Automating VPN Management

By Scott Hilton, Vice President Product Management
Assured Digital, Inc.

Although many network managers, users and executives agree on the benefits of virtual private networking, the processes involved in setting up and managing VPNs are not so well understood.

In fact, VPN setup and management have proven problematic for network managers for three reasons. First, the basic setup functions for VPN devices must be performed manually and, often, at the remote installation site. This introduces risks of inconsistent policy settings and potential security breaches. Second, manual setup takes time and introduces complexity into larger systems installations. The VPN configuration that worked in a controlled, laboratory environment may not be able to scale up to the real-world needs of an aggressive rollout schedule. Third, network topologies change continuously, and VPN devices have been severely limited in their abilities to adapt to such changes.

For network managers everywhere, VPN management has become a serious concern. Standards, such as the IETF's IPSec security protocol suite, represent a strong beginning. But the larger management challenges posed by production VPNs are more likely to be solved by newer VPN technologies that are putting advanced automation tools to work in second generation products.

VPN Benefits

Virtual private networking has quickly become an important productivity tool for organizations of all sizes, and across all major industries. The VPN works by building a tunnel -- actually a circuit-like path -- through a common WAN infrastructure such as the Internet.

For companies deploying VPNs, the benefits are substantial. First, they take advantage of the lower telecommunications costs and unparalleled flexibility of Internet communications. Second, they preserve the privacy and inherent security of private line and frame relay networks. To the user on a LAN, or the telecommuter dialing into the enterprise via an ISP, encryption and tunneling are completely transparent.

Still, VPNs do come at a price, and as some network managers have discovered, that price can include healthy doses of time and effort required to set up and manage the VPNs themselves. Now, thanks to increasing degrees of automation to help with the care, feeding and handling of VPN devices, network managers

are finding their own reasons to like the new technology.

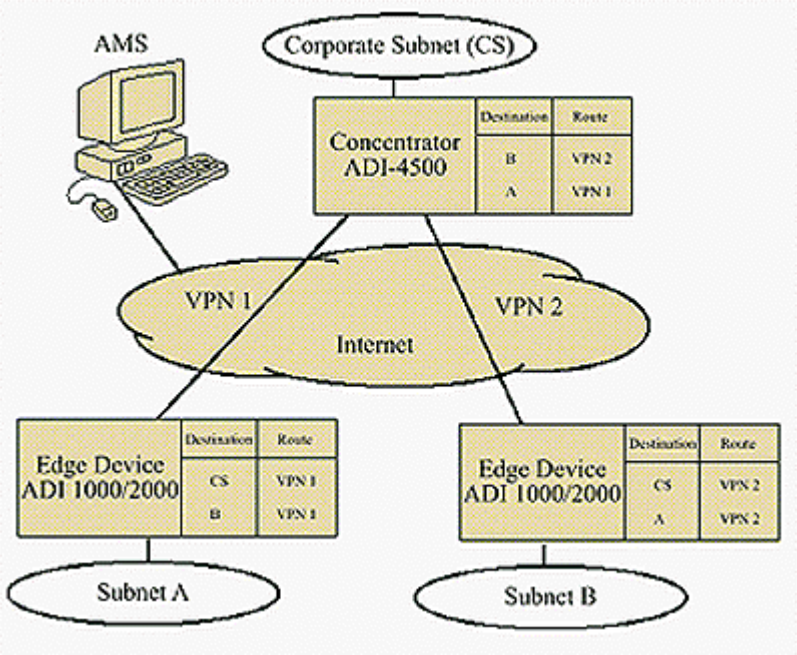
Second-Generation Features

Although software-based VPN applications are available today, hardware-based VPN architectures have grown popular largely because of their greater performance.

First-generation units were typically single-function devices, able only to create tunnels or implement security protocols. They were limited in scalability and difficult to manage in large networks. Newer, second-generation devices have now integrated networking intelligence and management automation with their tunneling and security functions.

Second-generation VPN devices generally include basic encryption / decryption units and multi-user concentrators. VPN remote encryption / decryption devices are frequently placed in campus buildings and branch offices; the concentrators go in corporate or division headquarters.

Figure 1:
A simple VPN setup might look like this, with two VPN edge devices talking to the head-office VPN concentrator. This is all controlled via a management console, with each device consulting its routing tables to make forwarding decisions.



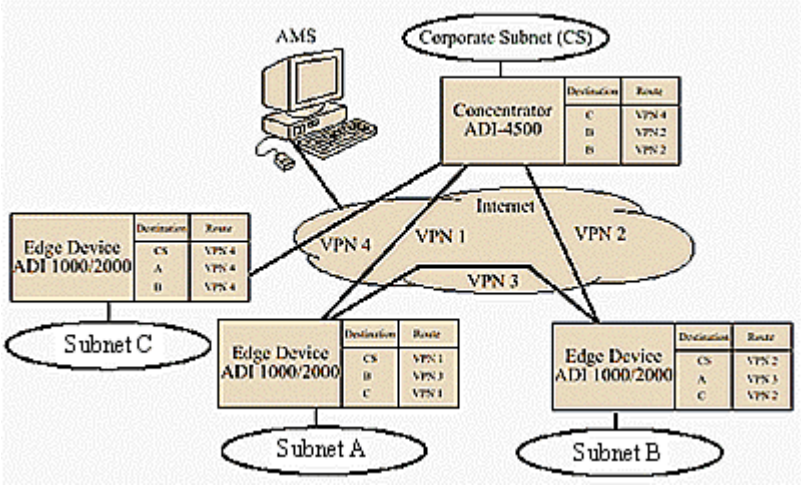
The VPN devices typically serve as gateways for users on LAN subnets, and all use the IPSec protocol to create the tunnels and supply the security framework

for the tunneled packets.

Securing, Connecting VPN Devices
Setting up the VPN devices requires management attention at a number of points in the process: in security, for device authentication, authorization and setting overall security policies, and in network connectivity for configuring, provisioning and managing the devices.

Performed manually, these steps require that trained technicians be onsite -- otherwise, setup is left to local office personnel who are unfamiliar with the complexities of security and networking. Automation solves this problem by permitting central setup and safe, automated administration throughout these major setup steps.

Figure 2:
As the network grows, management automation becomes increasingly critical in a dynamic, meshed environment. Note in the network diagram below that the management console created a second VPN path between Subnet A and Subnet B in order to accommodate an increase in traffic. In an automated system, this scenario can be multiplied hundreds of times and still work effectively and efficiently -- something that is impossible with manual setup.



VPN Security:
Device Authentication
The first step in adding a new VPN device to a network is to authenticate that device's identity. With first-generation units, the network manager or technician would perform authentication manually. The technician would use a "shared-secret" password technique to authenticate the new device with another (known) member of the network. This would require traveling to the remote site, or sending the password via diskette or password regular mail.

By contrast, in an automated system the network manager or technician starts by loading the automated management software into a central policy server. From that central site, the management software communicates through a highly secure control protocol to perform device authentication remotely.

Device authentication is now a process of exchanging digital certificates, based on the X.509 standard defined by the International Telecommunication Union. The integrity of digital certificates is guaranteed -- and certificates are issued -- by a trusted third-party known as a certificate authority, or CA.

This represents an improvement over the password method, but the need for the CA also adds its own measure of complexity. As a solution, some second-generation systems further automate and simplify the process by permitting X.509 certificates to be burned into VPN devices at the time of manufacture. These devices now have a hardware-strength cryptographic identity, and they avoid the remote security risk of device substitution, which might foil even the CA-issued certificates.

Authorization

The next setup step is to determine the new device's database and network access privileges. With a manual installation, authorization is vulnerable because it is performed at the remote site. Anyone who can access the VPN device can modify authorization parameters. In an automated system, authorization is performed from the management console, so it is inherently simpler -- and more secure.

Setting Security Policy

Security policy can cover a half dozen items, from type of encryption protocol to key rollover interval (encryption keys are "rolled over," or changed, at regular intervals). Performed manually, the process is both tedious and risky, since few remote offices have security-savvy technicians on site. An automated system permits security settings to be maintained centrally, then downloaded to new devices as needed; this ensures setup quality and maintains consistency with corporate policy guidelines.

Also, automated wizards can be applied to make the job easier. For instance, a security policy wizard might have several strength levels, each based on pre-determined corporate policy, plus a custom setting to override the defaults.

The highest level setting might be used for highly sensitive applications such as transmitting financial information. It might feature the greatest key strength for encryption (3DES, for example); the shortest-duration rollover interval; per-

packet (rather than per-session) authentication, plus several other parameters -- all selectable via a single mouse-click.

Network Connectivity:

Device Configuration

For device configuration, the network manager or technician sets the device's modes of operations and its network identity. Parameters include the VPN device's IP address and the IP addresses of supported devices and subnets; plus SNMP parameters, default parameters, and routing modes. In an automated system, these parameters can be set centrally, and applied automatically as new devices are introduced.

VPN Provisioning

VPN Provisioning involves the distribution of the device's network connections and configuration of its routing tables. To do this manually, the technician must possess comprehensive knowledge of the organization's network topologies -- especially difficult in large, heavily networked environments. In branch offices, provisioning might fall to an office worker, inputting instructions from a desktop PC, through a serial cable.

In an automated system, provisioning takes place where the network expertise and the network-diagramming tools reside -- centrally. Moreover, the network manager or technician can make use of provisioning templates that simplify the process. And in some systems, the network manager can assign multiple logical VPN connections to a single-port VPN device -- the device will find the most cost-effective path for each new VPN session.

Ongoing Device Management

By their nature, VPNs should be easy to add, delete and modify. First generation systems carried only limited router intelligence, so changes in network connections or subnet topologies required manual updates of static routing tables. Worse, network failures could go undetected -- except, of course, by the VPN users.

Newer VPN systems are using intelligent, dynamic routing protocols such as RIP (Routing Internet Protocol) and OSPF (Open Shortest Path First) to automate the optimization of VPN routes and to implement self-discovery and self-correcting paths.

For instance, intelligent VPN devices can now update their own routing tables, based on status messages sent regularly from other intelligent VPN devices. If a device fails, or if its communications link goes down, its status messages stop, and the other devices automatically update their tables to exclude the failed link.

In a RIP-based system, the number of hops required for each VPN connection is part of each device's forwarding decision. With OSPF, other information can be used, including delay, available bandwidth or shortest path. In the case where the network manager provisioned multiple logical VPN paths, the intelligent device consults its table as each new session is activated to determine which available path is most cost-effective and highest-performing.

Benefits of Automation

Thanks to the management tools and techniques available in second generation VPN systems, the newer encryption / decryption devices come very close to being both self-configuring and self-healing.

To become a full-fledged, fully-secured member of a corporate VPN network, for instance, a new VPN device needs nothing more than its own, burned-in X.509 certificate -- its "cryptographic identity" -- and the IP address of the management server. Once its identity is established by the central system, all other security and network connectivity parameters will be downloaded automatically.

When that device joins the active network, it will automatically signal its presence, and other devices will add it to their routing tables. Likewise, if a device fails, the others will learn, automatically, and adjust their tables -- all without network manager intervention.

These features eliminate much of the tedium tasks and risks of manual setup and management -- a blessing for network managers. Just as important, VPNs can now be justified for large-scale installations, since central automation contributes mightily to their ability to scale to hundreds or thousands of users.

For these users, and their organizations, management automation will play an important role in advancing the cause -- and increasing the benefits -- of virtual private networking in the days ahead.

####