Tunnel-less VPN with Cisco Group Encrypted Transport (GET)

December 2006

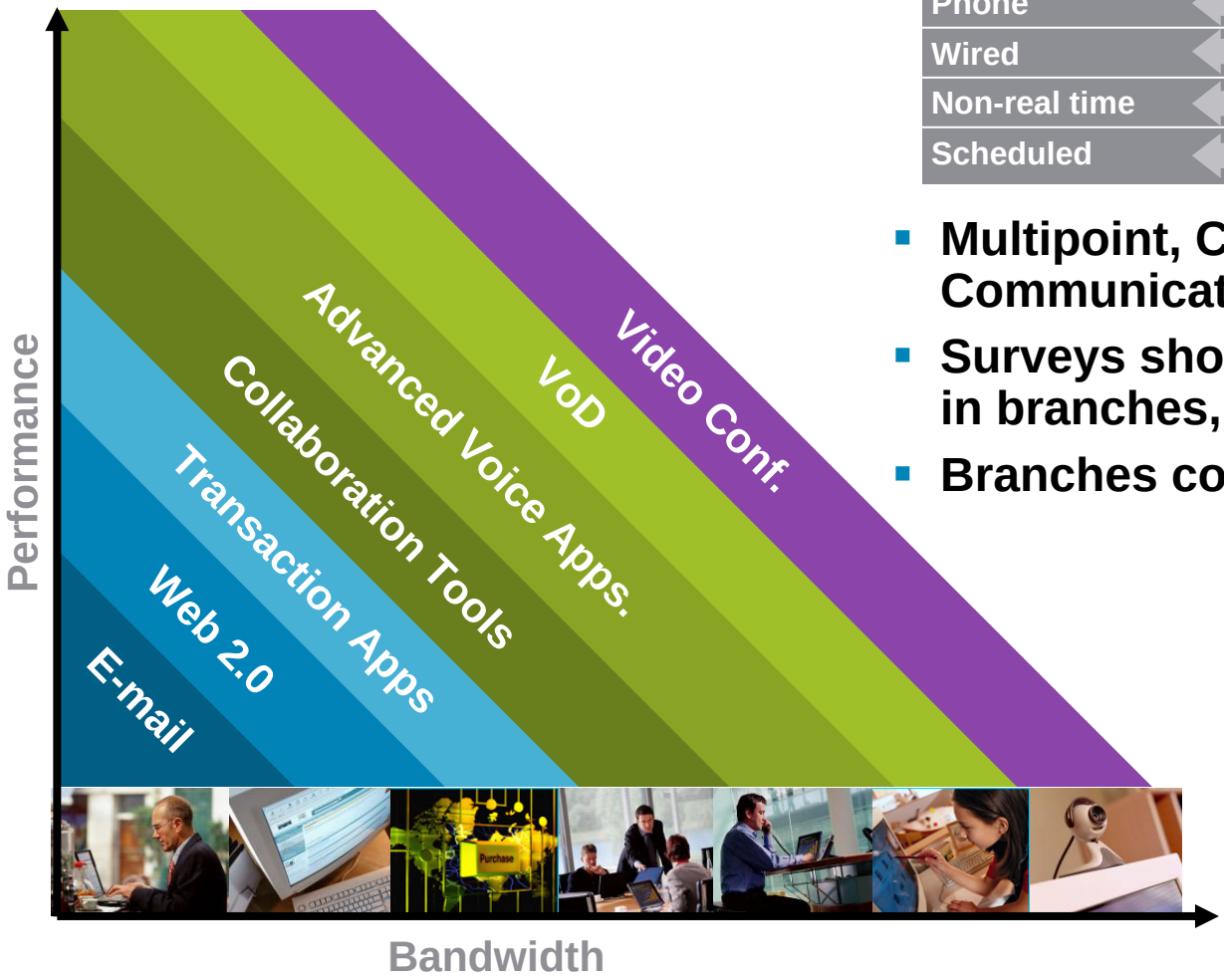
Agenda

- Trends in Enterprise Branch Communications
- Need for Tunnel-less VPNs
- Announcing Group Encrypted Transport (GET) VPN
- How Group Encrypted Transport (GET) VPN works
- Cisco GET VPN Use Cases

New Business Realities
Empowered Branch

Technology Innovation

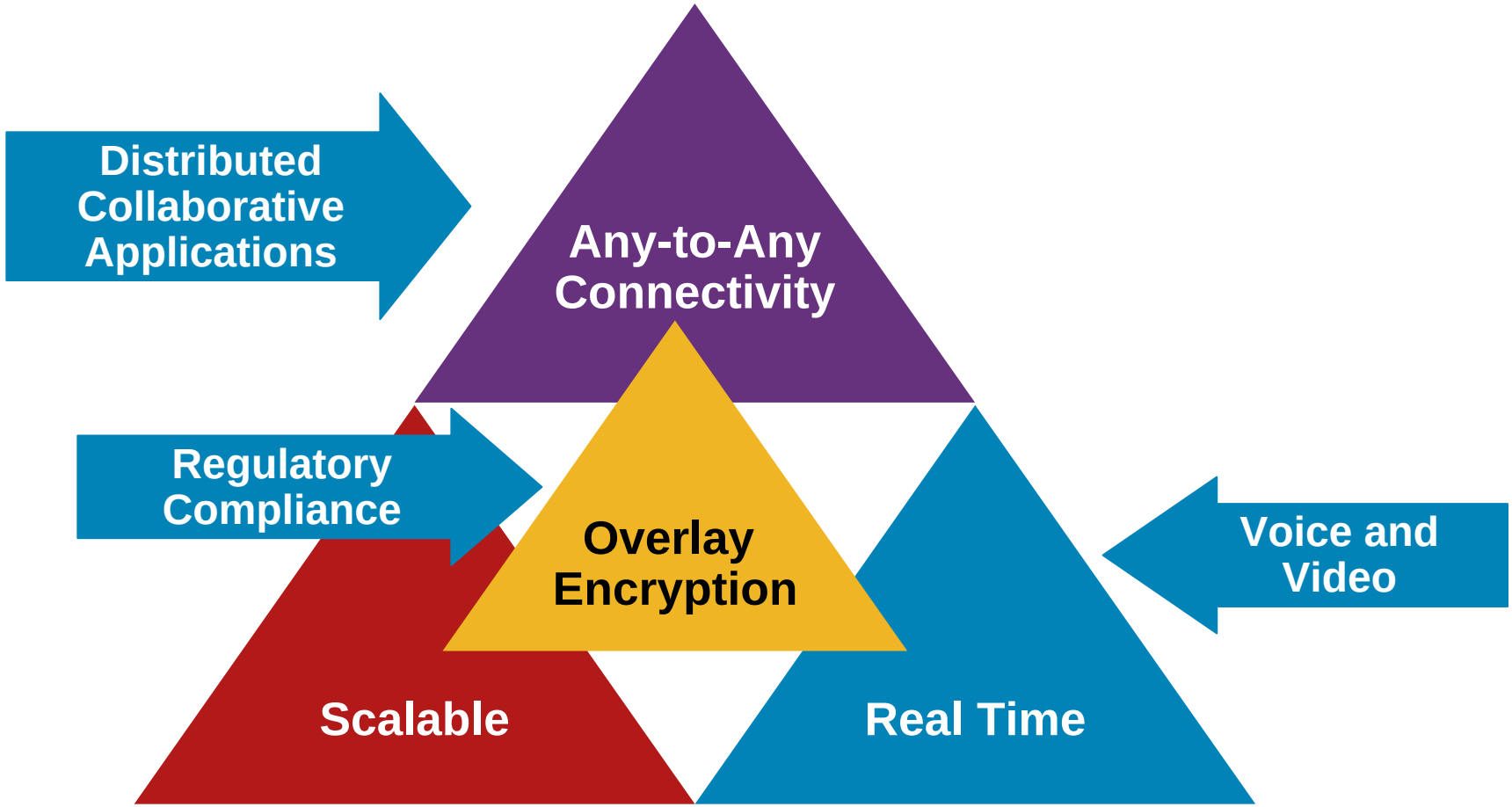
Point-to-point	Multipoint
Voice-only	Rich-media
Phone	PC/PDA
Wired	Wireless
Non-real time	Real time
Scheduled	Ad hoc



- **Multipoint, Collaborative Branch Communications**
- **Surveys show >35% of all employees are in branches, and growing**
- **Branches consume 70-90% of resources**

Most employees can NOT take full advantage of these today, unless network infrastructure keeps up

The Business Challenge:
Resolving Collaboration-Security Trade-offs

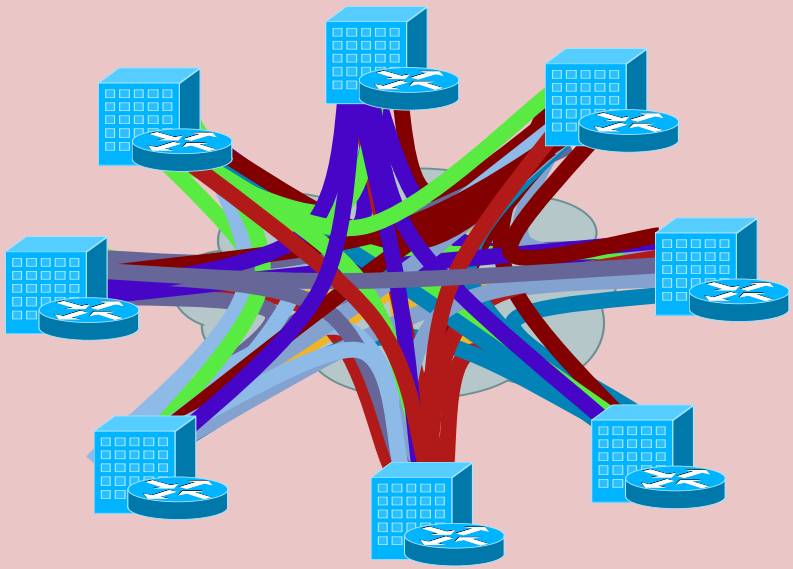


Today's enterprise WAN technologies force a trade-off between collaborative branch applications and security

Tunnel-less VPN - A New Security Model

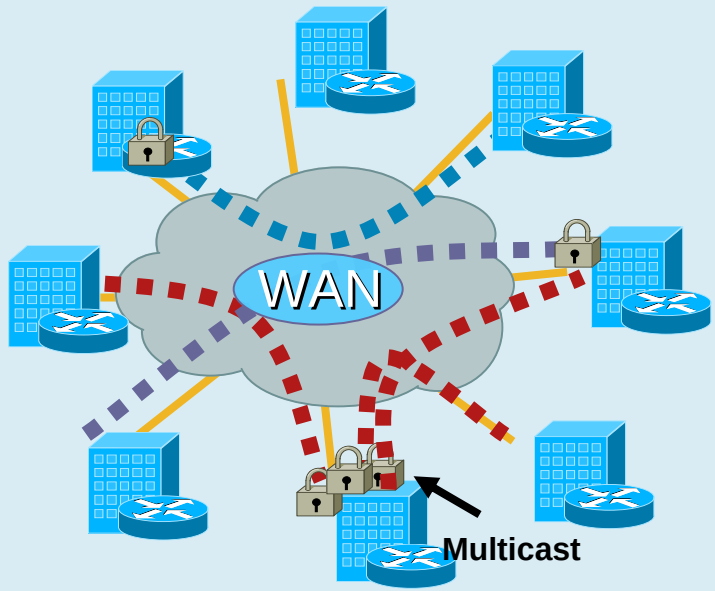
Any-to-Any encryption

IPsec Point-to-Point Tunnels



- Scalability—an issue (N^2 problem)
- Any-to-any instant connectivity can't be done to scale
- Overlay routing
- Limited advanced QoS
- Multicast replication inefficient

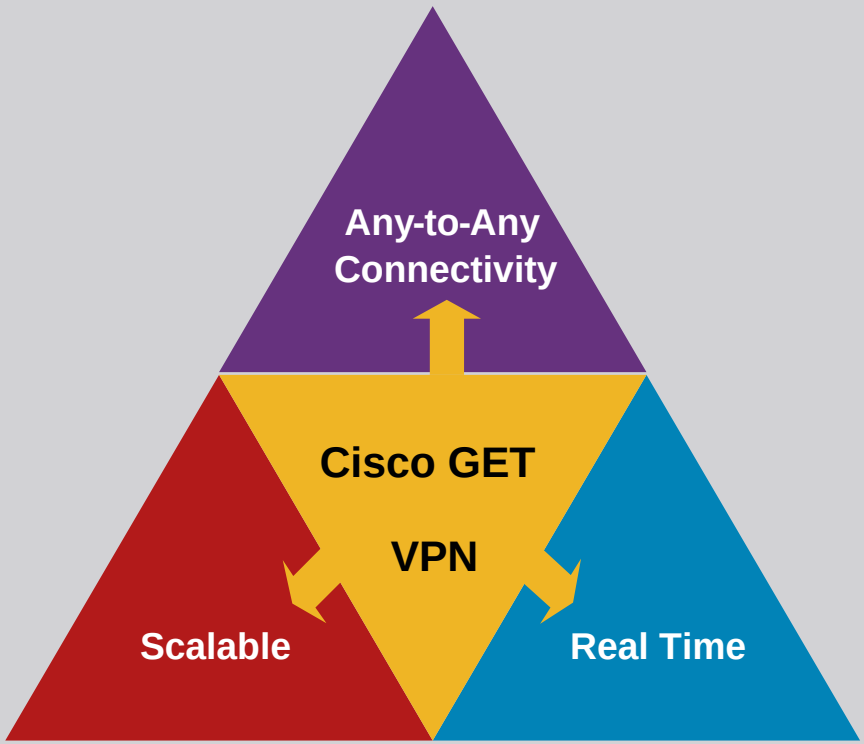
Tunnel-less VPN



- Scalable architecture
- Any-to-any instant connectivity to high-scale
- No overlays – native routing
- Advanced QoS
- Efficient Multicast replication

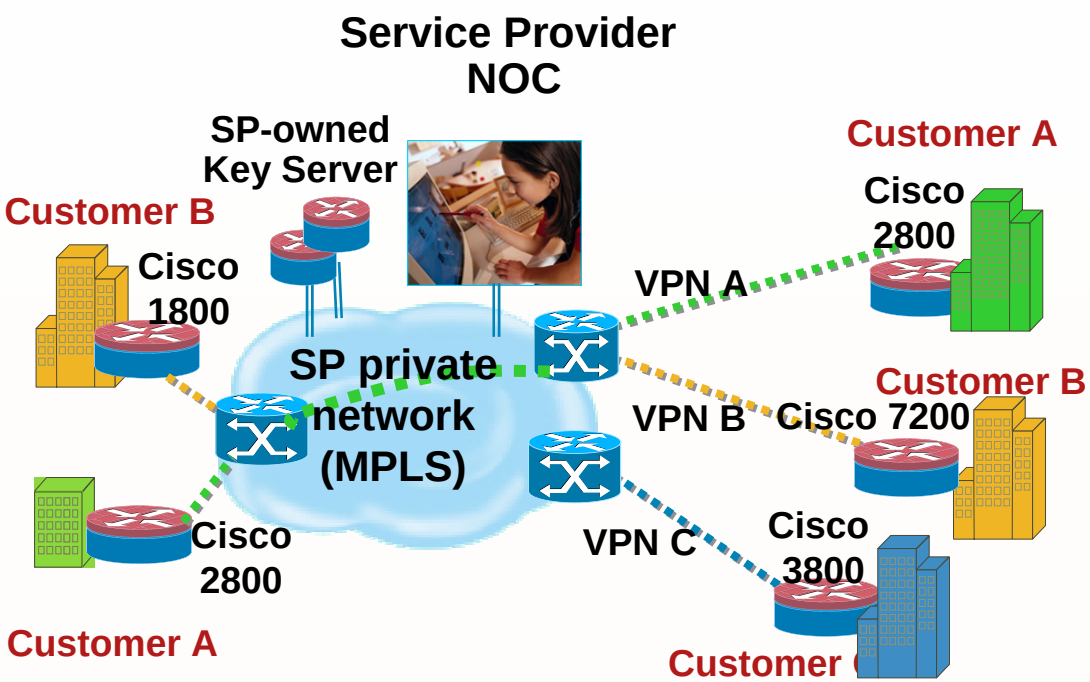
Announcing Cisco Group Encrypted Transport (GET) VPN – Solution for Tunnel-less VPNs

Cisco GET VPN delivers a revolutionary solution for tunnel-less, any-to-any branch confidential communications



- Large-scale any-to-any encrypted communications
- Native routing without tunnel overlay
- Optimal for QoS and Multicast support - improves application performance
- Transport agnostic - private LAN/WAN, FR/AATM, IP, MPLS
- Offers flexible span of control among subscribers and providers
- Available on Cisco Integrated Services Routers; Cisco 7200 and Cisco 7301 with Cisco IOS 12.4(11)T

Managed Tunnel-less VPN Services



- **Encrypted traffic is demand-driven**
- **ISR can have "VRF-aware contexts"**
- **Centrally managed key servers enable Group encryption**

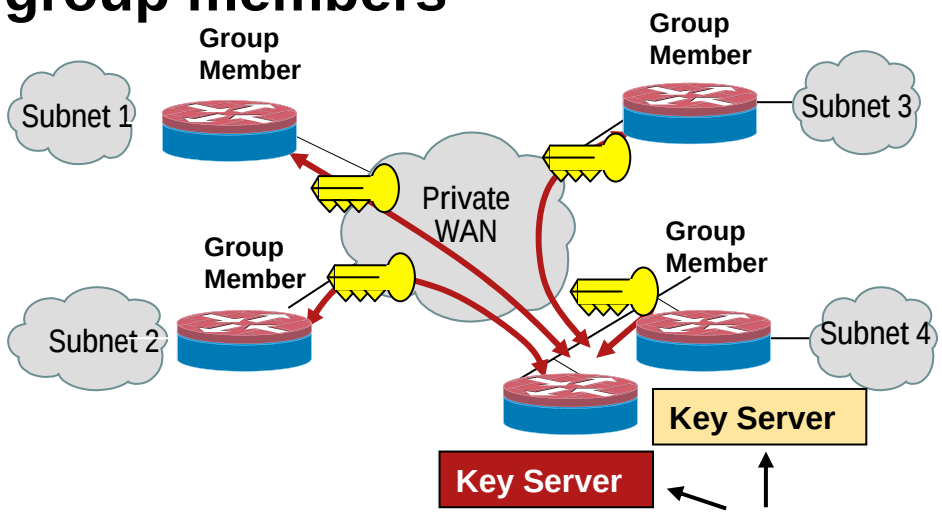
- Service integration delivers greater value, stronger branding
- Increased security
  - Helps businesses comply with regulations viz. HIPAA, PCI
- Operational simplicity
  - Centralized key-server reduces complexity
  - Easy service rollout
- Optimized network utilization
- Service innovation, unique offering
- Services Upsell

How Cisco GET VPN Works

GET simplifies security policy and key distribution by using Group Domain of Interpretation (GDOI)

- GDOI:
  - A key distribution mechanism
  - Group Key Model
  - Standards-based (RFC 3547)
- GET uses GDOI and adds:
  - Cooperative Key Servers for high availability & geographic distribution
  - Secure Unicast/Multicast control/data plane via encryption
  - Unicast/Multicast key distribution

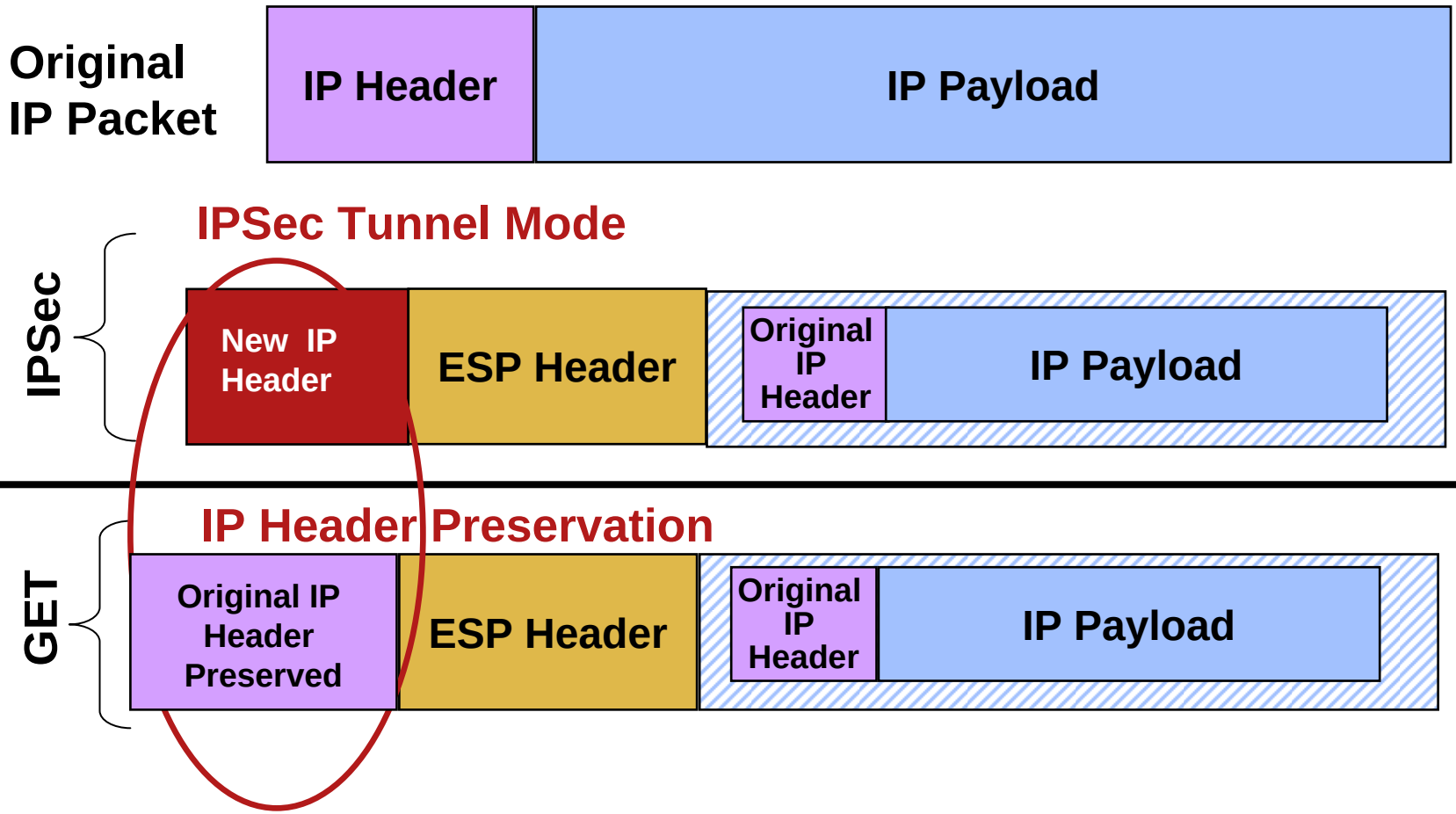
Key Server: Authenticates group members, distributes keys and policies; group member provisioning is minimized. Application traffic is encrypted by group members



GET adds cooperative Key Servers for high availability

How GET VPN Prevents Overlay Routing

Cisco GET VPN uses IP header preservation to mitigate routing overlay and to preserve QoS and multicast capabilities

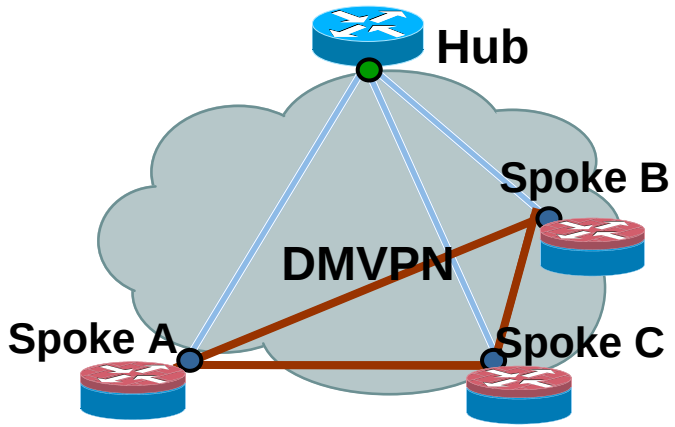


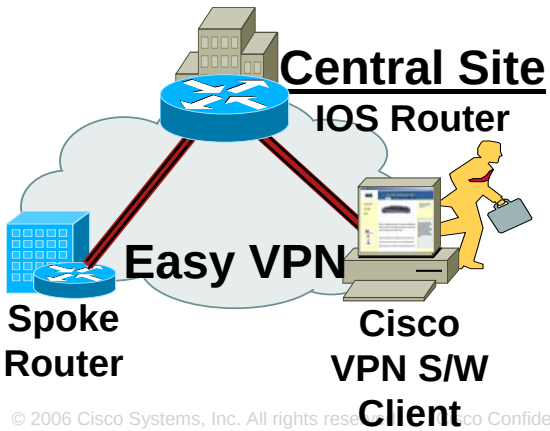
Cisco IOS VPN Solution Evolution

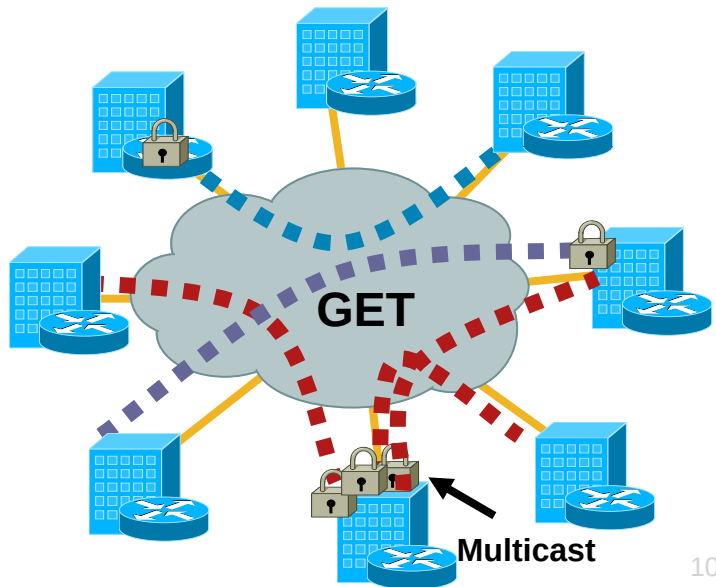
Innovations in Confidential Communications

Cisco Advanced Site-to-Site VPNs

1. **Hub-and-Spoke VPNs**
   - IPSec+GRE: (Static Tunnels with Routing)
   - Easy VPN (Dynamic Policy/Config Push)
   - DMVPN (Zero Touch with Dynamic Routing)
2. **Dynamic Spoke-to-Spoke VPNs**
   - DMVPN (On-Demand Partial-Mesh)
3. **Tunnel-Less Any-to-Any VPNs**
   - Group Encrypted Transport (GET) VPN







Cisco GET VPN Use Cases

Key Use Case	Customer	Features
Encryption of IP packets sent over Satellite Links	Organizations who wish to secure video communications through use of BB satellite	Hardware Acceleration support Native Multicast Encryption
Reduce delays in Spoke-Spoke DMVPN network	DMVPN Enterprise customers who are deploying voice and wish to reduce the delays in setting up voice calls between spokes	GDOI with DMVPN Instant spoke-spoke connectivity
Control Plane Updates protection	Enterprise financial customers who wish to secure PIM/IGP/BGP to control traffic in their network	IGP/BGP/PIM control packets encryption

Example Customer #1 —Manufacturing

Technology Manufacturer

- More branch offices in other countries than in the United States
- Currently implementing VoIP
- QoS issues in dealing with International carriers are forcing a move to Multiprotocol Label Switching (MPLS)
- Concerned about security:

  Compliance: Company is compliant with MPLS today, but wants to stay ahead of the auditors without having to redeploy equipment at branch locations

  Concern about provisioning errors: confidential data can be leaked

  Management: Not encrypting WAN links today because of trade-off between QoS and security on MPLS—“a nightmare”

Example Customer #2—Banking

Large, National U.S. Bank with MPLS Network

Concerned about security:

- Compliance: Need to comply with SOX, payment card industry (PCI) regulations—if more than one carrier is used for MPLS, bank must encrypt
- Concern for provisioning errors: Confidential customer data can be leaked; in that case, customers would have to be notified, and fines would be levied
- Management: Not encrypting WAN links today because of management complexity

Example Customer #3—Retail

Large U.S. retailer has MPLS Network with plans for Unified Communications, Call Center

Concerned about security:

- Compliance: Payment card industry (PCI) regulations—states that if more than one carrier is used for MPLS, retailer must encrypt
- Concern for provisioning errors: Confidential customer data can be leaked; in that case, customers would have to be notified, and fines would be levied
- Management: Not encrypting WAN links today because of trade-off between QoS and security on MPLS

Cisco GET VPN Ordering Guide

Router Platforms	SKUs
Cisco 870, 1800, 2800, 3700 and 3800 Series Routers Cisco 7301 and 7200 Series Routers	All Security Bundles with 12.4(11)T or later
Cisco 870, 1800, 2800, 3700 and 3800 Series Routers Cisco 7301 and 7200 Series Routers	Non Security SKUs upgraded with Cisco IOS Advanced Security or higher image

Summary

- Enterprise WAN technologies previously forced a trade-off between QoS-enabled branch interconnectivity and security
- Cisco introduces Group Encrypted Transport (GET) VPN, a next-generation WAN security technology:
  - Easy-to-manage, high-scale, any-to-any encrypted communications
  - Secured packets use existing WAN-agnostic routing infrastructure without tunnels
  - Networkwide QoS and Multicast capabilities preserved; improves application performance
  - Offers flexible span of control among subscribers and providers
- GET VPN's group-key mechanism simplifies key management and reduces latency, improving any-to-any connectivity capabilities
- IP header preservation prevents overlay routing