PRODUCT BULLETIN NO. 2854

CISCO IOS SOFTWARE RELEASES 12.2(18)SXE NEW SECURITY FEATURES AND HARDWARE SUPPORT

This product bulletin highlights security features in Cisco IOS® Software Release 12.2(18)SXE.

1. CISCO IOS SOFTWARE RELEASE 12.2S INTRODUCTION

Cisco IOS Software Release 12.2S is designed for Enterprise campus and Service Provider edge networks that require world-class IP and Multiprotocol Label Switching (MPLS) services. The Cisco Catalyst® Switches and high-end routers in Release 12.2S provide secure, converged network services in the most demanding Enterprise and Service Provider environments, from the wiring closet and data center to the WAN aggregation edge.

The infrastructure innovation and technology leadership in Release 12.2S enable advanced Ethernet LAN switching, Metro Ethernet, and Broadband Aggregation services through enhancements in High Availability, Security, MPLS, VPNs, and IP Routing and Services.

Releases 12.2(22)S, 12.2(20)S, 12.2(18)S, and 12.2(14)S are available from Cisco.com. For detailed information about the features and hardware supported in each of these releases, refer to Release 12.2S New Features and Hardware Support, Product Bulletin No. 2216.

Derived from Release 12.2(14)S, Release 12.2SX provides Release 12.2S functionality and new features and hardware support for the Cisco Catalyst 6500 Series Switch and Cisco 7600 Series Router.

In addition to Release 12.2(18)SXD, Releases 12.2(17d)SXB, 12.2(17b)SXA, 12.2(17a)SX, and 12.2(14)SX are available from Cisco.com. For detailed information about the features and hardware supported in each of these releases, please visit:

- http://www.cisco.com/en/US/products/sw/iosswrel/ps5012/prod_bulletins_list.html
- http://www.cisco.com/en/US/products/hw/switches/ps708/prod_bulletins_list.html

1.1 Release 12.2SX Ordering Information, Feature Sets, and Image Names

Refer to the “Feature Sets” section of the Release 12.2SX release notes for information about Release 12.2SX orderable product numbers, feature sets, and image names.

- http://www.cisco.com/en/US/products/hw/switches/ps708/prod_release_note09186a00801c8339.html
- http://www.cisco.com/en/US/products/hw/switches/ps708/prod_release_note09186a008019e1e9.html

1.2 Additional Information

- Cisco IOS Software Release 12.2S: http://www.cisco.com/go/release122s/
- Cisco IOS Software Release feedback and questions: http://www.cisco.com/warp/public/732/feedback/release/
- Release 12.2SX Release Notes: http://www.cisco.com/en/US/products/hw/switches/ps708/prod_release_note09186a00801c8339.html
- Cisco IOS Software Product Lifecycle Dates & Milestones: http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/prod_bulletin0900aecd801eda8a.html
- Cisco IOS Software Center: http://www.cisco.com/kobayashi/library/12.2/index.shtml

1.3 Release 12.2(18)SXE Hardware and Security Feature Highlights

Dynamic Multipoint VPN

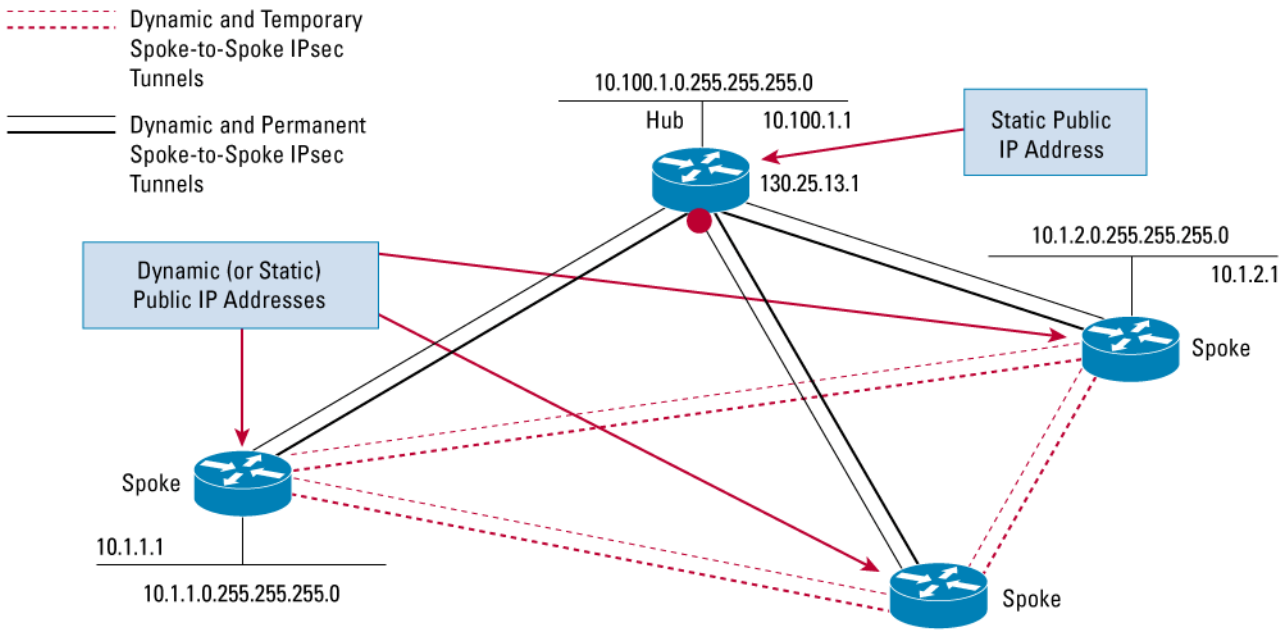
Dynamic Multipoint VPN (DMVPN) combines multipoint Generic Routing Encapsulation (mGRE) tunnels, IPsec encryption, and Next Hop Resolution Protocol (NHRP) routing to provide users a streamlined method of configuring large hub-to-spoke IPsec VPNs and enables dynamic discovery of tunnel endpoints. DMVPN eliminates the requirement for defining static crypto maps for site-to-site VPNs.

This feature relies on the following two Cisco technologies:

- **NHRP:** a client and server protocol where the hub is the server and the spokes are the clients. The hub maintains an NHRP database of the public interface addresses of the each spoke. Each spoke registers its real address when it boots and queries the NHRP database for real addresses of the destination spokes in order to build direct tunnels.
- **mGRE Tunnel Interface:** allows a single GRE interface to support multiple IPsec tunnels and simplifies the size and complexity of the configuration.

The topology shown in Figure 1 and the corresponding bullets explain how this feature works.

Figure 1. DMVPN



- Each spoke has a permanent IPsec tunnel to the hub, not to the other spokes within the network. Each spoke registers as clients of the NHRP server.
- When a spoke needs to send a packet to a destination (private) subnet on another spoke, it queries the NHRP server for the real (outside) address of the destination (target) spoke.
- After the originating spoke learns the peer address of the target spoke, it can initiate a dynamic IPsec tunnel to the target spoke.
- The spoke-to-spoke tunnel is built over the multipoint GRE interface.
- The spoke-to-spoke links are established on demand whenever there is traffic between the spokes. Thereafter, packets are able to bypass the hub and use the spoke-to-spoke tunnel.

Benefits

- Hub Router Configuration Reduction

  - Currently, for each spoke router, there is a separate block of configuration lines on the hub router that define the crypto map characteristics, the crypto access list, and the GRE tunnel interface. This feature allows users to configure a single multipoint GRE tunnel interface, a single IPsec profile, and no crypto access lists on the hub router to handle all spoke routers. Thus, the size of the configuration on the hub router remains constant even if spoke routers are added to the network.
- Automatic IPsec Encryption Initiation
  - GRE has the peer source and destination address configured or resolved with NHRP. Thus, this feature allows IPsec to be immediately triggered for the point-to-point GRE tunneling or when the GRE peer address is resolved via NHRP for the multipoint GRE tunnel.
- Support for Dynamically Addressed Spoke Routers
  - When using point-to-point GRE and IPsec hub-and-spoke VPN networks, the physical interface IP address of the spoke routers must be known when configuring the hub router because IP address must be configured as the GRE tunnel destination address. This feature allows spoke routers to have dynamic physical interface IP addresses (common for cable and DSL connections). When the spoke router comes online, it will send registration packets to the hub router: Within these registration packets is the current physical interface IP address of this spoke.
- Simplifies the burden of headend management and thus reduces the total cost of ownership.

Additional Information

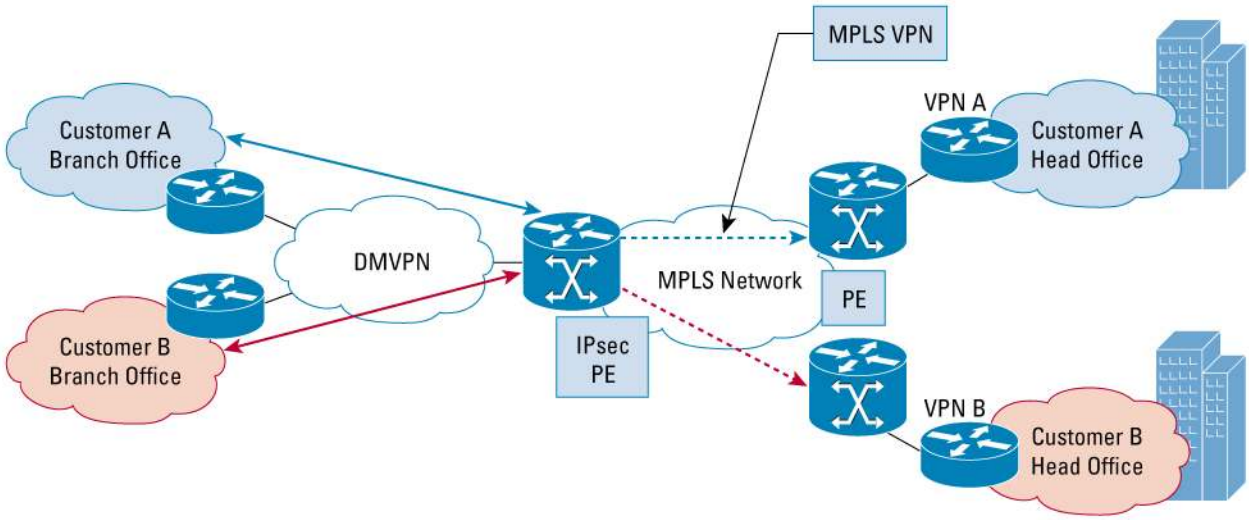
- http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a0080110ba1.html
- http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122sx/12218sxe/index.htm

Product Management Contact: IOS-Security-PM@cisco.com

VPN Routing and Forwarding---Aware Dynamic Multipoint VPN

VPN Routing and Forwarding (VRF) Instance Integrated Dynamic Multipoint VPN (DMVPN) enables users to map site-to-site DMVPN IPsec sessions into Multiprotocol Label Switching (MPLS) VPNs. This allows service providers to extend their existing MPLS VPN service by mapping off-net sites (typically a branch office) to their respective VPNs. IPsec sessions are terminated on the DMVPN PE device and traffic is placed in VRFs for MPLS VPN connectivity. Specifically, work was done to extend the Next Hop Routing Protocol (NHRP) to look into the VRF Tables while building the database of spoke addresses in the hub.

Figure 2. VRF Aware DMVPN



Benefits

- DMVPNs can be used to extend the MPLS networks deployed by service providers to leverage the ease of configuration of hub and spokes, support for dynamically addressed CPEs and zero touch provisioning for adding new spokes into a DMVPN.
- DMVPN architecture can unite many spokes into a single multipoint GRE interface, removing the need for a distinct physical/logical interface for each spoke in a native IPsec installation.

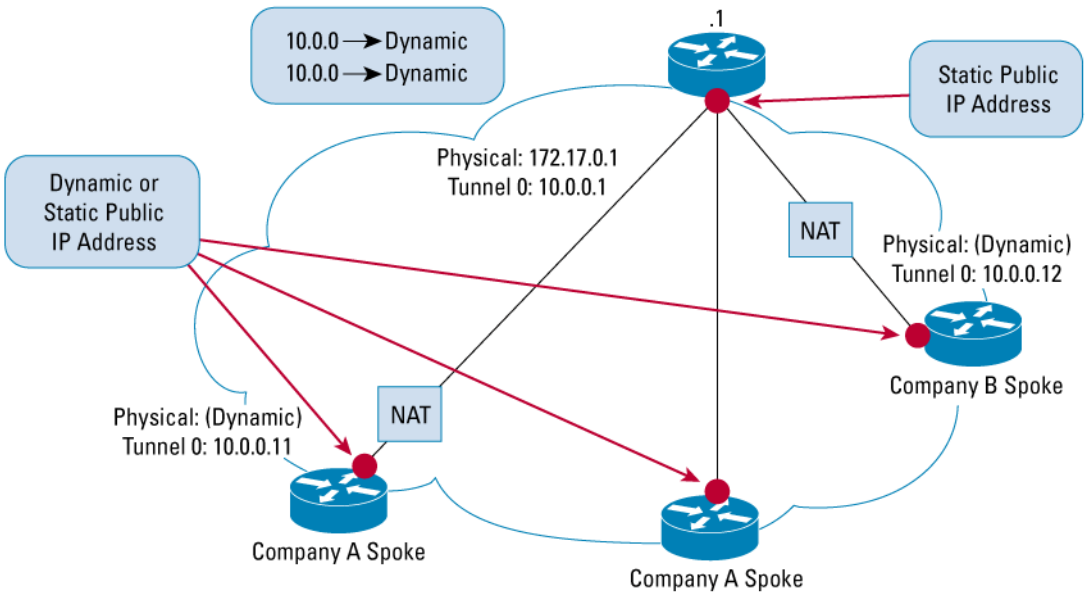
Product Management Contact: IOS-Security-PM@cisco.com

Network Address Translation Transparency Aware Dynamic Multipoint VPN

It is not uncommon to situate a remote DMVPN spoke behind a NAT box, where a Port Address Translation (PAT) is enabled. When the DMVPN spokes need to send a packet to a destination (private) subnet behind another spoke, they query the Next Hop Resolution Protocol (NHRP) server for the real (outside) address of the destination spoke. The DMVPN hub maintains a NHRP database of the tunnel endpoints and the physical address of the spokes.

Figure 3 illustrates that it is typical for spokes in a DMVPN cloud to be given the same physical address by the NAT boxes sitting in front of them. As the spokes often times have no control over the addresses provided to them by the ISP, DMVPN was enhanced to work for spokes behind a NAT Box.

Figure 3. NAT Transparency Aware DMVPN



Benefits

Provides deployment flexibility when spoke routers are behind NAT boxes.

Additional Information

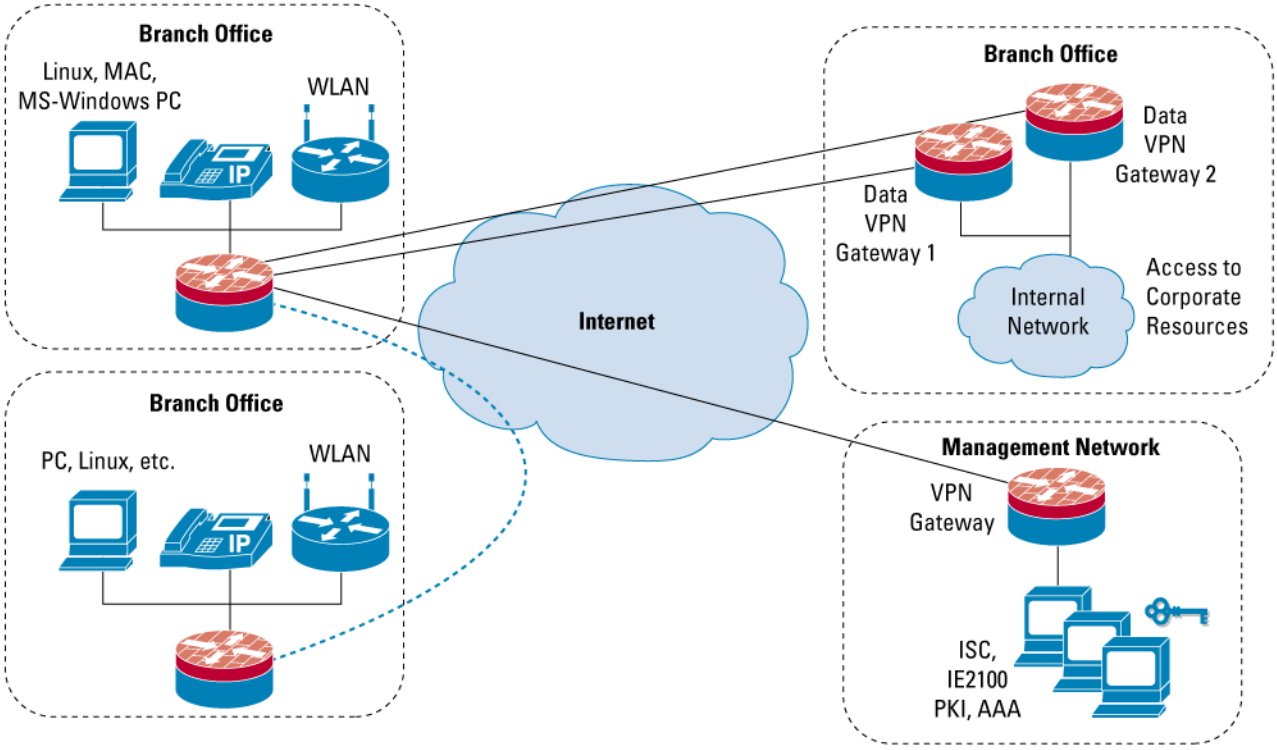
http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/prod_bulletin09186a00801d7229.html#wp1003905

Product Management Contact: IOS-Security-PM@cisco.com

Dynamic Multipoint VPN Spoke-to-Spoke Functionality

Dynamic Multipoint VPN (DMVPN) Spoke-to-Spoke Functionality allows dynamic on-demand direct spoke-to-spoke tunnels to be created between two DMVPN spoke CPEs without traversing the hub. This feature enables production-ready spoke-to-spoke functionality in single- and multi-hub environments in a DMVPN network. It also incorporates increased spoke-to-spoke resiliency and redundancy in multi-hub configurations.

Figure 4. DMVPN Spoke-to-Spoke Functionality



Benefits

- Direct spoke-to-spoke tunnels
  - This functionality allows direct spoke-to-spoke tunnel creation between two branch offices without the traffic having to go through the hub. Spokes can take advantage of an internet connection directly available between them. This leads to reduced latency and jitter for spoke-to-spoke traffic and improved bandwidth utilization. DMVPN networks deliver a lower cost per MByte of Bandwidth than native IPsec networks because the spoke-to-spoke traffic is not restricted by hub bandwidth utilization and at the same time it does not add any additional overhead to the hub bandwidth utilization.
- Avoids dual encrypts and decrypts
  - Native IPsec and IPsec + GRE networks are organized as hub and spoke networks. As a result, all spoke-to-spoke traffic traversing the hub and requiring a dual encrypt and decrypt for all traffic putting an additional burden on the hub CPU. DMVPN alleviates the problem by creating direct on-demand spoke-to-spoke tunnels.
- Smaller spoke CPEs can participate in a virtual on-demand full mesh
  - DMVPN allows smaller spoke CPE to participate in a virtual on-demand full mesh. Creating and managing a full mesh is often not possible for smaller spoke CPE, which cannot handle more than a dozen IPsec tunnels. DMVPN allows the spokes to create tunnels to other spokes on demand and tear down the tunnels after use

Additional Information

- http://www.cisco.com/en/US/tech/tk583/tk372/technologies_white_paper09186a008018983e.shtml
- http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122sx/12218sxe/index.htm

Product Management Contact: IOS-Security-PM@cisco.com

SafeNet IPsec VPN Client Support

Cisco IOS Software headends that terminate SafeNet clients need to be able to support multiple groups of SafeNet clients using different wildcard preshared keys. Each key is placed in a keyring, which is bound to a specific interface address, so that the headend knows which key the client may be using.

Key Rollover for Certificate Renewal

Key Rollover for Certificate Renewal provides Policy Based Routing for IPv6 equivalent to IPv4.

Port Security with 4096 Secure MAC addresses

Increased system wide limit of 1024 secure MAC addresses to 4096 secure addresses.

Port Security with Sticky MAC Address

Port Security with Sticky MAC Address converts dynamically learned MAC addresses to configured addresses automatically.

Encapsulated Remote SPAN

Encapsulated Remote SPAN allows monitoring of traffic across Layer 3 networks.

SPAN Destination Port Permit List

SPAN Destination Port Permit List allows configuring a list of ports that are allowed to be SPAN destination ports. The intended use of this feature is as a safeguard to prevent the accidental misconfiguration of a port.

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

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

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

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

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

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

205267.b_ETMG_SH_4.05

Printed in the USA