CHAPTER 2

V3PN Solution Overview and Best Practices

This chapter presents a high-level overview of V3PN to give the reader a quick reference as to the capabilities of this solution. The remainder of this document will then go into an increasing level of detail on planning, design, product selection, and implementation of a V3PN.

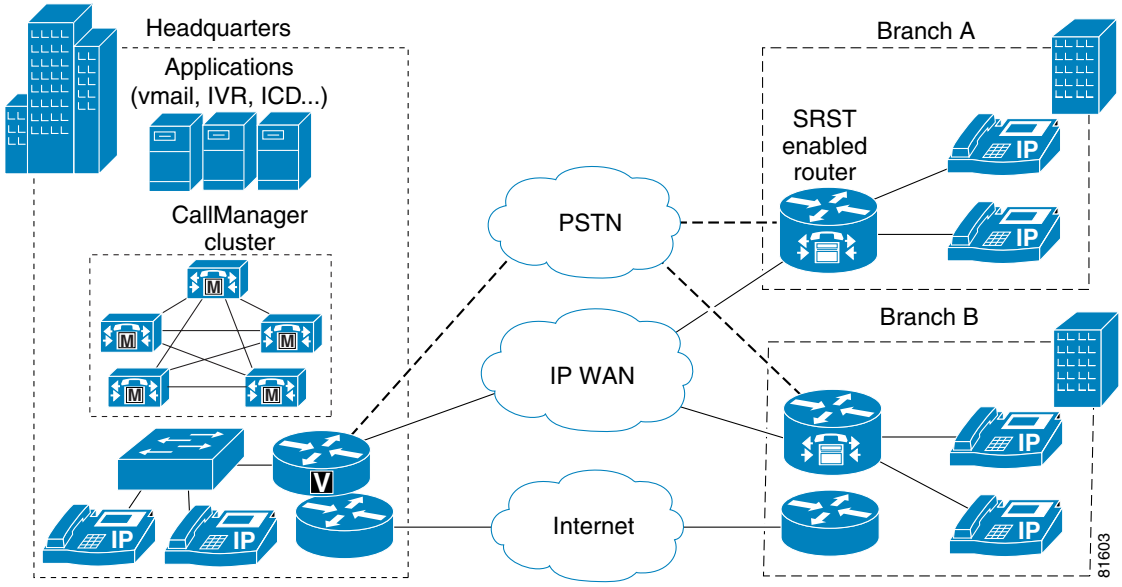
Specific topics in this chapter are:

- Solution Overview, page 2-2
- Solution Characteristics, page 2-4
- General Best Practices Guidelines, page 2-5
- General Solution Caveats, page 2-6

Solution Overview

Figure 2-1 depicts a typical deployment of IP Telephony using a Centralized Call Processing model.

Figure 2-1 IP Telephony Over Private WAN

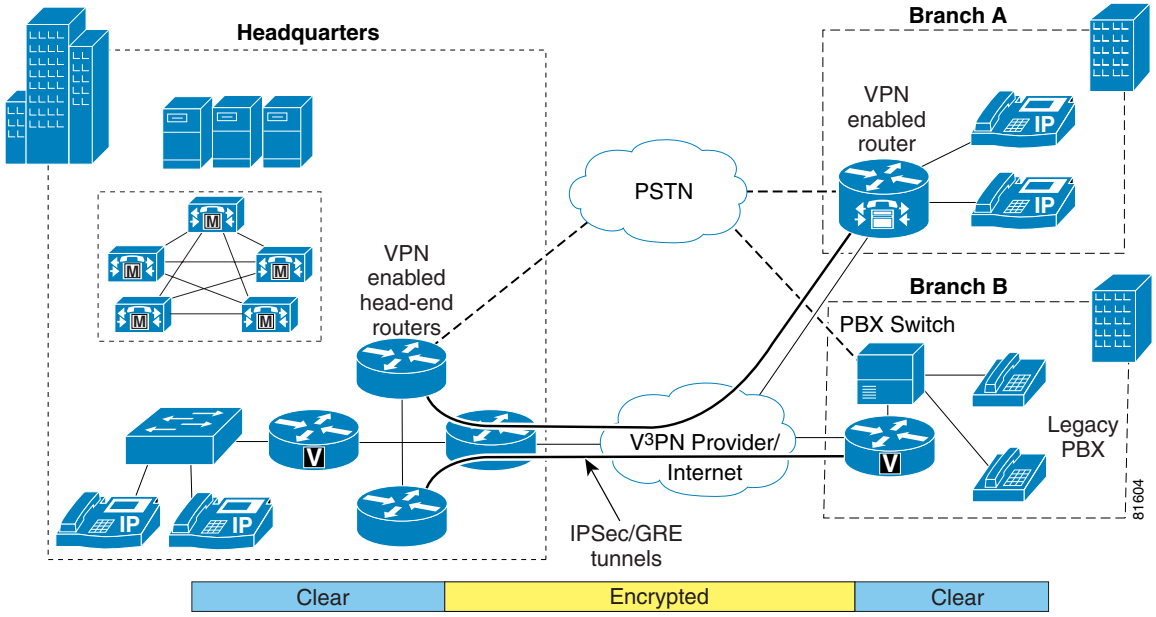


In this arrangement, a Call Manager cluster is deployed at the large central location. Branches might deploy Survivable Remote Site Telephony (SRST), which provides for local call processing to the PSTN in the case of loss of connection to the central site. The PSTN links can also be used for local off-net calling. Connectivity between the central site and branch locations is over a Private WAN technology like FR or ATM. Signaling traffic (such as H.323) is sent over the Private WAN links to the Call Manager cluster at the central site. Voice conversations are established and bearer traffic also flows over the Private WAN links.

Typically, the large central site and large branch locations will have separate connections to an ISP to provide Internet access to the corporation.

Figure 2-2 illustrates this same enterprise implementation with its IP Telephony deployment using a V^{3}PN strategy.

Figure 2-2 IP Telephony Over V^{3}PN



Notice that the IP telephony deployment remains unchanged. But in this deployment, connectivity between the central site and branch locations is over a V^{3}PN provider. Signaling traffic (such as H.323) is sent *encrypted* over the VPN (IPSec/GRE) tunnels to the Call Manager cluster at the central site. Voice conversations are established and bearer traffic also flows *encrypted* over the VPN tunnels.

The encryption provided by IPSec provides an additional level of security for voice conversations. However, neither the IP Phones, Call Manager Cluster, or voice applications such as voice mail servers are aware, nor need to be aware, that their traffic is being transported over a VPN tunnel and being encrypted during transport. The VPN is transparent to these applications.

Another advantage is that typically the V^{3}PN service provider can offer a Layer-3 IP *pipe* such that both the VPN services and Internet services can exist over the single connection to each location. This reduces recurring connection costs as well as reduces the number of devices required for deployment.

Solution Characteristics

Table 2-1 presents the general solution characteristics for V^{3}PN deployments.

Table 2-1 V^{3}PN Solution Characteristics Summary

Solution Characteristics
Secure Triple Data Encryption Standard (3DES) voice, video, and data traffic can be simultaneously transported over the same IPSec VPN tunnels with QoS enabled for high priority traffic, similar to a private WAN, such as Frame Relay and ATM.
Based on Cisco IOS VPN Routers for resiliency, high availability, and a building block approach to high scalability that can support thousands of branch offices.
Scalability and performance evaluation was performed with IPSEC and GRE tunnels although the performance numbers in this document can also be used as a conservative guideline for IPSec only deployments.
The VPN tunnels can be managed by the enterprise or offered by the service provider as a managed service.
IP Telephony traffic traversing an IPSec VPN is transparent to all users and personnel managing the IP Telephony network.
Standard IP Telephony features, such as SRST and different Codec types, are preserved and still possible over V^{3}PN.
Admission control for IP Telephony is handled the same for VPN tunnels as would be for a Private Frame Relay PVC connecting two branch offices together where admission control is based on the max VoIP traffic permitted across a given IPSec tunnel.
Integrated branch routers providing service provider/Internet connection, VPN tunnel termination, IP Telephony gateway, and Cisco IOS Firewall functionality are possible.

General Best Practices Guidelines

Table 2-2 presents a list of *best practices* that have been established through a combination of design experience, scalability and performance evaluation, and internal Cisco trials.

Table 2-2 V³PN Solution Best Practices Guidelines Summary

Solution Best Practices
Deploy hardware-accelerated Encryption on all platforms that support them. SW-based encryption adds unacceptable latency and jitter that significantly degrade voice quality.
Hub-and-spoke IPSec topology is recommended (partial meshing is also possible).
Maximum of 240 (120 active, 120 backup) IP GRE tunnels per head-end router were evaluated, due to the size of the current testbed. Future tests will evaluate up to 480 branches.
Target maximum CPU utilization on each router not to exceed percent that under test maintained EIGRP adjacency on all IP GRE tunnels during failure testing.
IPSec with GRE tunnels are required if IP Multicast or routing protocols (using IP Multicast) is required.
QoS Pre-Classify must be enabled on VPN devices where applicable to ensure appropriate QoS criteria of the encrypted packet can be applied on the egress WAN interface. See the "QoS Pre-Classify" section on page 4-12 for more information.
G.729 (20 msec sampling at 50 pps) is recommended due to bandwidth consumption after IPSec and GRE overhead are added to the voice packets. See the "Bandwidth Provisioning for WAN Edge QoS" section on page 4-5 for more information.
Select appropriate Cisco IOS VPN Router products per scalability and performance requirements, as well as link speed that will be deployed. See Chapter 5, "Product Selection" for more information.
Branch VPN Routers will typically provide both QoS and VPN tunnel termination on an integrated device, while Head-end VPN Routers will typically have a device providing service provider link termination and QoS that is separate from the VPN tunnel termination device.
Use a Cisco Powered Network service provider designated as an *IP Multi-service VPN* provider to ensure the high priority voice and video traffic can be prioritized across the service provider's network. See the "Service Provider Recommendations" section on page 4-24 for more information.
Enterprises that have tunnels that traverse multiple service providers must ensure that QoS markings (ToS, IP Precedence or DSCP) and prioritization are preserved and honored when crossing SP boundaries.
Seek a service level agreement (SLA) from the service provider that meets the enterprise organization's needs in terms of end-to-end delay, jitter and dropped packets. This is analogous to an SLA an enterprise would arrange with a private WAN provider offering Frame Relay or ATM service.

General Solution Caveats

Table 2-3 presents a list of caveats for the solution.

]

Table 2-3 V³PN Solution Implementation Caveats

Solution Caveats
Compressed RTP (cRTP) and IPSec are incompatible standards. The RTP header is already encrypted when the packet reaches the cRTP engine and therefore cannot be compressed. Industry standardization bodies are currently considering alternative bandwidth optimization techniques for encrypted tunnels.
In Cisco IOS software releases prior to 12.2(13)T, the IPSec Crypto Engine has a FIFO entrance queue. In Cisco IOS software release 12.2(13)T and higher, an LLQ for the IPSec Crypto Engine is supported. See the "Crypto Engine QoS" section on page 4-20 for more information.
The majority of voice traffic was simulated RTP streams using the NetIQ Chariot test tool, however a real CallManager and IP phones were configured and used for verification.
SRST was implicitly verified, but no performance and scalability evaluation was performed. SRST is supported in Cisco 12.2(7)T on the Cisco 2600 and Cisco 3600 platforms, and on the Cisco 175x series routers in Cisco IOS 12.2(4)XW.
QoS Pre-Classify is supported in 12.2(4)YB on the 1700 series. This is a Business Unit (BU) *special* Cisco IOS software release. All other branch platforms evaluated were running T-train Cisco IOS software.
Multilink PPP was found to have limitations, causing some platforms to drop into process switching and thereby reducing performance. These limitations are being addressed in a future Cisco IOS software release. Frame Relay and HDLC were verified, others such as ATM were not.
At the central site, QoS can be configured on either the VPN head-end devices or on a separate service provider/Internet link terminating device. While both configurations are supported, it is recommended to have separate devices at the central site for scalability.
On branch products (Cisco 2600, Cisco 3600, and Cisco 3700 VPN routers), voice cards and VPN hardware-acceleration cards (AIM) are not supported in 12.2(8)T when installed in the same router. This capability is supported in 12.2(11)T.
The Cisco 806 VPN Router does not support SRST, QoS Pre-Classify, or hardware-accelerated encryption.
The Cisco 806 VPN Router had performance limitations with latency and jitter. It is not a recommended platform for V³PN.