



CISCO SYSTEMS

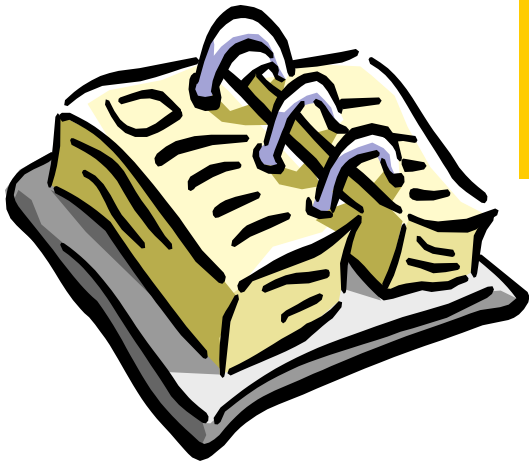


Understanding MPLS/VPN Security Issues

SEC-370

Michael Behringer <mbehring@cisco.com>

Agenda



- **Analysis of MPLS/VPN Security**
- **Security Recommendations**
- **MPLS Security Architectures**
 - Internet Access**
 - Firewalling Options**
- **Attacking an MPLS Network**
- **IPsec and MPLS**
- **Summary**

The Principle: A “Virtual Router”

Cisco.com

Virtual Routing and Forwarding Instance

**Route Distinguisher:
Makes VPN routes unique**

```
!  
ip vrf Customer_A  
  rd 100:110  
  route-target export 100:1000  
  route-target import 100:1000  
!  
interface Serial0/1  
  ip vrf forwarding Customer_A  
!
```

**Export this VRF with
community 100:1000**

**Import routes from
other VRFs with
community 100:1000**

**Assign Interface to
“Virtual Router”**

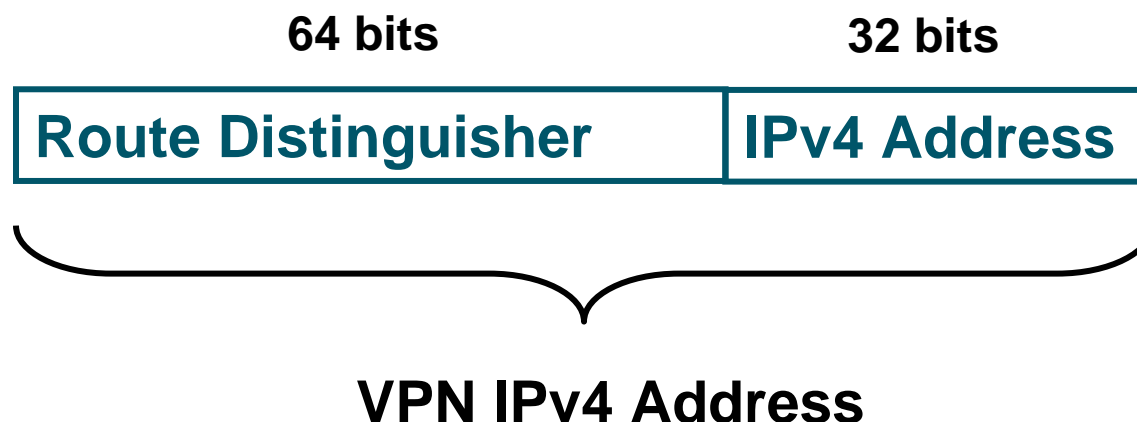
General VPN Security Requirements

Cisco.com

- **Address Space and Routing Separation**
- **Hiding of the MPLS Core Structure**
- **Resistance to Attacks**
- **Impossibility of VPN Spoofing**

Working assumption: The core (PE+P) is secure

Address Space Separation

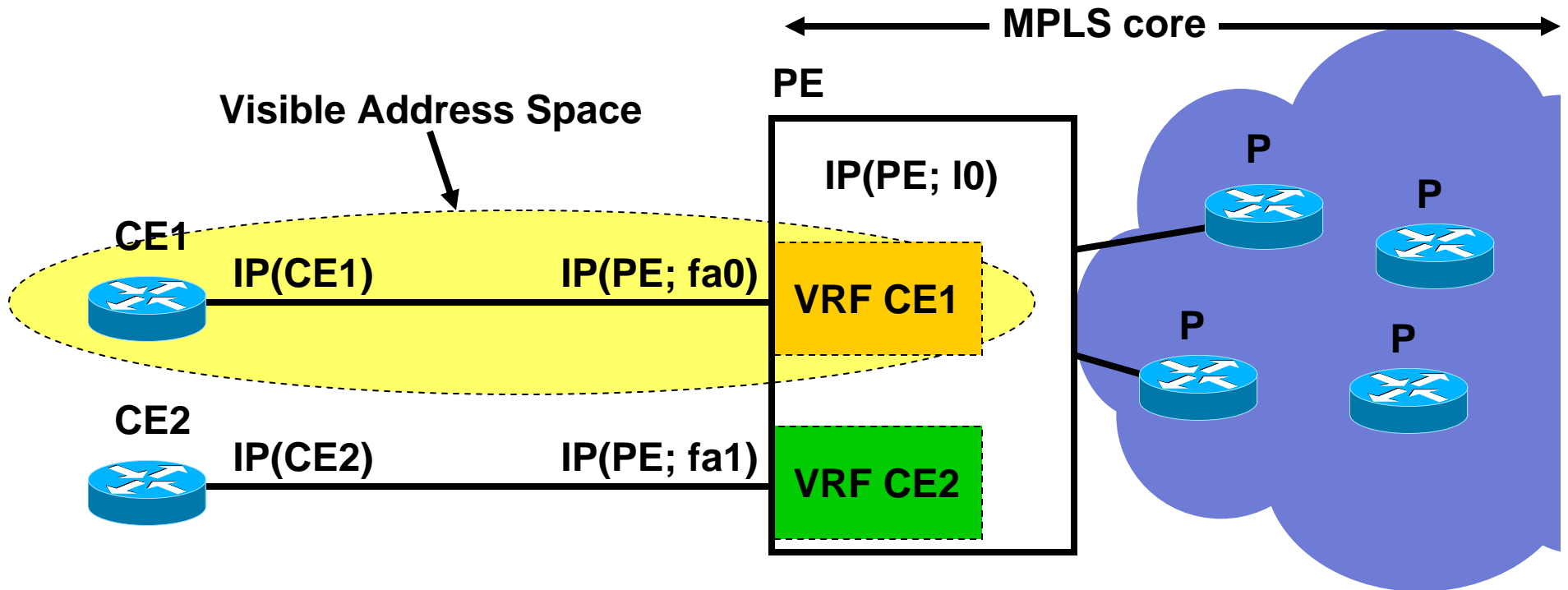


Within the MPLS core all addresses are unique due to the Route Distinguisher

Routing Separation

- **Each (sub-) interface is assigned to a VRF**
- **Each VRF has a RD (route distinguisher)**
- **Routing instance: within one RD**
 - > **within one VRF**
 - > **Routing Separation**

Hiding of the MPLS Core Structure



- VRF contains MPLS IPv4 addresses
- Only peering Interface (on PE) exposed (-> CE)!
-> ACL or unnumbered

Resistance to Attacks: Where and How?

- **Where can you attack?**

Address and Routing Separation, thus:

Only Attack point: peering PE

- **How?**

- Intrusions

(telnet, SNMP, ..., routing protocol)

- DoS

See ISP Essentials

Secure
with ACLs

Secure
with MD5

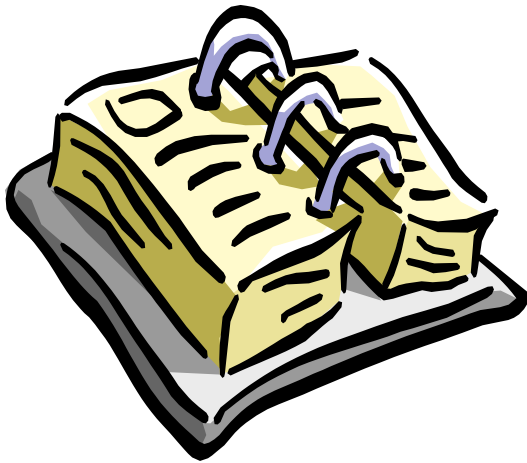
Label Spoofing

- **PE router expects IP packet from CE**
- **Labelled packets will be dropped**
- **Thus no spoofing possible**

Comparison with ATM / FR

	ATM/FR	MPLS
Address space separation	yes	yes
Routing separation	yes	yes
Resistance to attacks	yes	yes
Resistance to Label Spoofing	yes	yes
Direct CE-CE Authentication (layer 3)	yes	with IPsec

Agenda



- **Analysis of MPLS/VPN Security**
- **Security Recommendations**
- **MPLS Security Architectures**
 - Internet Access**
 - Firewalling Options**
- **Attacking an MPLS Network**
- **IPsec and MPLS**
- **Summary**

Security Recommendations for ISPs

- **Secure devices (PE, P): They are trusted!**
- **CE-PE interface: Secure with ACLs**
- **Static PE-CE routing where possible**
- **If routing: Use authentication (MD5)**
- **Separation of CE-PE links where possible (Internet / VPN)**
- **LDP authentication (MD5)**
- **VRF: Define maximum number of routes**

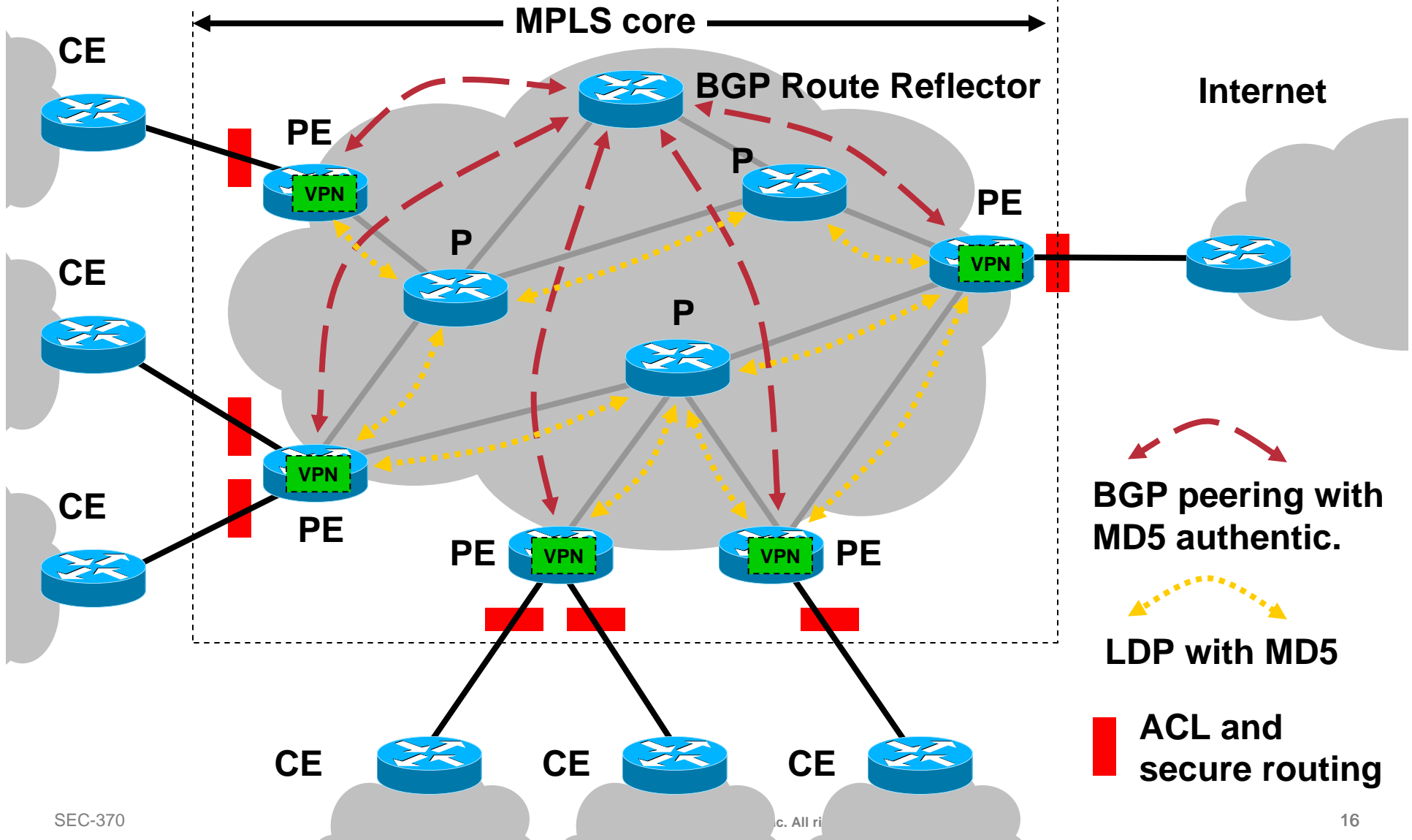
Note: Overall security depends on weakest link!

PE-CE Routing Security

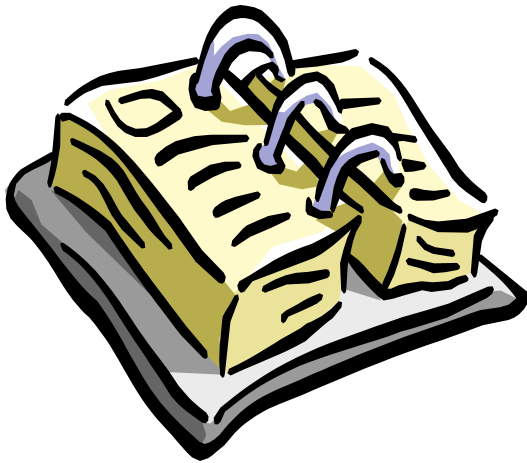
In order of security preference:

1. **Static**: If no dynamic routing required (no security implications)
2. **BGP**: For redundancy and dynamic updates (many security features)
3. **RIPv2**: If BGP not supported (limited security features)

Securing the MPLS Core



Agenda



- **Analysis of MPLS/VPN Security**
- **Security Recommendations**
- **MPLS Security Architectures**
 - Internet Access**
 - Firewalling Options**
- **Attacking an MPLS Network**
- **IPsec and MPLS**
- **Summary**

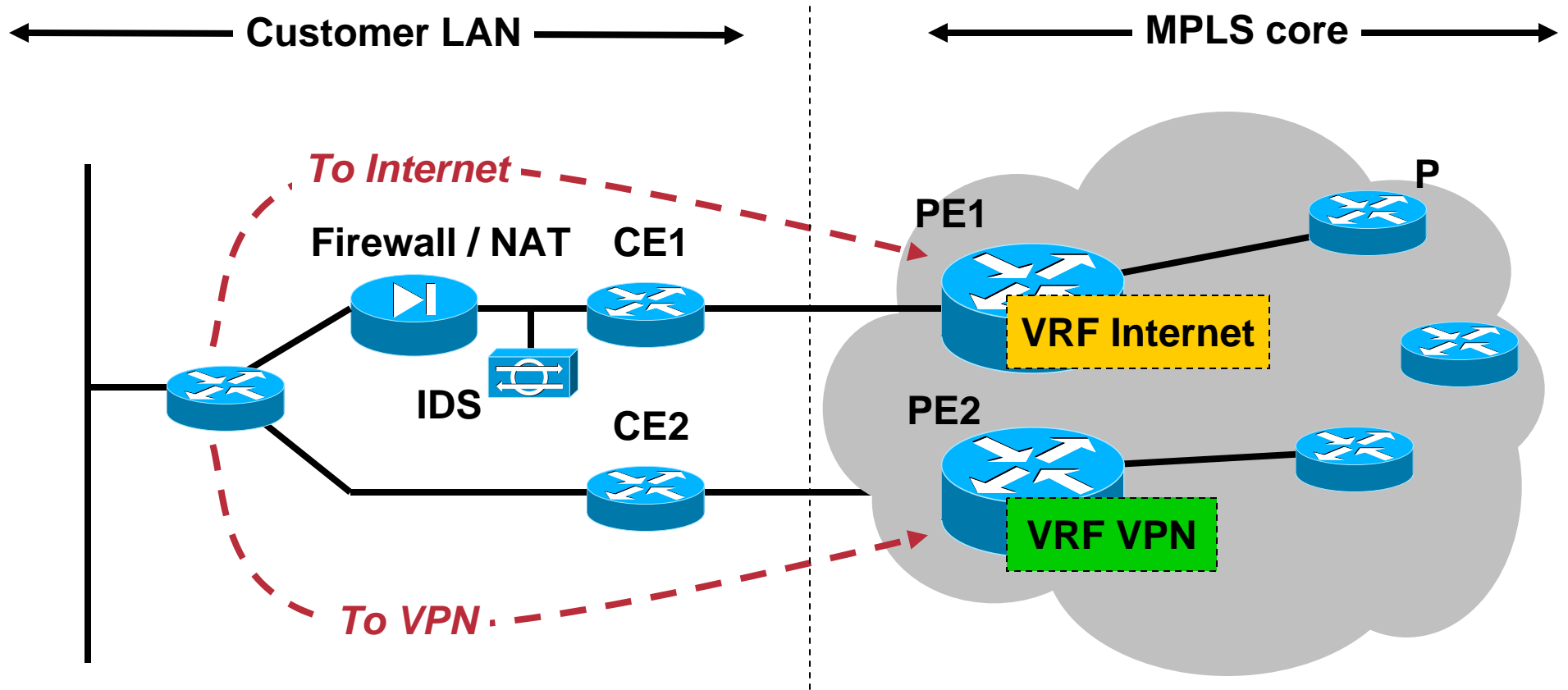
MPLS Internet Architectures: Principles

Cisco.com

- **Core supports VPNs *and* Internet**
- **VPNs remain separated**
- **Internet as an option for a VPN**
- **Essential: Firewalling**

Separate VPN and Internet Access

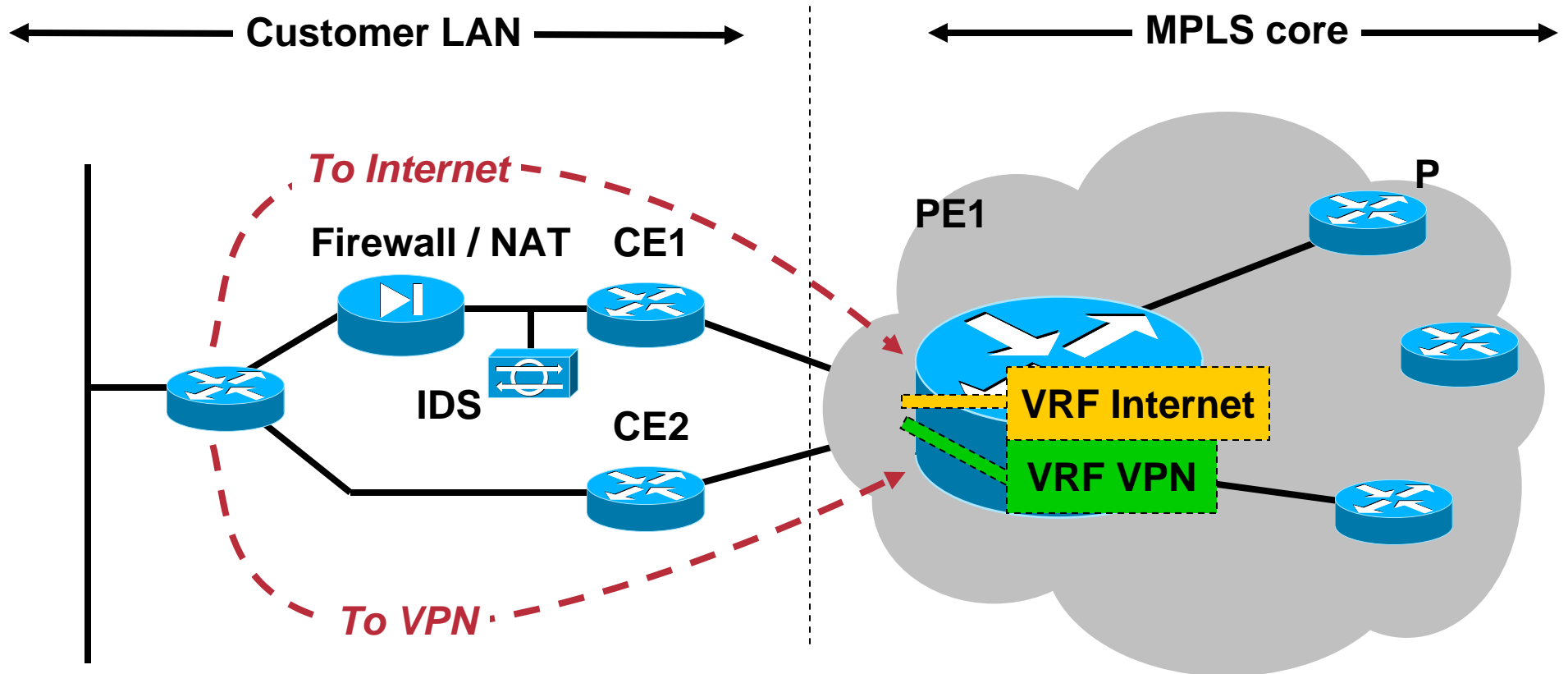
Cisco.com



- **Separation:** +++
- **DoS resistance:** +++
- **Cost:** \$\$\$ (Two lines and two PEs: Expensive!)

Separate Access Lines + CEs, one PE

Cisco.com



- **Separation:** +++
- **DoS resistance:** ++ (DoS might impact VPN on PE)
- **Cost:** \$\$ (Two lines, but only one PE)

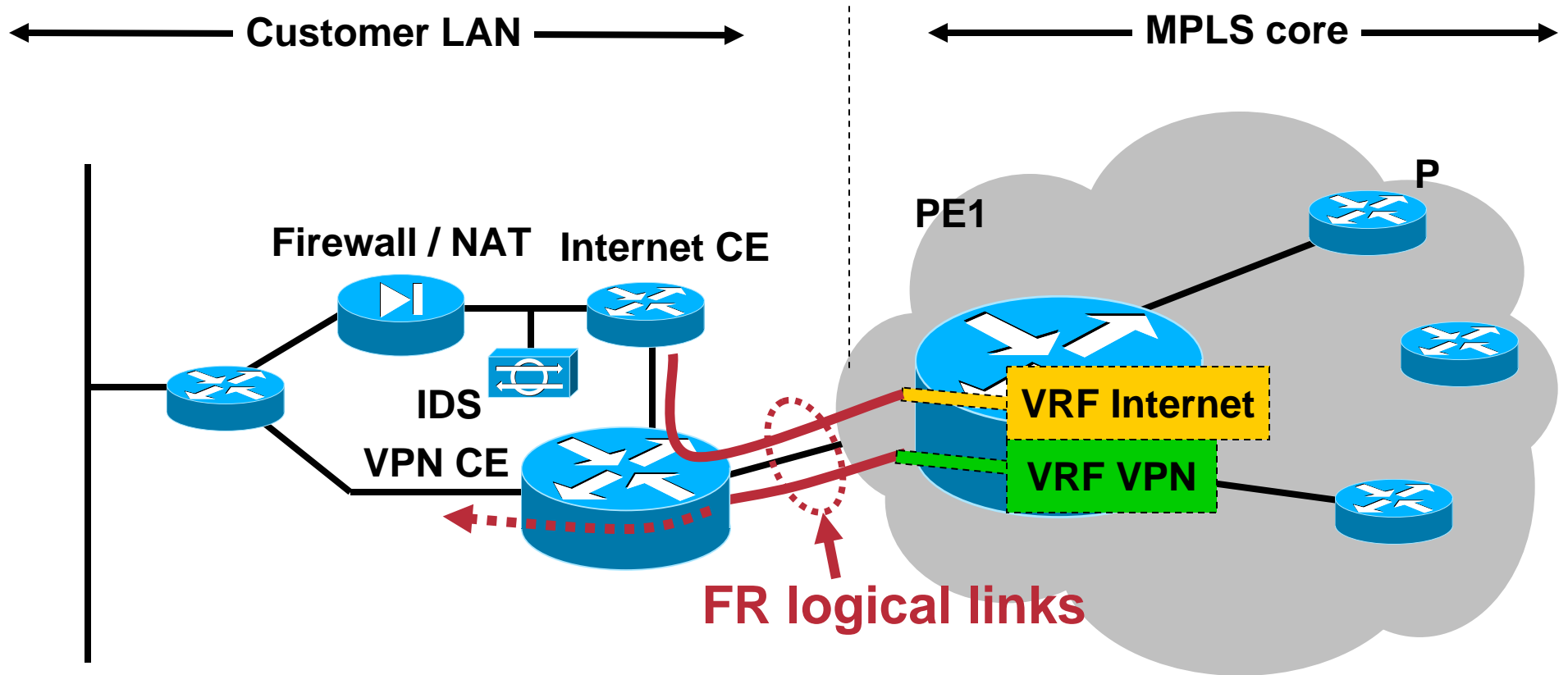
Using a Single Access Line

Requirements to share a line:

- **PE requires separate sub-interfaces**
- **CE requires separate sub-interfaces**
- **CE side requires separate routing**

Shared Access Line, Frame Relay

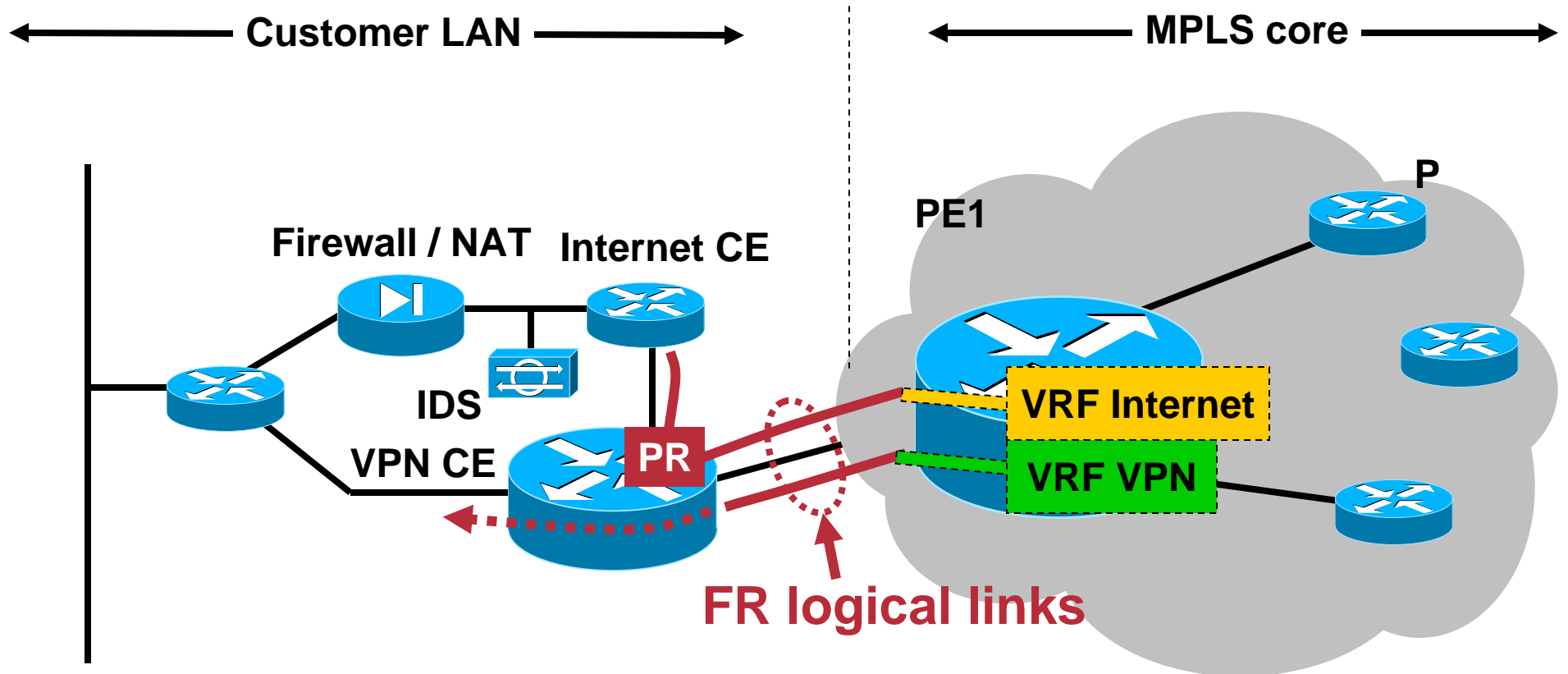
Cisco.com



- **Separation:** +++
- **DoS resistance:** + (DoS might affect VPN on PE, line, CE)
- **Cost:** \$

Shared Access Line, Policy Routing

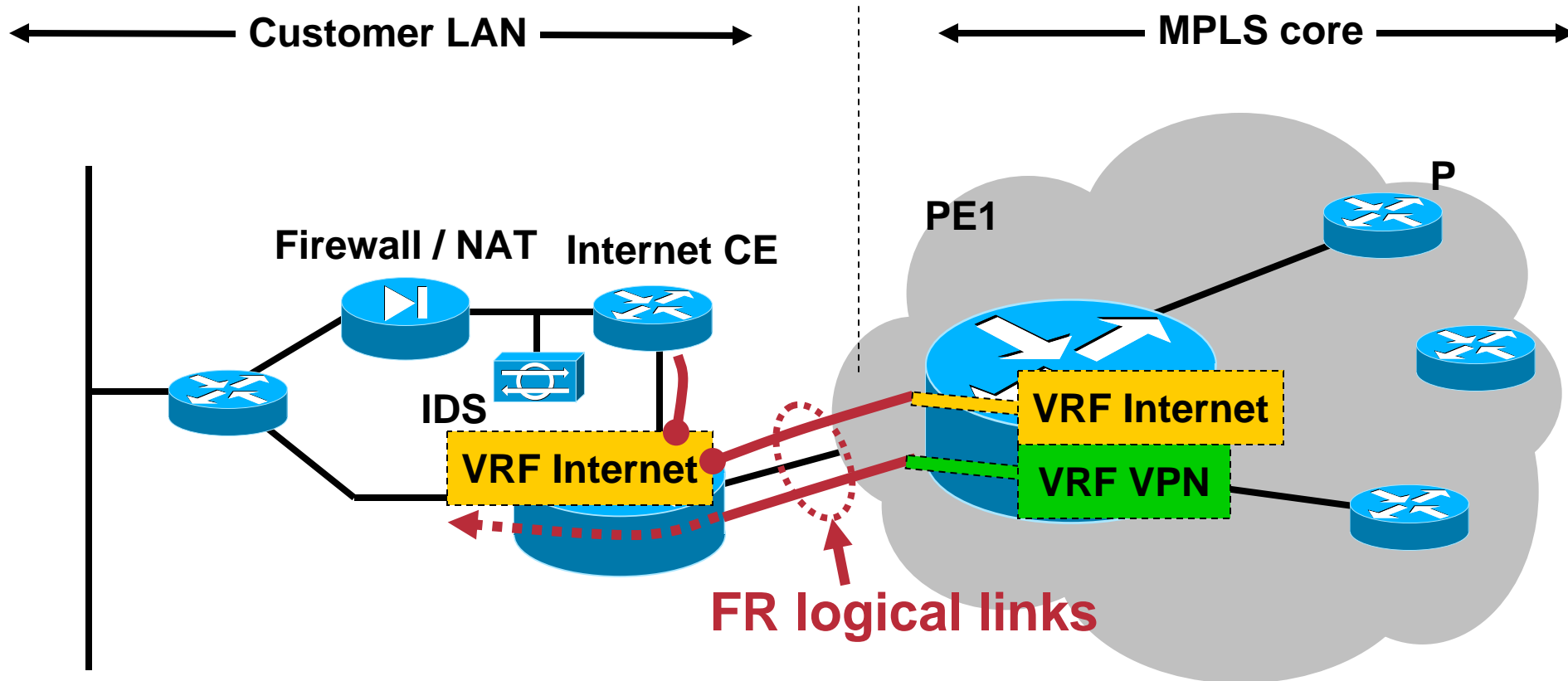
Cisco.com



- **Separation:** +++
- **DoS resistance:** + (DoS might affect VPN on PE, line, CE)
- **Cost:** \$

Shared Access Line, CE with VRFs

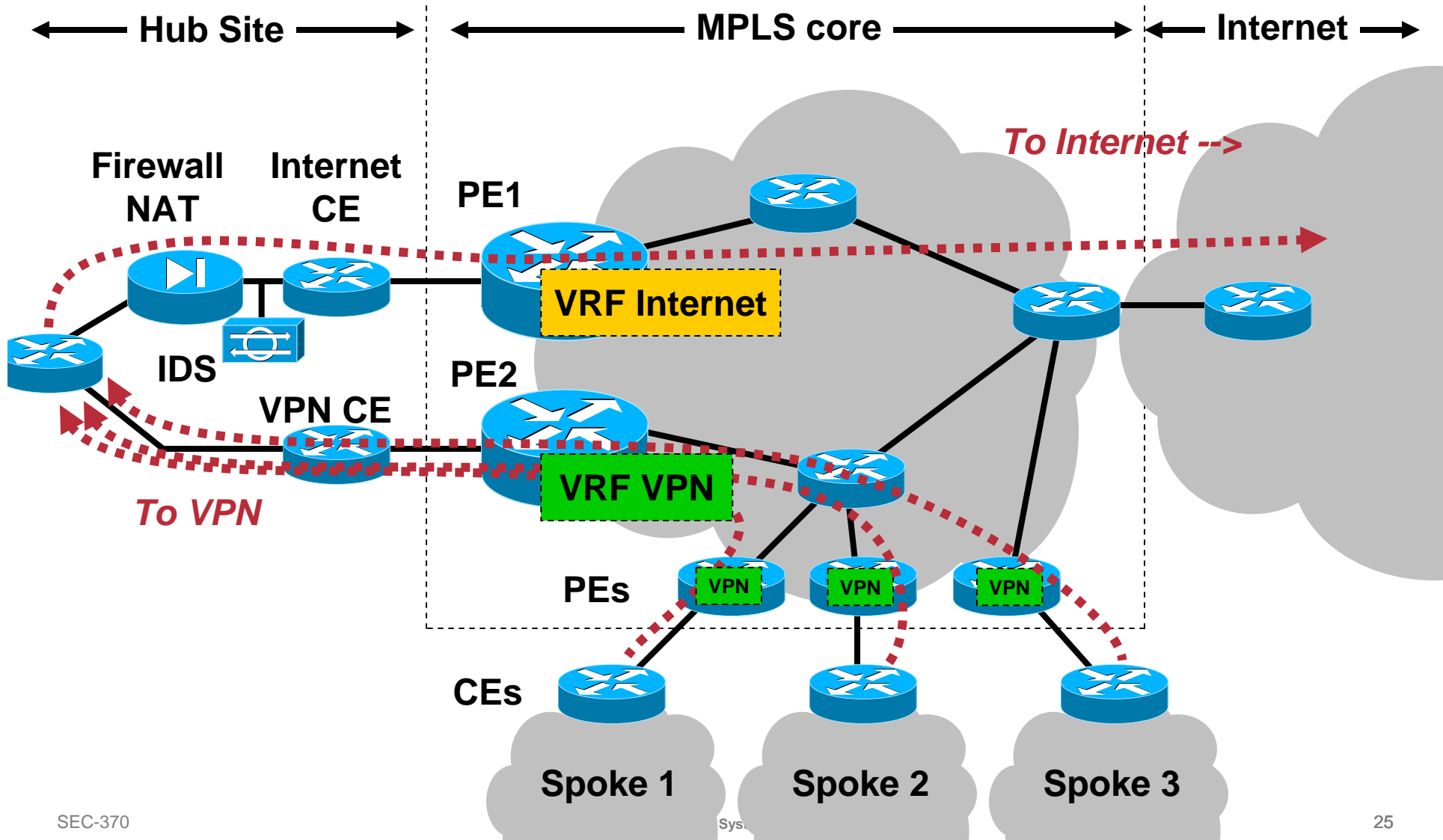
Cisco.com



- **Separation:** +++
- **DoS resistance:** + (DoS might affect VPN on PE, line, CE)
- **Cost:** \$

Hub-and-Spoke VPN with Internet Access

Cisco.com

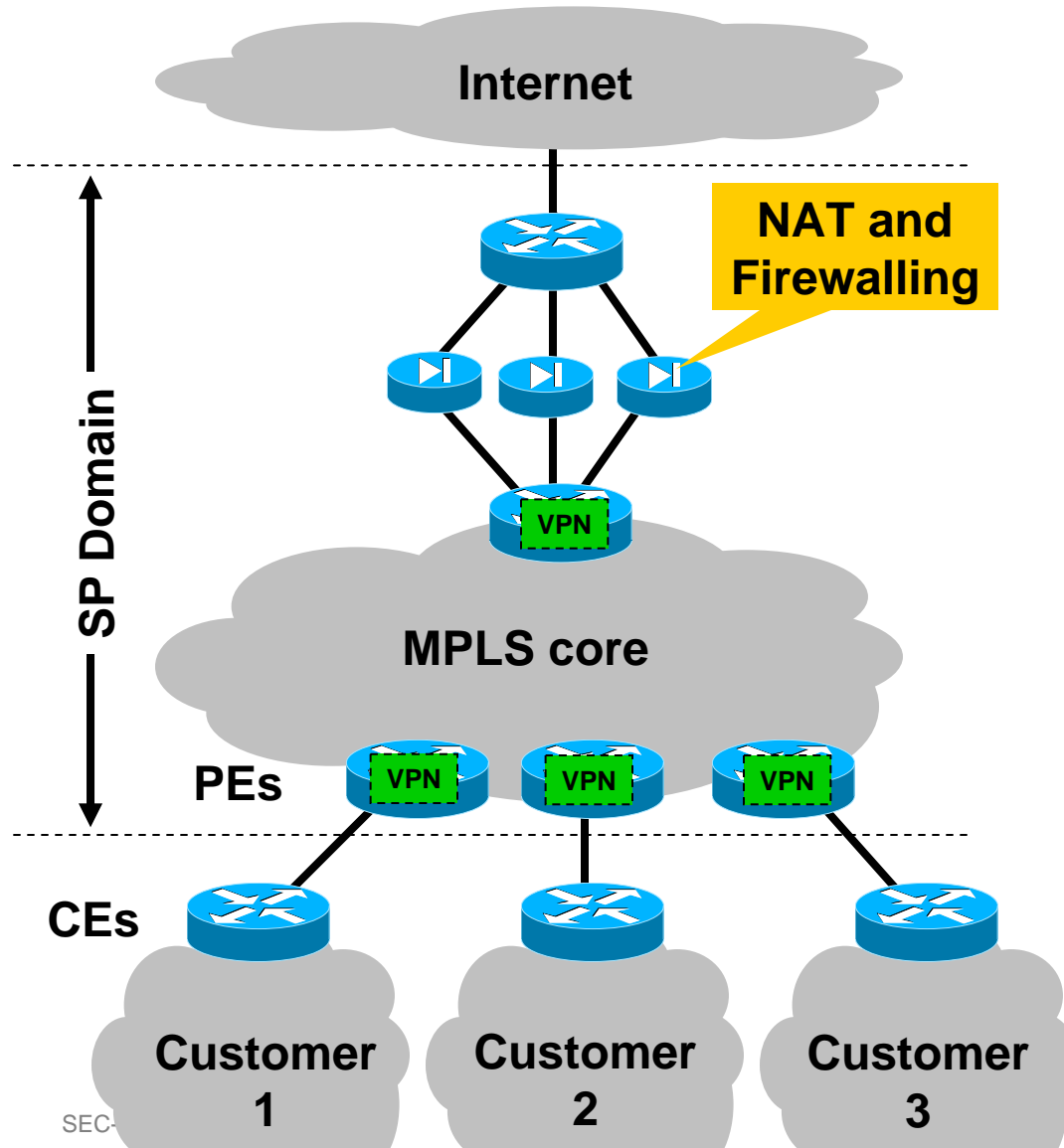


Alternative Topologies

- **Full VPN mesh, one Internet Access**
- **Internet access at several sites**
 - > **Several firewalls needed**
 - > **More complex**
- **Internet Access from all sites**
 - > **Complex, one firewall per site**

Central Firewalling: Option 1: Stacking Firewalls

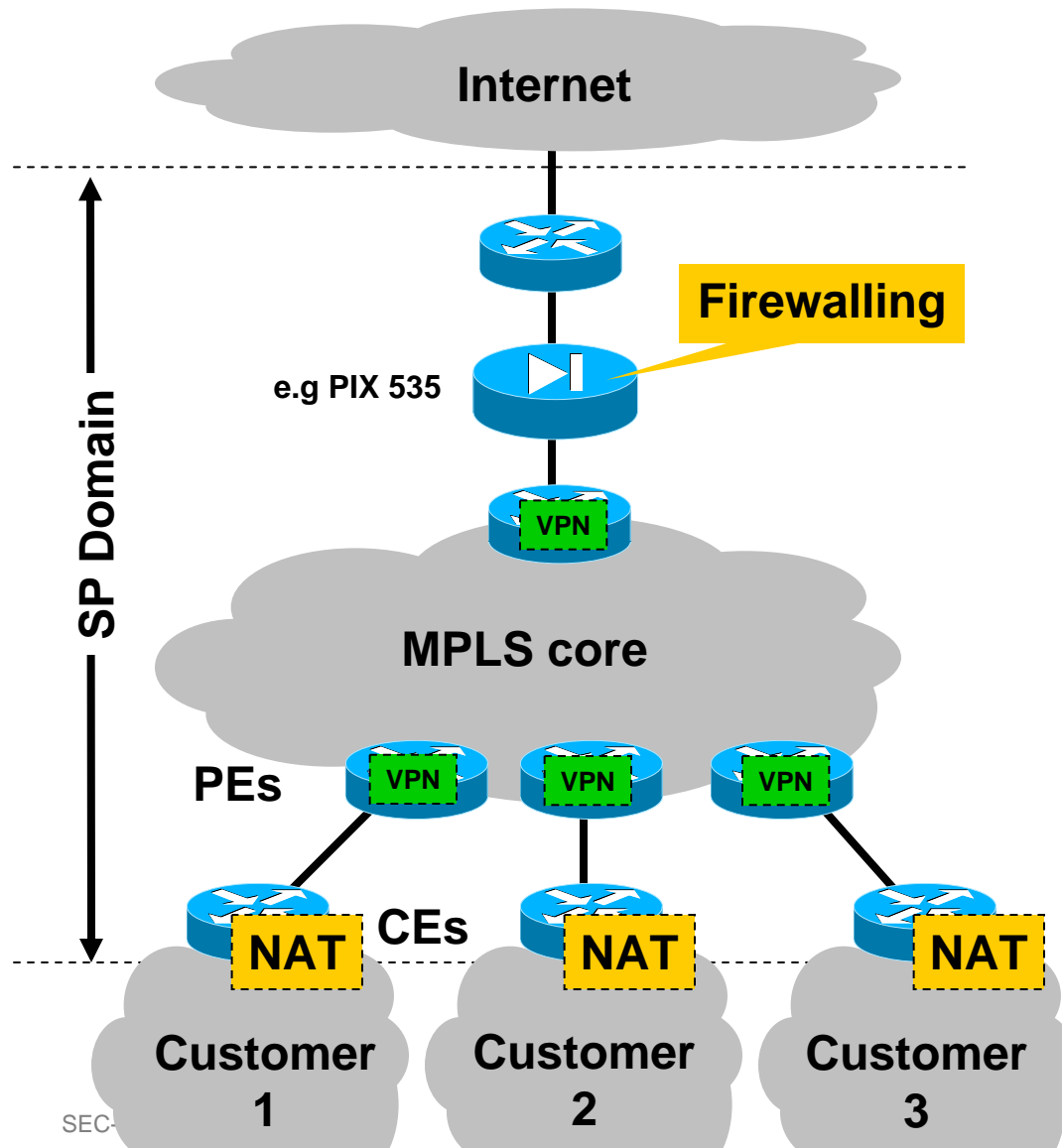
Cisco.com



- + Central Management
- + Strong firewalls
- + Customer can choose firewall
- + Different policies per customer possible
- + CEs not touched
- One firewall per customer

Central Firewalling: Option 2: NAT on CE, one central FW

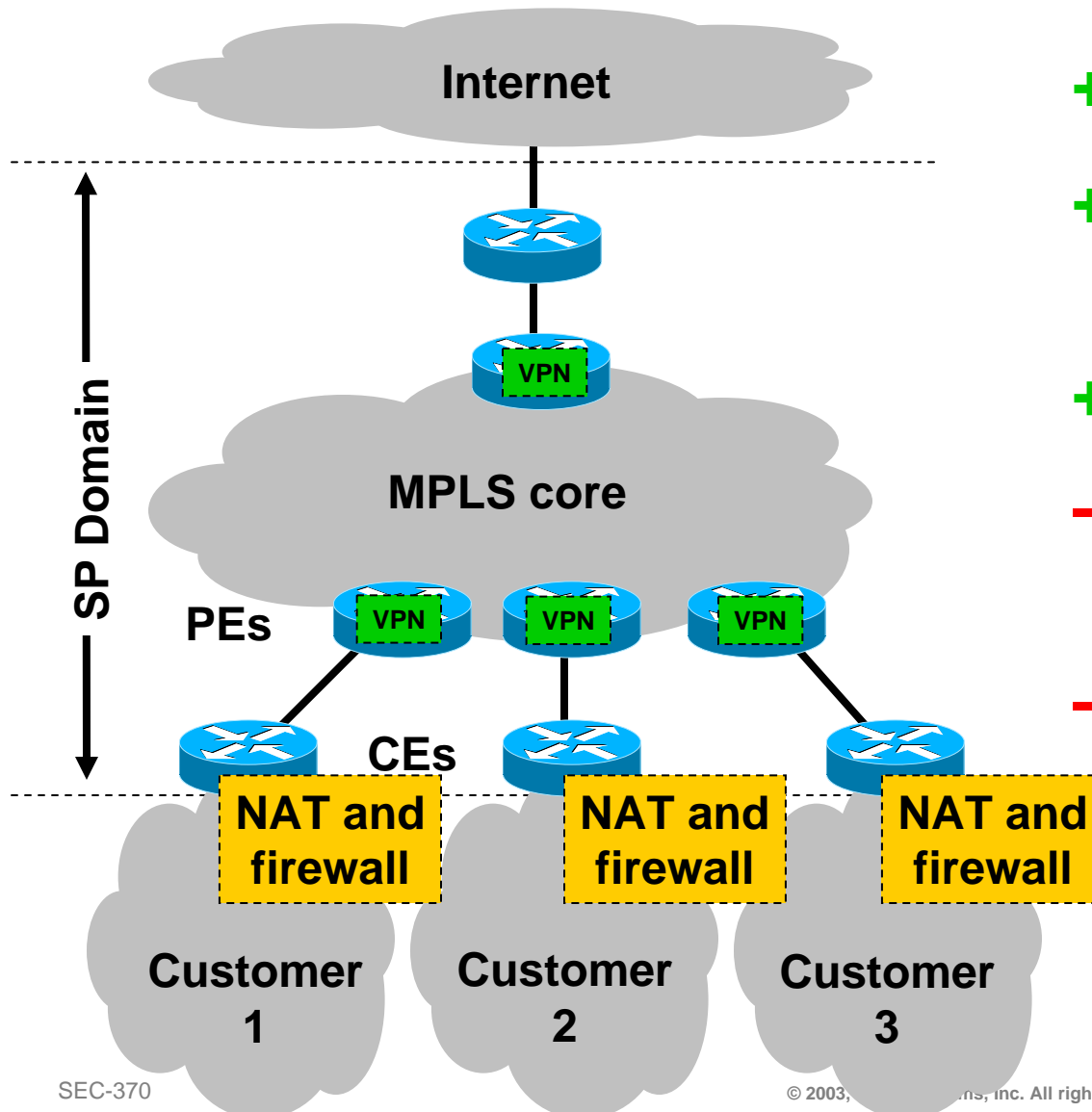
Cisco.com



- + Central Management
- + One strong firewall
- + Easy to deploy
- Customer cannot pick his firewall
- CEs need config

Central Firewalling: Option 3: IOS Firewall on CE

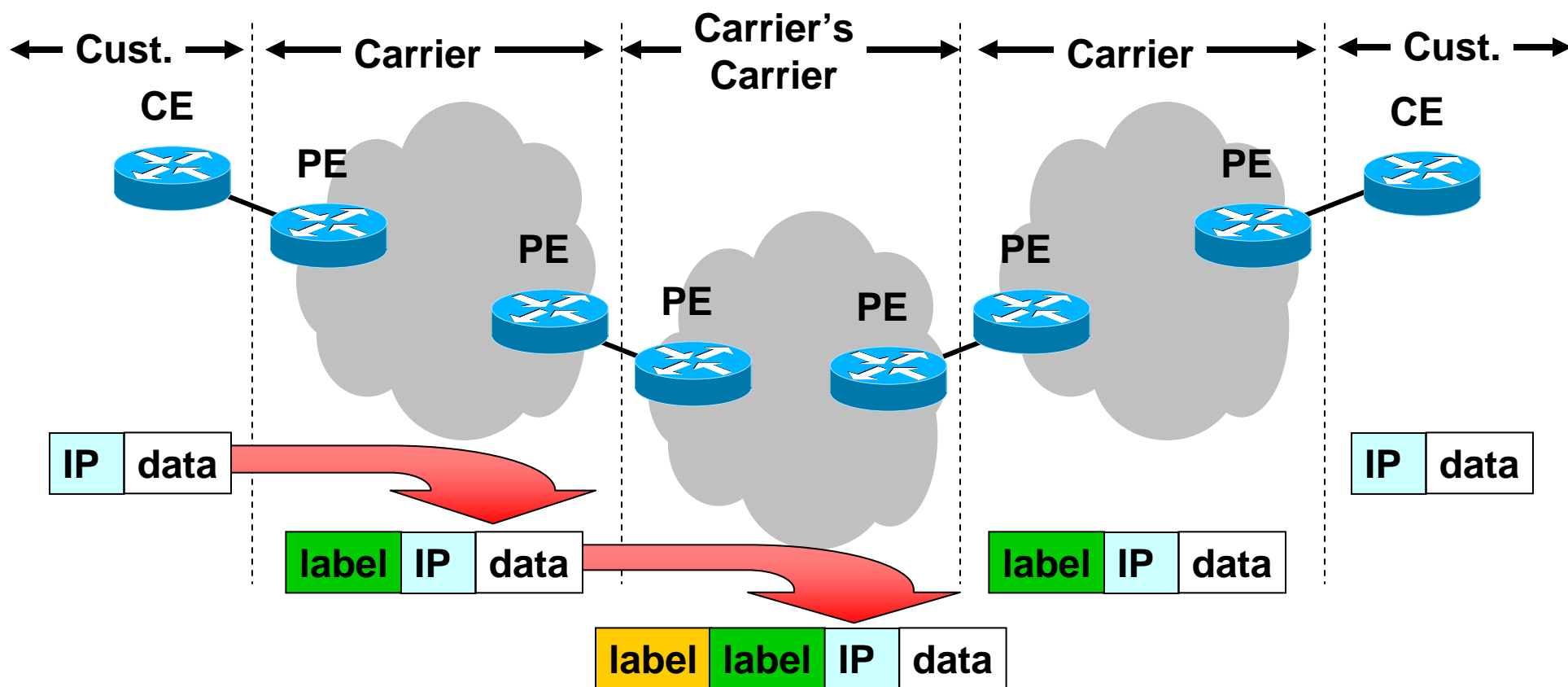
Cisco.com



- + Economic
- + One firewall per customer
- + No central devices
- Management more difficult
- CEs need config

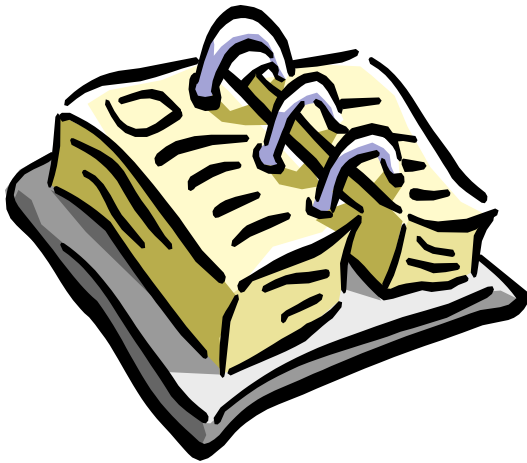
A Word on Carrier's Carrier

Cisco.com



- Same principles as in normal MPLS
- Customer trusts carrier who trusts carrier

Agenda



- **Analysis of MPLS/VPN Security**
- **Security Recommendations**
- **MPLS Security Architectures**
 - Internet Access**
 - Firewalling Options**
- **Attacking an MPLS Network**
- **IPsec and MPLS**
- **Summary**

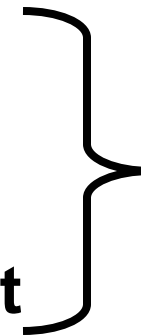
Ways to Attack

- **“Intrusion”**: Get un-authorized access

Theory: Not possible (as shown before)

Practice: Depends on:

- Vendor implementation
- Correct config and management



No Trust?



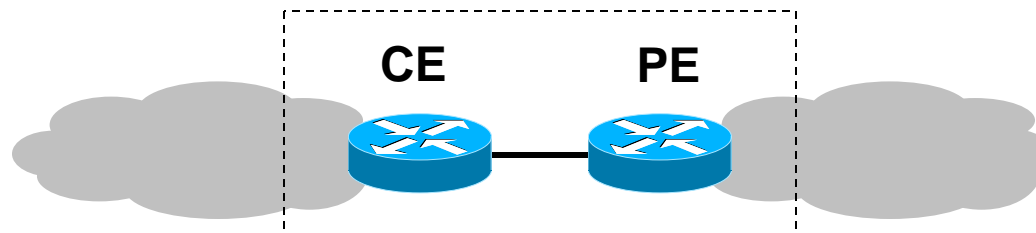
Use IPsec
between CEs!

- **“Denial-of-Service”**: Deny access of others

Much more interesting...

DoS against MPLS

- **DoS is about Resource Starvation, one of:**
 - **Bandwidth**
 - **CPU**
 - **Memory (buffers, routing tables, ...)**
- **In MPLS, we have to examine:**



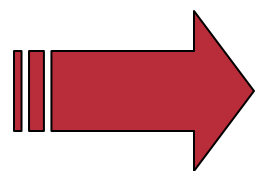
- **Rest is the same as in other networks**

Attacking a CE from MPLS (other VPN)

Cisco.com

- **Is the CE reachable from the MPLS side?**
 - > **only if this is an Internet CE, otherwise not!**
(CE-PE addressing is part of VPN!)
- **For Internet CEs:**

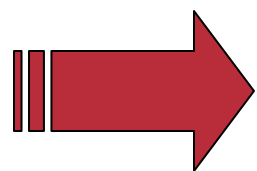
Same security rules apply as for any other access router.



MPLS hides VPN-CEs: Secure!
Internet CEs: Same as in other networks

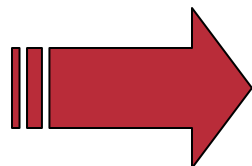
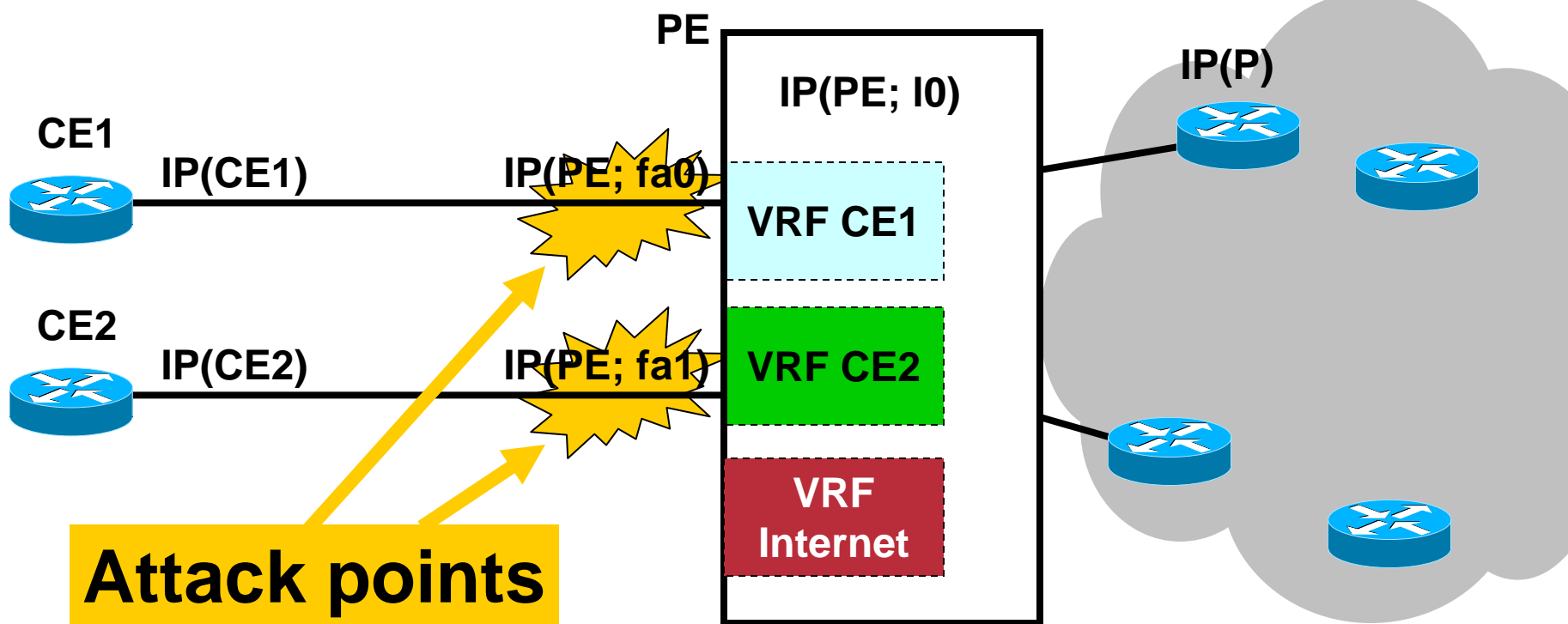
Attacking a CE-PE Line

- **Also depends on reachability of CE or the VPN behind it**
- **Only an issue for Lines to Internet-CEs**
Same considerations as in normal networks
- **If CE-PE line shared (VPN and Internet):**
DoS on Internet may influence VPN! Use CAR!



MPLS hides VPN-CEs: Secure!
Internet CEs: Same as in other networks

Attacking a PE Router



Only visible: "your" interface and interfaces of Internet CEs

DoS Attacks to PE can come from:

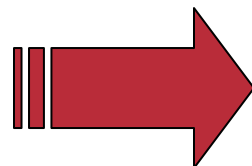
Cisco.com

- **Other VPN**, connected to same PE
- **Internet**, if PE carries Internet VRF

Possible Attacks:

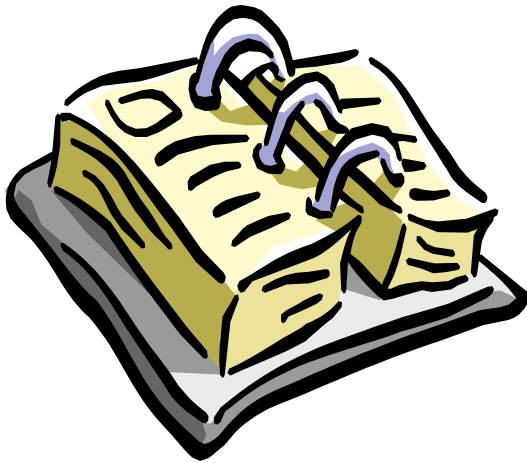
- **Resource starvation on PE**

Too many routing updates, too many SNMP requests, small servers, ...



Has to be secured

Agenda



- **Analysis of MPLS/VPN Security**
- **Security Recommendations**
- **MPLS Security Architectures**
 - Internet Access**
 - Firewalling Options**
- **Attacking an MPLS Network**
- **IPsec and MPLS**
- **Summary**

Use IPsec if you need:

- **Encryption of traffic**
 - **Direct authentication of CEs**
 - **Integrity of traffic**
 - **Replay detection**
-
- **Or: If you don't want to trust your ISP for traffic separation!**

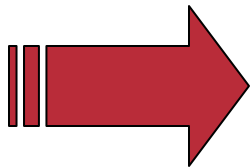
IPsec Topologies

- CE to CE (static cryptomap)
- Hub and Spoke (dynamic cryptomap)



Full Mesh with TED: Ideal!!!

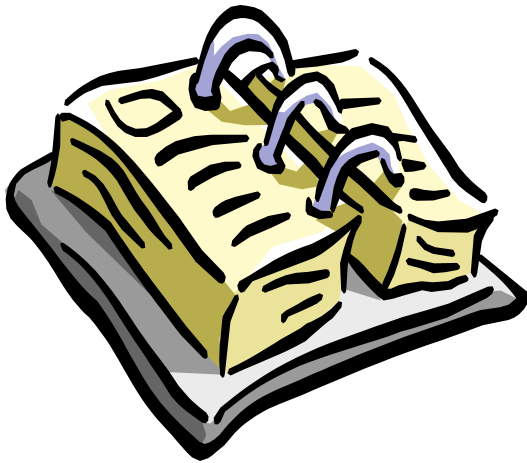
MPLS/VPN and TED are an ideal combination!!



**IPsec is independent of MPLS
IPsec and MPLS work together**

Agenda

Cisco.com



- **Analysis of MPLS/VPN Security**
- **Security Recommendations**
- **MPLS Security Architectures**
 - Internet Access**
 - Firewalling Options**
- **Attacking an MPLS Network**
- **IPsec and MPLS**
- **Summary**

MPLS doesn't provide:

- **Protection against mis-configurations in the core**
- **Protection against attacks from within the core**
- **Confidentiality, authentication, integrity, anti-replay -> Use IPsec if required**
- **Customer network security**

Conclusions

- **MPLS VPNs can be secured as well as ATM/FR VPNs**
- **Depends on correct configuration and function of the core**
- **Use IPsec if you don't trust core**
- **There are many ways to map VPNs with Internet access securely onto MPLS**

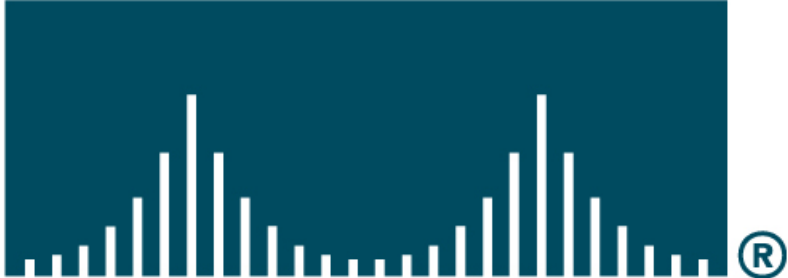
Understanding MPLS/VPN Security Issues

Session SEC-370

Please Complete Your Evaluation Form

Session SEC-370

CISCO SYSTEMS



EMPOWERING THE
INTERNET GENERATIONSM