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 portfolio of new capabilities, including security, voice, and IP services, with powerful hardware support to deliver advanced services for Enterprise and access customers. It will be issued as a series of regularly scheduled individual releases, which Cisco will ultimately consolidate to form the next major release.

Release 12.4(11)T, the fifth release of the 12.4T family, delivers new Layer 2 VPN transport over Multiprotocol Label Switching (MPLS) capabilities, enhanced MPLS management, Mobile IPv6 authorization and identity support, next-generation WAN encryption technology (Group Encrypted Transport VPN), and support for the high performance Network Processing Engine G2 and VPN Service Adapter for the Cisco 7200 Series Router.

Release 12.4(9)T, the fourth release of the 12.4T family, delivers improved manageability, integrated IP communications capability, enhanced HTTP and P2P security, and faster routing protocol convergence.

Release 12.4(6)T, the third release of the 12.4T family, delivers 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, the second 12.4T release, enhances threat protection against malicious worm and virus attacks, improves performance monitoring of VoIP networks, and extends support for secure concurrent services on the Cisco 1800 Series router.

Figure 1
Major Release and New Technology Release Relationship
1.1) Migration Guide


**Note:** Software releases that reach End of Sale are no longer orderable, but are still available to customers under maintenance contracts for downloading from Cisco.com and the Cisco Technical Assistance Center (TAC).

Figure 2 illustrates the current migration path from Cisco IOS Release 12.3T or 12.3 (or prior) into Release 12.4T or 12.4.

**Figure 2**
Release 12.4T Migration Plan

![Release 12.3T or 12.3 X Releases](image)

Release 12.4(10)

Release 12.4(11)T

Cisco IOS Software Release 12.4T continues to undergo rigorous ongoing testing and review cycles to continuously improve and increase reliability and quality. Unlike the Major Release 12.4 family, Release 12.4T integrates new technologies and features with every new release. Release 12.4T will be updated via regular maintenance releases to include improvements resulting from the testing cycle.

**Note:** Maintenance updates for Release 12.3T ceased upon the introduction of Releases 12.4 and 12.4T. Therefore users of Release 12.3T (or prior releases) should move to Releases 12.4 or 12.4T in order to receive maintenance updates.

Each Cisco IOS Software new technology release is built upon the previous release. It adds new software features hardware support and software fixes for previous major releases and new technology releases. Customers interested in upgrading to Release 12.4 or 12.4T should determine their functionality needs and choose the appropriate release.

1.2) Release 12.4T Additional Information

- **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**
  

- **Changes to Cisco IOS Software Product Support in Release 12.4T, Product Bulletin No. 3000**
  
  http://www.cisco.com/go/124thardware/
• **Cisco IOS Software Center**
  Download Cisco IOS Software releases and access software upgrade planners.

• **Cisco Feature Navigator**
  A web-based application that allows you to quickly match Cisco IOS Software releases to features to hardware.

• **Cisco Software Advisor**
  Determine the minimum supported software for selected hardware.

• **Cisco IOS Upgrade Planner**
  View all major releases, hardware, and software features from a single interface.
  [http://www.cisco.com/cgi-bin/Software/Iosplanner/Planner-tool/iosplanner.cgi](http://www.cisco.com/cgi-bin/Software/Iosplanner/Planner-tool/iosplanner.cgi)

1.3) **Cisco IOS Packaging**

**Figure 3**
Cisco IOS Packaging for Cisco Routers

Beginning in Release 12.4(4)T, the Advanced Security image will include Border Gateway Protocol (BGP). Prior to Release 12.4(4)T, users needed Advanced IP Services in order to deploy both Security and BGP in the same image.
Cisco IOS IP Service Level Agreements (SLAs) was removed from the Cisco IOS Packaging IP Base package as of Release 12.3(3). IP Base package is a low memory footprint package with a reduced set of Cisco IOS Software functionality. Beginning with Release 12.4(2)T, the IP Base package will only have the Responder and Internet Control Message Protocol (ICMP) echo operation functionalities. Complete Cisco IOS IP SLAs functionality is available in all other Cisco IOS Software packages.
2) RELEASE 12.4(11)T HIGHLIGHTS

Table 1  Release 12.4(11)T Feature Highlights

<table>
<thead>
<tr>
<th>2.1) Cisco IOS Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1.1) Cisco IOS SSL VPN Enhancements</td>
</tr>
<tr>
<td>2.1.2) SSL VPN Netegrity Single Sign-on (SSO) Support</td>
</tr>
<tr>
<td>2.1.3) SSL VPN Application ACL Support</td>
</tr>
<tr>
<td>2.1.4) SSL VPN Port-forwarding Enhancement</td>
</tr>
<tr>
<td>2.1.5) SSL VPN Debug Infrastructure</td>
</tr>
<tr>
<td>2.1.6) SSL VPN URL Obfuscation Support</td>
</tr>
<tr>
<td>2.1.7) Group Encrypted Transport (GET) VPN</td>
</tr>
<tr>
<td>2.1.8) MPLS VPN (RFC 2547) over Dynamic Multipoint VPN (DMVPN)</td>
</tr>
<tr>
<td>2.1.9) EasyVPN Phase 8.0 Enhancements</td>
</tr>
<tr>
<td>2.1.10) Cisco IOS Firewall H.323 Registration, Admission, and Status (RAS) Message Inspection Support</td>
</tr>
<tr>
<td>2.1.11) Cisco IOS Intrusion Prevention System (IPS) Version 5.0 Signature Format Support</td>
</tr>
</tbody>
</table>

2.1) Cisco IOS Security

2.1.1) 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 4 illustrates a user case scenario for customers implementing Cisco IOS SSL VPN effectively at the branch router.
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 5 provides more portfolio and license pricing details.
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

2.1.2) 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 6 illustrates what the implementation would look like in a customer network.
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.

### 2.1.3) 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.

2.1.4) 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 (i.e.: 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.

Table 2 provides a quick comparison between the old and new port-forwarding enhancement.

<table>
<thead>
<tr>
<th>Feature</th>
<th>hosts file update</th>
<th>Ports &lt;= 1024</th>
<th>Registry Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Original Port forwarding applet in Cisco IOS Release 12.4(6)T</td>
<td>Optional</td>
<td>Optional</td>
<td>Not needed</td>
</tr>
<tr>
<td>Enhanced Port forwarding using HTTP Proxy in Cisco IOS Release 12.4(11)T</td>
<td>Not needed</td>
<td>Not needed</td>
<td>Required</td>
</tr>
</tbody>
</table>

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.
2.1.5) 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.

2.1.6) 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:


Would become a randomly generated URL:


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
2.1.7) 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 7
Group Encrypted Transport

<table>
<thead>
<tr>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>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).</td>
</tr>
</tbody>
</table>
### Table 3  Summary of key GET features

<table>
<thead>
<tr>
<th><strong>Group Domain of Interpretation</strong></th>
<th>GDOI (RFC 3547) is the key management protocol that establishes security associations among authorized group member routers.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IP Header Preservation</strong></td>
<td>The original IP header in IPsec packets is preserved.</td>
</tr>
<tr>
<td><strong>Centralized Key and Policy Management</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Key Server High Availability</strong></td>
<td>The key server, responsible for pushing keys and policies, supports high availability by synchronizing keys and the policy database with a secondary key server.</td>
</tr>
<tr>
<td><strong>Support for Anti-replay</strong></td>
<td>Anti-replay support protects against Man-in-the-Middle attacks.</td>
</tr>
<tr>
<td><strong>Encryption Support</strong></td>
<td>DES, 3DES and AES</td>
</tr>
</tbody>
</table>

#### 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

<table>
<thead>
<tr>
<th><strong>Routers</strong></th>
<th>• Cisco 870, 1800, 2800, 3800, 7200, 7301 Series Routers</th>
</tr>
</thead>
</table>
| **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

2.1.8) 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.
As shown in Figure 8, 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

<table>
<thead>
<tr>
<th>Routers</th>
<th>• Cisco 1800, 2800, 3800, 7200, 7301 Series Routers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hub Devices</td>
<td>• Cisco 7200VXR with NPE-G1 or higher</td>
</tr>
<tr>
<td>Spoke Devices</td>
<td>• Cisco Integrated Services Router (ISR) Series 1800, 2800, 3700, 3800, 7200, 7301</td>
</tr>
</tbody>
</table>

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

2.1.9) 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).
## 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

<table>
<thead>
<tr>
<th>Routers</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Cisco 800, 1800, 2800, 3700, 3800, 7200 Series, and 7301, Routers</td>
</tr>
</tbody>
</table>

## Product Management Contact:

ask-stg-ios-pm@cisco.com

### 2.1.10) 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

2.1.11) 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

3) RELEASE 12.4(9)T HIGHLIGHTS

Table 4  Release 12.4(9)T Feature Highlights

3.1) Cisco IOS Security

3.1.1) Cisco IOS Firewall Enhancements
3.1.2) Cisco EasyVPN 7.1
3.1.3) DMVPN Manageability Enhancements
3.1.4) Virtual Private Network (VPN) Advanced Integration Module (AIM) for Cisco 1841/2800/3800 Integrated Services Routers (ISRs)
3.1.5) Cisco IOS WebVPN—Auto-Applet Port Forwarding Download
3.1.6) Cisco IOS WebVPN—HTTP Authentication
3.1.7) Cisco IOS WebVPN—RADIUS Accounting
3.1) Cisco IOS Security

3.1.1) 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 10**

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 Router


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

3.1.2) 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 11
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](http://www.cisco.com/go/easyvpn)

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

3.1.3) **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
3.1.4) 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.

- 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**

<table>
<thead>
<tr>
<th>Routers</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Cisco 870, 1800, 2800, 3700, 3800, and 7200 Series</td>
</tr>
<tr>
<td>• Cisco 7301 Router</td>
</tr>
</tbody>
</table>

**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/](http://www.cisco.com/go/webvpn/)

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

3.1.3) 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 used “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

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

Cisco Systems, Inc.
All contents are Copyright © 1992–2006 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.
Page 24 of 49
3.1.4) 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 12
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
3.1.5) 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 13**
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
3.1.6) 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 (i.e., 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

3.1.7) 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 (i.e., 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 14**
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)

3.1.8) 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 (i.e., “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 Figure 12 and the corresponding bullets explain how this protocol works:
Figure 15
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

<table>
<thead>
<tr>
<th>Previous Limitation</th>
<th>New Feature</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>No native Multicast encryption</td>
<td>Standard and Flexible Framework implementing a Tuneless architecture</td>
<td>Framework offers unprecedented flexibility (e.g. supports Multicast and Unicast) Day 1 transparent interoperability between various core Cisco IOS technologies</td>
</tr>
<tr>
<td>No security for native multicast in Multicast VPN (mVPN) type architectures</td>
<td>Native Multicast encryption</td>
<td>Supports Multicast encryption in mVPN architectures</td>
</tr>
<tr>
<td>The value of the “Core” network mitigated Single point of failure</td>
<td>Leverage core for Multicast replication</td>
<td>New Architecture leverages the core and investment costs spent on building core</td>
</tr>
</tbody>
</table>
3.1.9) 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 800, 870, 1700, 1800, 2600, 2800, 3600, 3700, 3800, and 7200 Series
|         | Cisco 7301 Router

**Additional Information:**

- [http://www.cisco.com/go/nfp](http://www.cisco.com/go/nfp)

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

3.1.10) 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](http://www.cisco.com/go/nfp)

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

<table>
<thead>
<tr>
<th>Routers</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Cisco 1800, 2600XM, 2800, 3700, 3800, 7200 and 7301 Series Routers</td>
<td></td>
</tr>
<tr>
<td>• Cisco 830, 850, 870, 1701, 1711, 1712, 1721, 1751, 1751-V, 1760, and 2691 Routers</td>
<td></td>
</tr>
</tbody>
</table>

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

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

3.1.11) 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 16

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

4) RELEASE 12.4(4)T HIGHLIGHTS

Table 5  Release 12.4(4)T Security Feature Highlights

| 4.1) Cisco IOS Security                  |
| 4.1.1) Flexible Packet Matching         |
| 4.1.2) Application Firewall for Instant Message Traffic Enforcement |
| 4.1.3) VRF-Aware Domain Name System     |
| 4.1.4) Easy VPN Phase 6                 |
| 4.1.5) Control Plane Protection         |
| 4.1.6) VRF-Aware IPSec MIB              |
| 4.1.7) IPv6 Support for Site-Site IPSec VPN |
| 4.1.8) Dynamic Multipoint VPN Quality of Service Support |

4.1) Cisco IOS Security

4.1.1) 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.
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
4.1.2) 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

4.1.3) 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.
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:

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

4.1.4) 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

<table>
<thead>
<tr>
<th>Routers</th>
<th>Cisco 800, 1700, 1800, 2600, 2800, 3600, 3700, 3800, and 7200 Series, and Cisco 7301 Router</th>
</tr>
</thead>
</table>

### 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/](http://www.cisco.com/go/ipsec/)

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

#### 4.1.5) 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

<table>
<thead>
<tr>
<th>Routers</th>
<th>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</th>
</tr>
</thead>
</table>


**Product Management Contact:** ask-stg-ios-pm@cisco.com
4.1.6) 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 include VPN Management data support for both site-to-site and remote-access deployments. The feature can be applied in the context of an IPsec, IPsec+GRE, and Virtual Tunnel Interface tunnel.

**Figure 19**
VRF-Aware IPsec MIB

**Enable Customers to Get VPN Specific Management Data Per-VRF**

---

**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**

<table>
<thead>
<tr>
<th>Routers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco 800, 1700, 1800, 2600, 2800, 3600, 3700, 3800, and 7200 Series, and Cisco 7301 Router</td>
</tr>
</tbody>
</table>

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

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

4.1.7) 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 20**
IPv6 Support for Site-Site IPsec VPN

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

<table>
<thead>
<tr>
<th>IPv6 Features</th>
<th>Customer Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Native IPv6 Support</strong></td>
<td>• Flexibility between v4 or v6 networks</td>
</tr>
<tr>
<td>• Support Site-Site Deployments</td>
<td></td>
</tr>
<tr>
<td><strong>Tunnel Mode IPv6 IPsec Encapsulation</strong></td>
<td>• Supports both Unicast and Multicast traffic</td>
</tr>
<tr>
<td>• 1:1 relationship between tunnels and 2 sites with a dedicated logical interface</td>
<td></td>
</tr>
<tr>
<td><strong>Cisco Vendor Interoperability</strong></td>
<td>• Cross vendor interoperability</td>
</tr>
<tr>
<td>• Can work with other vendor who 2 can support setting IP Proxy any any</td>
<td></td>
</tr>
</tbody>
</table>

![IPv6 Corporate WAN Diagram](image-url)
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

4.1.8) 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 to Queuing before Crypto Engine**: 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.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Solution Addressed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic Shaping for Spoke Overrun</td>
<td>Partial</td>
</tr>
<tr>
<td>Prioritization of Routing Updates</td>
<td>Yes</td>
</tr>
<tr>
<td>Scalability</td>
<td>Max 255 Spokes</td>
</tr>
</tbody>
</table>

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
5.1) Cisco IOS Security

5.1.1) 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.

5.1.2) 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 21
Without Transparent Cisco IOS IPS

Figure 22 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.
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

5.1.3) 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 23
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

5.1.4) 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

5.1.5) 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 24**
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

5.1.6) 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**

<table>
<thead>
<tr>
<th>Routers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco 800, 1700, 1800, 2600, 2800, 3600, 3700, 3800, and 7200 Series</td>
</tr>
</tbody>
</table>

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

5.1.7) 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 25**

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

5.1.8) 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)
Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco Web site at www.cisco.com/go/offices

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