

## Updated Cisco Network-Based Security Services Solution 2.5

PB 396190

### Solution Overview

The Cisco® Network-Based Security Services solution delivers virtualized security services in an integrated fashion on innovative Cisco platforms in service provider and enterprise environments. The Cisco Network-Based Security Services Solution 2.5 extends the offering in Cisco IOS® Software Releases 12.4(4)T1 and 12.2(18)SXE4 on Cisco 7200 and 7300 Series Routers and Cisco 7600 Series Routers/Cisco Catalyst® 6500 Series Switches, respectively, with the addition of the features described in Tables 1 and 2.

**Table 1.** New Features in Cisco IOS Software Release 12.4(4)T1 for Cisco 7200 and 7300 Series Routers

Feature	Description
<b>VRF-aware Cisco IOS Firewalls</b>	VRF-aware firewall functions offer virtual firewalls for isolated route space and overlapping addresses.
<b>VRF-aware IPsec Box-box Active/Standby Stateful Failover</b>	Stateful failover for IPsec enables a router to continue processing and forwarding IPsec packets after a planned or unplanned outage occurs. Customers employ a backup (secondary) router that automatically takes over the tasks of the active (primary) router if the active router loses connectivity for any reason. This process is transparent to the user and does not require adjustment or reconfiguration of any remote peer.
<b>IPsec Virtual Tunnel Interfaces with Enhanced Easy VPN</b>	Cisco Dynamic Virtual Tunnel Interface (DVTI) is a new method that can be used by customers with Cisco Easy VPN for both server and remote configurations. The tunnels provide an on-demand separate virtual access interface for each Easy VPN connection. The configuration of the virtual access interfaces is cloned from a virtual template configuration, which includes the IPsec configuration and any Cisco IOS Software feature configured on the virtual template interface, such as quality of service (QoS), NetFlow, or access control lists (ACLs). Included are enhancements to Easy VPN clients with support for download of configurations from the Easy VPN server to the clients, public key infrastructure (PKI) enhancements as part of the authorization wherein username for extended authentication is derived from the certificate handed by the client. DVTI also allows customers to have unique Internet Key Exchange (IKE) endpoint per enterprise customers on the headend without wasting more logical interfaces.
<b>Cisco VPN Acceleration Module 2+</b>	The Cisco VPN Acceleration Module 2+ (VAM2+) for Cisco 7200 Series and Cisco 7301 Routers provides high-performance encryption/compression and key generation services for IPsec VPN applications. Like the VAM2, the VAM2+ supports both Data Encryption Standard (DES), Triple DES (3DES), and Advanced Encryption Standard (AES) 128-bit keys, but adds hardware-acceleration for 192- and 256-bit AES keys. The VAM2+ continues to integrate hardware-assisted Layer 3 compression services with its encryption services, conserving bandwidth and lowering network connection costs over secured links. This combination of security features and advanced network services offers a flexible, integrated approach to accommodate the most diverse enterprise or service provider network environments.

**Table 2.** New Features in Cisco IOS Software Release 12.2(18)SXE4 for Cisco 7600 Series Routers/Cisco Catalyst 6500 Series Switches

Feature	Description
<b>Native DMVPN per VRF</b>	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 branch offices) to their respective VPNs. IPsec sessions are terminated on the DMVPN provider edge 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.
<b>VRF-Aware IPsec Stateful Failover</b>	Routing over IPsec tunnels, dead-peer detection (DPD), Hot Standby Router Protocol (HSRP) plus reverse route injection (RRI), and intrachassis and interchassis stateful failover for both IPsec and generic routing encapsulation (GRE) provide superior VPN resiliency and high availability.
<b>Multiple VPN Blades per Chassis (up to six) with VRF-aware IPsec</b>	A total of six IPsec SPA modules can be configured with VRF-aware IPsec.
<b>1000 VRF-lite per Platform</b>	The systems based on the Cisco Catalyst 6500 Series/7600 Series Supervisor Engine 720-3BXL support a total of 1000 VRFs per chassis.
<b>IPsec VPN SPA with AES and Jumbo Frame Support</b>	In addition to supporting DES and 3DES, the Cisco IPsec VPN SPA supports AES, including all key sizes (128-, 192-, and 256-bit keys). Designed to be the next-generation encryption technology, AES offers IPsec VPN security and interoperability. The Cisco IPsec VPN SPA supports jumbo frames up to 9100 bytes without the need for fragmentation by the supervisor module.

In addition:

- Dorado Software has been accepted in the Cisco Technology Developer Program to manage and provision Cisco Network-Based Security Solutions
- Sales and support of Dorado's "Redcell Network-Based Security – Cisco Edition" are handled by Dorado Software; contact sales@doradosoftware.com

### For More Information

- For more information about the Cisco Network-Based Security Solutions, visit: [http://www.cisco.com/en/US/netsol/ns482/networking\\_solutions\\_sub\\_solution.html](http://www.cisco.com/en/US/netsol/ns482/networking_solutions_sub_solution.html)
- For more information about the Cisco Technology Developer Program, visit: <http://www.cisco.com/web/partners/pr46/tdp/overview.html>

