CISCO SYSTEMS

QoS DESIGN FOR IPsec VPNs

AT–A–GLANCE

IPsec VPNs achieve network segregation and privacy via encryption. IPsec VPNs are built by overlaying a point-to-point mesh over the Internet using Layer 3-encrypted tunnels. Encryption/decryption is performed at these tunnel endpoints, and the protected traffic is carried across the shared network.

Three main QoS considerations specific to IPsec VPNs are:

1) Additional bandwidth required by IPsec encryption and authentication

2) Marginal time element required at each point where encryption/decryption takes place

3) Anti-Replay interactions

1) IPsec BANDWIDTH OVERHEAD

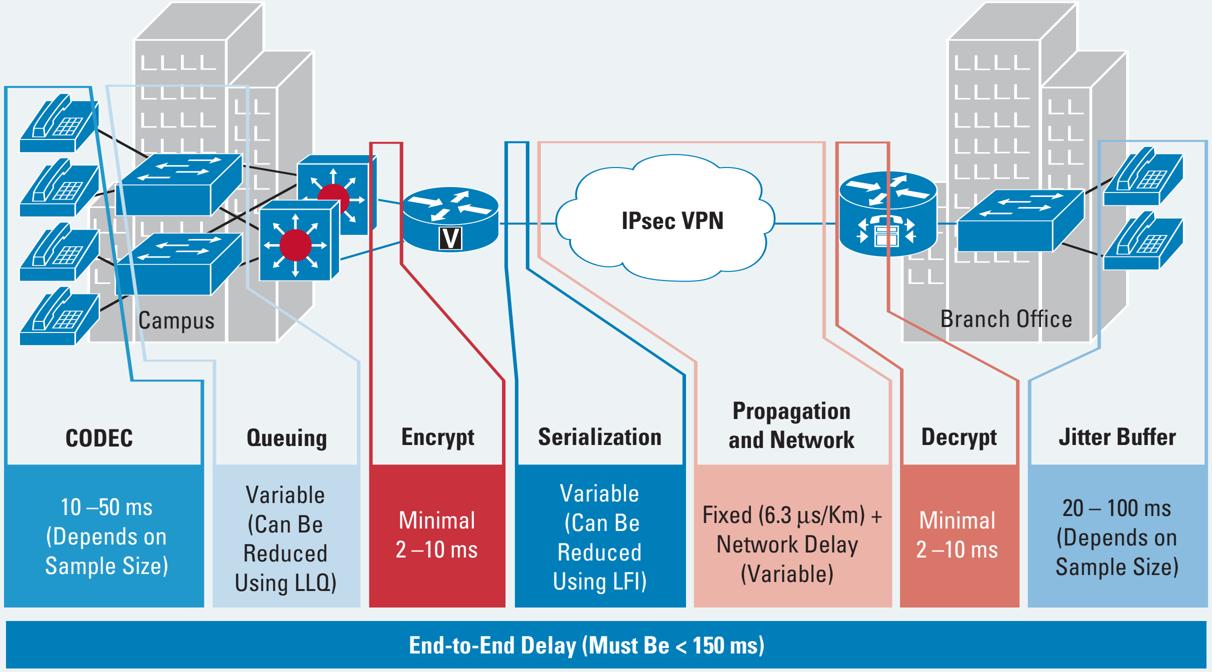
The additional bandwidth required to encrypt and authenticate a packet needs to be factored into account when provisioning QoS policies.

This is especially important for Voice over IP (VoIP), where IPsec could more than double the size of a G.729 voice packet, as shown below.

The Layer 3 data rate for a G.729 call (at 50 pps) is 24 kbps (60 Bytes * 8 bits * 50 pps). IP GRE tunnel overhead adds 24 bytes per packet. IPsec ESP adds another 52 bytes. The combined additional overhead increases the rate from 24 kbps (clear voice) to just less than 56 kbps (IPsec ESP tunnelmode encrypted voice).

2) ENCRYPTION/DECRYPTION DELAYS

A marginal time element for encryption and decryption should be factored into the end-to-end delay budget for realtime applications, such as VoIP. Typically these processes require 2–10 ms per hop, but may be doubled in the case of spoke-to-spoke VoIP calls that are homed through a central VPN headend hub.



CODEC	Queuing	Encrypt	Serialization	Propagation and Network	Decrypt	Jitter Buffer
10 –50 ms (Depends on Sample Size)	Variable (Can Be Reduced Using LLQ)	Minimal 2 –10 ms	Variable (Can Be Reduced Using LFI)	Fixed (6.3 µs/Km) + Network Delay (Variable)	Minimal 2 –10 ms	20 – 100 ms (Depends on Sample Size)

End-to-End Delay (Must Be < 150 ms)

G.729 VoIP 60 Bytes →

IP Hdr	UDP Hdr	RTP Hdr	Voice

IPsec Hdr	ESP Hdr	ESP IV	GRE IP Hdr	GRE	IP Hdr	UDP Hdr	RTP Hdr	Voice	ESP Pad/NH	ESP Auth
20	8	8	20	4	20	8	12	20	2-257	12

IPsec ESP Tunnel Mode G.729 VoIP - 136 Bytes

3) ANTI-REPLAY INTERACTIONS

Anti-Relay is a standards-defined mechanism to protect IPsec VPNs from hackers. If packets arrive outside of a 64-byte window, then they are considered hacked and are dropped prior to decryption. QoS queuing policies may re-order packets such that they fall outside of the Anti-Replay window. Therefore, IPsec VPN QoS policies need to be properly tuned to minimize Anti-Replay drops.