DMVPN Extends Business Ready Teleworker

Cisco IOS DMVPN reinforces teleworker initiative with unmatched end-to-end security, connectivity, deployment, and management.

BY PLAMEN NEDELTCHEV, GAUTAM AGGARWAL, HELDER ANTUNES, AND DAVID IACOBACCI

THE EXISTING MYRIAD OF IP-BASED virtual private network (VPN) solutions allows enterprises to provide secure home access to corporate resources for three main categories of users: "road warriors" (workers who travel extensively), "day extenders" (employees who access their corporate network from home after regular business hours), and full-time telecommuters. Every Cisco VPN solution can be successfully used as a single solution in each of these categories; however, client- or Web-based VPN solutions target mainly the needs of road warriors, while Cisco site-to-site IOS® VPN solutions address the needs of day extenders and small/remote and branch offices. The latest Cisco IOS VPN solution reinforces the Business Ready Teleworker initiative. It extends and improves end-to-end connectivity, end-to-end deployment models, and end-to-end management. This VPN innovation also provides enterprise-class connectivity; enterprise-quality voice, video, data, and multicast; and unprecedented, layered IOS security features within a Cisco routing protocols framework. In its full evolution, the end-to-end solution will encompass secure, interoperable networks including data, voice-over-IP (VoIP), and wireless LAN (WLAN) networks for enterprises and Internet service providers (ISPs).

From a features standpoint, this new extension divides into four major components: end-to-end layered security, IOS-based end-to-end connectivity, end-to-end deployment, and end-to-end management (see table, page 62). An end-to-end model can significantly reduce operational, support, and management costs, which in general represent 80 percent of total cost of ownership (TCO), according to Sage Research.

The Headend and Remote Sites

At the ***headend,*** the solution incorporates Cisco IP Solution Center (ISC), Intelligence Engine 2100 (IE2100) Series Cisco Networking Services (CNS) engine, IOS-based Public Key Infrastructure authentication, authorization, and accounting (PKI-AAA) integration, a security management gateway, and numerous security data gateways. The headend fully controls the remote site based on an enhanced set of CNS agents running on the remote routers.

At the ***remote site,*** the solution incorporates a low-end router (typically Cisco 830 Series for home users) or midrange router (Cisco 1700, 2600, or 3600 series for branch users), and easy-to-deploy IOS security features such as antitheft protection, configuration integrity protection, and a variety of authentication mechanisms including Auth-Proxy-AAA and port IEEE 802.1X-AAA. Based on configurable policies at the headend, the remote site can be enhanced with features such as Cisco Network Admission Control (NAC), Network-Based Application Recognition (NBAR), and intrusion detection system (IDS).

To facilitate end-to-end interoperability, a great deal of automation is designed into the solution (see table, IOS End-to-End Management, page 62).

End-to-End Connectivity

Dynamic Multipoint VPN (DMVPN) is a key factor in achieving the end-to-end connectivity model, essentially incorporating Cisco routing protocols framework into IP Security (IPSec) VPN framework, which converts the secure peer-to-peer VPN into a secure end-to-end VPN. As a technology, DMVPN comprises IPSec, Next Hop Resolution Protocol (NHRP), and multipoint Generic Routing Encapsulation (mGRE).

From a design perspective, DMVPN offers unmatched flexibility, allowing dynamic hub-to-spoke, virtual partial-mesh architectures, and in its extreme virtual full-mesh architectures (note that large full-mesh architectures can be expensive and difficult to manage in time-division multiplexing and Frame Relay environments). From a deployment perspective, DMVPN simplifies the burden of headend management and thus reduces TCO.

Automated End-to-End Deployment

In general, enterprises and ISPs apply the following basic deployment models:

- In-house model—IT team configures the router and sends it to the branch or home user; the most cost-

For an overview of the components that make up the Cisco Business Ready Teleworker solution, see "Business Ready Teleworker At a Glance," page 15.

END-TO-END VPN AT A GLANCE

IOS End-to-End Layered Security

Device and User Authentication and Antitheft Protection

- Secure RSA Lock Key
- Secure ARP-Proxy
- Auth-Proxy-AAA
- IEEE 802.1X-AAA

IOS-Based PKI

- Certificate Server (CA and RA Modes)
- PKI-AAA Integration
- Auto-Enrollment
- Multiple Trust Points

Underlying Security Features

- IPSec (3DES or AES)
- Stateful Firewall
- NBAR and IDS

IOS End-to-End Connectivity

DMVPN

- Failover/Load Balancing
- Dynamic Routing
- Full-Mesh and Partial-Mesh Topologies
- Hub-to-Spoke and Spoke-to-Spoke Tunnels; Permanent and On-Demand Tunnels
- mGRE, IPSec, NHRP; Transport and Tunnel Modes
- Multiple DMVPN Clouds per Headend Router; Resilience

Full Support of IP Applications

- Data
- VoIP
- QoS
- Wi-Fi
- Multicast
- Video

IOS End-to-End Deployment

Configuration Automation IP Solution Center

Cisco CNS 2100 Series Intelligence Engine

- CNS Configuration Engine
- CNS Notification Engine
- CNS Image Management Engine

Automated Zero Touch Deployment

- Bootstrap Configuration and PKI Certificates (EzSDD)
- Dynamic Addressing

Automated Policy Deployment, Redeployment, and Audit

- DMVPN/IPSec
- Firewall
- QoS
- NAT
- NBAR and IDS

IOS End-to-End Management

Ongoing Management IP Solution Center

Cisco IE2100-Based CNS Notification Engine

- CNS Configuration Engine
- CNS Notification Engine
- CNS Image Management Engine

EMAN Framework Integration

- Automated User Service Application and Entitlement
- Automated Configuration/ Preconfiguration and Audit
- Automated Image Management
- Automated Control, Monitoring, and Security Management
- Interactive/Automated Decision Making and Service Termination
- Antivirus, Antiworm, and DoS Protection (per Identification)
- Automated Event Log Management
- Automated Notification of the Support Teams

LOW TCO, BIG BENEFITS: An end-to-end, highly automated approach enables enterprises to maintain low TCO even when increasing and enhancing the feature set of the solution.

ineffective model. Works relatively well for small and midsized businesses or deployments.

- Outsource/out-task model—Some large enterprises prefer to outsource to one big customer with global presence, who performs the initial task of configuration and logistics, while the enterprise ensures the provisioning. This model adds to the cost of both the acquisition of assets and deployment management.
- Out-of-house model—Some large enterprises or ISPs can use their own staging facilities for initial or complete CPE configuration. The CPE is shipped to the end user /administrator; adds an additional cost to the acquisition of the assets. Sometimes the cost can be significant compared to the purchase price.
- Touchless or ZTD model—Requires presence of at least one user with necessary credentials (AAA account in the corporate AAA server); most frugal model; no extra cost associated.

Of course, these models can vary significantly, and their comprehensive details and cost analyses are beyond the scope of this article. Suffice to say that Business Ready Teleworker supports all common deployment scenarios; however, maintaining the lowest TCO requires the no-cost-associated model to be applied. As noted, in the ZTD model, the remote site can be automatically deployed/decommissioned/redeployed. ZTD is based on a new Cisco IOS Software feature called *Easy Secure Device Deployment (EzSDD)*. While very simple for end users, ZTD is not quite as simple on the backend. Therefore, ZTD is a "virtually simple," fast process that requires all the components of the system work in sync and all scenarios be anticipated and automated.

Let's assume the common case. A home user has subscribed for cable ISP service, and the ISP has provided a cable modem for him. The user can connect his PC to the cable modem, obtain his IP address via Dynamic Host Control Protocol (DHCP), and connect to the Internet. In the most general case, the user can use Security Device Manager (SDM) to configure his router with Point-to-Point Protocol over Ethernet (PPPoE) or Static IP and connect to the Internet. Meanwhile, the home user applies for VPN service from his company, obtains approval, and orders a new Cisco 830 Series Router. After he receives the router at his home office, he connects the router to his cable modem, obtains an IP address from the router (typically 10.10.10.0/24 range), and gets connected to the Internet.

PLAMEN NEDELTCHEV, Ph.D, network engineer with the Intelligent Network Solutions team at Cisco, is author of *Troubleshooting Remote Access Networks*, Cisco Press. He can be reached at pnedeltc@cisco.com.

GAUTAM AGGARWAL, CCIE® No. 4714, is a manager of software development in the Internet Technologies Division at Cisco, specializing in VPN and network security. He can be reached at gaggarwa@cisco.com.

HELDER ANTUNES is a senior development manager in the Internet Technologies Division at Cisco, specializing in network security. He can be reached at helder@cisco.com.

DAVID IACOBACCI is a network engineer with the Intelligent Network Solutions team at Cisco, specializing in VPN and home networking. He can be reached at diacobac@cisco.com.

To be deployed as a VPN user with his company, there are three easy-to-understand steps (from the end user's perspective):

Step one (welcome)—User launches a browser and types in the browser's address filed: http://10.10.10.1/ezsdd/welcome.

Step two (introduction)—User prompted to type a URL in the Web page, https://www.join-mycompany.com/ezsdd/intro, and to press "Next."

Step three (complete)—User prompted for user name and one-time-password ("OTP," this is provided to the user by the IT group or integrator). After a while, his browser will announce "Complete" state and prompt him to release/renew his PC's IP address.

At the headend, this "virtually simple" process (as expected) is a little more complicated and includes a preparation and an action phase. In the preparation phase, while the user is waiting for his router to arrive, the ISC will be configured and all policies will be in "Wait_to_deploy" (Pause) state. In the action phase, the user (Introducer) interacts with CPE (Petitioner), which establishes Trusted Transitive Introduction (TTI) relationship with a CERT router (Registrar). Registrar acts as a proxy for the user authentication. After successful authentication, it intercepts the login_name and requests a general, customized initial bootstrap configuration from ISC, which is pasted into Petitioner's (CPE's) running configuration. The CNS agent is activated. A CNS "connect" event is sent to CNS Engine, which forwards the "connect" message to ISC. All waiting policies are sent to the CPE over the management tunnel. The last Service Request (policy) will complete the process, which on average lasts about 200 seconds.

Automated End-to-End Management

The first and foremost objective of Business Ready Teleworker is managing security. For this solution, based on a broad set of application programming interfaces (APIs) and Simple Object Access Protocol/Extensible Markup Language (SOAP/XML), every new deployment can be integrated into the existing enterprise or ISP infrastructure and interact with AAA, Domain Name System (DNS), and DHCP services. The remote site is fully controlled and managed, and the security policies can be applied, changed, and audited. Therefore, many of the traditional headend functions such as antivirus/antiworm protections and anti-DoS attacks can be managed at the remote site (if identified), effectively increasing the availability of the headend site and corporate network.

In Cisco's global IT deployment, the headend is integrated into the Cisco IT framework. With an in-house management tool suite created by Cisco IT, EMAN incorporates the built-in intelligence of the system using a variety of available APIs and interacts with Cisco ISC and IE2100-based CNS engines. EMAN brings additional features such as monitoring and performance trending, thresholds-based alerts and notifications, as well as image management. In its ultimate functionality, management covers the whole spectrum of information services: monitoring, analyzing, and decision making.

Cisco ISC introduces and supports the notion of fully managed service (FMS). If any configuration changes are scheduled and performed from ISC/EMAN, FMS will accept and register the change. If the change is originated from a non-ISC/EMAN source, FMS triggers a set of functions to audit the CPE's configuration and notifies the supporting teams about configuration/policy change, security violation, connect/disconnect events, and the like. Furthermore, if a policy violation is identified or virus/worm attack or DoS is discovered, the EMAN will trigger an automated/interactive process to prevent the violation.

Non-Cisco customers can plug in additional logic to adjust the system to the way they typically operate or to their management system. The EMAN experience and scripts and available APIs would allow every enterprise or ISP to apply their own set of policies or procedures to control and manage the security risks in their environments.

Unmatched Integration

Cisco's extension to the Business Ready Teleworker solution offers a level of networking and security integration unmatched in the industry to date. Virtual simplicity, maximum automation of management, design flexibility, and scalability are key factors in large-scale (global) deployment and management, and in achieving these factors, this Business Ready Teleworker solution effectively allows low TCO to be maintained.

Cisco's own global deployment includes architectural and design solutions that enable enterprise home, enterprise branch, and ISP deployment models, and provide enterprise-class connectivity, and enterprise-quality voice, video, data, and multicast. The real potential exists for other enterprises to incorporate or integrate the whole solution, or a subset of it, into their existing network environment.

◆ ◆ ◆

The authors express their appreciation to the following Cisco people, who contributed to this article: Mike Sullenberger, Max Pritikin, Henry White, Jennifer Redovian, Dalia Geller, Hom Bahmanyar, Ajith Thrivikramannair, and Pedro Leonardo. ▲▲

FURTHER READING

- **Business Ready Teleworker portal: cisco.com/go/teleworker**
- **DMVPN white paper: cisco.com/packet/162_7c1**