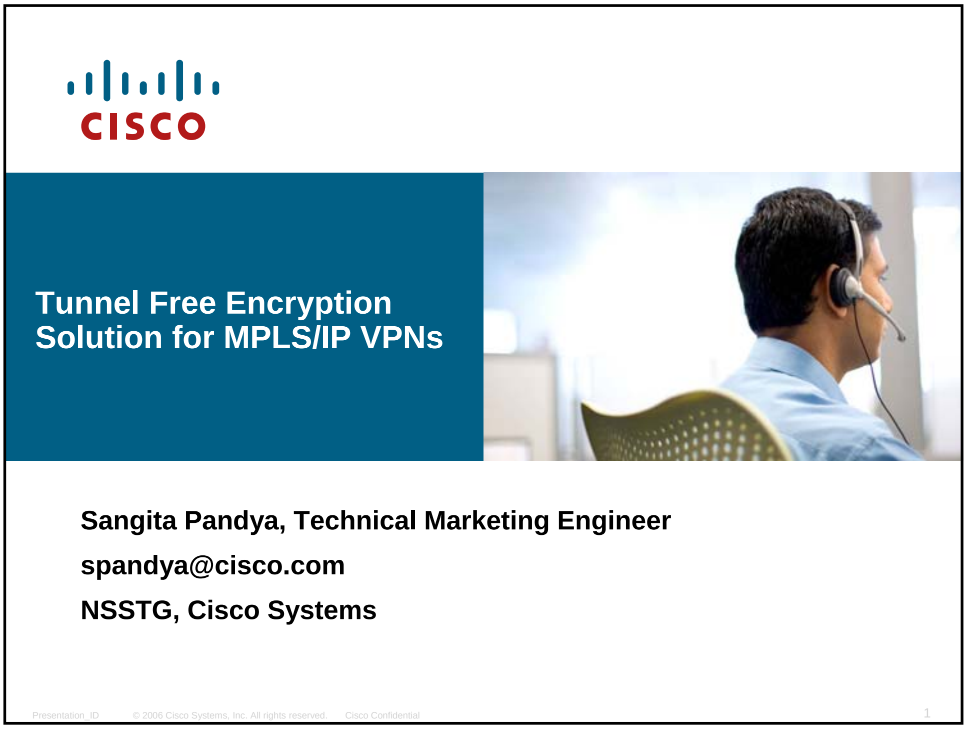
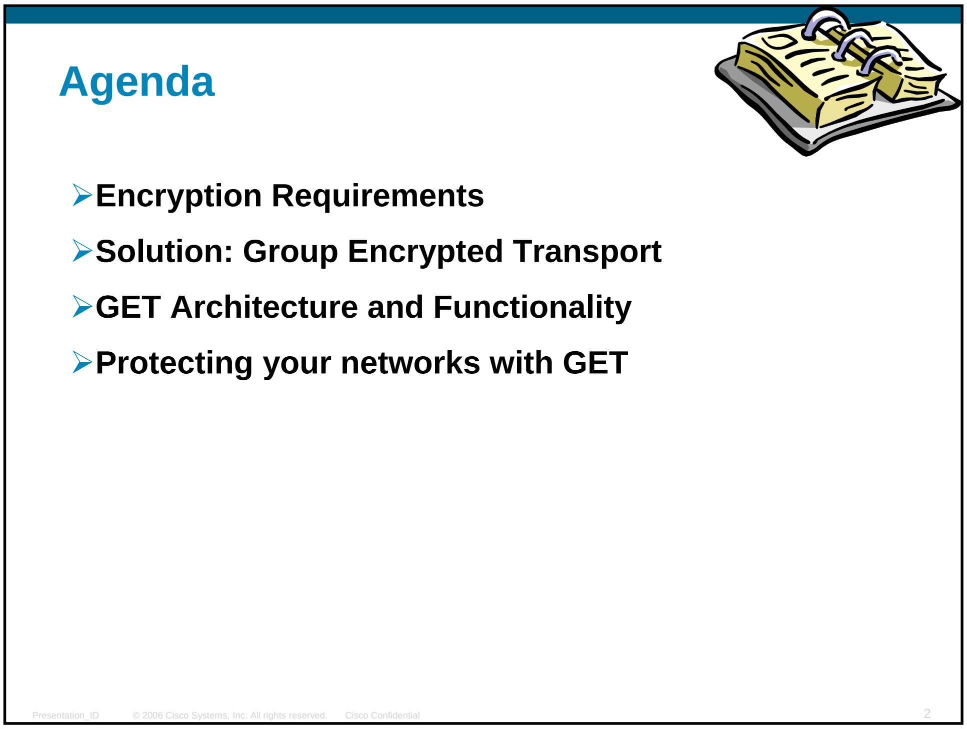


Tunnel Free Encryption Solution for MPLS/IP VPNs

Sangita Pandya, Technical Marketing Engineer

spandya@cisco.com

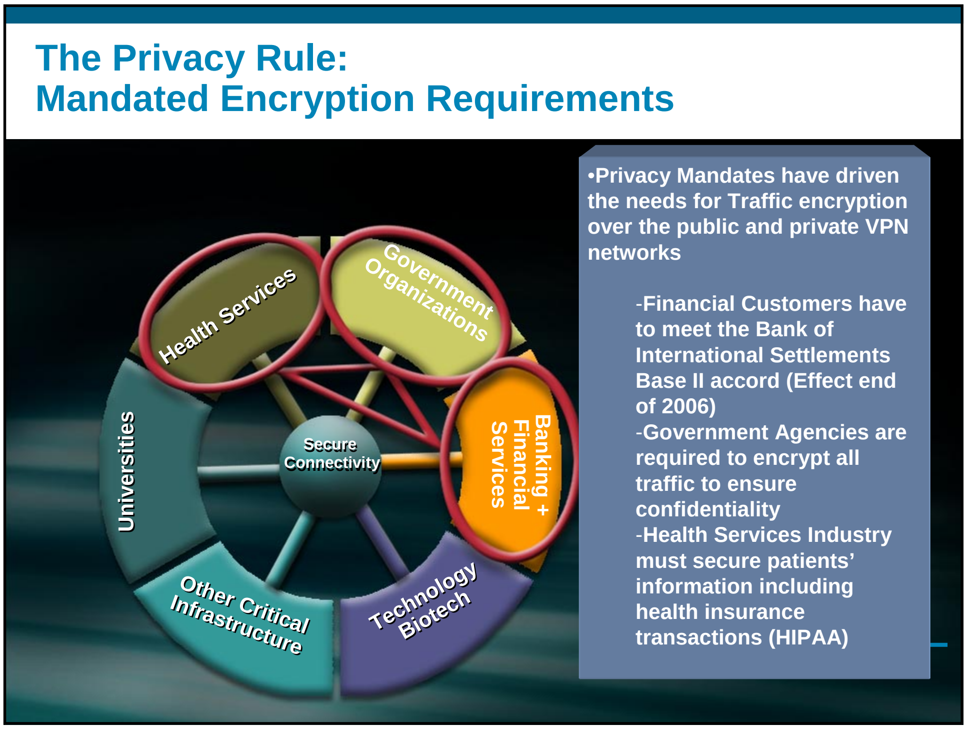
NSSTG, Cisco Systems



Agenda

- ➢Encryption Requirements
- ➢Solution: Group Encrypted Transport
- ➢GET Architecture and Functionality
- ➢Protecting your networks with GET

Encryption Requirements



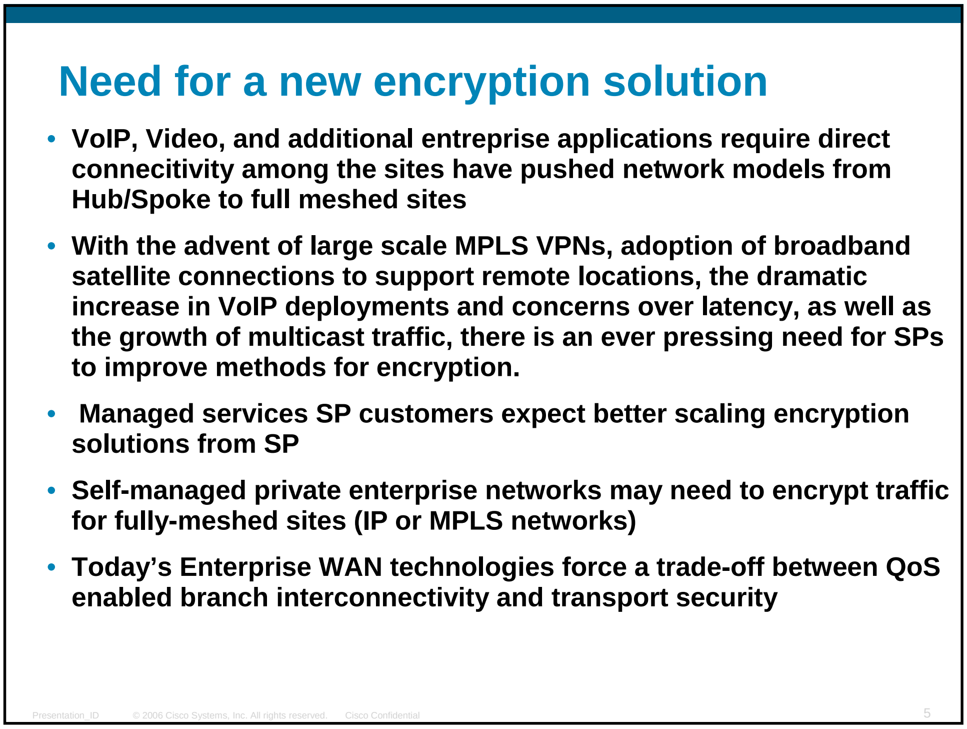
The Privacy Rule: Mandated Encryption Requirements

- Privacy Mandates have driven the needs for Traffic encryption over the public and private VPN networks

  -Financial Customers have to meet the Bank of International Settlements Base II accord (Effect end of 2006)

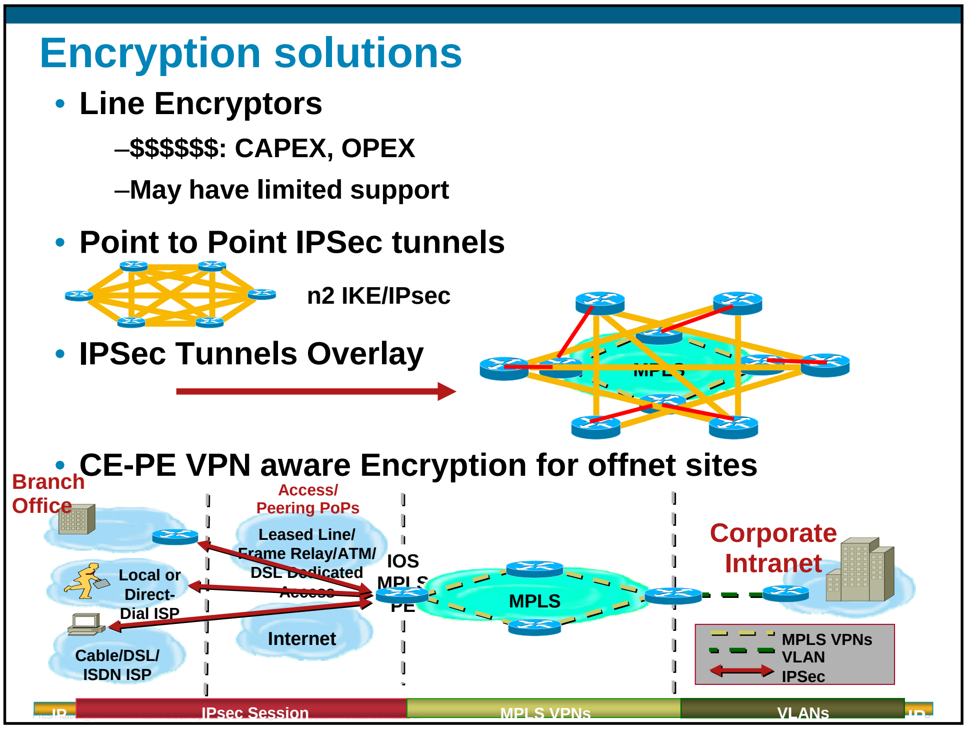
  -Government Agencies are required to encrypt all traffic to ensure confidentiality

  -Health Services Industry must secure patients' information including health insurance transactions (HIPAA)



Need for a new encryption solution

- VoIP, Video, and additional entreprise applications require direct connecitivity among the sites have pushed network models from Hub/Spoke to full meshed sites
- With the advent of large scale MPLS VPNs, adoption of broadband satellite connections to support remote locations, the dramatic increase in VoIP deployments and concerns over latency, as well as the growth of multicast traffic, there is an ever pressing need for SPs to improve methods for encryption.
- Managed services SP customers expect better scaling encryption solutions from SP
- Self-managed private enterprise networks may need to encrypt traffic for fully-meshed sites (IP or MPLS networks)
- Today's Enterprise WAN technologies force a trade-off between QoS enabled branch interconnectivity and transport security



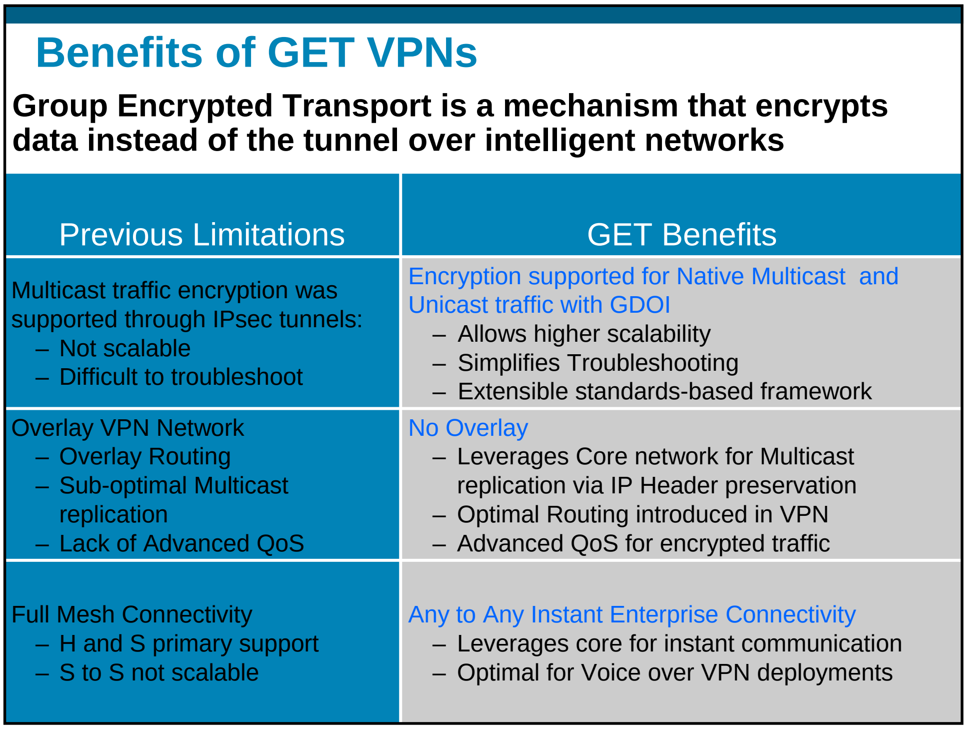
Encryption solutions

- Line Encryptors
  - –$$$$$$: CAPEX, OPEX
  - –May have limited support
- Point to Point IPSec tunnels

n2 IKE/IPsec

- IPSec Tunnels Overlay
- CE-PE VPN aware Encryption for offnet sites

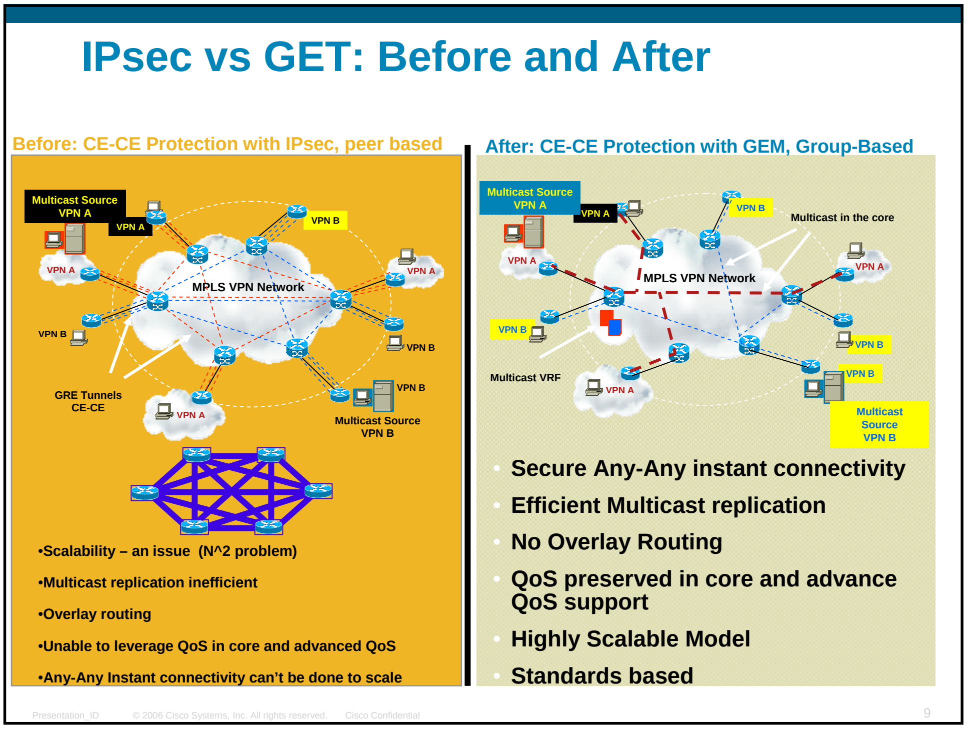
GET: Group Encrypted Transport



Benefits of GET VPNs

Group Encrypted Transport is a mechanism that encrypts data instead of the tunnel over intelligent networks

Previous Limitations	GET Benefits
Multicast traffic encryption was supported through IPsec tunnels: – Not scalable – Difficult to troubleshoot	Encryption supported for Native Multicast and Unicast traffic with GDOI – Allows higher scalability – Simplifies Troubleshooting – Extensible standards-based framework
Overlay VPN Network – Overlay Routing – Sub-optimal Multicast replication – Lack of Advanced QoS	No Overlay – Leverages Core network for Multicast replication via IP Header preservation – Optimal Routing introduced in VPN – Advanced QoS for encrypted traffic
Full Mesh Connectivity – H and S primary support – S to S not scalable	Any to Any Instant Enterprise Connectivity – Leverages core for instant communication – Optimal for Voice over VPN deployments



IPsec vs GET: Before and After

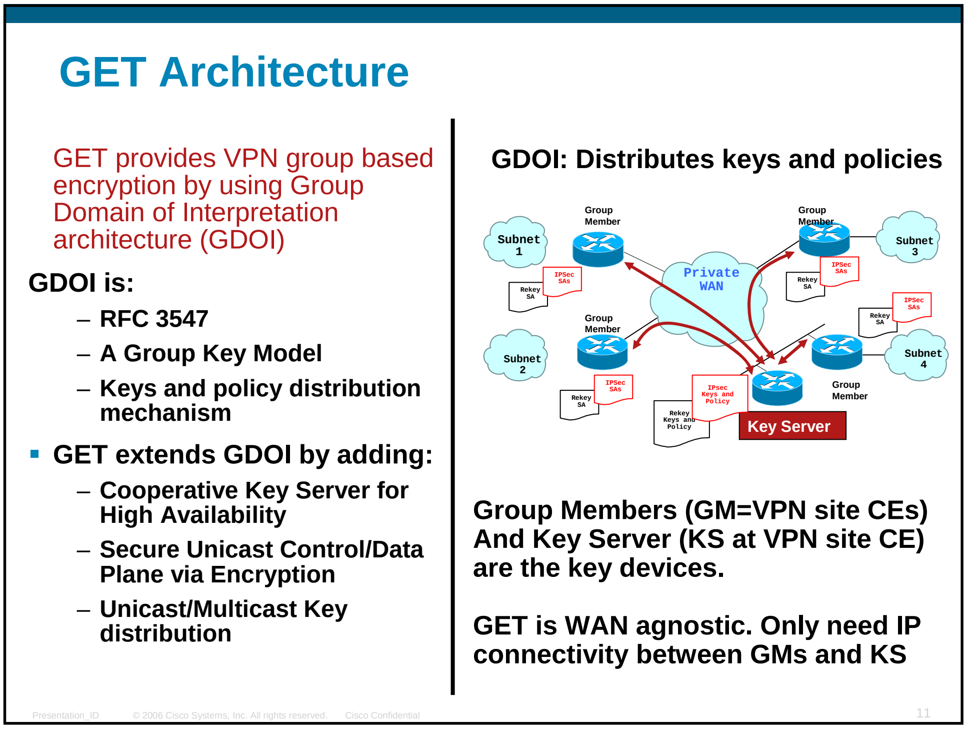
Before: CE-CE Protection with IPsec, peer based

- Scalability – an issue (N^2 problem)
- Multicast replication inefficient
- Overlay routing
- Unable to leverage QoS in core and advanced QoS
- Any-Any Instant connectivity can't be done to scale

After: CE-CE Protection with GEM, Group-Based

- Secure Any-Any instant connectivity
- Efficient Multicast replication
- No Overlay Routing
- QoS preserved in core and advance QoS support
- Highly Scalable Model
- Standards based

GET Architecture & Functionality



GET Architecture

GET provides VPN group based encryption by using Group Domain of Interpretation architecture (GDOI)

GDOI is:

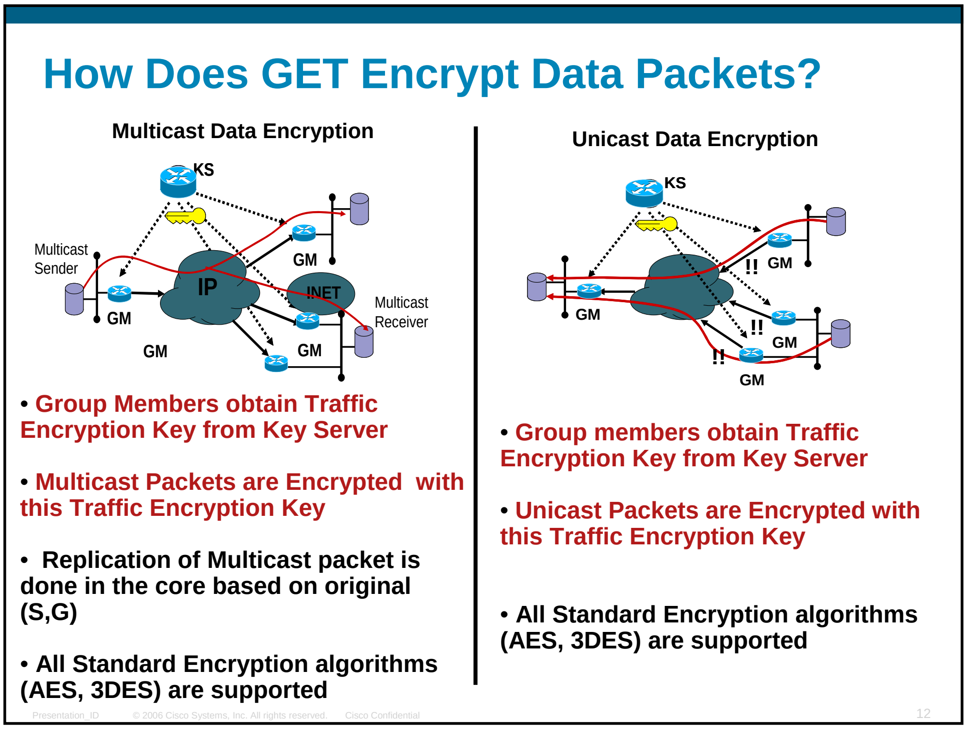
- RFC 3547
- A Group Key Model
- Keys and policy distribution mechanism

- GET extends GDOI by adding:
  - Cooperative Key Server for High Availability
  - Secure Unicast Control/Data Plane via Encryption
  - Unicast/Multicast Key distribution

GDOI: Distributes keys and policies

Group Members (GM=VPN site CEs) And Key Server (KS at VPN site CE) are the key devices.

GET is WAN agnostic. Only need IP connectivity between GMs and KS



How Does GET Encrypt Data Packets?

Multicast Data Encryption

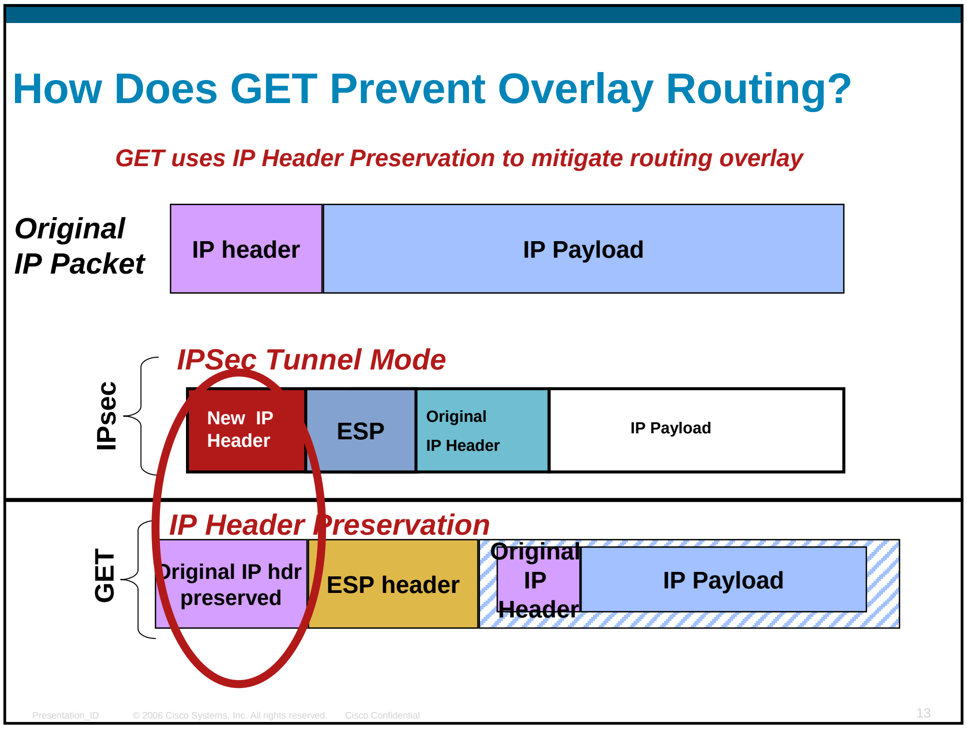
KS
Multicast Sender
GM
IP
GM
INET
Multicast Receiver
GM
GM

- Group Members obtain Traffic Encryption Key from Key Server
- Multicast Packets are Encrypted with this Traffic Encryption Key
- Replication of Multicast packet is done in the core based on original (S,G)
- All Standard Encryption algorithms (AES, 3DES) are supported

Unicast Data Encryption

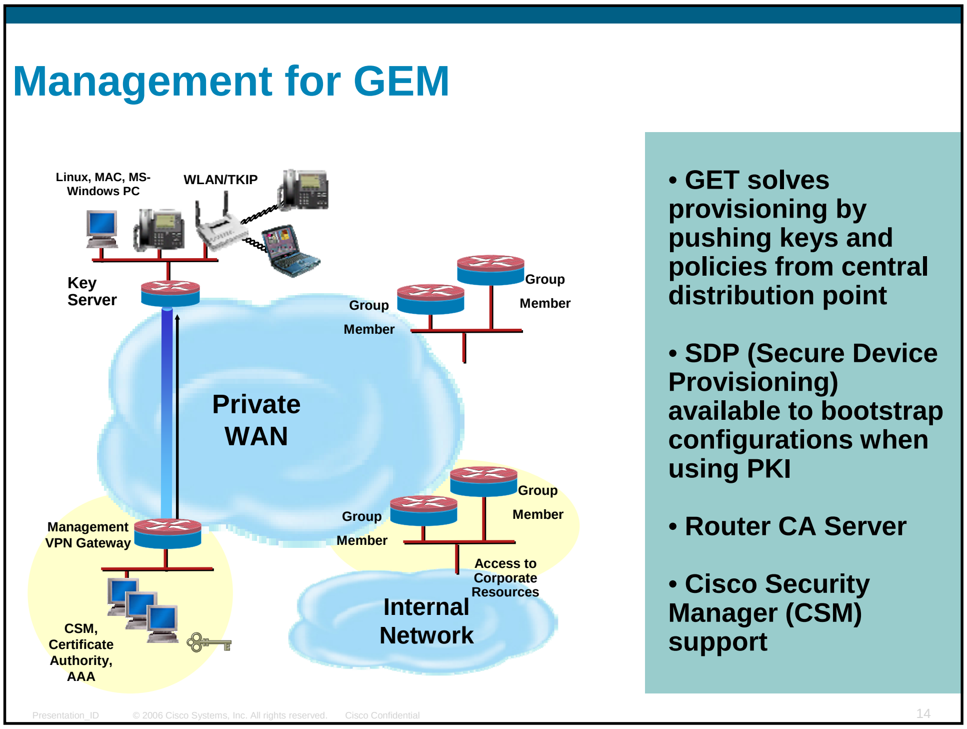
KS
!! GM
GM
!!
GM
!!
GM

- Group members obtain Traffic Encryption Key from Key Server
- Unicast Packets are Encrypted with this Traffic Encryption Key
- All Standard Encryption algorithms (AES, 3DES) are supported



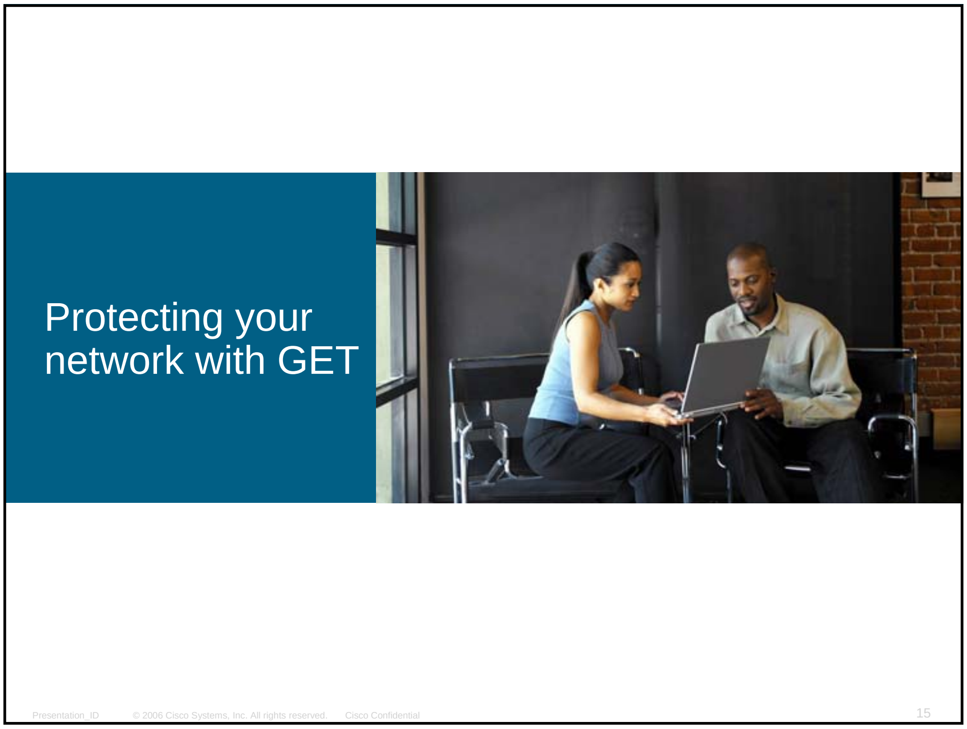
How Does GET Prevent Overlay Routing?

GET uses IP Header Preservation to mitigate routing overlay

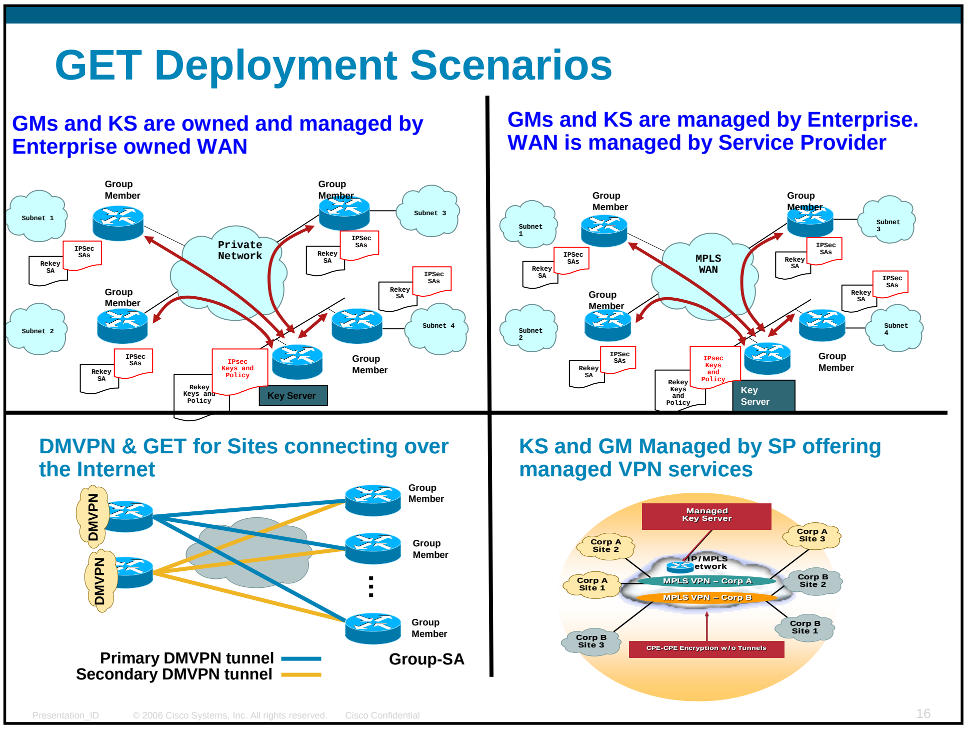


Management for GEM

- GET solves provisioning by pushing keys and policies from central distribution point
- SDP (Secure Device Provisioning) available to bootstrap configurations when using PKI
- Router CA Server
- Cisco Security Manager (CSM) support



Protecting your network with GET



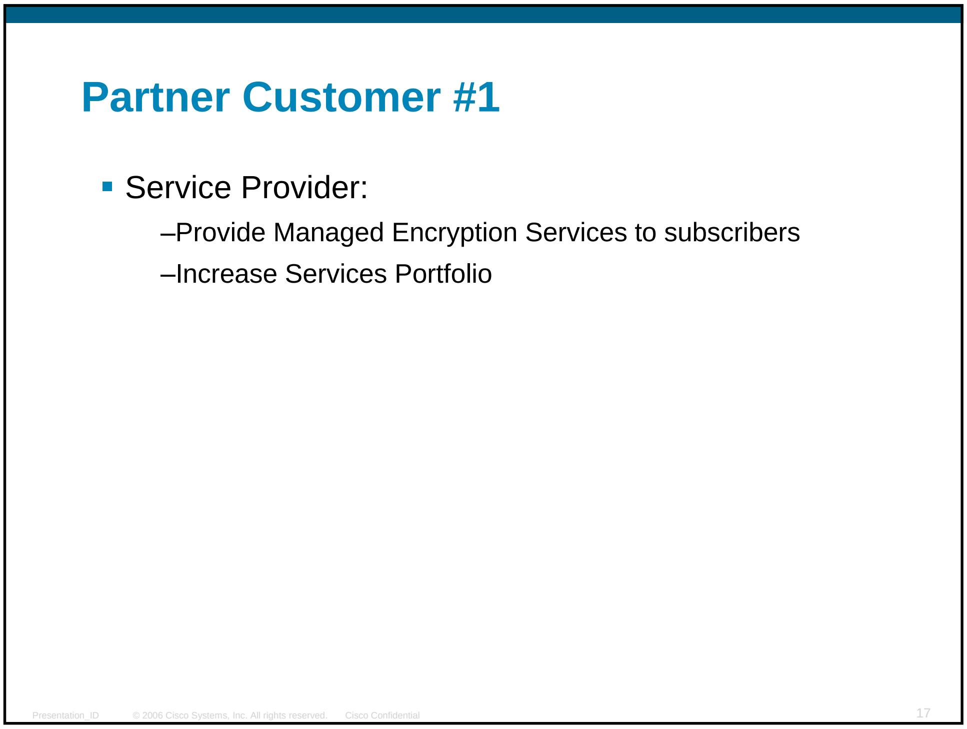
GET Deployment Scenarios

GMs and KS are owned and managed by Enterprise owned WAN

GMs and KS are managed by Enterprise. WAN is managed by Service Provider

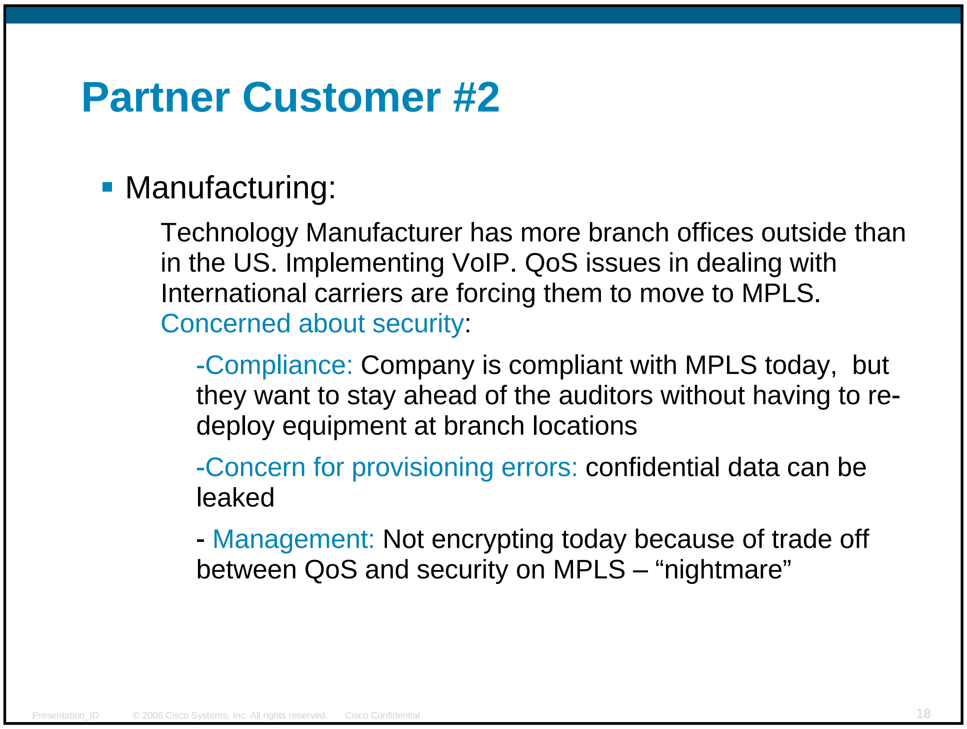
DMVPN & GET for Sites connecting over the Internet

KS and GM Managed by SP offering managed VPN services



Partner Customer #1

- Service Provider:
  - –Provide Managed Encryption Services to subscribers
  - –Increase Services Portfolio



Partner Customer #2

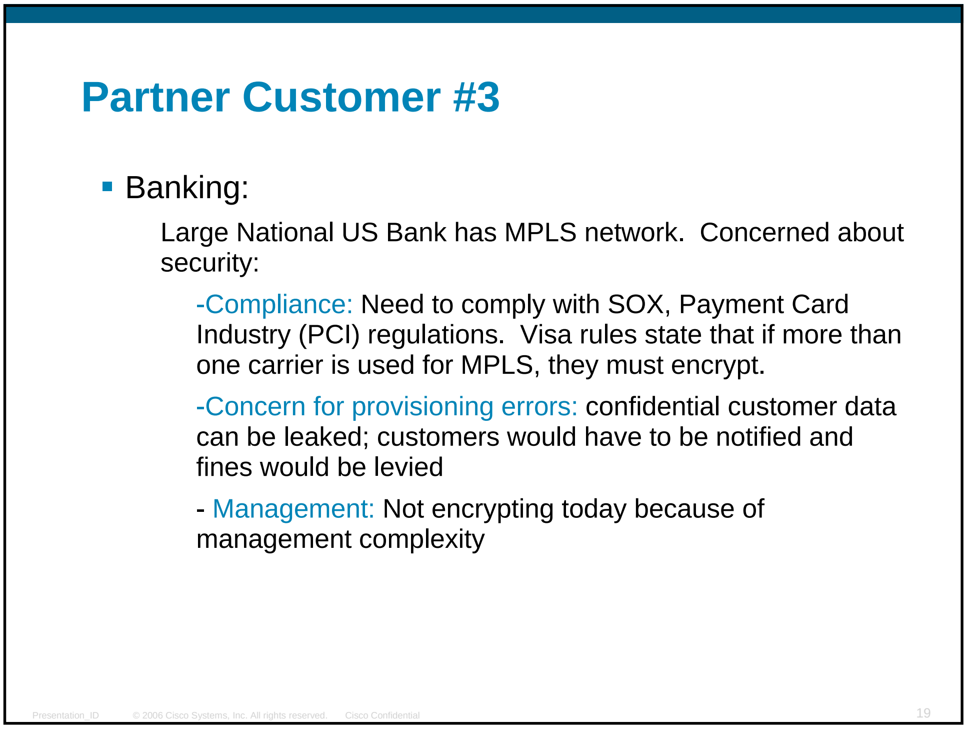
- Manufacturing:

  Technology Manufacturer has more branch offices outside than in the US. Implementing VoIP. QoS issues in dealing with International carriers are forcing them to move to MPLS. Concerned about security:

  -Compliance: Company is compliant with MPLS today, but they want to stay ahead of the auditors without having to re-deploy equipment at branch locations

  -Concern for provisioning errors: confidential data can be leaked

  - Management: Not encrypting today because of trade off between QoS and security on MPLS – “nightmare”



Partner Customer #3

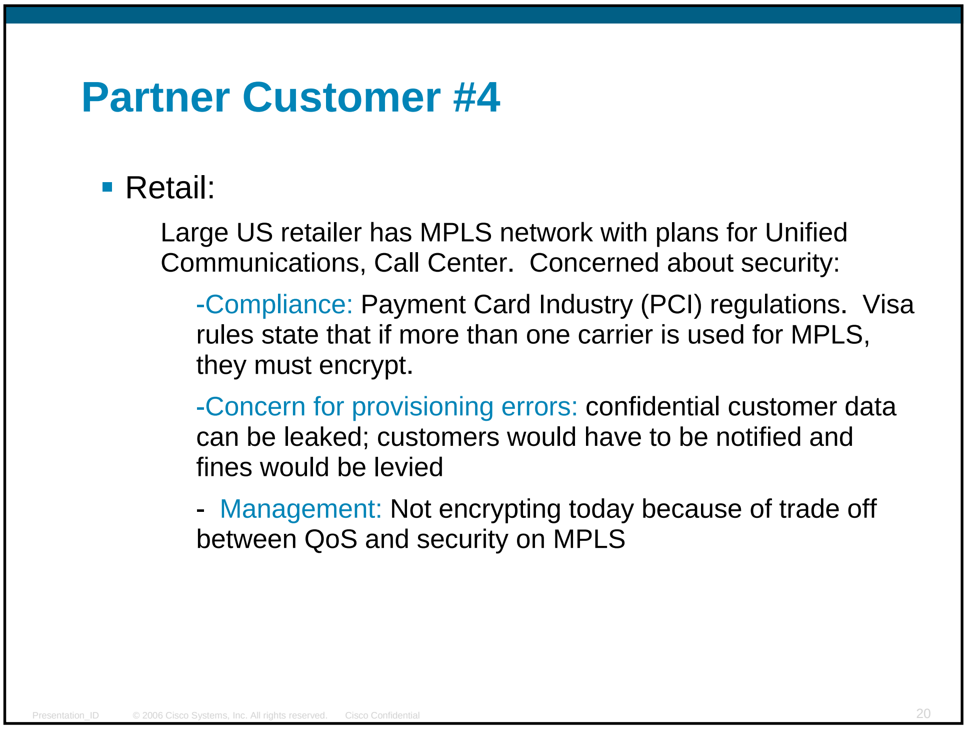
- Banking:

  Large National US Bank has MPLS network. Concerned about security:

  -Compliance: Need to comply with SOX, Payment Card Industry (PCI) regulations. Visa rules state that if more than one carrier is used for MPLS, they must encrypt.

  -Concern for provisioning errors: confidential customer data can be leaked; customers would have to be notified and fines would be levied

  - Management: Not encrypting today because of management complexity



Partner Customer #4

- Retail:

  Large US retailer has MPLS network with plans for Unified Communications, Call Center. Concerned about security:

  -Compliance: Payment Card Industry (PCI) regulations. Visa rules state that if more than one carrier is used for MPLS, they must encrypt.

  -Concern for provisioning errors: confidential customer data can be leaked; customers would have to be notified and fines would be levied

  - Management: Not encrypting today because of trade off between QoS and security on MPLS

Q&A

CISCO