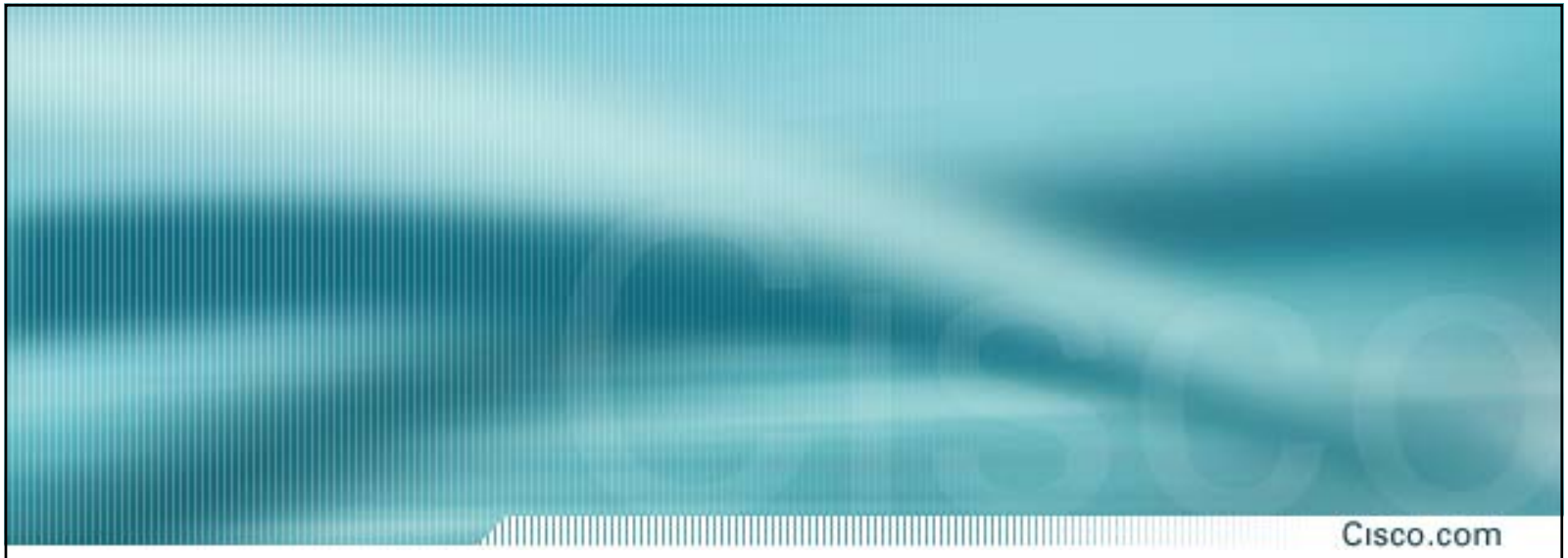


Deploying Integrated IPSec and MPLS VPN Solutions

Nitul Patel

Technical Marketing Engineer, VPN Solutions

March 3rd, 2003

Agenda

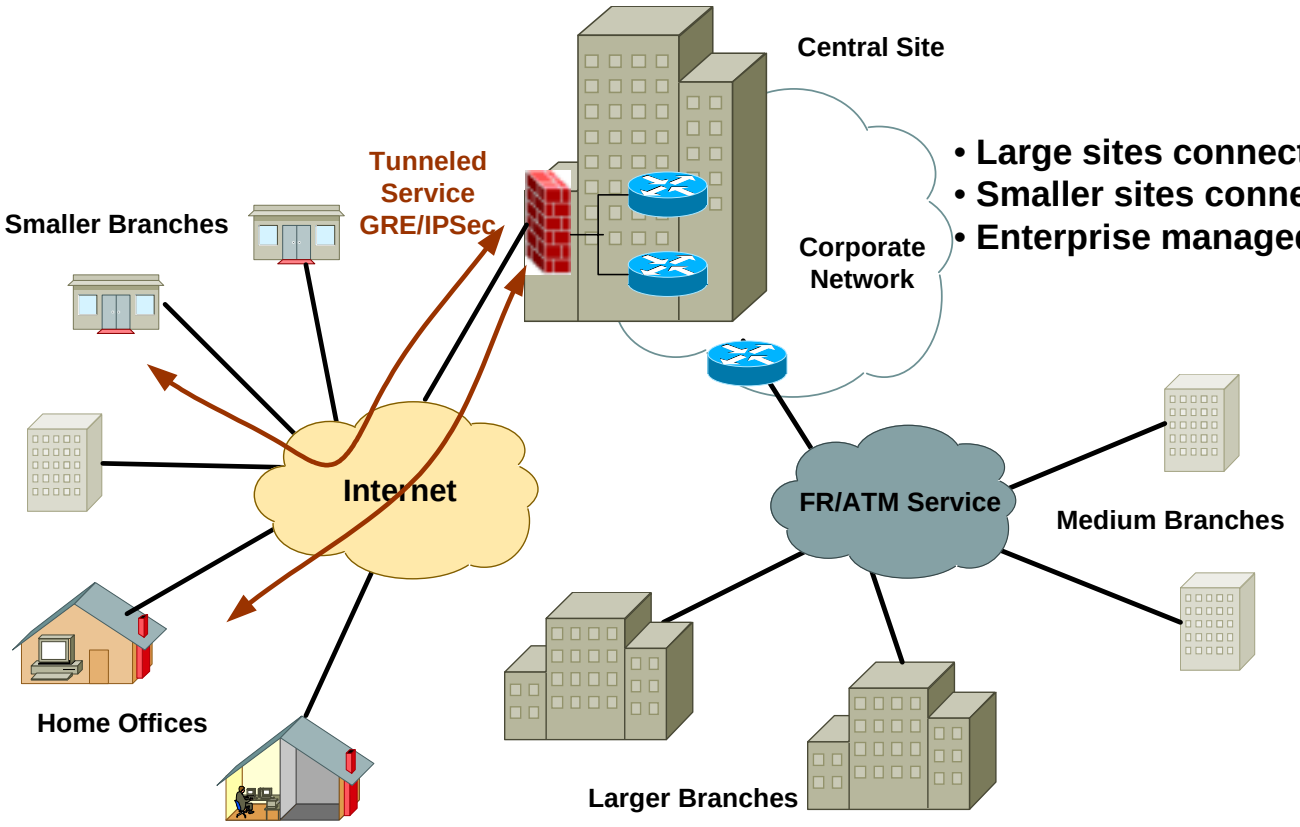
Cisco.com

- VPNs – IPSec and MPLS
- IPSec and MPLS VPN Integration
  - Solution Overview
  - Deployment Models
- How does it all work?
- Key Features
- Solution Management

VPN – Virtual Private Network

- Seamless interconnectivity of various networks of an enterprise(s) across geographically disperse locations.
- Encompass branch offices, SOHOs & telecommuters.
- Support private address space & dynamic routing.
- Support existing applications & services.

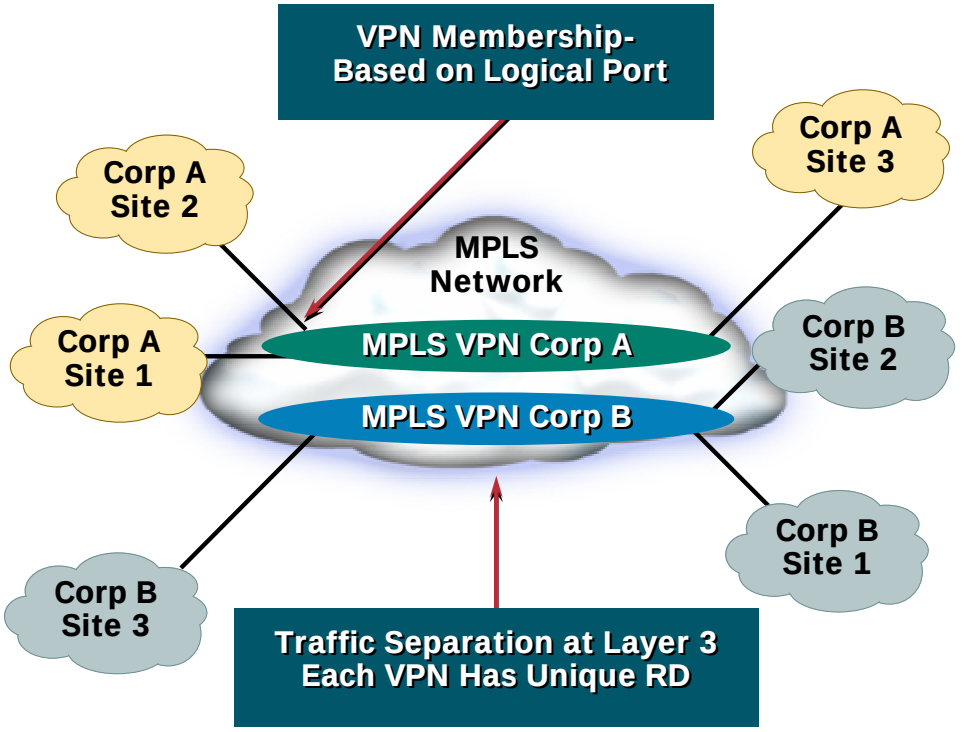
Traditional Enterprise VPN – Secure Access



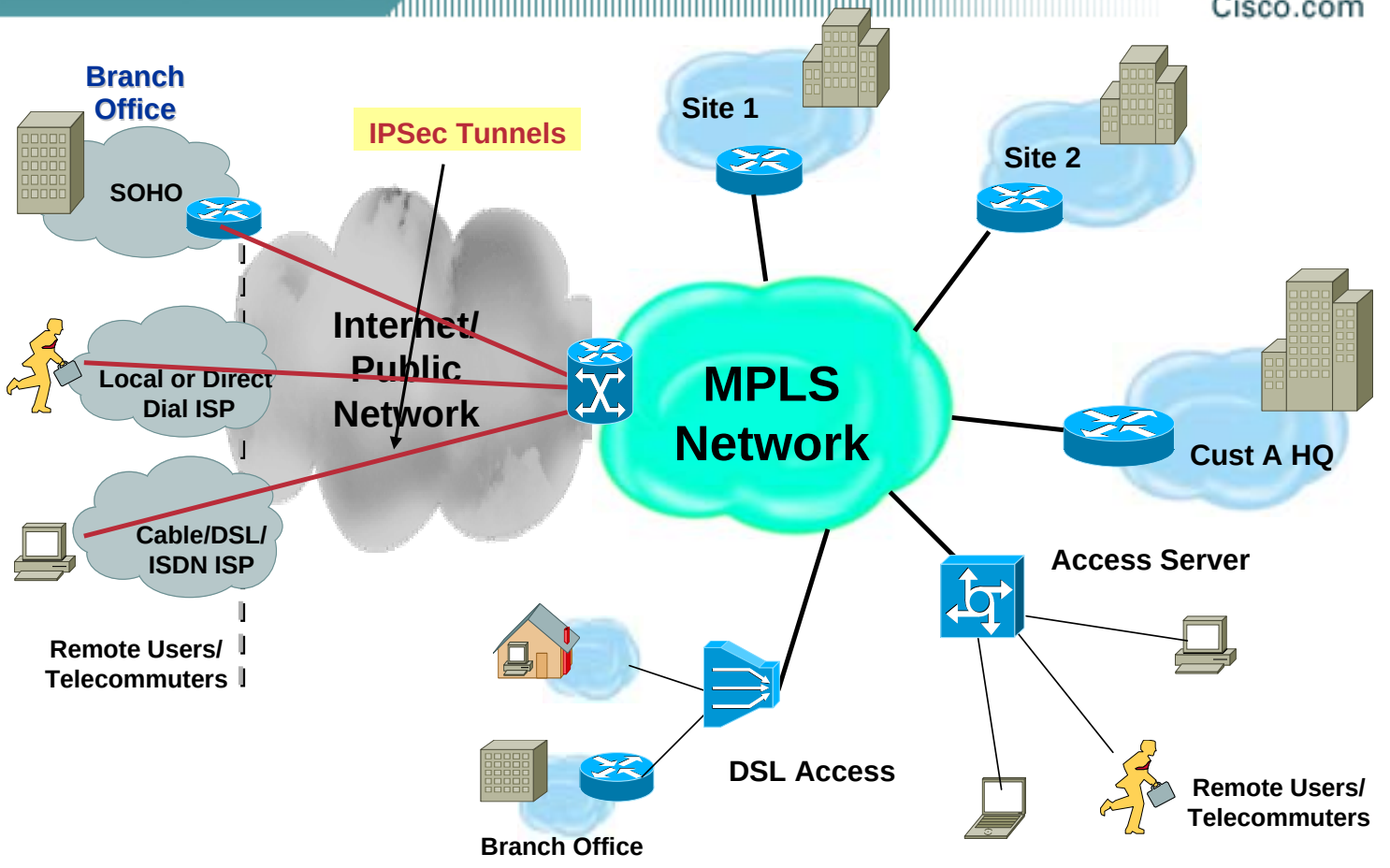
- Large sites connected via FR/ATM.
- Smaller sites connected via IPSec.
- Enterprise managed IPSec.

MPLS Layer 3 VPNs

- Scalable VPNs
- IP QoS and Traffic Engineering
- Easy to manage and No VC provisioning required
- Hub/Spoke or Mesh Topologies can easily be deployed
- Provides a level of Security equivalent to Frame-relay and ATM
- Supports the deployment of new value-added applications
- Customer IP address freedom



IPSec & MPLS Integration



Enterprise VPN – Complete Solution

- Large sites serviced by MPLS VPNs.
- Scalable & easily manageable access model.
- No IPSec management on the headend for IPSec.
- Complete VPN solution from a single provider.
- Outsourcing of Access - Revenue generating opportunities for SP.

Why IPSec?

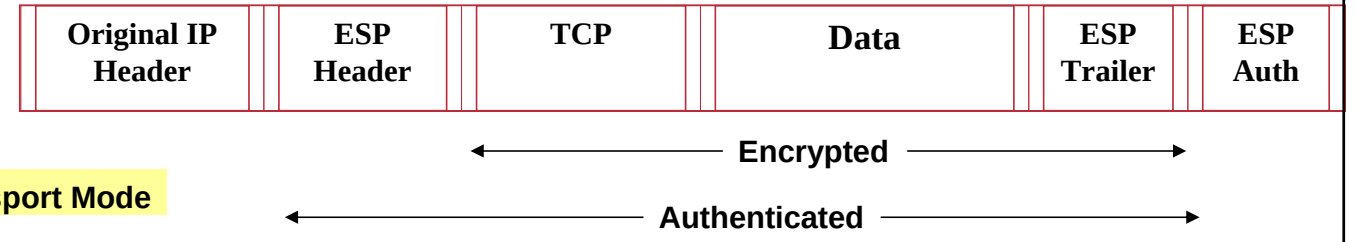
- **Has inbuilt mechanisms to provide:**
  - **Data Confidentiality thru encryption.**
  - **Data Integrity thru packet authentication.**
  - **Origin Authentication thru source verification.**
  - **Replay Protection thru sequence numbers.**
- **Ideal to provide data security across public networks.**
- **IPSec consists of:**
  - **IKE: Key negotiation & management**
  - **IPSec: Data authentication (AH) & encryption (ESP)**

IPSec – ESP Modes

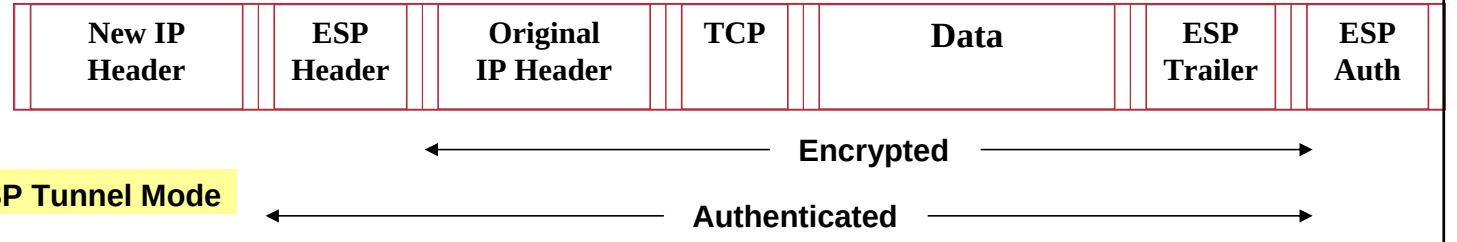
Cisco.com

Original IP Packet

ESP Transport Mode



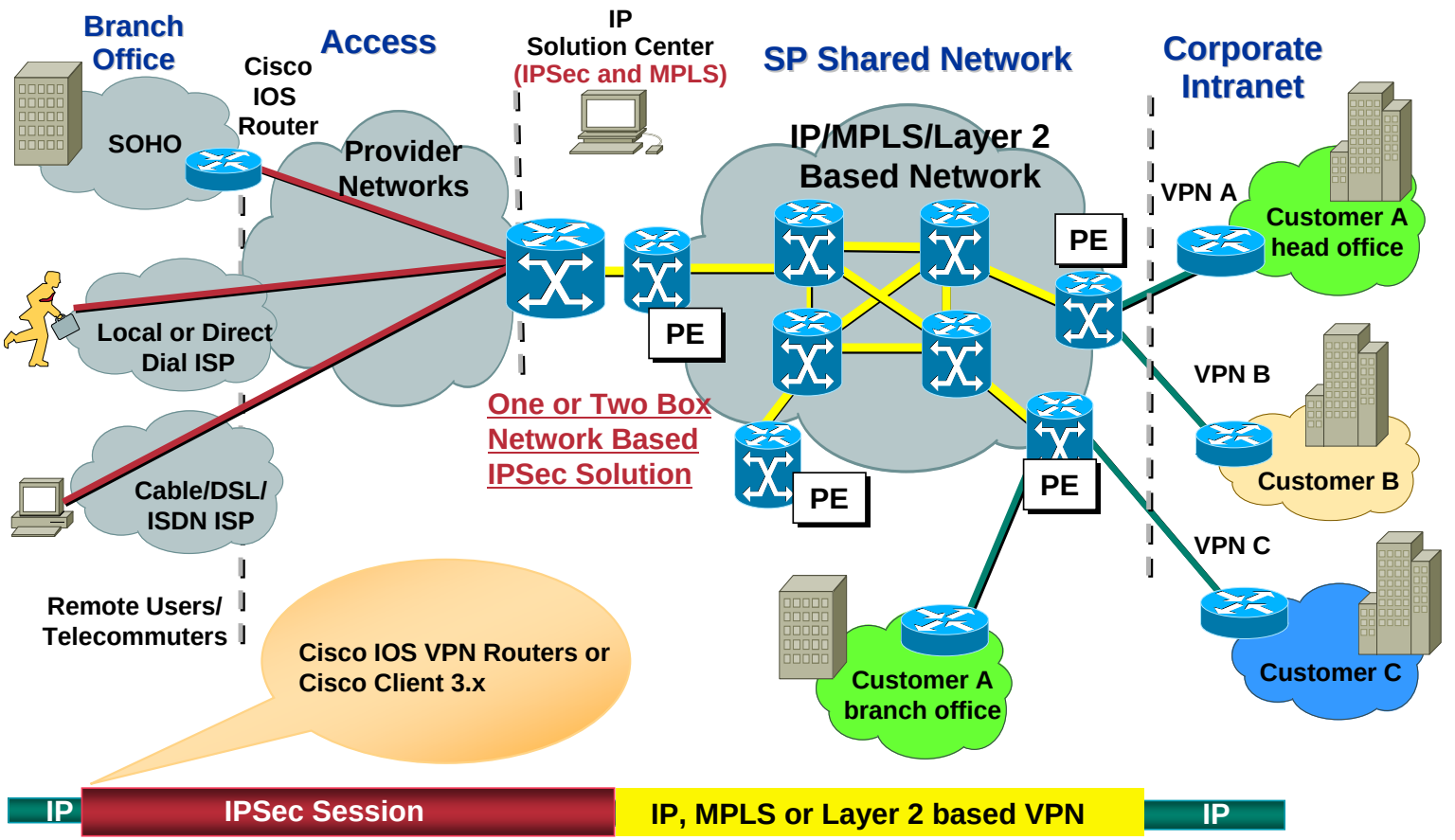
ESP Tunnel Mode



Agenda

- VPNs – IPSec and MPLS
- IPSec and MPLS VPN Integration
  - Solution Overview
  - Deployment Models
- How does it all work?
- Key Features
- Solution Management

IPSec to MPLS Integration – Solution Overview



Solution Overview

- Site-to-Site and remote access VPN service over public/private infrastructure
- Single box to terminate IPSec session for multiple enterprises (VPNs).
- Support private addressing schemes
- Integrate off-net users into MPLS VPN/L3VPN/L2VPN.

One Box and Two Box Solution

Cisco.com

One Box Solution

- Same device is the IPSec aggregator as well as the PE.
- Ideal for small PoPs or smaller SPs since separate device not required

Two Box Solution

- Separates Edge from Access
- Multiple aggregators can feed into a single PE
- Requires use of statics/routing protocol between aggregator & PE on per VPN basis
- Makes edge/core management easier due to decreased number of PEs
- 2 devices helps the solution scale better

Solution Benefits

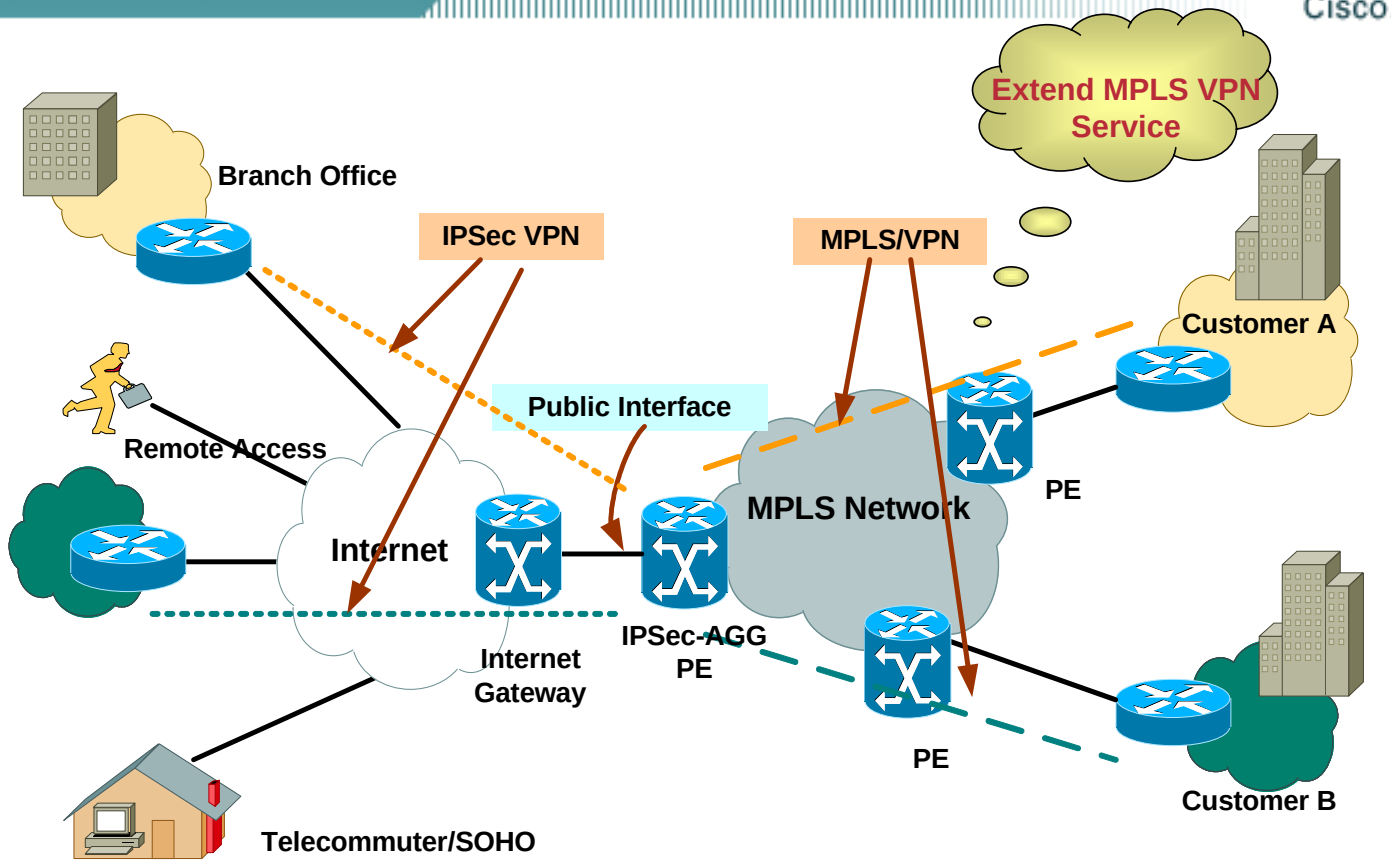
- **Off-Net to MPLS-VPN benefits:**
  - **Extend MPLS-VPN toward Internet or Extranet and increase foot print.**
- **Network Based IPSec VPN solution benefits:**
  - **L2 provider (Frame Relay, ATM, leased line or 802.1Q) can provide secure connectivity to customer's remote sites where provider does not have L2 infrastructure.**
  - **L3 provider can offer VPN service over GRE tunnels in the backbone (encrypted/unencrypted).**
- **Mobile operators when offering data services can offer secure access services**

Agenda

Cisco.com

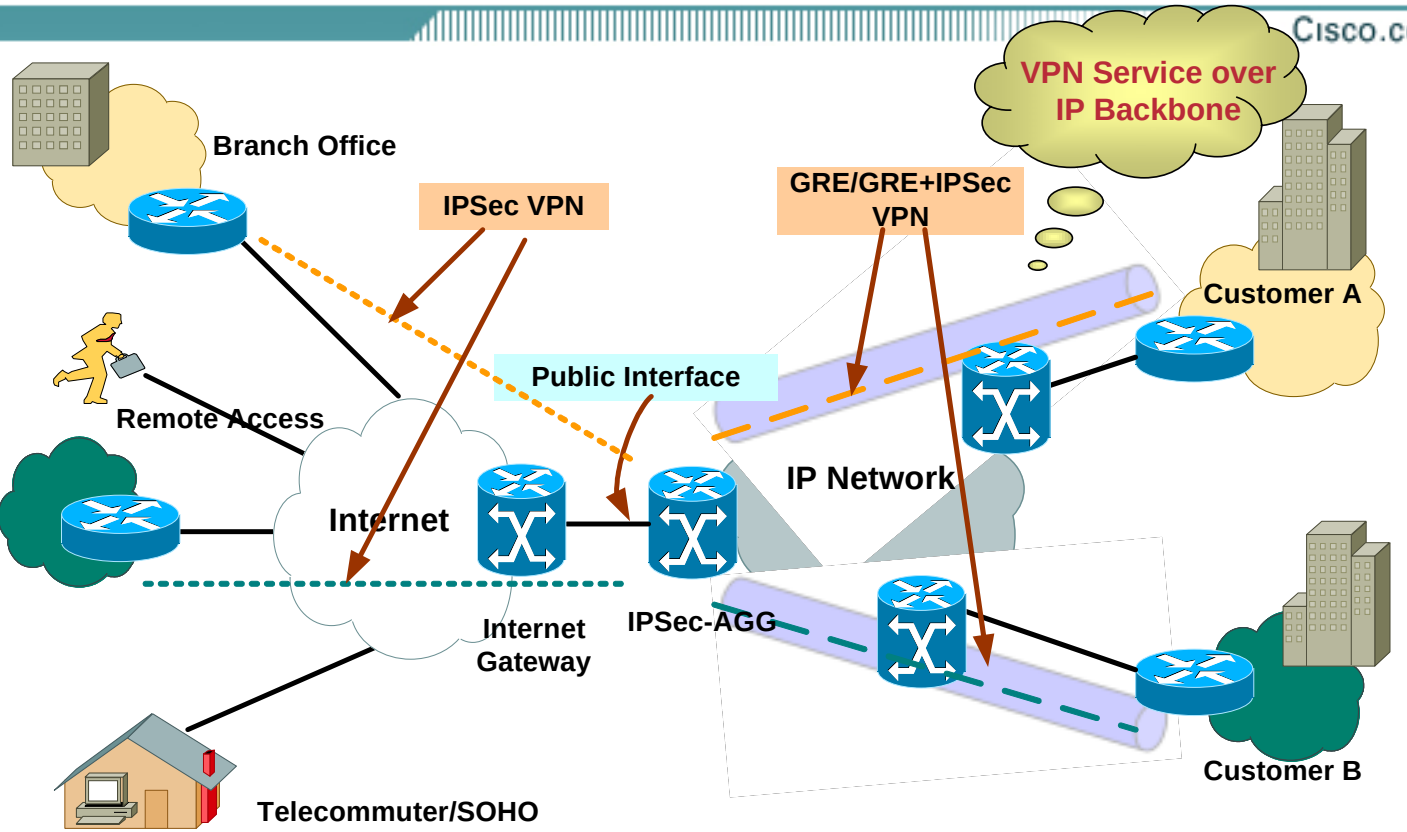
- VPNs – IPSec and MPLS
- IPSec and MPLS VPN Integration
  - Solution Overview
  - Deployment Models
- How does it all work?
- Key Features
- Solution Management

Deployment Models – IPSec to MPLS VPN



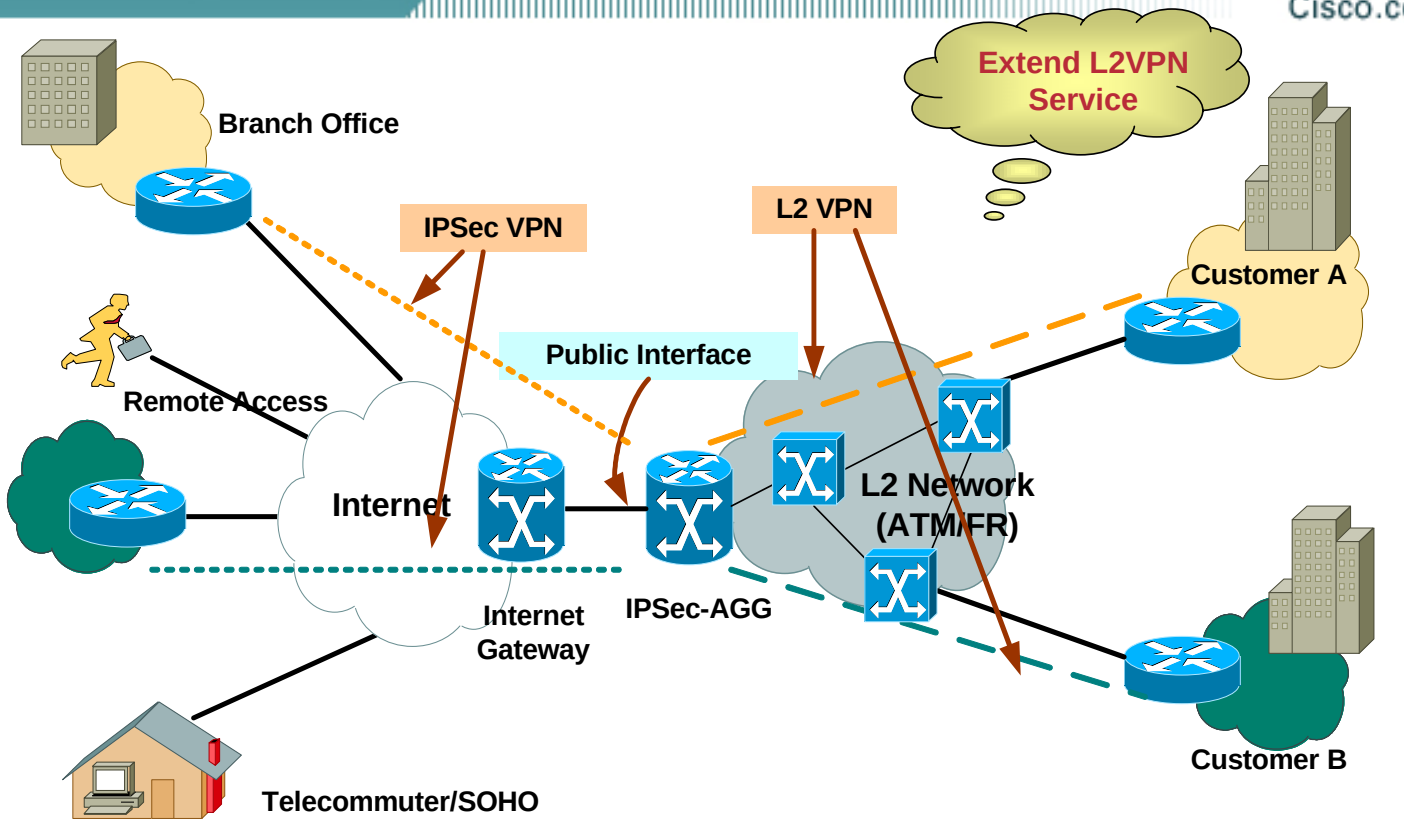
Mapping offnet users into MPLS VPNs.

Deployment Models – IPSec to GRE/IPSec



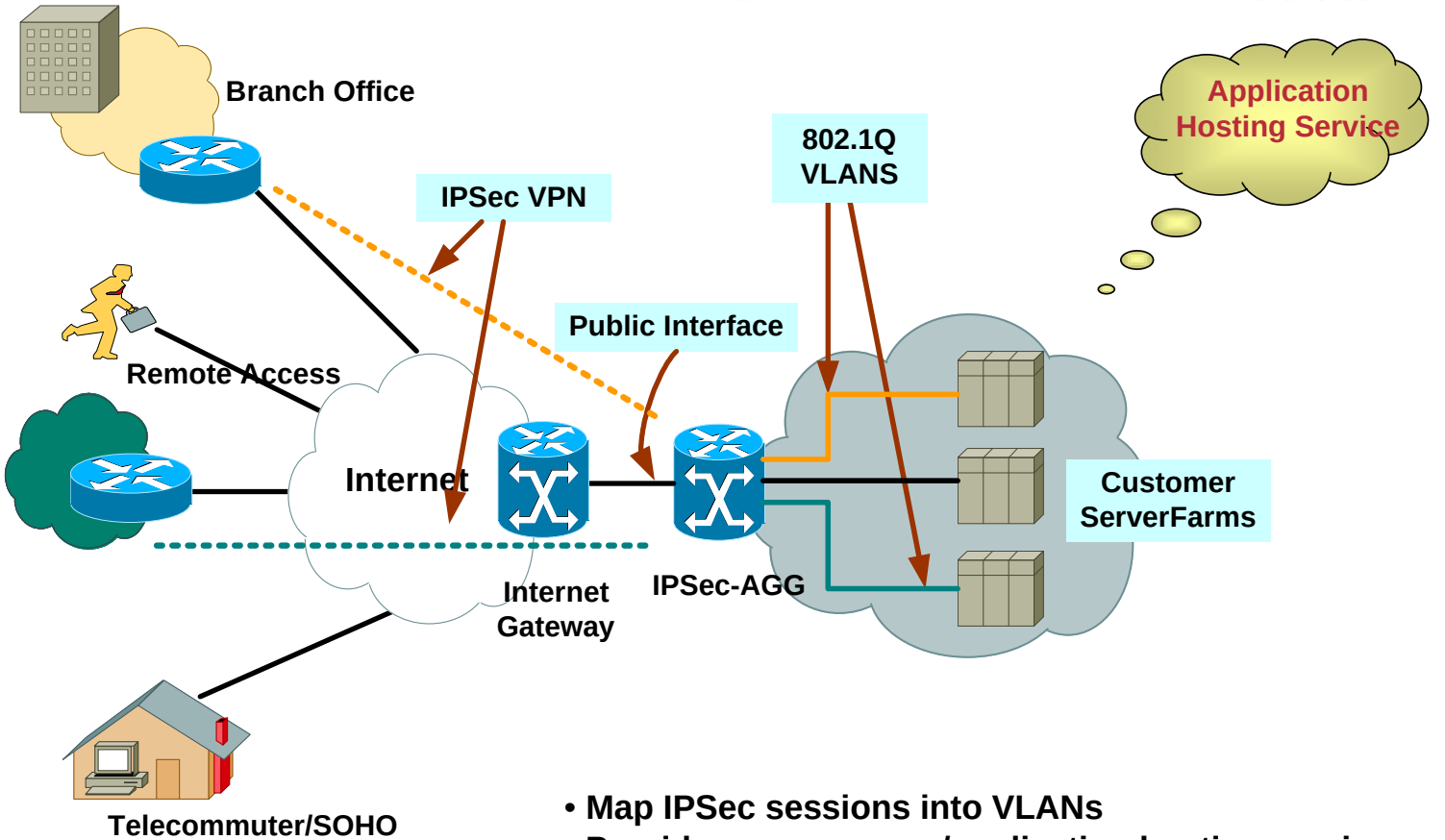
- IP Service Provider can provide secure offnet access.
- SPs who are transitioning to a MPLS backbone can also offer service.

Deployment Models – IPSec to L2VPN



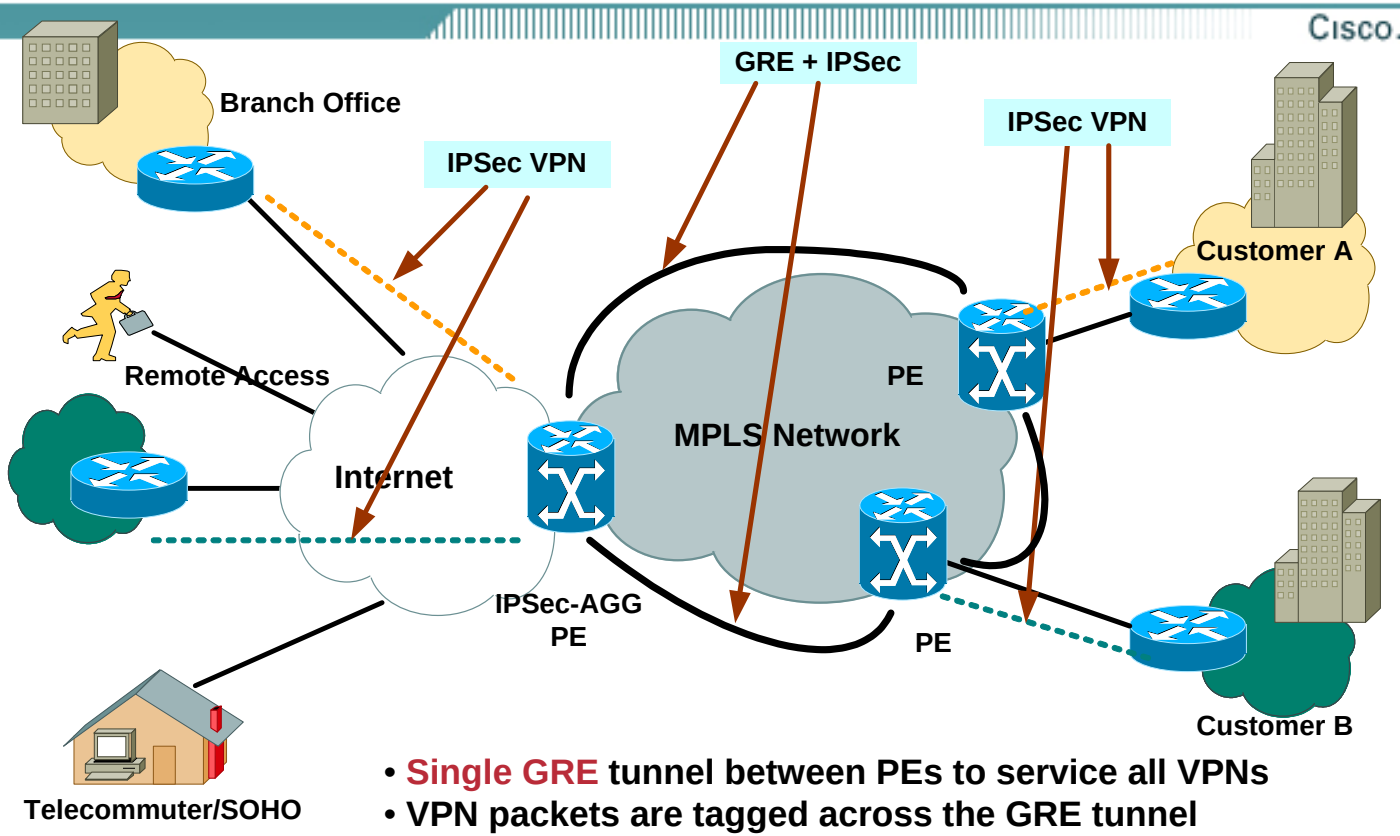
Mapping Offnet users to FR/ATM PVC per customer.

Deployment Models – IPSec to 802.1Q



- Map IPSec sessions into VLANs
- Provide secure server/application hosting service

Deployment Models – IPSec to GREoMPLS



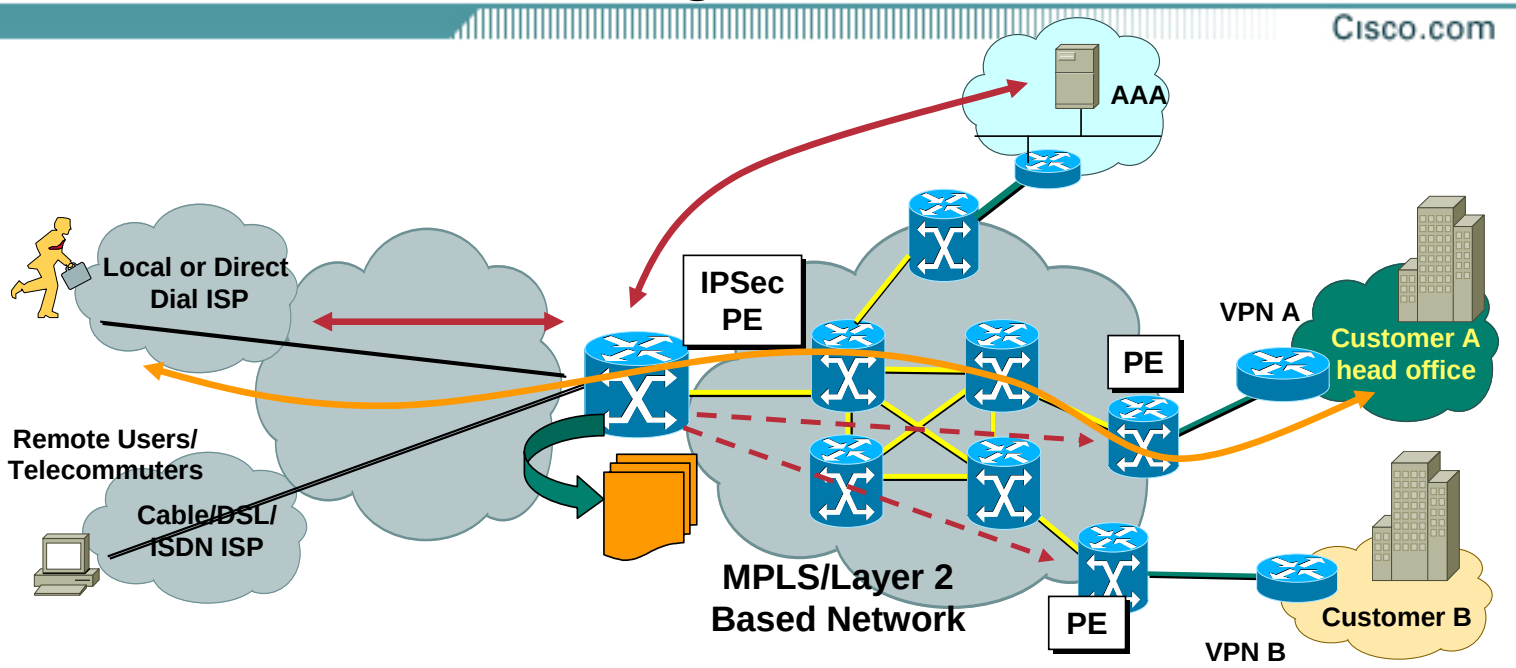
- **Single GRE** tunnel between PEs to service all VPNs
- VPN packets are tagged across the GRE tunnel
- Provide security across MPLS cloud
- Useful in case of VPNs spread across multiple transport providers (CSC)

Agenda

Cisco.com

- VPN – IPSec and MPLS
- IPSec and MPLS VPN Integration
  - Solution Overview
  - Deployment Models
- How does it all work?
- Key Features
- Solution Management

Remote Access Integration



1a. User connects to the public address. Sends request for new SA.

2a. Group info such as Pre-shared key, dns, domain, address pool are downloaded from Radius.
2b. ISAKMP policy parameters are negotiated.

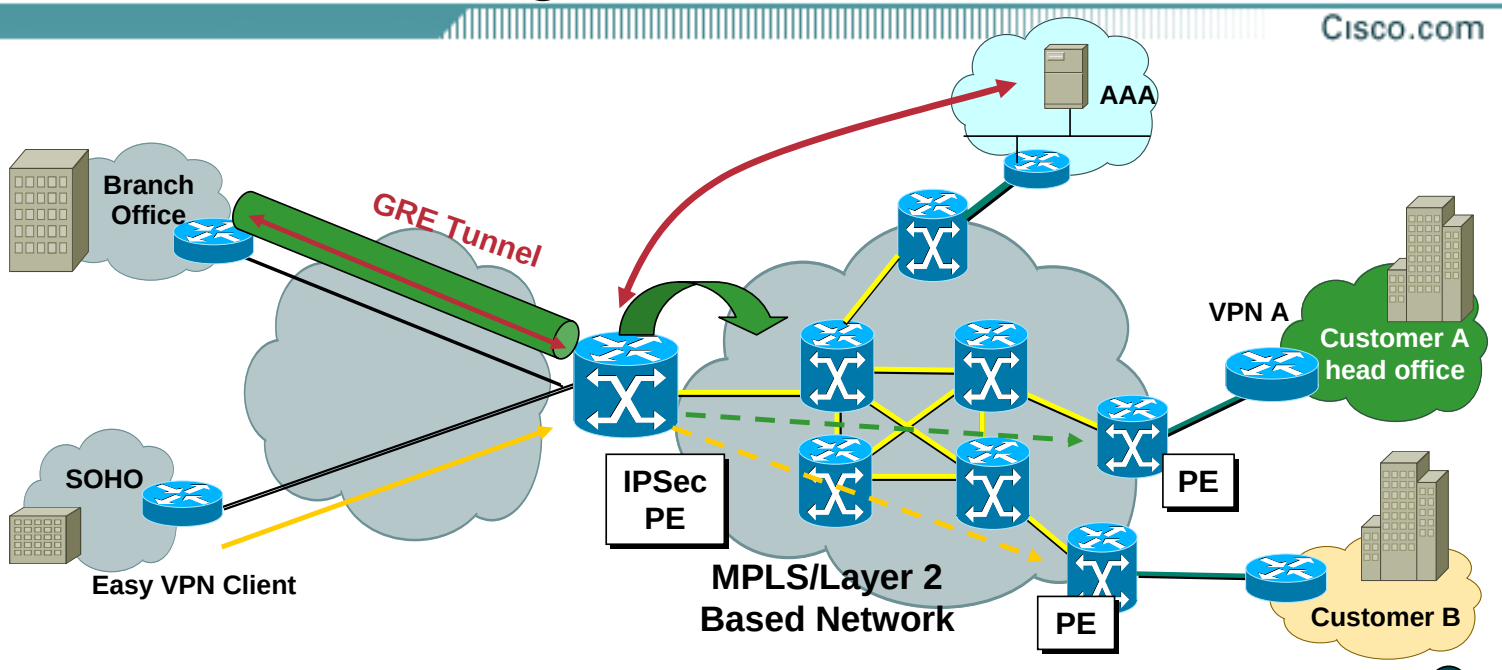
3. User is authenticated via Xauth.

4. IPSec proposals incl transform set are exchanged & Phase 2 SAs are created.
User is assigned an IP address from the VRF pool

5. RRI installs the route in the VRF routing table which can be redistributed across the VPN via BGP.

6. User now has VPN connectivity into corporate.

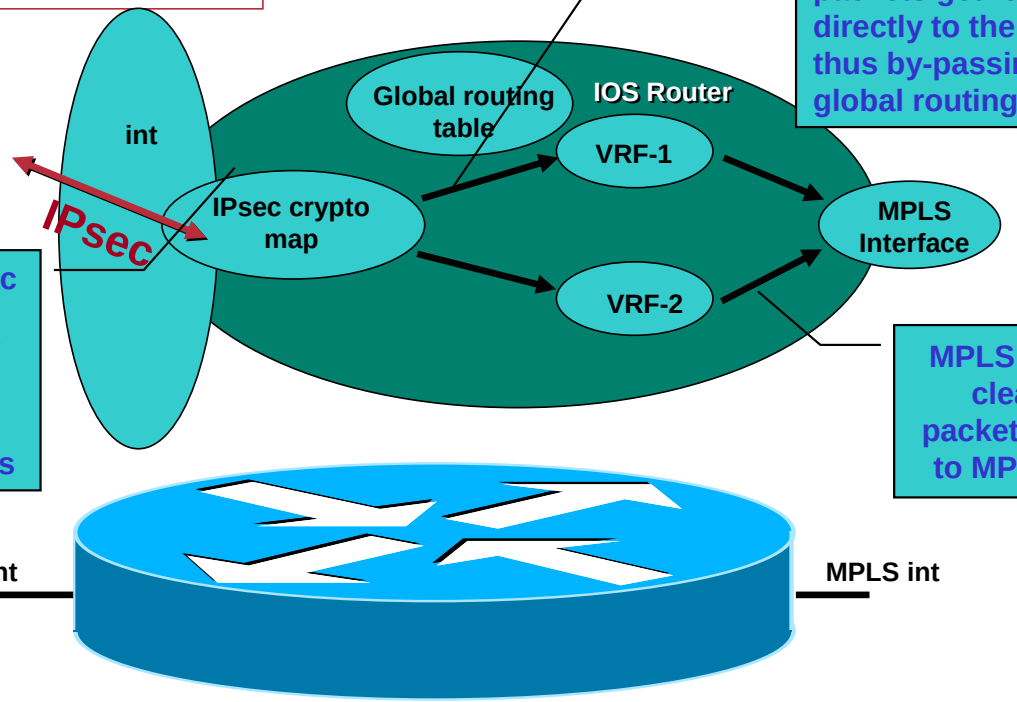
Site-to-Site Integration



- GRE tunnels can be used to carry routing protocols. IPSec is used in transport mode.
- Each peer is individually defined on the aggregator.
- Single public interface can be used to terminate multiple VPNs as VRF classification is done on the GRE interface and not on the physical interface.
- EzVPN clients (800/1700) can be used in a similar mode as the unified VPN client.

Packet Forwarding – VRF Aware IKE/IPSec

Inside the IPsec/MPLS PE Router



• Decrypted clear-text packets get forwarded directly to the right VRF thus by-passing the global routing table.

• Based on IKE, the IPsec tunnel is directly associated with the VRF
• VRF association can locally defined or downloaded from Radius

MPLS wrapped clear-text packets forward to MPLS VPNs

No limitations !!! Works for both site-to-site and client-to-concentrator type of IPsec tunnels.

VRF-Aware IKE/IPSec – ISAKMP Profile


```
crypto keyring coke
  pre-shared-key address 12.0.0.2 key coke123
!
crypto isakmp policy 2
  authentication pre-share
!
crypto isakmp profile coke
  vrf coke
  keyring coke
  match identity ip-address 12.0.0.2 255.255.255.255
!
crypto ipsec transform-set tset esp-des esp-md5-hmac
crypto map vpn 1 ipsec-isakmp
  set peer 12.0.0.2
  set transform-set tset
  set isakmp-profile coke
  match address 101
!
interface FastEthernet4/0
  ip address 12.0.0.1 255.255.255.0
  crypto map vpn
```

Agenda

- VPN – IPSec and MPLS
- IPSec and MPLS VPN Integration
  - Solution Overview
  - Deployment Models
- How does it all work?
- Key Features
- Solution Management

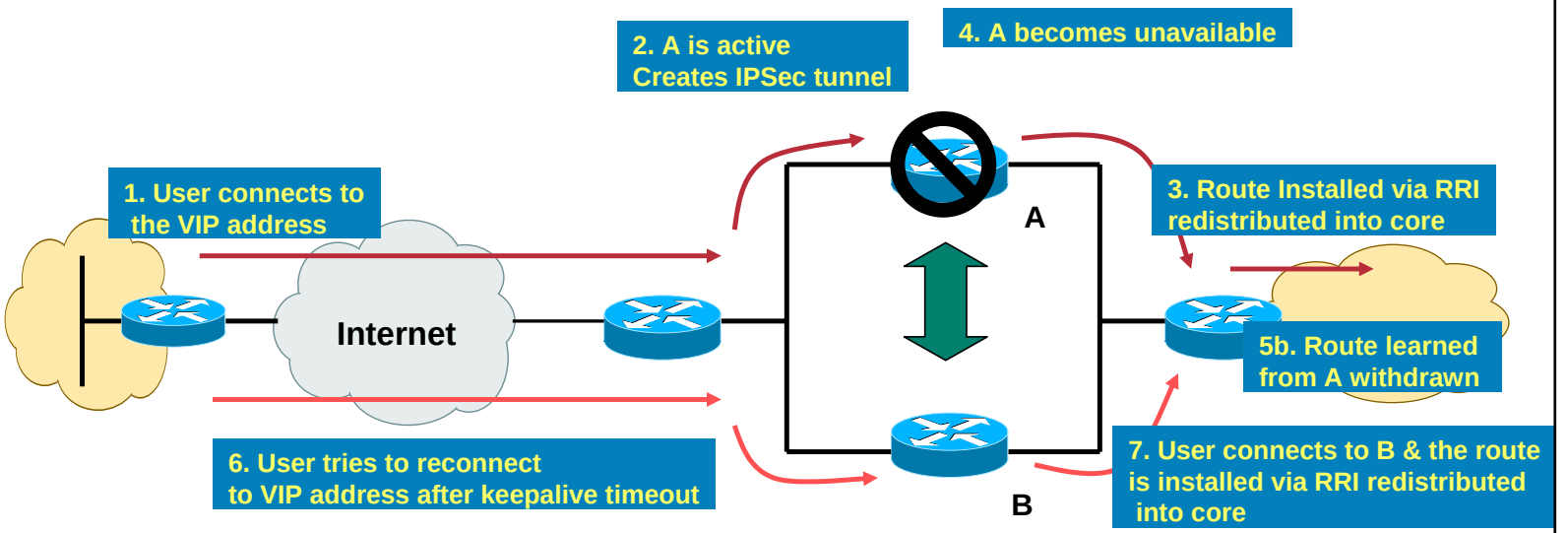
Key Features

- VPN Client Support for remote access
- GRE tunnels for site-to-site routing protocol support
- GRE Keepalives to avoid black holing of data across public network
- Overlapping IP address across multiple customers
- Scalable Dead Peer Detection (DPD) keepalive mechanism
- Stateless Failover using HSRP

Key Features

- Single public facing interface/IP address for all the VPNs
- Easy VPN client – minimum configuration on CPEs
- NAT Transparency – allows IPSec through NAT devices by encapsulating ESP in a UDP wrapper
- Radius based IPSec accounting for VPN clients
- Server load balancing for scalability & high availability

Stateless Failover – HSRP + Reverse Route Injection



- Client connects to HSRP VIP, attaches to Active .
- After QM success, route to client created by RRI and advertised to inside router.
- Returning traffic (from inside) destined for client is sent via the correct router.
- HSRP can also be used on both interfaces - allowing inside gateways to use HSRP VIP as their default route.

HSRP + Reverse Route Injection

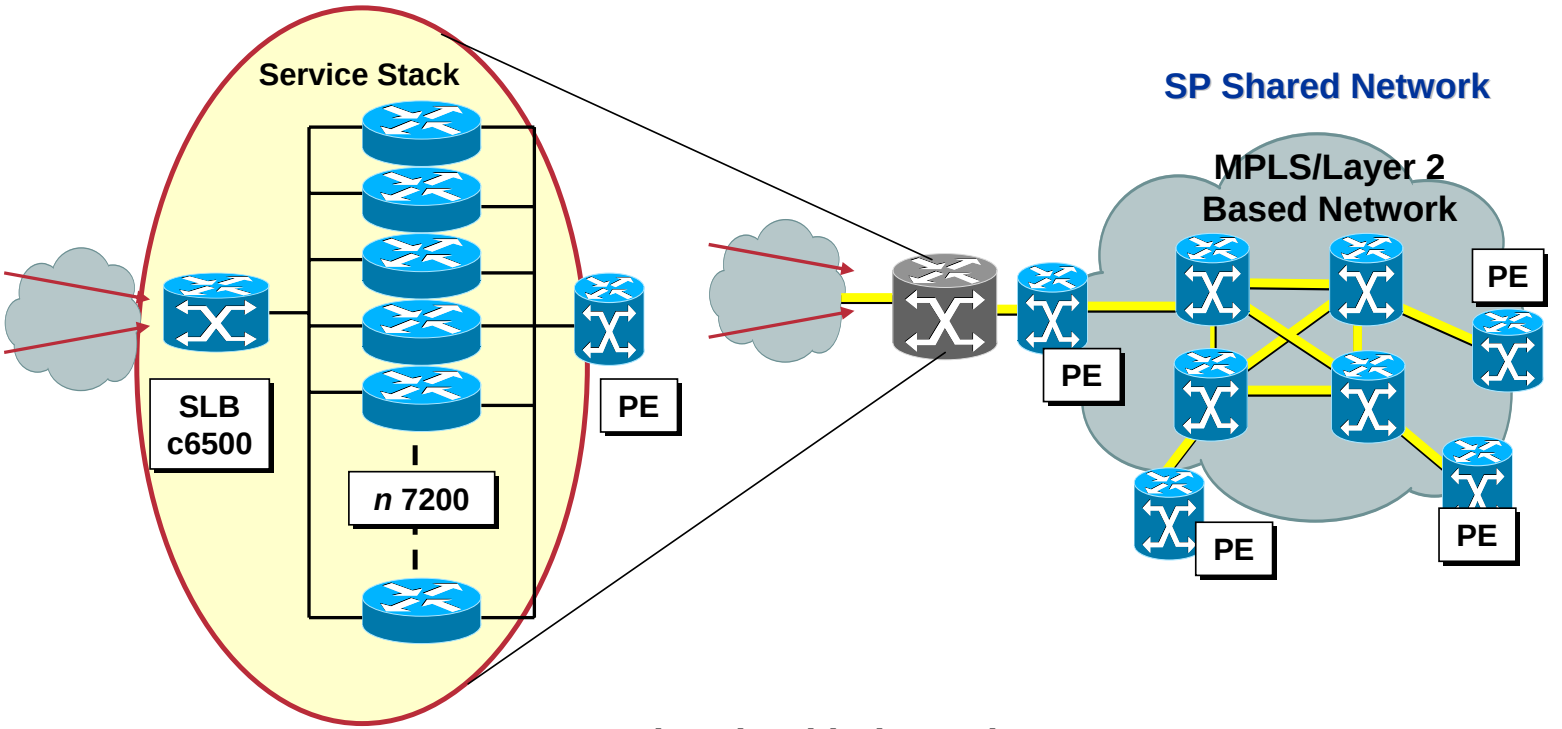
HSRP

- Use HSRP VIP as tunnel endpoint
- In the case of failover HSRP tells crypto to clean-up connection info
- Use HSRP benefits such as interface tracking, primary/secondary management
- Remotes need only to connect to HSRP VIP, avoids multiple connections and gateway lists

RRI

- Avoids asymmetrical routing problems
- Injects routes into dynamic routing process, so avoids the need for static routes

Server Load Balancing



- c6500SLB used to load balance between *n* IPSec aggregators.
- Users connect to a single IP address – SLB takes care of rest
- Supported for Remote Access VPN clients only.

Server Load Balancing


```
ip slb serverfarm IPSEC
 failaction purge
 probe SERVER-PROBE
 !
 real 30.1.1.1
  weight 1
  maxconns 100
  inservice
 !
 real 30.1.1.2
  weight 1
  maxconns 100
  inservice
```

```
ip slb probe SERVER-PROBE ping
 interval 30
 faildetect 3
```

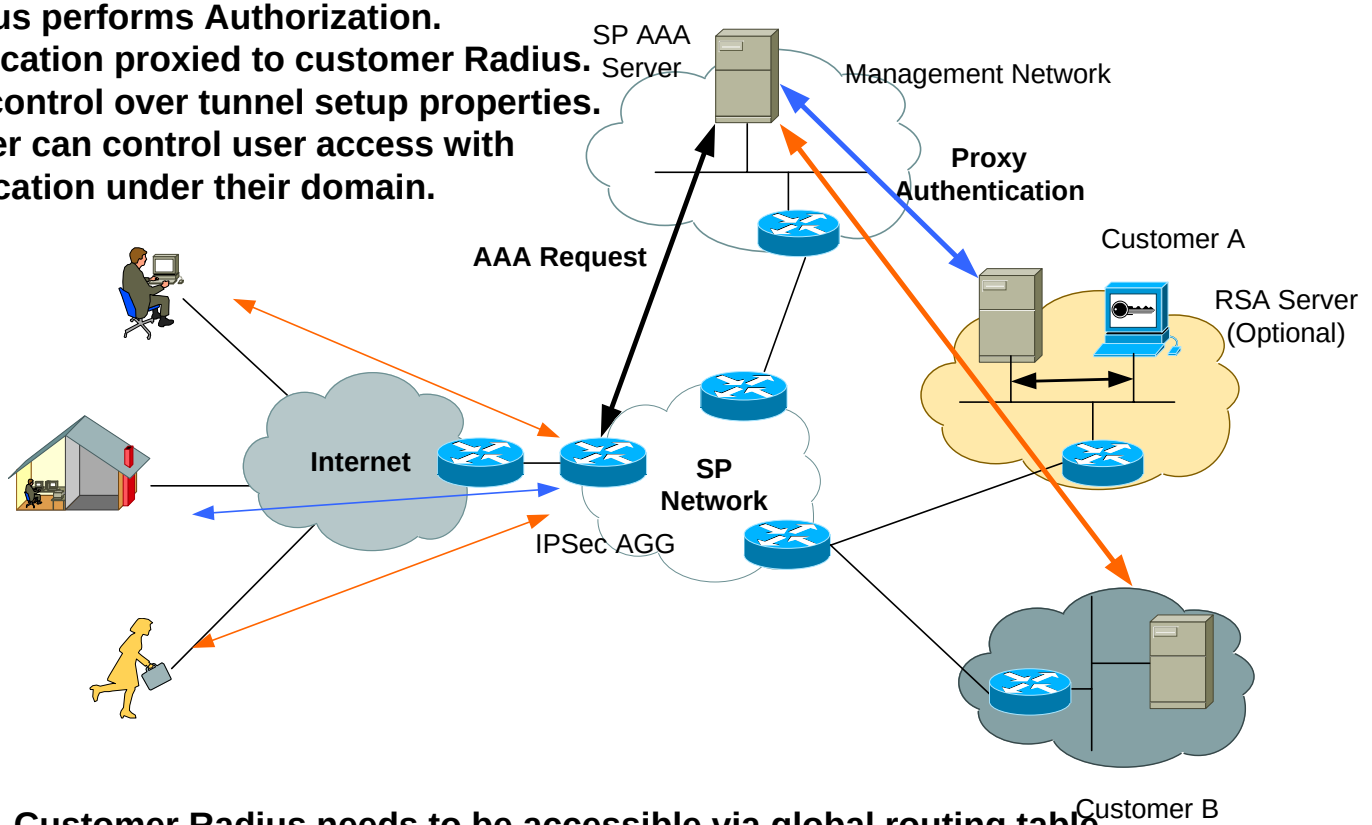
```
ip slb vserver IPSEC-ESP
 virtual 220.1.1.1 esp
 serverfarm IPSEC
 sticky 6000 group 1
 idle 3650
 inservice
!
ip slb vserver IPSEC-ISAKMP
 virtual 220.1.1.1 udp isakmp
 serverfarm IPSEC
 sticky 6000 group 1
 idle 3650
 inservice
```

AAA Options - Radius

- Local AAA – SP Radius performs authentication & authorization
- Proxy AAA
- Per-VRF AAA
- IPSec AAA Accounting
- Proxy - Secure ID support of New PIN/Next PIN

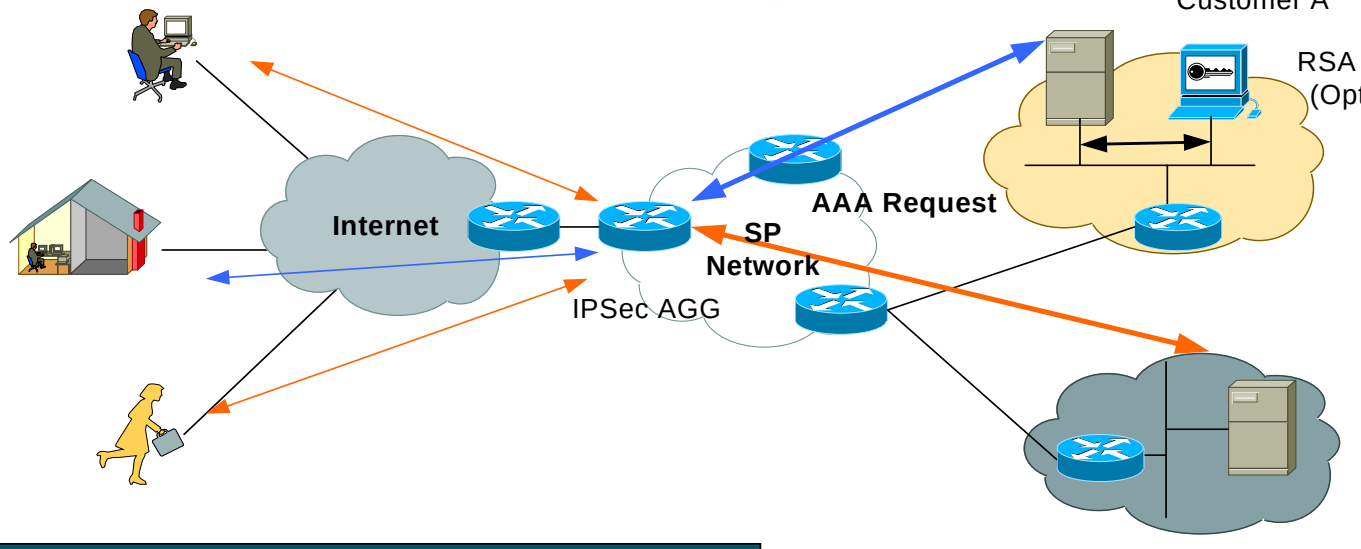
Proxy AAA

- SP Radius performs Authorization.
- Authentication proxied to customer Radius.
- SP has control over tunnel setup properties.
- Customer can control user access with authentication under their domain.



Drawback – Customer Radius needs to be accessible via global routing table.

Per-VRF AAA




```
aaa group server radius coke-ra
  server-priavate 192.168.1.222 key Cisco
  ip vrf forwarding coke
!
aaa authentication login coke group coke-ra
aaa authorization network coke groupcoke-ra
!
crypto map crypmap client authentication list coke
crypto map crypmap isakmp authorization list coke
```

- Customer Radius performs authen/author
- Dual accounting (SP as well as customer Radius) supported
- Customer Radius reachable via VRF – global reachability not required
- SP loses authorization control over incoming users

IPSec Radius Accounting

Cisco.com

Dual Accounting to both SP as well as Customer Radius supported for VRF aware AAA.

- **Some of the attributes in Start record include:**
  - **1; User-Name**
  - **4; Nas-IP-Address**
  - **5; Nas-Port**
  - **6; Service-Type**
  - **64; Tunnel-Type**
  - **VSA; Phase_1_ID**
  - **VSA; VRF-ID**

- **Some of the attributes in Stop record include:**
  - **42; Acct-Input-Octets**
  - **43; Acct-Output-Octets**
  - **46; Acct-Session-Time**
  - **47; Acct-Input-Packets**
  - **48; Acct-Output-Packets**
  - **49; Acct-Terminate-Cause**

Internet Access Options

- **Split Tunneling Enabled**
  - **IPSec is used for VPN traffic only.**
- **Split Tunneling Disabled**
  - **IPSec is used for VPN as well as non-VPN traffic.**
  - **Enterprises may prefer the Internet traffic to traverse their firewalls.**
  - **Or the VPN SP can provide Internet access directly as a additional service.**

Agenda

- VPN – IPSec and MPLS
- IPSec and MPLS VPN Integration
  - Solution Overview
  - Deployment Models
- How does it all work?
- Key Features
- Solution Management

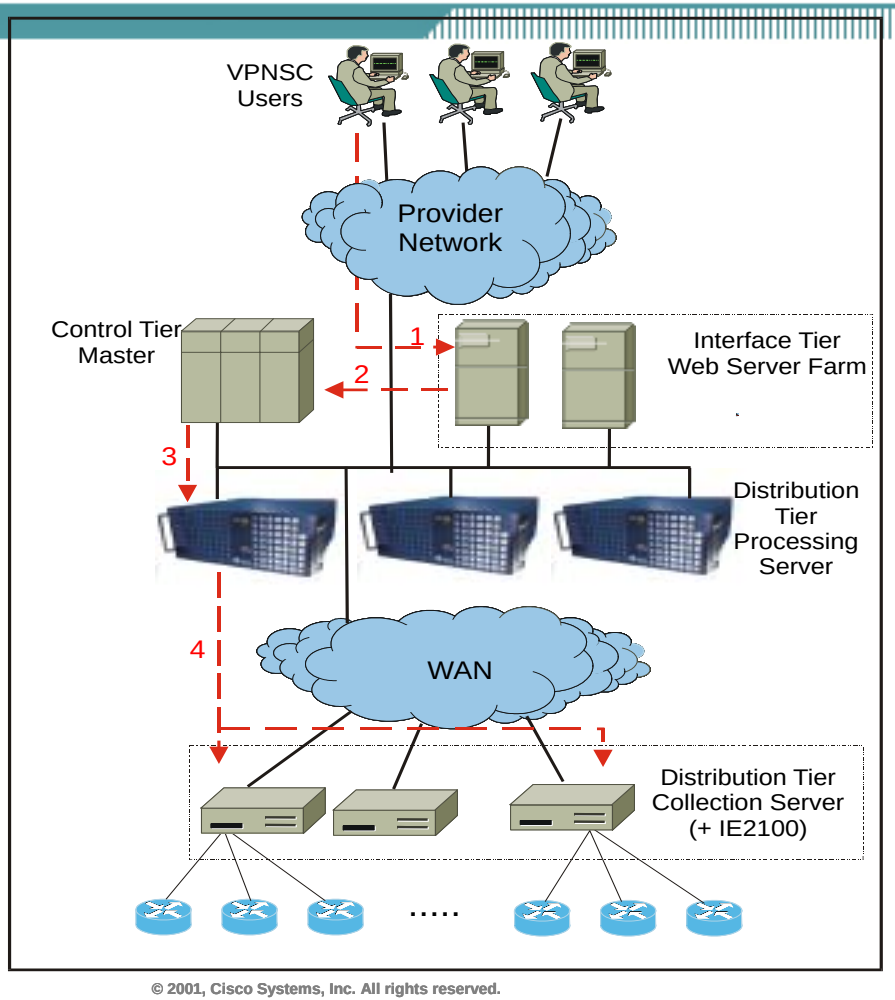
NMS/OSS

- **Fault Management**
  - MIBs and traps in the Cisco-IPSec-Flow-Monitor-MIB
  - Currently traps are generated on tunnel up/down status
  - More traps in the process of being added
  - Enhance the existing IPSec MIBs to be VRF aware
  - MIBs such IF-MIB & MPLS-VPN MIB used
- **Configuration**
  - Solution provisioning to be done using ISC 3.0 (IP Solution Center)
  - Support IPSec as well as MPLS VPN provisioning

NMS/OSS

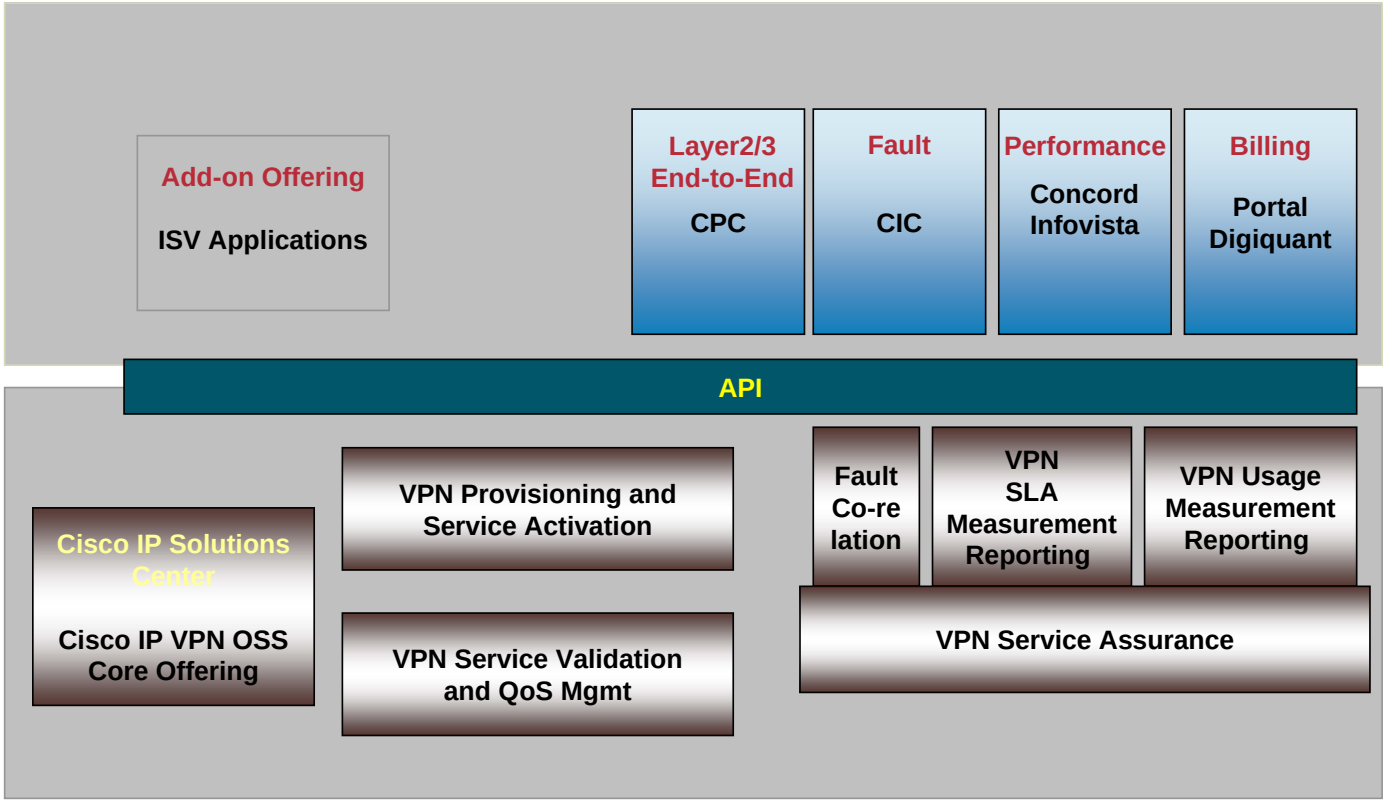
- **Accounting**
  - **Radius based IPSec accounting for remote access clients**
  - **Dual Accounting to SP/Customer AAA server**
- **Performance**
  - **Primarily accomplished by the use of the Cisco-IPSec-Flow-Monitor-MIB.**
  - **Provides a number of accounting and error statistics for the IKE and IPSec tunnels.**
  - **Integration with other applications for performance & fault management**
- **Security**
  - **Use separate IPSec tunnels for management purpose**
  - **Normal network security through firewalls and ACLs.**

ISC 3.0 Distributed Architecture



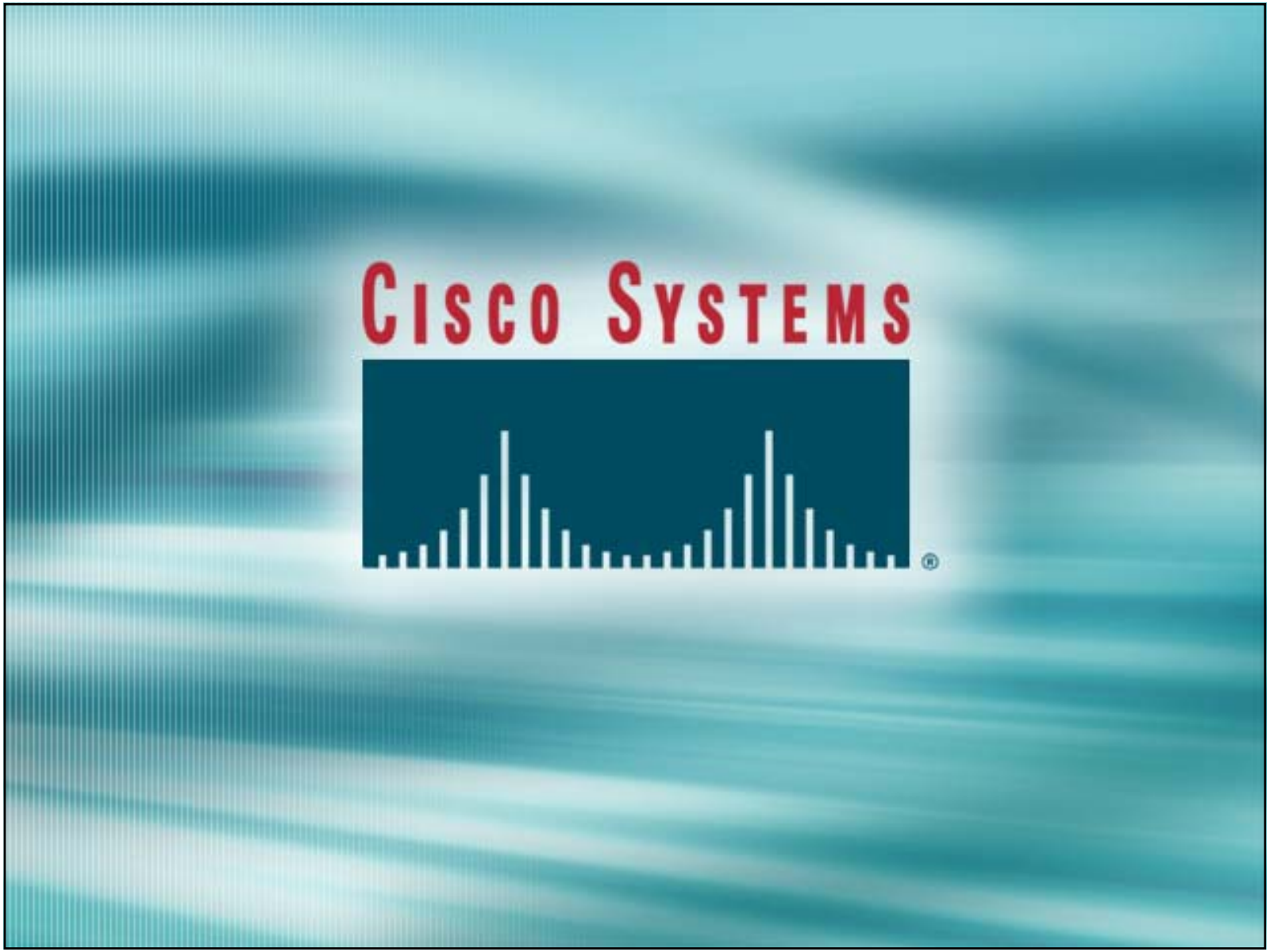
- **Four Tier Architecture**
  - **Client Tier**
  - **Interface Tier - Sustain large number of concurrent users**
  - **Distribution Tier - Support large number of concurrent running tasks**
  - **Control Tier - Allows for Central Control and Monitoring of the whole system**
- **Designed to address front-end and back-end scalability**
- **Coherent service model design ensures information consistency and visibility among different services**

ISC Enabled: Complete FCAPS OSS Solution



IPSec and MPLS Integration – Summary

- MPLS provides scalable VPN connectivity
- IPSec provides secure remote access connectivity into MPLS VPNs
- Integration allows SP to offer a comprehensive VPN service
- Cisco packaged solution provides additional revenue opportunities to SPs
- Solution addresses scalability, high availability, provisioning & management along with seamless integration with existing services


CISCO SYSTEMS