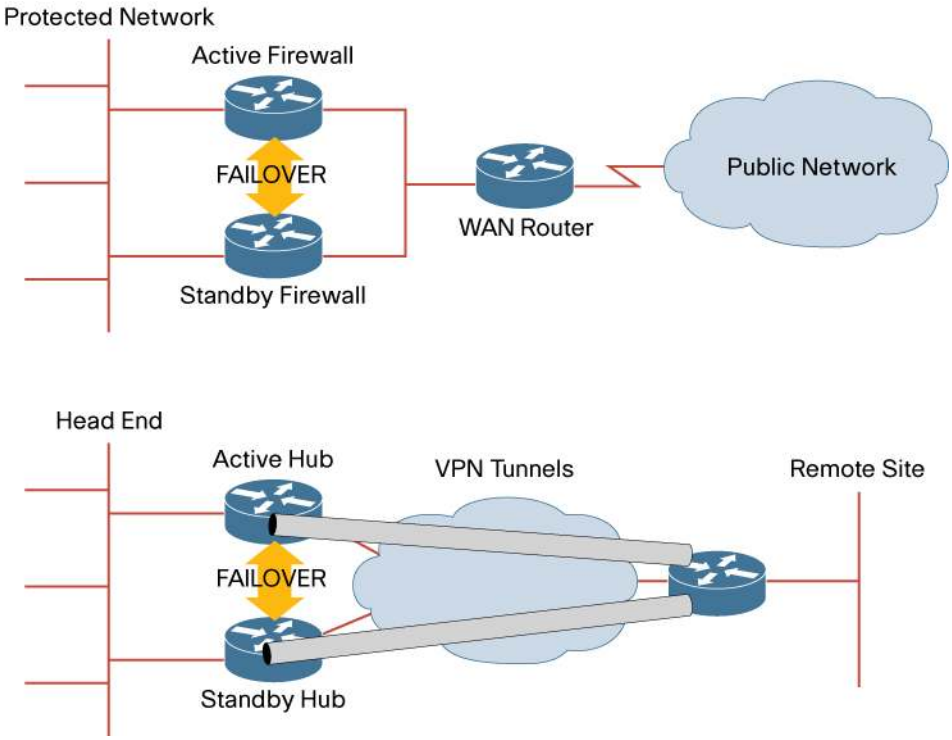
Release 12.4(6)T introduces a series of enhancement to Cisco IOS Firewall:

- Firewall Stateful Failover
- Zone-Based Policy Configuration
- Cisco Unified Firewall MIB

Firewall Stateful Failover

Firewall Stateful Failover enables Active/Standby failover between two routers for Firewall functionality. This functionality works in conjunction with Hot Standby Router Protocol (HSRP) on either LAN or VPN links to maintain Firewall session state, and to enable active connections to continue during a router or circuit failure. This enables a highly available Firewall solution that maximizes network uptime and security.

Figure 35. Topology for Firewall Stateful Failover for both LAN and VPN Applications.



Hardware

Routers	• Cisco 3700, 3800, and 7200 Series

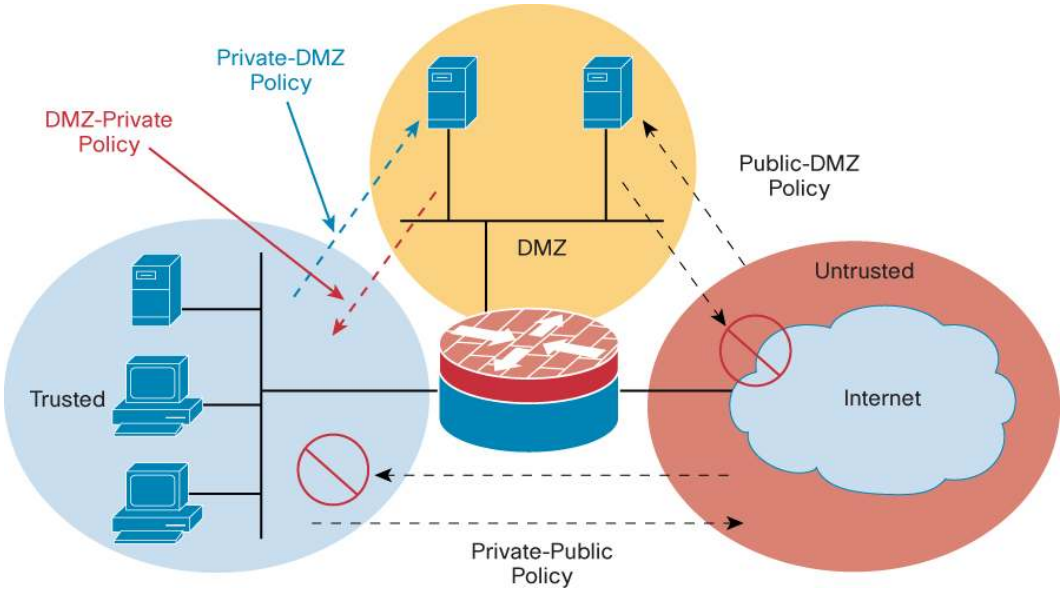
Zone-Based Policy Configuration

Improved firewall policy configuration means network administrators can more easily understand the effect of firewall policies on network traffic. This functionality allows grouping of physical and virtual interfaces into zones to simplify logical network topology. The creation of these zones enables the application of Firewall policies on a zone-to-zone basis, instead of having to configure policies separately on each interface. With this functionality, configuration is easier to understand, which enables:

1. Firewall policies that are configured on traffic moving between zones
2. Simplified troubleshooting, as inter-zone traffic can be used to test different firewall policies

Zone-to-zone policies can apply differing policies to different groups of hosts or networks based on ip address lists. This offers more granular application of security policies and allows easier integration of security policies with network management applications.

Figure 36. Zone-Based Policy Configuration



Hardware

Routers	• Cisco 800, 1700, 1800, 2600, 2800, 3600, 3700, 3800, and 7200 Series • Cisco 7301 Router

Cisco Unified Firewall MIB

The Cisco Unified Firewall MIB offers a unified SNMP standards based monitoring interface for functionality on all Cisco Firewall products: Cisco IOS Firewall, Cisco PIX, and Cisco Firewall Service Blades for Catalyst platforms. The Unified Firewall MIB offers statistics collection and monitoring for Stateful Packet Inspection, URL Filtering, and Application Inspection.

Benefits

- Highly available firewalls with maximum network uptime and security
- Simplified and more granular firewall policy application
- Easier integration of security policies with network management applications
- Cost-effective integrated firewall and security solutions with simplified deployment

Hardware

Routers	• Cisco 800, 1700, 1800, 2600, 2800, 3600, 3700, 3800, and 7200 Series • Cisco 7301 Router

Product Management Contact: Jonathan Gohstand (jgohstan@cisco.com)

7.1.2) Cisco IOS Web VPN

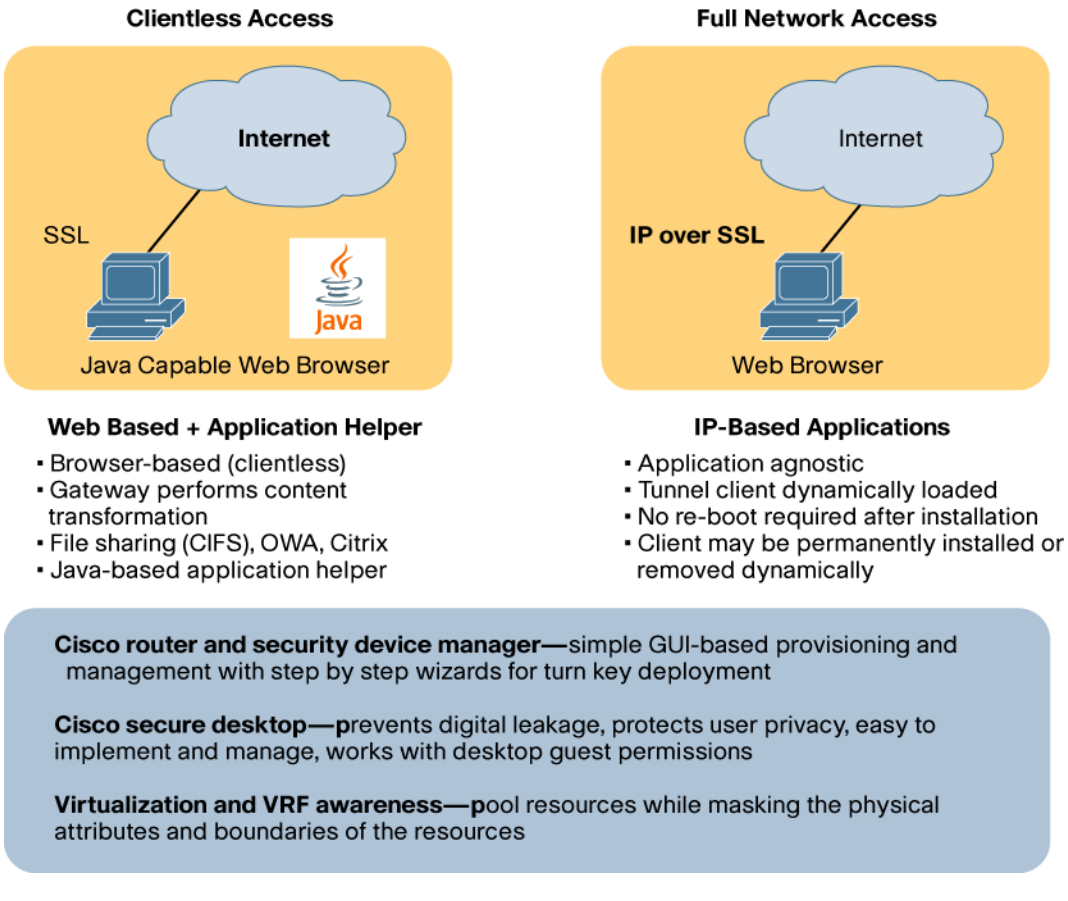
Cisco IOS WebVPN is a Secure Socket Layer (SSL) based VPN solution that provides “clientless” remote-access by employing a web browser as the remote user’s VPN client. A web browser has already been installed on most personal computers, so no further application installation is required to securely access network resources. Cisco IOS WebVPN makes it easy to deploy remote access to internal applications on a single integrated network device. It delivers comprehensive endpoint and network security with Cisco Secure Desktop for endpoint security

and integrated network security features like firewall, access controls, intrusion prevention, and application control. Cisco IOS WebVPN offers a clean, cost-effective SSL VPN solution capable of host assessment, malware protection, privacy and post-session clean-up.

WebVPN in Cisco IOS Software supports two functional modes:

- Clientless mode provides secure access to private web resources, and will provide access to web content. This is useful for accessing most content that would generally be accessed via a browser (ie: Internet, databases, or online tools).
- Network Access mode supports virtually any application with a persistent "LAN-like" connectivity via the Cisco SSL VPN Client that is dynamically and transparently loaded on the remote host.

Figure 37. WebVPN Solution Overview



Benefits

- Uses a standard web browser to access the corporate network without the installation of additional clients on the client machine
- SSL encryption native to browser provides transport security
- Accessible from non-corporate machines, such as airport kiosks
- Easy firewall/network traversal from any location
- Seamless wireless roaming
- Integrated network security features (ie: firewall, access controls, intrusion prevention, and application control)

- Clientless: standard HTML content transformation, native Citrix support, Java based application helper, and Windows file shares
- Security and Device Manager (SDM) provides a simple GUI based provisioning and management with step-by-step wizards for turn key deployment.
- Cisco Secure Desktop prevents digital leakage, protects user privacy, and integrates with desktop guest permissions, without complicated implementation or management
- Virtualization and VRF awareness: pool resources while masking the physical attributes and boundaries of the resources

Hardware

Routers	• Cisco 800, 1700, 1800, 2600, 2800, 3600, 3700, 3800, and 7200 Series • Cisco 7301 Router

Considerations

If WebVPN needs to be enabled on the router that is running HTTP Secure Server, the administrator must configure an IP address for WebVPN using the “gateway-addr” keyword option of the “webvpn enable” command.

Complex Web content may not work with Clientless mode and therefore may require the use of Network Access mode.

Additional Information: http://www.cisco.com/go/webvpn/

Product Management Contact: Gary Sockrider (ask-stg-ios-pm@cisco.com)

7.1.3) Scalability Enhancements for Dynamic Multipoint VPN with Next Hop Resolution Protocol-Cisco Express Forwarding
DMVPN control protocol Next Hop Resolution Protocol (NHRP) RFC2332, and its interaction with Cisco Express Forwarding is optimized to allow:

1. **Route Summarization**

   In a DMVPN network, the hub is the central repository for routing information. All spokes send their routes to the hub and the hub redistributes these routes to all of the other spokes. Prior to these enhancements, all individual routes were required to learn from the spoke routers must be sent to all of the other spoke routers. Each spoke had to have full routing information about the networks behind all other spokes, in order for a spoke to build spoke-spoke dynamic tunnels. This enhancement eliminates this requirement and allows the hub router to summarize the routing information that it advertises to the spokes routers. It also maintains support for dynamic spoke-spoke tunnels.

   The Route summarization is enabled on the hub router to reduce the routing load on the hub router, and the routing table size on the spoke router. An additional benefit of route summarization is that the number of routes advertised decreases dramatically from a hub to a spoke.

2. **Increase in scalability of a DMVPN Spoke-Spoke**

   This increase in scalability occurs when multiple hub routers are enabled when using the Open Shortest Path First (OSPF) routing protocol. Prior to this feature in order to get the correct routes on the spoke routers to support dynamic spoke-spoke tunnels OSPF had to be use “broadcast” network mode. Because of this we couldn’t have more then two hub routers. This feature, allows OSPF point-multipoint network mode to be used on a DMVPN network which removes the restriction of not allowing more then two hubs, yet still allowing dynamic

spoke-spoke tunnels. Note: Both before and after this feature the DMVPN network must be configured in the same OSPF area.

3. **Increase in scalability of a DMVPN Network**

   The increase in scalability of a DMVPN network, by relaxing the requirement that the hub routers be connected in a loop (daisy chain). The daisy chaining requirement was needed to forward NHRP protocol packets and some data packets between the hubs. This feature allows the forwarding of these packets between the hubs to be more direct, rather then having to travel around the complete chain of hub routers. For example a DMVPN network with 8 hubs would require that an NHRP resolution request/reply travel the complete 8 hub chain resulting in a total of 8 hops. With this feature you can configure a primary hub that is connected to all 8 secondary hubs, in which case an NHRP resolution reply/request would travel via the primary hub, 4 hops total, to get between any pair of secondary hubs. This also allows the creation of multi-level hierarchical hub-and-spoke DMVPN networks, which can better match the DMVPN network structure with the pattern of data flow.

Benefits

Previous Limitation	New Feature	**Benefits**
Large routing tables at the spokes can cause network instability	Route Summarization	Improve network and bandwidth utilization
Delays in setting up voice calls between spokes	Voice packets Cisco Express Forwarding switched via hub	Reduced latency during call setup
Complex interconnection of hubs to expand DMVPN Spoke-to-Spoke Networks Single point of failure	Simplified hub network design	Improved resiliency Failure of a single hub will not affect the rest of the DMVPN network

Hardware

Routers	• Cisco 800, 870, 1700, 1800, 2600, 2800, 3700, 3800, and 7200 Series • Cisco 7301 Router

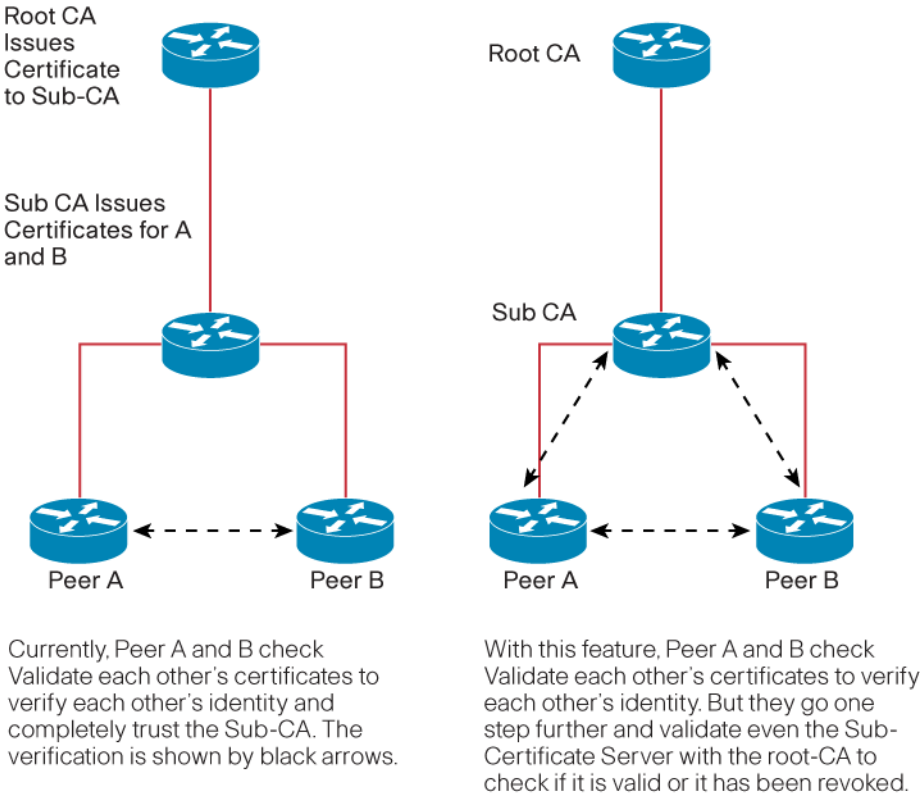
Product Management Contact: Siva Natarajan (ask-stg-ios-pm@cisco.com)

7.1.4) Complete Certificate Chain Validation in Cisco IOS Public Key Infrastructure

Cisco IOS Public Key Infrastructure (PKI) deployments currently validate the first trusted certificate. If the trustpoint that issued the certificate is a sub Certificate Authority (CA), it may be required to validate the certificate from the parent's trustpoint settings. The Complete Certificate Chain Validation enables full path processing via enhanced CLI.

For Example: If the trustpoint issuing the certificates to the two peers is a sub Certificate Authority, it may be necessary to verify its authenticity by contacting either the root CA server or some other trustpoint to see if it has been revoked or not for added security.

Figure 38. Complete Certificate Chain Validation in Cisco IOS PKI



Benefits

- Strengthens peer PKI credentials by verifying the authenticity of the sub Certificate Server that has issued PKI credentials

Hardware

Routers	• Cisco 800, 1700, 1800, 2600, 2800, 3600, 3700, 3800, and 7200 Series

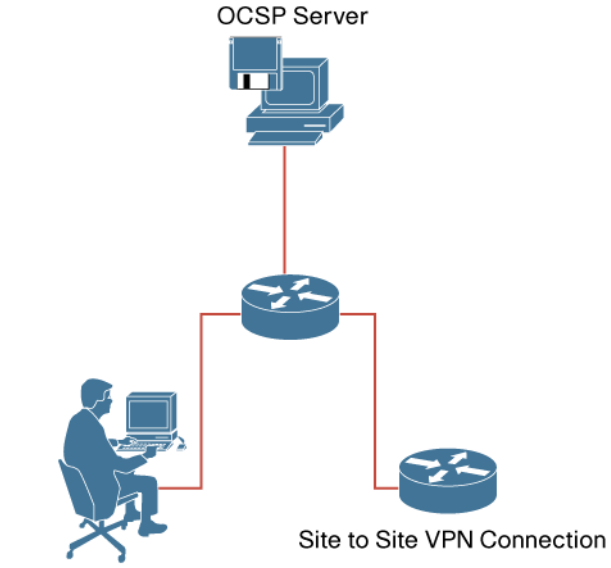
Product Management Contact: Jai Balasubramaniyan (ask-stg-ios-pm@cisco.com)

7.1.5) Enhanced Online Certificate Status Protocol in Cisco IOS Public Key Infrastructure
Conventional Public Key Infrastructure (PKI) deployments check the Certification Revocation Lists (CRLs) residing on the end host to validate a certificate. Online Certificate Status Protocol (OCSP) provides an alternative to CRLs that determine the status of a certificate. For example, when a user attempts to access a server, OCSP sends a request for certificate status information and responds back to the user on the status of the certificate. This overcomes the chief limitations of CRLs: it eliminates the need to download updates frequently. This also creates a more scalable infrastructure for determining the validity of certificates.

Other enhancements enable the recognition of different trust models, including Self-Signed Certificates and certificates signed by non root-CA, when branch offices maintain their own OCSP servers.

PKI Clients should be flexible enough to recognize these trust models for OCSP Servers where the certificate has been granted by authorities other than the root-CA server.

Figure 39. Enhanced Online Certificate Status Protocol in Cisco IOS PKI



Benefits

- Scalable alternative to CRLs
- Supports multiple OCSP servers in branch office scenarios in a Cisco IOS PKI network
- Flexibility in trust models of OCSP enable self signed certificates and certificates signed by CA Servers other than root

Hardware

Routers	• Cisco 800, 1700, 1800, 2600, 2800, 3600, 3700, 3800, and 7200 Series

Product Management Contact: Jai Balasubramaniyan (ask-stg-ios-pm@cisco.com)

7.1.6) EasyVPN Password Aging via Authentication, Authorization and Accounting

EasyVPN environments currently initiate authentication by the software client/router connecting the end user. These Password Authentication Protocol (PAP)-based clients would send the username and password to the EasyVPN Server, which in turn would generate an Authentication, Authorization and Accounting (AAA) request to an authentication server (ie: Cisco ACS, Microsoft AD Server). If the password has expired, the authentication server would reply back with an authentication failure. The reason for the failure is not passed back to the user, so the user will not know that it was due to password expiration.

With EasyVPN Password Aging via Authentication, Authorization and Accounting, Authentication Servers can notify the client that the password has expired, while providing a generic way for the end user to change the password. This feature will work with the Cisco ACS as well as Microsoft AD server (which calls for support of the MSCHAPv1/v2 authentication support).

Benefits

- User has the opportunity to change expired passwords without administrator intervention
- Identifies the cause for authentication denial

Hardware

Routers	• 800, 1700, 1800, 2600, 2800, 3700, 3800, and 7200 Series

Product Management Contact: Jai Balasubramaniyan (ask-stg-ios-pm@cisco.com)

7.1.7) EasyVPN Dynamic Firewall/Access Control List Policy Push to Cisco VPN Software Client
EasyVPN Dynamic Firewall/Access Control List Policy Push to Cisco VPN Software Client enhances the Cisco IOS EasyVPN server to push firewall policies to Personal Firewall products integrated with the Cisco EasyVPN Software Client running on the client's computer. This functionality has been tested with personal firewalls (ie: Cisco Security Agent, Cisco Integrated Client Firewall software, and Zone Labs—ZoneAlarm®).

Configuration Policy Push (CPP) is not a replacement for a perimeter firewall; rather, it creates another layer of security in remote access VPN installations and aids the administration by allowing one to push specific firewall policies to the end hosts. A split tunnel at the client end enables access to corporate network, while at the same time, exposes the clients to attacks from the Internet. The objective of this feature is to provide additional security to the clients, so that the VPN Concentrator/EasyVPN Server can make a decision to allow/deny the IPsec tunnel, if the client does not have the required firewall policy.

The EasyVPN client initially proposes the firewall functionality it supports to the Server. Based on the firewall policy configured on the Server, it will either accept one of the policies proposed by the client, proceed with no client firewall support or terminate the tunnel setup. The firewall configuration policies are configured on the Server, and these will be sent to the client. The client enforces firewall policies.

Figure 40. EasyVPN Dynamic Firewall/Access Control List Policy Push to Cisco VPN Software Client

Benefits

- Improves security against split tunneling, by enabling Cisco IOS EasyVPN Servers to configure Personal Firewalls on client machines
- EasyVPN Servers can choose to disallow clients that do not have the latest firewall configuration policies from joining the VPN Network

Hardware

Routers	• Cisco 800, 1700, 1800, 2600, 2800, 3600, 3700, 3800, and 7200 Series

Product Management Contact: Jai Balasubramaniyan (ask-stg-ios-pm@cisco.com)

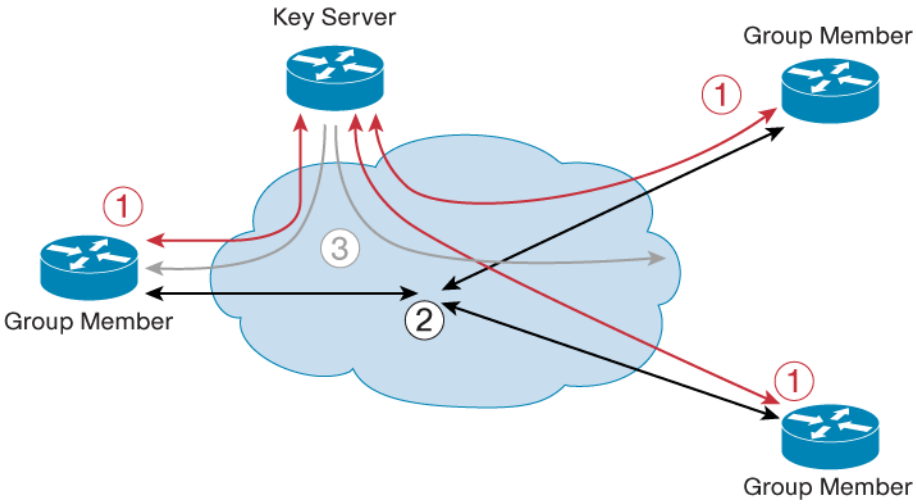
7.1.8) Secure Multicast

Secure Multicast is a set of features necessary to secure IP Multicast group traffic originating on, or flowing through, a Cisco IOS Software device. Secure Multicast combines the keying protocol Group Domain of Interpretation (GDOI) with IPsec encryption to provide users an efficient method to secure IP Multicast group traffic. It enables the router to apply encryption to non-tunneled (ie: “native”) IP multicast packets and eliminates the requirement to configure tunnels to protect multicast traffic.

Secure Multicast relies on the following two Internet standards:

GDOI is defined as the ISAKMP Domain of Interpretation (DOI) for group key management. In a group management model, the GDOI protocol operates between a group member and a “Group Controller/Key Server” (GCKS), which establishes security associations among authorized group members. The ISAKMP defines two phases of negotiation. GDOI is protected by a Phase 1 ISAKMP security association. The Phase 2 exchange is defined in the IETF by RFC3547. The topology shown in the figure below and the corresponding bullets explain how this protocol works:

Figure 41. Secure Multicast



Topology 1 illustrates the protocol flows necessary for group members to participate in a group:

1. Group members register with the key server. The key server authenticates and authorizes the group members, and downloads the IPsec policy and keys necessary for them to encrypt and decrypt IP multicast packets.
2. Group members exchange IP multicast packets encrypted with IPsec.
3. As needed, the key server pushes a re-key message to the group members. The re-key message contains new IPsec policy and keys to use when old IPsec Security Associations (SAs) expire. Re-key messages are sent in advance to SA expiration time to ensure that there are always valid group keys available.

Cisco IOS IPsec is a well known RFC (RFC 2401) that defines an architecture to provide various security services for traffic at the IP layer. IETF RFC 2401 describes the components and how they fit together with each other and into the IP environment.

A variety of IP multicast applications benefit from the encryption of native IP multicast packets. For a complete list of applications, visit http://www.cisco.com/go/multicast/.

Benefits

Previous Limitation	New Feature	**Benefits**
No native Multicast encryption	Standard and Flexible Framework implementing a Tuneless architecture	Framework offers unprecedented flexibility (e.g. supports Multicast and Unicast) Day 1 transparent interoperability between various core Cisco IOS technologies
No security for native multicast in Multicast VPN (mVPN) type architectures	Native Multicast encryption	Supports Multicast encryption in mVPN architectures
The value of the "Core" network mitigated Single point of failure	Leverage core for Multicast replication	New Architecture leverages the core and investment costs spent on building core

Hardware

Routers	• Cisco 800, 870, 1700, 1800, 2600, 2800, 3600, 3700, 3800, and 7200 Series • Cisco 7301 Router

Product Management Contact: Siva Natarajan (ask-stg-ios-pm@cisco.com)

7.1.9) Control Plane Logging

Control Plane Protection enables users to filter and rate-limit the packets going to the router's control plane, and discard malicious and/or error packets using features such as Control Plane Policing, port-filtering and queue-thresholding. The Control Plane Logging feature adds a way to allow logging of the packets dropped or permitted by these features.

Benefits

- The ability to log packets destined to a router's control-plane
- Enables identification of what is permitted or denied by the deployed Control Plane Protection policy
- Assists in developing and refining Control Plane Protection policies by identifying control-plane traffic

Hardware

Routers	• Cisco 1800, 2600XM, 2800, 3700, 3800, 7200 and 7301 Series Routers • Cisco 830, 850, 870, 1701, 1711, 1712, 1721, 1751, 1751-V, 1760, and 2691 Routers

Additional Information:

- http://www.cisco.com/go/nfp
- http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124newft/124t/124t4/htcpp.htm

Product Management Contact: Dan Hamilton (ask-stg-ios-pm@cisco.com)

7.1.10) Management Plane Protection

Management Plane Protection (MPP) enables user to restrict the interfaces on which network management packets can enter a device. With this feature, network operators can designate one or more router interfaces as management interfaces. Device management traffic can enter a

device through these management interfaces. After MPP is enabled, no interfaces except the designated management interfaces will accept network management traffic destined to the device.

Benefits

- Greater access control for managing a device than allowing management protocols on all interfaces
- Improved performance for data packets on non-management interfaces
- Simplifies the task of using per-interface ACLs to restrict management access to the device
- Fewer ACLs needed to restrict access to the device
- Management packet floods on switching and routing interfaces are prevented from reaching the CPU

Hardware

Routers	• Cisco 1800, 2600XM, 2800, 3700, 3800, 7200 and 7301 Series Routers • Cisco 830, 850, 870, 1701, 1711, 1712, 1721, 1751, 1751-V, 1760, and 2691 Routers

Additional Information: http://www.cisco.com/go/nfp

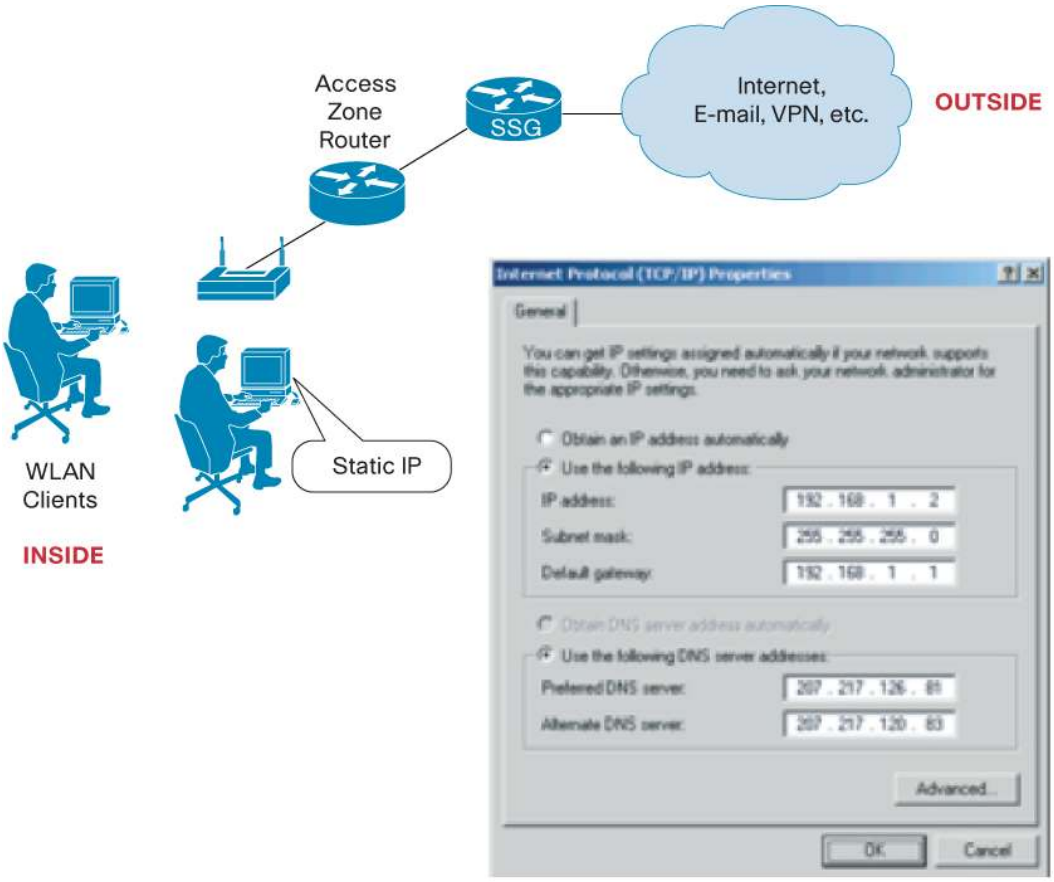
Product Management Contact: Dan Hamilton (ask-stg-ios-pm@cisco.com)

7.1.11) Network Address Translation ARP Ping

The existing WLAN-Network Address Translation (NAT) feature running at the Access Zone Routers (AZRs) allows users with Static IP address, who do not want to change their IP address, to continue using services of the public Wireless LAN provider. WLAN-NAT will create NAT entries for Static IP clients, and also provide them a routable address. NAT ARP Ping will address additional supports for the existing WLAN-NAT feature.

ARP Ping: With the current WLAN-NAT design, when the Static-IP client's NAT-entry times-out, the NAT entry and the secure-ARP entry associated to this client are deleted. An ACCOUNTING-STOP message will be sent to the Service Selection Gateway (SSG) and the Static-IP client's RADIUS object is removed. Re-authentication with the SSG is needed for the same client to again gain access to the services. With the new requirement, the NAT entry and the secure-ARP entry should not be deleted when the Static-IP client still exists in the network with its IP address for which it was authenticated. An ARP Ping is necessary to determine Static-IP client existences and to restart the NAT-entry timer.

Figure 42. NAT ARP Ping



Benefits

- The static IP configured laptop devices can work seamlessly with the wireless LAN infrastructure without changing the laptop settings.

Hardware

Routers	• Cisco 800, 17/1800, 2600XM, 2800, 3700, 3800, 7200, and AS5000 Series Routers • Cisco 7301 Router

8) Release 12.4(4)T Highlights

Table 10. Release 12.4(4)T Feature Highlights

8.1) Cisco IOS Security
8.1.1) Flexible Packet Matching
8.1.2) Application Firewall for Instant Message Traffic Enforcement
8.1.3) VRF-Aware Domain Name System
8.1.4) Easy VPN Phase 6
8.1.5) Control Plane Protection
8.1.6) VRF-Aware IPsec MIB
8.1.7) IPv6 Support for Site-Site IPsec VPN
8.1.8) Dynamic Multipoint VPN Quality of Service Support

8.1) Cisco IOS Security

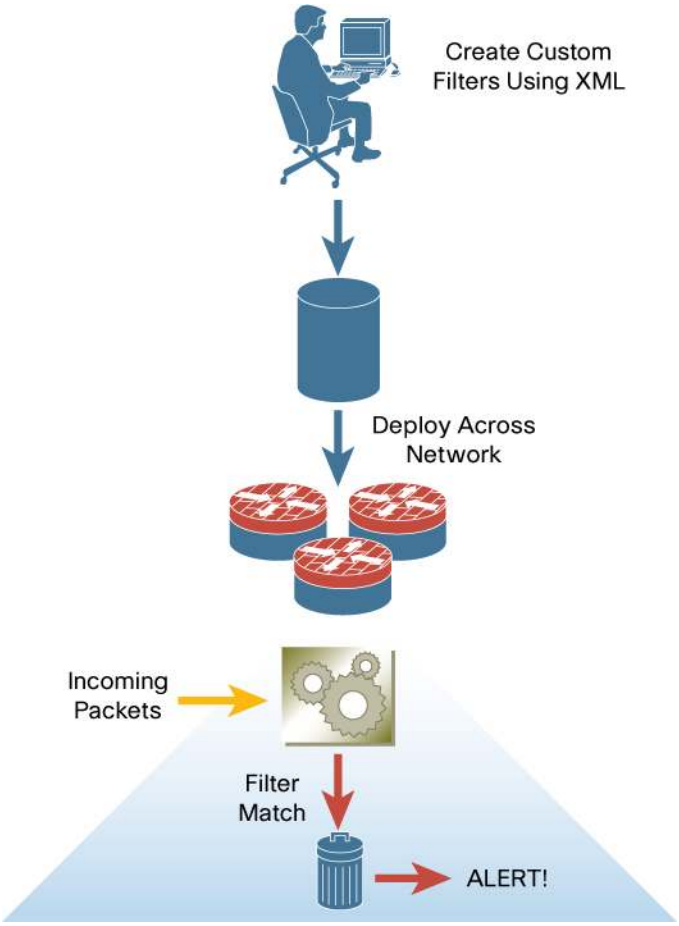
8.1.1) Flexible Packet Matching

Flexible Packet Matching (FPM) is a packet classification feature that allows users to define one or more classes of network traffic by pairing a rich set of standard matching operators with user-defined protocol header fields. FPM further extends the network traffic class definition capability to include new CLI syntax to offset into a user-defined protocol header and, furthermore, into the data portion of the packet.

FPM is the next-generation Access Control List (ACL) technology that provides rapid first line of defense against malicious traffic at the entry point into the network. It features powerful custom pattern matching deep within packet header or payload, minimizing inadvertent blocking of legitimate business traffic.

FPM provides network security administrators with powerful tools to identify miscreant traffic as it enters the network, and to immediately drop and/or keep a log for audit purposes. Administrators can specify custom match patterns at multiple offsets within the packet. FPM includes ready-made definitions for standard protocols via Protocol Header Definition Files (PHDF), which simplify deployment. Customers can also customize and add extensions to PHDFs at device run time.

Figure 43. Cisco IOS FPM



Benefits

FPM enables users to create their own stateless packet classification criteria and to define policies with multiple actions (ie: drop, log or send ICMP unreachable) to immediately block new viruses, worms, and attacks. Essentially, FPM provides the means to inspect packets for characteristics regardless of the header fields involved. It provides a flexible Layer 2 through Layer 7 stateless classification mechanism.

Hardware

Routers	• Cisco 871 Series, 1700 (1701, 1711, 1712, 1721, 1751, 1751-V, 1760), 1800, 2600 (2600XM, 2691), 3700, 3800, 7200 and 7301 Series Routers

Considerations

This feature will only be available in Advanced Security, Advanced IP Services, and Advanced Enterprise Software packages.

Additional Information: http://www.cisco.com/go/fpm/

Product Management Contact: ask-stg-ios-pm@cisco.com

8.1.2) Application Firewall for Instant Message Traffic Enforcement

Application Firewall for Instant Messenger Traffic Enforcement reduces exposure to potential vulnerabilities from instant messenger clients. It offers flexible policy enforcement by allowing administrators to restrict user access to specific instant messenger services, such as text chat, voice or video chat, and file transfer, and ensures judicious use of network resources.

For example, Instant Messenger Traffic Enforcement can easily implement a policy that allows that text-chat capability in instant messenger, but denies access to additional services such as voice or video chat and file transfer. Additionally, audit-trail capability allows customers to monitor the volume of instant messenger traffic for specific users.

Benefits

- Can limit instant messenger usage within a network by enforcing instant messenger policy in a granular manner, thereby ensuring judicious use of network resources
- Reduces exposure to vulnerabilities from instant messenger clients

Hardware

Routers	• Cisco 1700 (1701, 1711, 1712, 1721, 1751, 1751-V, 1760), 1800, 2600 (2600XM, 2691), 2800, 3700, 3800, 7200 and 7301 Series Routers

Considerations

The feature will only be available in the Advanced Security, Advanced IP Services, and Advanced Enterprise Software packages.

Additional Information: http://www.cisco.com/go/firewall/

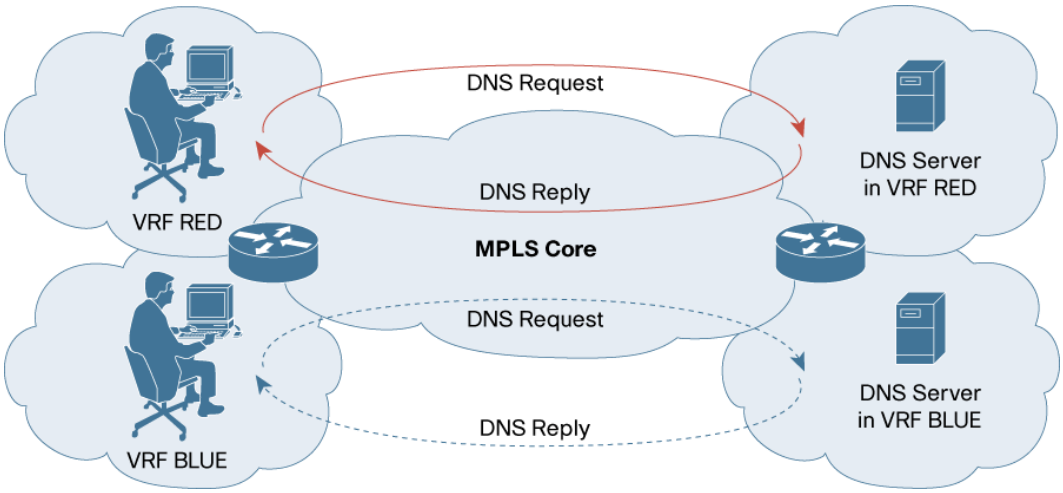
Product Management Contact: ask-stg-ios-pm@cisco.com

8.1.3) VRF-Aware Domain Name System

The Domain Name System (DNS) translates the names of network nodes into IP addresses on the Internet. The current Cisco IOS DNS feature assumes that all name lookups should be directed to preconfigured DNS servers in the global IP address space.

Virtual Routing and Forwarding (VRF)-aware DNS extends this functionality in the context of Multiprotocol Label Switching (MPLS) VPNs by allowing users to direct DNS queries within a given VRF to their respective DNS server within that VRF.

Figure 44. VRF-Aware DNS



Benefits

Facilitates SSL-based VPN deployments in corporate remote access networks, as an alternative to existing IPsec-based VPNs

Hardware

Routers	• Cisco 800 (830, 850, 870), 1700 (1701, 1711, 1712, 1721, 1751, 1751-V, 1760), 2600 (2600XM, 2691), 3600 (3631, 3660), 3700, 3800, 7200, 7301, and AS5000 Series Routers

Additional Information

Configuring DNS on Cisco Routers:
http://www.cisco.com/en/US/tech/tk648/tk362/technologies_tech_note09186a00800c525f.shtml

Product Management Contact: Mark Denny (mdenny@cisco.com)

8.1.4) Easy VPN Phase 6

- **Auto Configuration Update:** Allows users to push configuration changes to any number of Cisco IOS Easy VPN hardware clients.
- **Dial Backup Reactivate Primary Peer:** Easy VPN client continues the IKE SA setup attempt with primary server even after failover. Once the primary becomes available, the connection is re-established and the secondary is dropped.
- **Easy VPN Remote Dual Tunnel Support:** Allows two tunnels to be built from one remote device connecting to different head-end devices.
- **Easy VPN Syslog Enhancements:** Provides enhanced logs indicating detailed reasons for session establishment failures.

Benefits

- **Auto Configuration Update:** Provides zero touch provisioning of any feature, including voice and routing.
- Easy VPN can stop worms or attacks by enabling Access Control Lists (ACLs), Firewall, Cisco IOS Intrusion Prevention System (IPS), and Quality of Service (QoS). Easy VPN client cannot join the VPN unless it applies the configuration change.

- **Dial Backup Reactivate Primary Peer:** Maintains optimum connection at all times, and does not require use of dynamic routing protocol.
- **Easy VPN Remote Dual Tunnel Support:** Supports segregation of application traffic such as voice and data to disparate locations.
- **Easy VPN Syslog Enhancements:** Important events like authentication failure and its cause are logged, to make it easy to troubleshoot VPN client connectivity failures.

Hardware

Routers	• Cisco 800, 1700, 1800, 2600, 2800, 3600, 3700, 3800, and 7200 Series, and Cisco 7301 Router

Considerations

Auto Configuration Update: Release 12.4(4)T or higher must run on the router headend device

Additional Information: http://www.cisco.com/go/ipsec/

Product Management Contact: ask-stg-ios-pm@cisco.com

8.1.5) Control Plane Protection

Control Plane Protection (CPPr) protects a router's control and management planes, ensuring routing stability, availability, and packet delivery.

Network infrastructure attacks are becoming increasingly common, highlighting the need for infrastructure protection. Denial of Services (DoS) attacks are one kind of infrastructure attack which targets a router's control plane processor. The route processor is critical to network operation and any service disruption of the control plane traffic can lead to network outages that affect business operations. Cisco's Network Foundation Protection provides the tools, technologies and services to counter these and similar threats directed towards the heart of the system, the processor. Control Plane Policing (CoPP) introduced the concept of early rate-limiting aggregate and protocol specific control plane traffic. Control Plane Protection (CPPr) extends this control plane protection functionality by providing enhanced and granular control against DoS attacks.

Benefits

- Enhanced and granular protection against DoS attacks targeting infrastructure routers
- Better platform reliability and availability

Hardware

Routers	• Cisco 800 (830, 850, 870), 1700 (1701, 1711, 1712, 1721, 1751, 1751-V, 1760), 1800, 2600 (2600XM, 2691), 3700, 3800, 7200 and 7301 Series Routers

Additional Information (URLs): http://www.cisco.com/go/nfp/

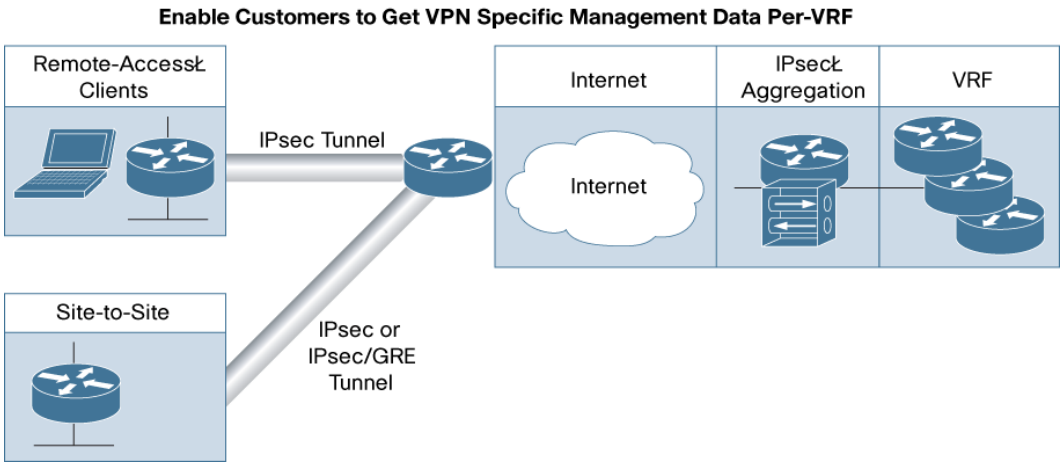
Product Management Contact: ask-stg-ios-pm@cisco.com

8.1.6) VRF-Aware IPsec MIB

Virtual Routing and Forwarding (VRF)-Aware IPsec introduced IPsec tunnel mapping to Multiprotocol Label Switching (MPLS) VPNs. With this capability, users can map IPsec tunnels to VRF instances using single public-facing IP addresses.

VRF-Aware IPsec MIB enables customers to collect and utilize per-VPN specific management data for ongoing operational needs. The granular components of this feature includes VPN Management data support for both site-site and remote-access deployments. The feature can be applied in the context of an IPsec, IPsec+GRE, and Virtual Tunnel Interface tunnel.

Figure 45. VRF-Aware IPsec MIB



Benefits

- Improved manageability for users who deploy VRF-Aware IPsec
- Enhanced value and flexibility: the tunnel agnostic nature of this feature reaffirms the flexibility in VPN solution choices, from a manageability perspective

Hardware

Routers	• Cisco 800, 1700, 1800, 2600, 2800, 3600, 3700, 3800, and 7200 Series, and Cisco 7301 Router

Additional Information (URLs): http://www.cisco.com/go/iossecurity/

Product Management Contact: ask-stg-ios-pm@cisco.com

8.1.7) IPv6 Support for Site-Site IPsec VPN

IPv6 is the next-generation network layer internet protocol intended to replace IPv4 in the TCP/IP suite of protocols. The primary objective for IPv6 is to increase Internet global address space to accommodate the rapidly increasing numbers of users and applications that require unique global IP addresses.

Cisco IOS IPsec functionality provides network data encryption at the IP packet level, offering a robust, standards-based security solution. It provides data authentication and anti-replay services, in addition to data confidentiality services. IPsec is the only way to implement secure VPNs. Customers can combine IPsec with other Cisco IOS Software functionality to build scalable, robust, and secure Quality of Service-aware VPNs.

IPv6 support for Site-to-Site IPsec VPNs enables businesses to use advanced encryption between router-router communications on an IPv6 network. IPv6 IPsec VPN supports tunnel mode for site-to-site IPsec protection of IPv6 traffic. The feature can use IPv6 IPsec encapsulation to protect both IPv6 unicast and multicast traffic. The supported features include:

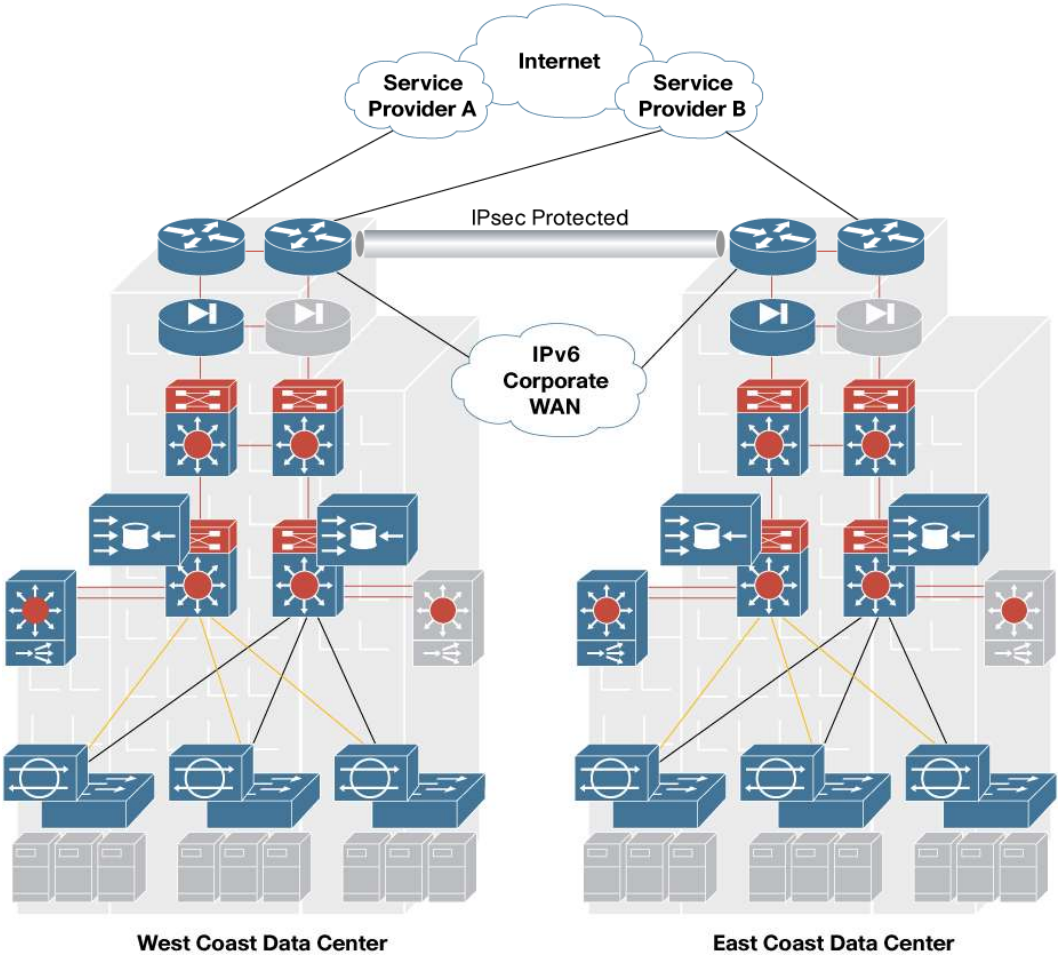
- Native IPv6 IPsec support: native IPv6 ipsec support for site-site deployments

- Tunnel Mode IPv6 IPsec encapsulation: tunnel mode introduces a one-to-one relationship between tunnels and sites with a dedicated logical interface
- Cross-vendor interoperability: flexibility to work with third party vendors under certain conditions.

Figure 46. IPv6 Support for Site-Site IPsec VPN

Enable Businesses to use Advanced Encryption Between Router-Router on an IPv6 Network

IPv6 Features	Customer Benefits
Native IPv6 Support ▪ Support Site-Site Deployments	▪ Flexibility between v4 or v6 networks
Tunnel Mode IPv6 IPsec Encapsulation ▪ 1:1 relationship between tunnels and Ł sites with a dedicated logical interface	▪ Supports both Unicast and Multicast traffic
Cisco Vendor Interoperability ▪ Can work with other vendor who Ł can support setting IP Proxy any any	▪ Cross vendor interoperability



Benefits

- Native IPv6 IPsec support: flexibility for customers to choose between secure IPv4 and IPv6 traffic
- Tunnel mode IPv6 IPsec encapsulation: flexibility for customers to run different traffic types, including unicast and multicast
- Cross vendor Interoperability: ability to work in an heterogeneous environment

Hardware

Routers	• Cisco 800, 1700, 1800, 2600, 2800, 3600, 3700, 3800, and 7200 Series, and Cisco 7301 Router

Additional Information: http://www.cisco.com/go/iossecurity/

Product Management Contact: ask-stg-ios-pm@cisco.com

8.1.8) Dynamic Multipoint VPN Quality of Service Support
Dynamic Multipoint VPN (DMVPN) Quality of Service (QoS) Support improves interoperation between IPsec and QoS technologies, in order to address different deployment models in Cisco VPN solutions.

The initial phase of Enhanced QoS Support for DMVPN introduces the following features:

- **Per-SA shaping on main interface:** Enables DMVPN customers to shape remote sites on the main interface. The Per-SA shaping on the main physical interface leverages the existing queuing implementation and ties the policy definitions of the remote under the main interface. Support for traffic shaping to ensure that the an enterprise accessing its service provider can meter all its traffic and send it out at a constant rate such that all its traffic passes through the service provider's policing functions.
- **Low Latency Queuing (LLQ) before Crypto Engine:** Introduces a single PQ for all egress and ingress packets. It enables per-tunnel LLQ classification and policing.
- **Enhancements to Queuing before Crypto Engine:** Helps classify packets into fair-queue such that there is one queue per tunnel based on Security Association.
- Enhancements include fair-queue system to provide per-SA fairness when crypto engine is congested, allocating Pak priority queues before crypto engine etc.
- **Prioritization of Routing Updates:** Routing updates occurring in the DMVPN network are prioritized by allocating a separate Queue.

Feature	Solution Addressed
Traffic Shaping for Spoke Overrun	Partial
Prioritization of Routing Updates	Yes
Scalability	Max 255 Spokes

Benefits

- Enhanced support for V3PN application in DMVPN networks
- Improved support for convergence of dynamic routing protocols
- Initial phase of Enhanced Quality of Service Support for Dynamic Multipoint VPN is the foundation that enables new network service offerings by service providers

Hardware

Routers	• Cisco 800, 1700, 1800, 2600, 2800, 3600, 3700, 3800, and 7200 Series, and Cisco 7301 Router

Additional Information: http://www.cisco.com/go/iossecurity/

Product Management Contact: ask-stg-ios-pm@cisco.com

9) Release 12.4(2)T Feature Technology Highlights

Table 11. Release 12.4(2)T Hardware and Feature Highlights

9.1) Cisco IOS Security

9.1.1) Cisco Router and Security Device Manager 2.1.2

Cisco Security and Router Device Manager (SDM) combines routing and security services management with ease of use, intelligent wizards, and in-depth troubleshooting capabilities to provide a tool that supports the benefits of integrating services onto the router. Customers can now synchronize the routing and security policies throughout the network, enjoy a more comprehensive view of their router services status, and reduce their operational costs.

The Cisco SDM user interface, online help, and tutorials have been translated into Japanese, Simplified Chinese, French, German, Spanish, and Italian. Microsoft Windows OS also supports these languages.

Benefits

Simplifies router and security management for native language users.

Hardware

Routers	• Cisco SB 100, 830, 850, 870, 1700, 1800, 2600XM, 2800, 3600, 3700, 3800, 7200VXR, and 7301 Series Routers

Additional Information: Cisco Router and Security Device Manager

Product Management Contact: ask-stg-ios-pm@cisco.com

9.1.2) Transparent Cisco IOS Intrusion Prevention System

Transparent Cisco IOS IPS simultaneously scans traffic at Layer 3 and Layer 2. It enables the network administrator to deploy IPS in an existing network without changing the statically addressed peripheral devices on the trusted network.

This is an example of a retail store environment in which wireless devices have been statically addressed. They need to access the database, but the danger is that someone in the parking lot

could potentially enter the network and avoid being scanned by IPS. This network is vulnerable to wireless access point intrusion.

Figure 47. Without Transparent Cisco IOS IPS

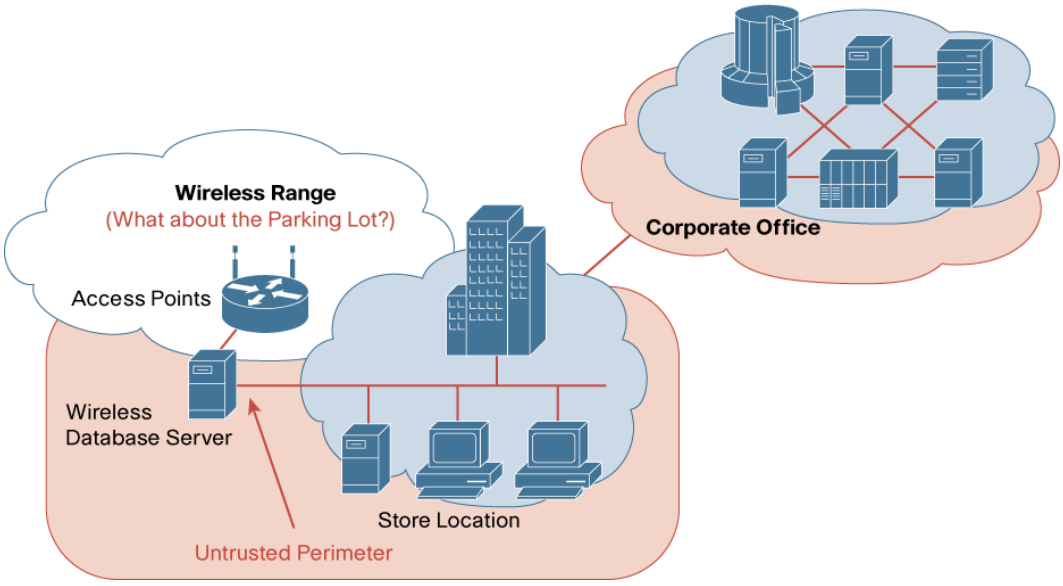
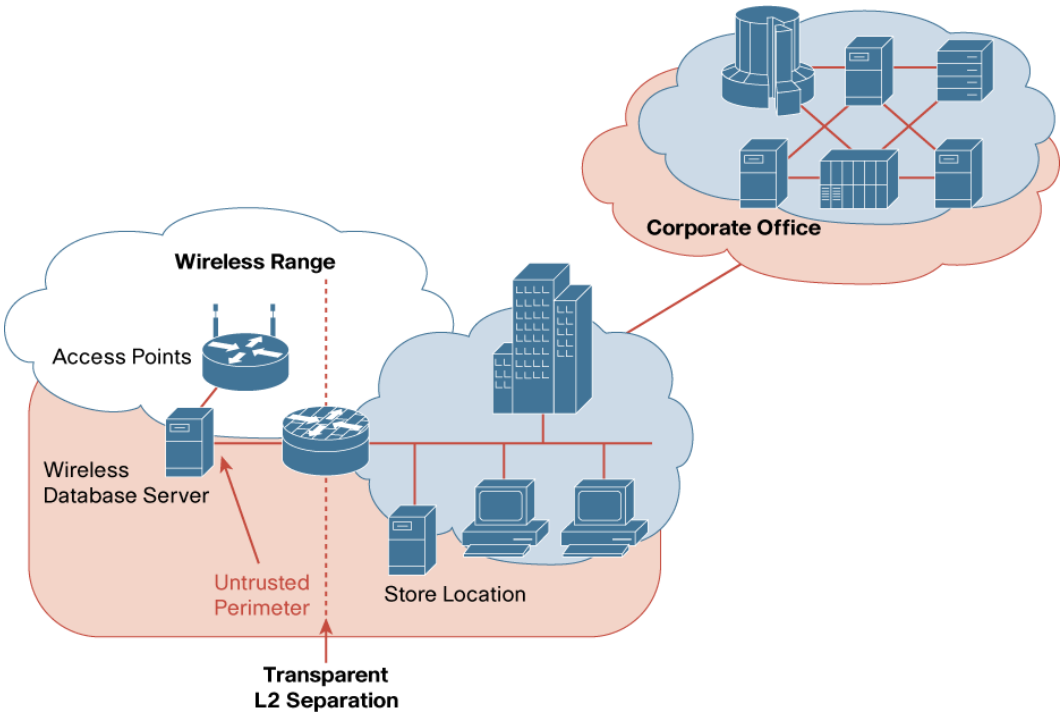


Figure 138 illustrates the effect of Transparent Cisco IOS IPS on a network. If a hacker tries to compromise the wireless side of the network, Cisco IOS IPS can scan the traffic and deny unwanted attacking traffic.

Figure 48. With Transparent Cisco IOS IPS



Transparent Cisco IOS IPS is configured with Layer 3 IPS rules using the “ip ips” command. The ‘ips in/out’ command can be configured on any of the bridged interfaces for Layer 2 protection while also being configured on any LAN or serial interfaces to provide traditional Layer 3 protection. The Transparent IPS operates on bridged packets and the layer 3 IPS continues to operate on routed packets.

Benefits

- Ability to insert IPS within an existing network.
- Eliminates the need to manually readdress previous statically defined devices, which is a tedious and resource intensive task.
- Provides both Layer 2 and Layer 3 IPS capabilities on the same router.
- Cisco IOS Software bridging supports any number of interfaces or sub-interfaces in a bridge-group.
- Supports multiple interfaces.

Hardware

Routers	• Cisco 830, 870, 1700, 1800, 2600XM, 2800, 3600, 3700, 3800, 7200, and 7301 Series Routers

Considerations

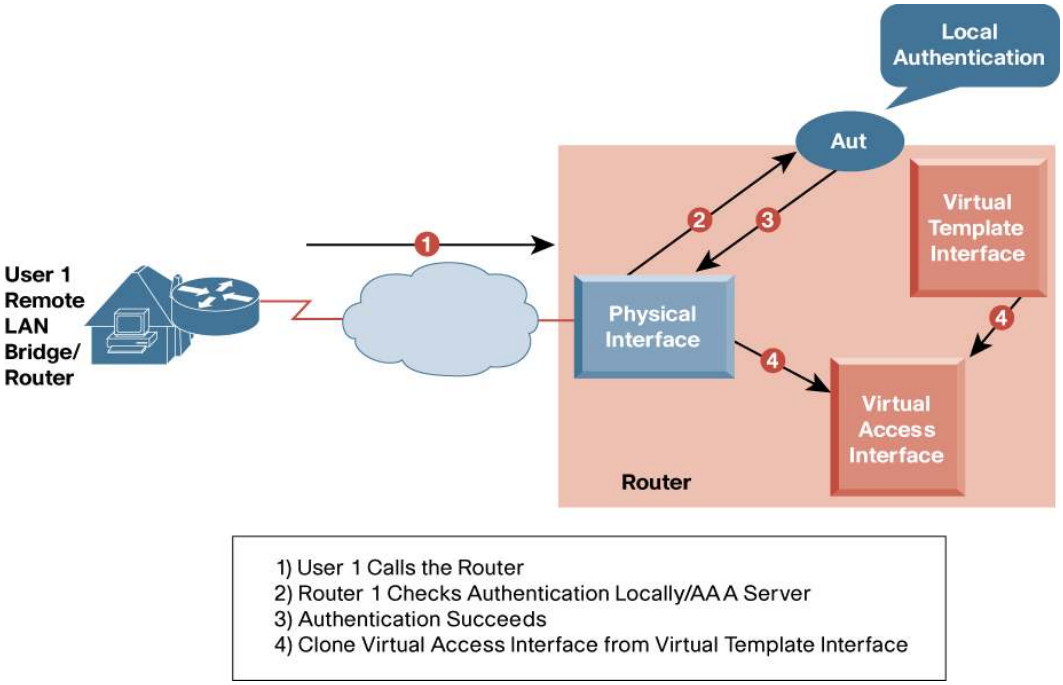
1. Transparent IPS only inspects TCP, UDP and ICMP traffic and supports 802.1Q vlan trunks.
2. Transparent IPS does not support ISL encapsulation. ISL VLANs will work when sub-interfaces are created and placed in the bridge-group.

Product Management Contact: ask-stg-ios-pm@cisco.com

9.1.3) Easy VPN Dynamic Virtual Tunnel Interfaces

An IPsec Virtual Tunnel Interface is an interface to support native IPsec tunneling. It has most of the properties of a physical interface. When combined with Easy VPN, it provides a very powerful solution—creating virtual IPsec interfaces dynamically (akin to what is currently done in the dial world) to enable the deployment of large scale IPsec networks with very minimal configuration.

Figure 49. Easy VPN Dynamic Virtual Tunnel Interfaces



Benefits

- Simplified VPN configuration.
  - Eliminates Crypto Maps, Crypto Access Control Lists (ACLs) for ease of management.
  - Minimal configuration on router allows rapid deployment of VPNs.
- Supports per-session features.
  - Per-user attributes such as QoS empower the Admin to set proactive policies in delivering the desired application performance, which results in increased user satisfaction and productivity.
- Integrated with Easy VPN solution.
  - Hardware client has a separate interface context to which tunnel specific features can be applied. This integration of features & investment protection results in lower total cost of ownership.
  - Easy VPN Server has Dynamic Virtual Tunnel Interface to which tunnel specific features can be applied providing the flexibility to customize configuration and security based on site-specific needs.
- Virtual Route Forwarding (VRF) configured on the interface.
  - Multiple VRFs can be terminated in multiple interfaces to simplify large scale Service Provider and Enterprise MPLS deployments.

Hardware

Routers	• Cisco SB 100, 830, 850, 870, 1700, 1800, 2600XM, 2800, 3600, 3700, 3800, 7200VXR, and 7301 Series Routers

Additional Information: Cisco IOS IPsec

Product Management Contact: ask-stg-ios-pm@cisco.com

9.1.4) Other Easy VPN Enhancements

Easy VPN Phase 5 includes the following enhancements to Easy VPN Server and Remote.

- Login banner to Easy VPN hardware clients—allows a banner message to be displayed after Web Based Tunnel Activation.
- Auto update for software clients—supports the new Auto Update feature in the Cisco VPN Client version 4.6 and above.
- Browser proxy configuration—allows the client's browser proxy configuration to be temporarily modified for the duration of the VPN session.

Benefits

- Login banner to Easy VPN hardware clients—enables regulatory compliance of notification and warnings via client side banner message. Also enhances manageability and ease of use.
- Auto update for software clients—eases upgrades and migration by automating software client updates.
- Browser proxy configuration—improves performance and usability by changing browser proxy settings on the fly to remove or modify settings that are invalid during a VPN session.

Hardware

Routers	• Cisco 830, 870, 1700, 1800, 2600XM, 2800, 3600, 3700, 3800, 7200VXR, and 7301 Series Routers

Additional Information: Cisco IOS IPsec

Product Management Contact: ask-stg-ios-pm@cisco.com

9.1.5) Certificate Authority Key Rollover

A Certificate Authority (CA) manages certificate requests and issues certificates to participating network devices. Before any PKI operations can begin, the CA generates its own public key pair and creates a self signed CA certificate; thereafter the CA can sign certificate requests and begin peer enrolment for all the members of the PKI.

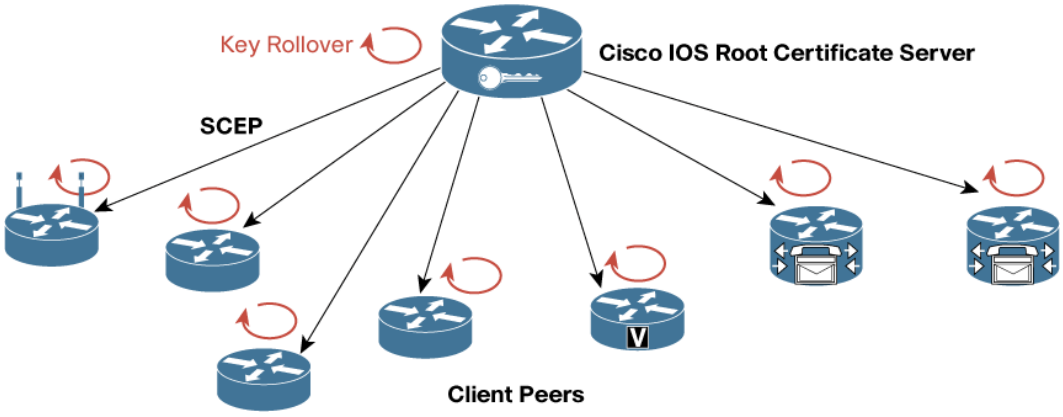
CAs, like their clients have certificates with expiration dates that need to be reissued when the current certificate is about to expire. CAs also have key pairs used to sign client certificates. When the CA certificate is expiring, it must generate a new certificate and associated keypairs. This process, called rollover, allows for continuous operation of the network while clients and the certificate servers are switching from an expiring CA certificate to a new CA certificate.

Rollover relies on the PKI infrastructure requirements of trust relationships and synchronized clocks. The PKI trust relationships allow the new CA certificate to be authenticated and it allows rollover to be accomplished without the loss of security. Synchronized clocks allow rollover and the

flag-moment (the moment of time when the current CA certificate expires) to be coordinated throughout the network.

This new CA certificate before it is active is distributed as a shadow certificate. The shadow certificate is sent along with the currently active certificate with the flag moment transition time (time left for the currently active certificate to expire). When the flag-moment occurs, the shadow certificate immediately becomes the active certificate and the previously active CA certificate is deleted.

Figure 50. Certificate Authority Key Rollover



Benefits

- This feature allows the ability for a root or subordinate CA to rollover expiring CA certificates and keys throughout the entire PKI network.
- Prior to this feature, the system administrator would have to manually enroll all PKI devices in the network on expiry of the root CA certificate.

Hardware

Routers	• Cisco 800, 1700, 1800, 2600, 2800, 3600, 3700, 3800, and 7200 Series Routers

Product Management Contact: ask-stg-ios-pm@cisco.com

9.1.6) Configurable Certificate Storage Location

In current versions of Cisco IOS Software, certificates are stored by default in the nvram of the router between reboots. Some Public Key Infrastructure (PKI) Endpoints may have an insufficient amount of nvram storage, and network administrators may wish to use alternate forms of local storage, such as a flash card. The user should be able to specify the type of local storage using configuration commands on the router.

A new PKI-specific CLI has been made available, allowing the user to specify the location where the certificates need to be stored. The choices for storage include all forms of local storage available on the router. The configuration setting takes effect when the running-configuration is saved and the router is reloaded. The default location will continue to be the nvram.

Benefits

Provides an alternate form of storage for certificates and improves manageability of the PKI by giving more options to the user.

Hardware

Routers	• Cisco 800, 1700, 1800, 2600, 2800, 3600, 3700, 3800, and 7200 Series

Product Management Contact: ask-stg-ios-pm@cisco.com

9.1.7) Network Address Translation Optimize Media Path for Session Initiation Protocol Traffic
This feature allows the creation of a shorter path for Session Initiation Protocol (SIP) media channels by distributing end-point IP addressing information via Session Descriptor Protocol (SDP) of SIP messages. This allows end points to communicate directly by using standard routing and eliminates the need for them to traverse through upstream NAT routers.

Figure 51. NAT Optimize Media Path for SIP Traffic

Benefits

- Media path can be shortened, thereby decreasing voice delay.
- Users can have more control on voice policy since media path will be closer to customer domain and not deep in the service provider cloud.

Hardware

Routers	• Cisco 1700, 1800, 2600, 2800, 3631, 3700, 3800, 7200, 7301, 7400, 800, SOHO 90, and UBR7200 Series Routers

Considerations

B1 and C1 (refer diagram above) should have unique IP Addresses and must have a route to each other for a direct media path to be established between them.

Product Management Contact: ask-stg-ios-pm@cisco.com

9.1.8) Zeroization
In the event where the security of a router is jeopardized, the information stored in the router can be used to the unauthorized person's advantage. Zeroization feature allows the end user to completely erase any trace of user data or binary code, including IP address, Cisco IOS Software, router configuration, or packetized data stored in any subsystem or memory device within the router. After the zeroization is activated, the router can be redeployed by downloading a new image.

Benefits

Allows users to clear the router of sensitive information to prevent unauthorized persons from using the equipment to their advantage.

Hardware

Routers	• Cisco 3200 Series Wireless and Mobile Routers

Additional Information: Cisco 3200 Series Wireless and Mobile Routers

Product Management Contact: Bradley Tips (btips@cisco.com)

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA

c25-409477-02 10/08