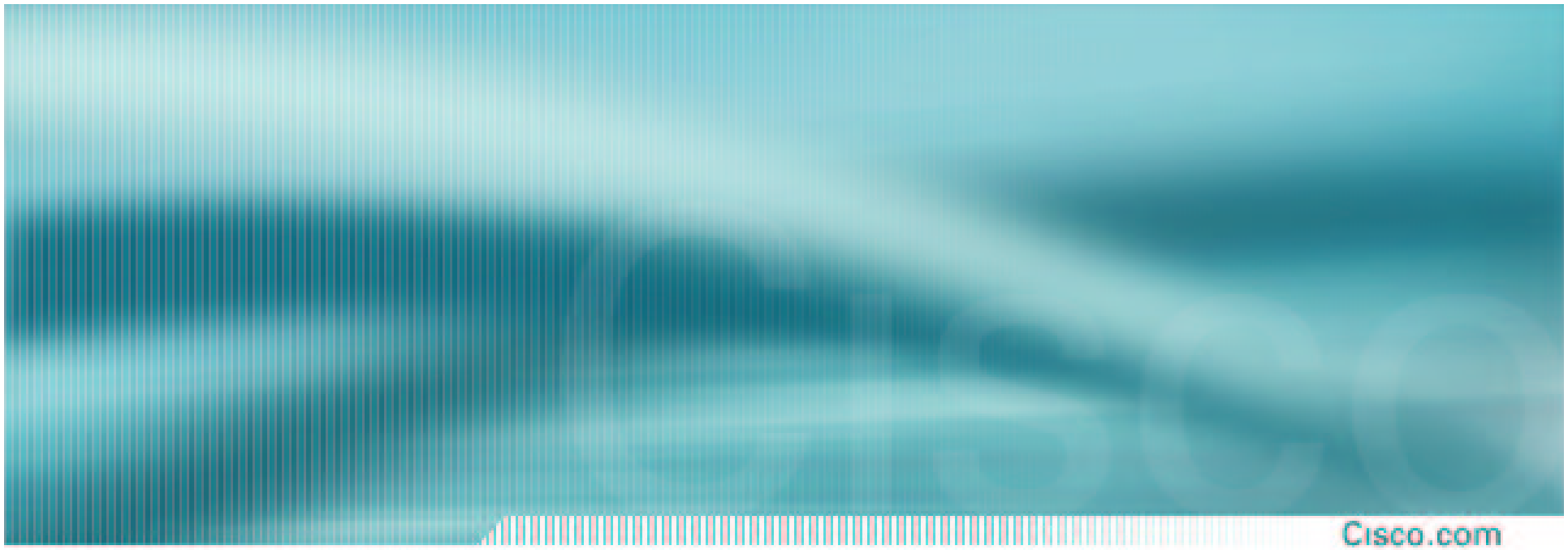
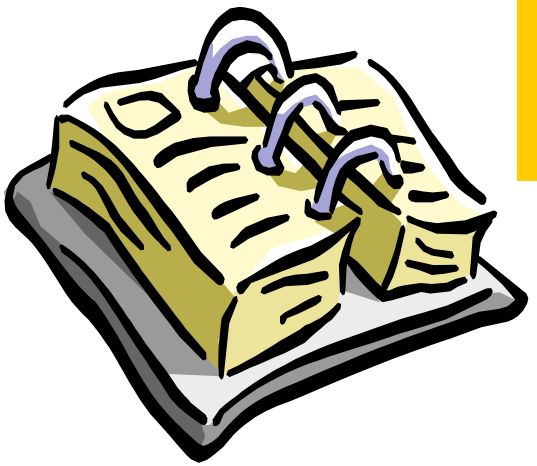

Cisco Systems



MPLS/VPN Security

Francisco Bolaños <fbolanos@cisco.com>

Agenda



- **Analysis of MPLS/VPN Security**
- **Security Recommendations**
- **MPLS Security Architectures**
  - **Internet Access**
  - **Firewalling Options**
- **Summary**

The Principle: A "Virtual Router"

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

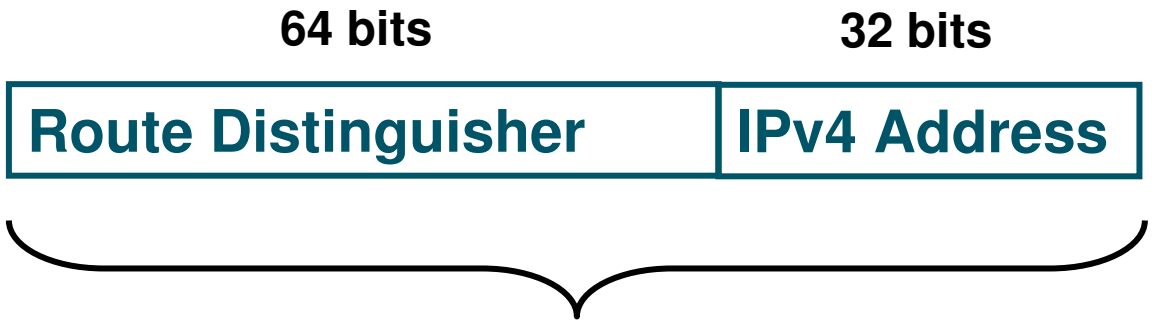
Assign Interface to "Virtual Router"

General VPN Security Requirements

- 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

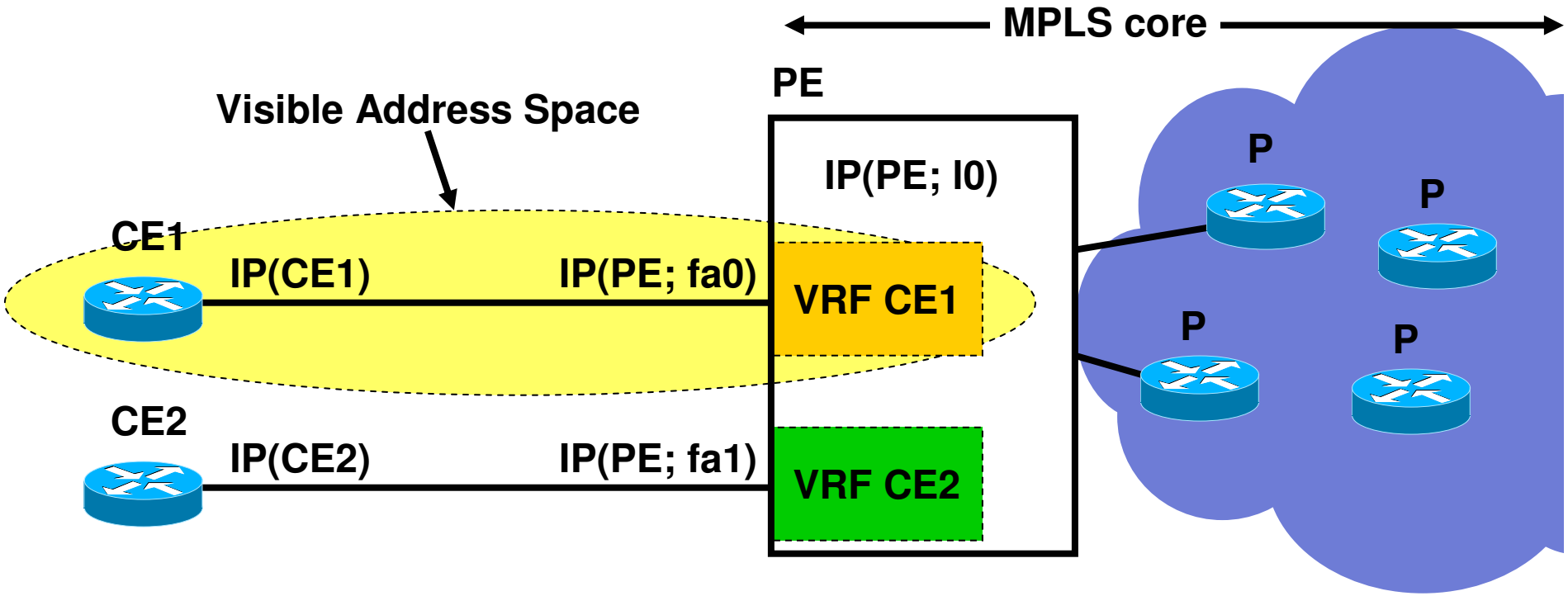
Routing Separation

Cisco.com

- 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

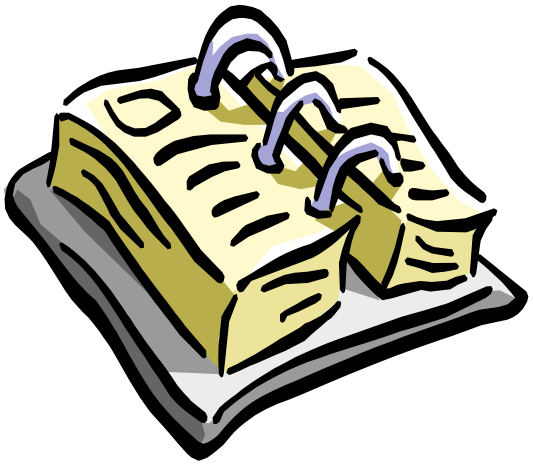
Label Spoofing

- 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
- Summary

Security Recommendations for ISPs

Cisco.com

- 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

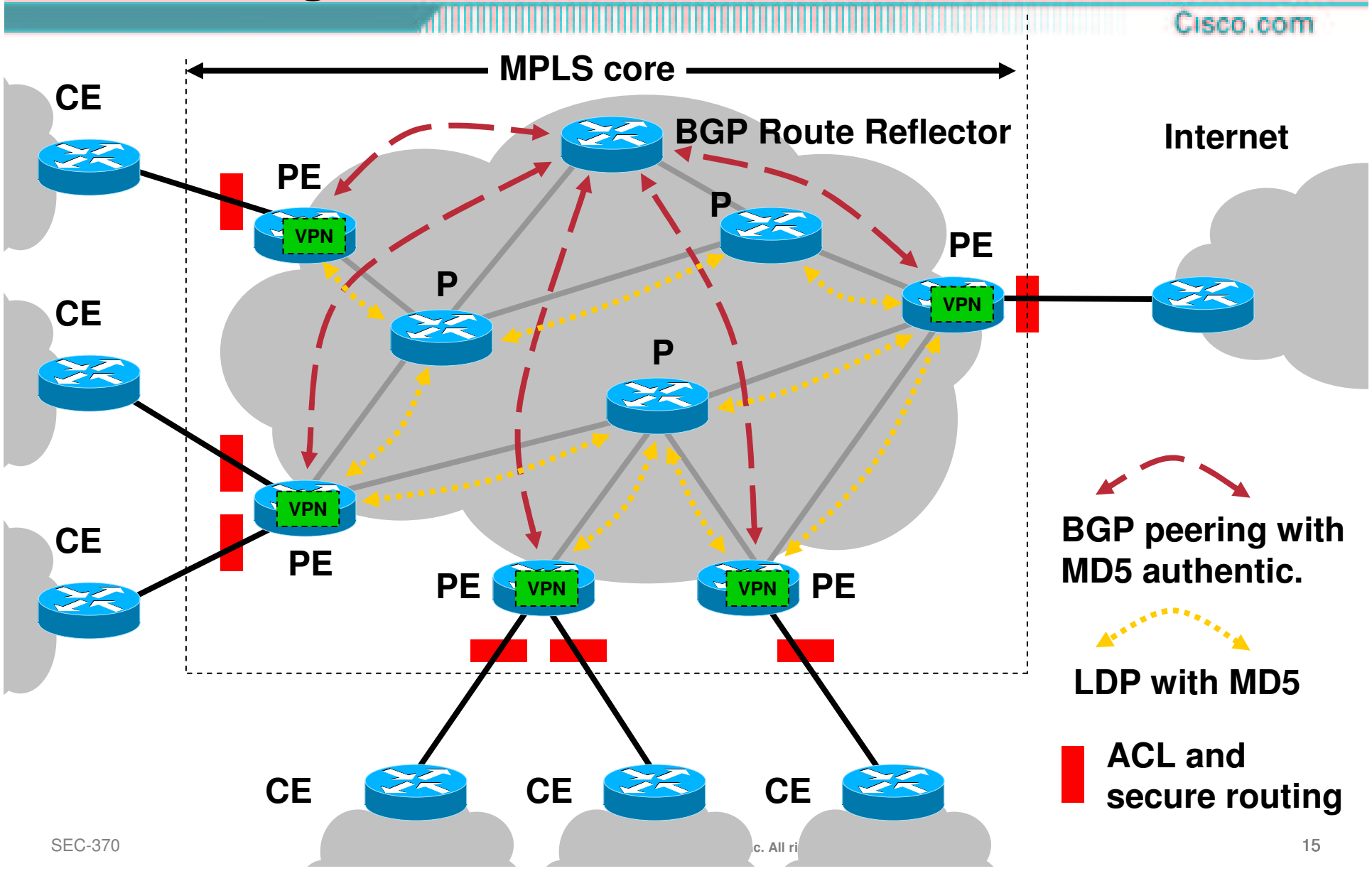
Note: Overall security depends on weakest link!

PE-CE Routing Security

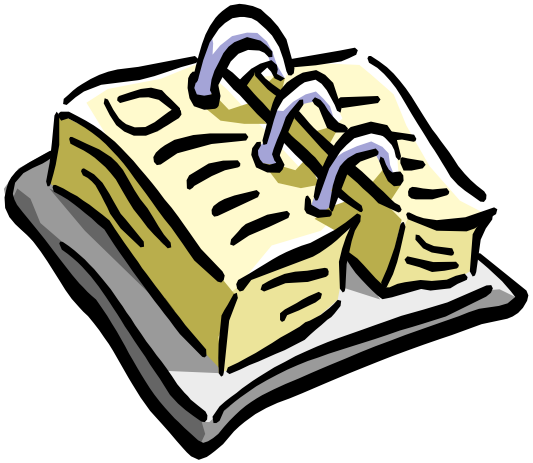
In order of security preference:

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



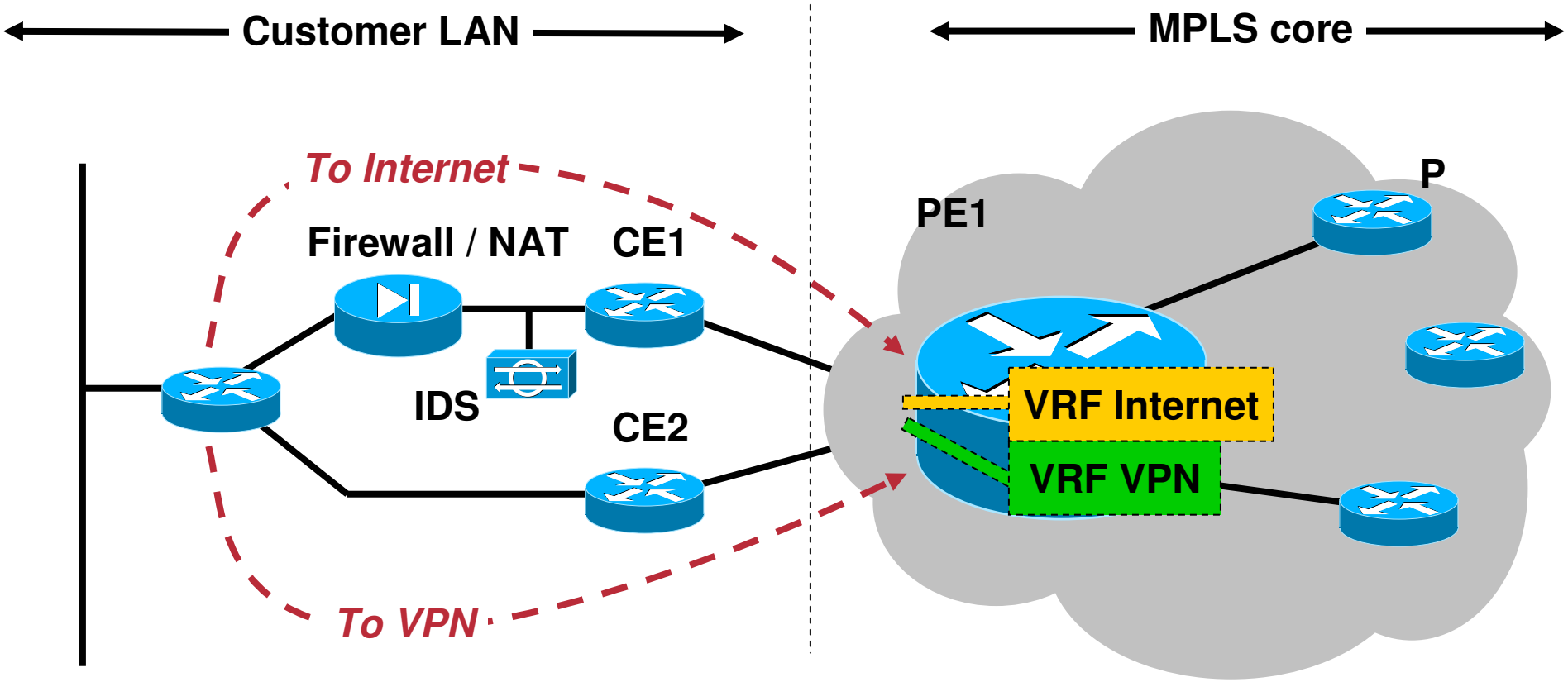
Agenda



- Analysis of MPLS/VPN Security
- Security Recommendations
- MPLS Security Architectures
  - Internet Access
  - Firewalling Options
- Summary

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

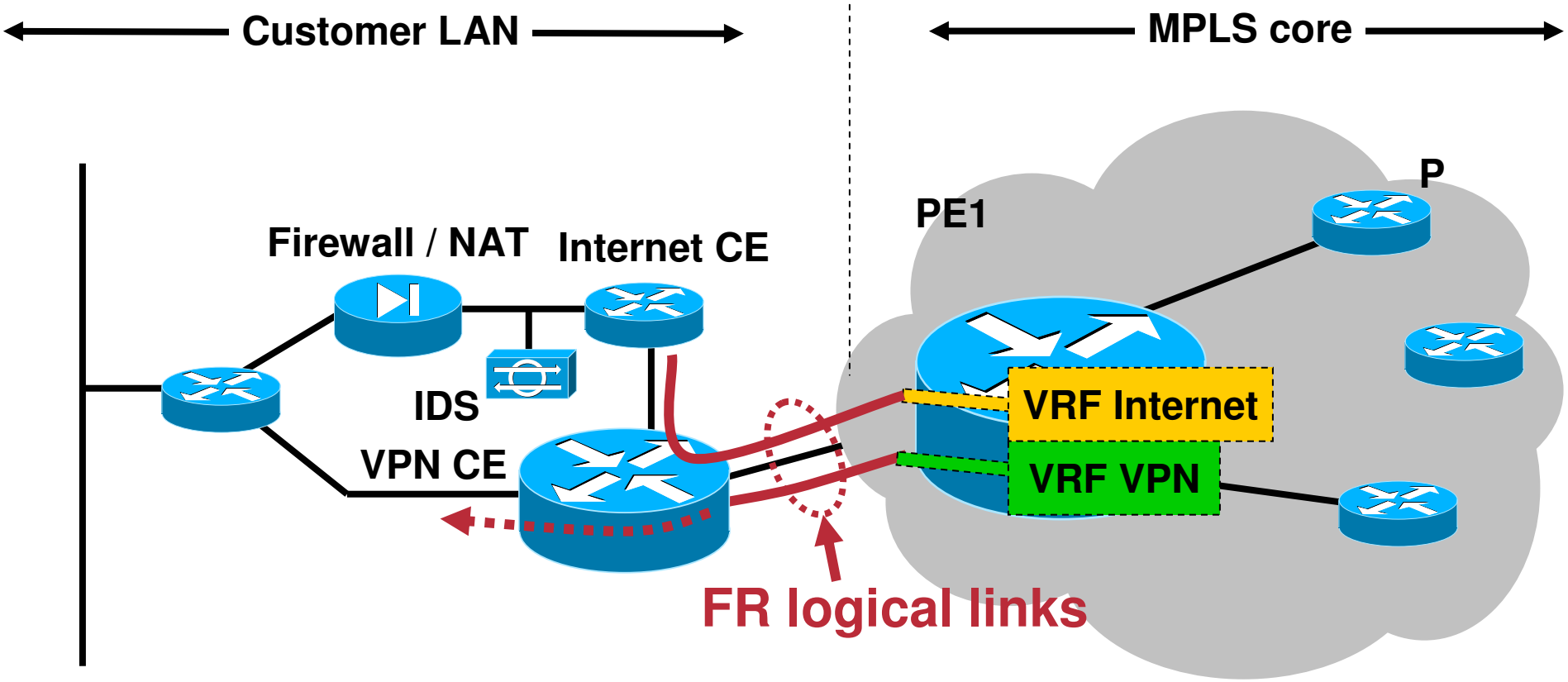
Cisco.com

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

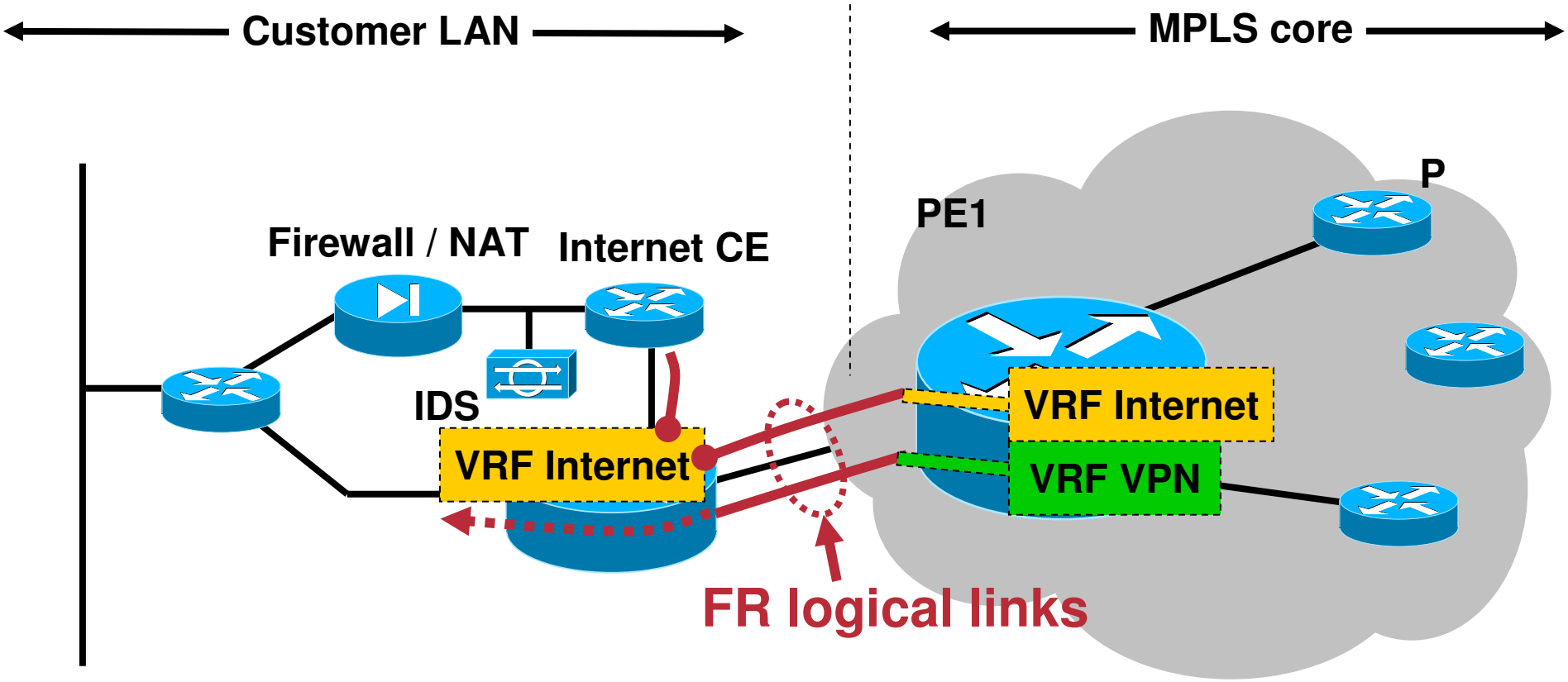
Cisco.com



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

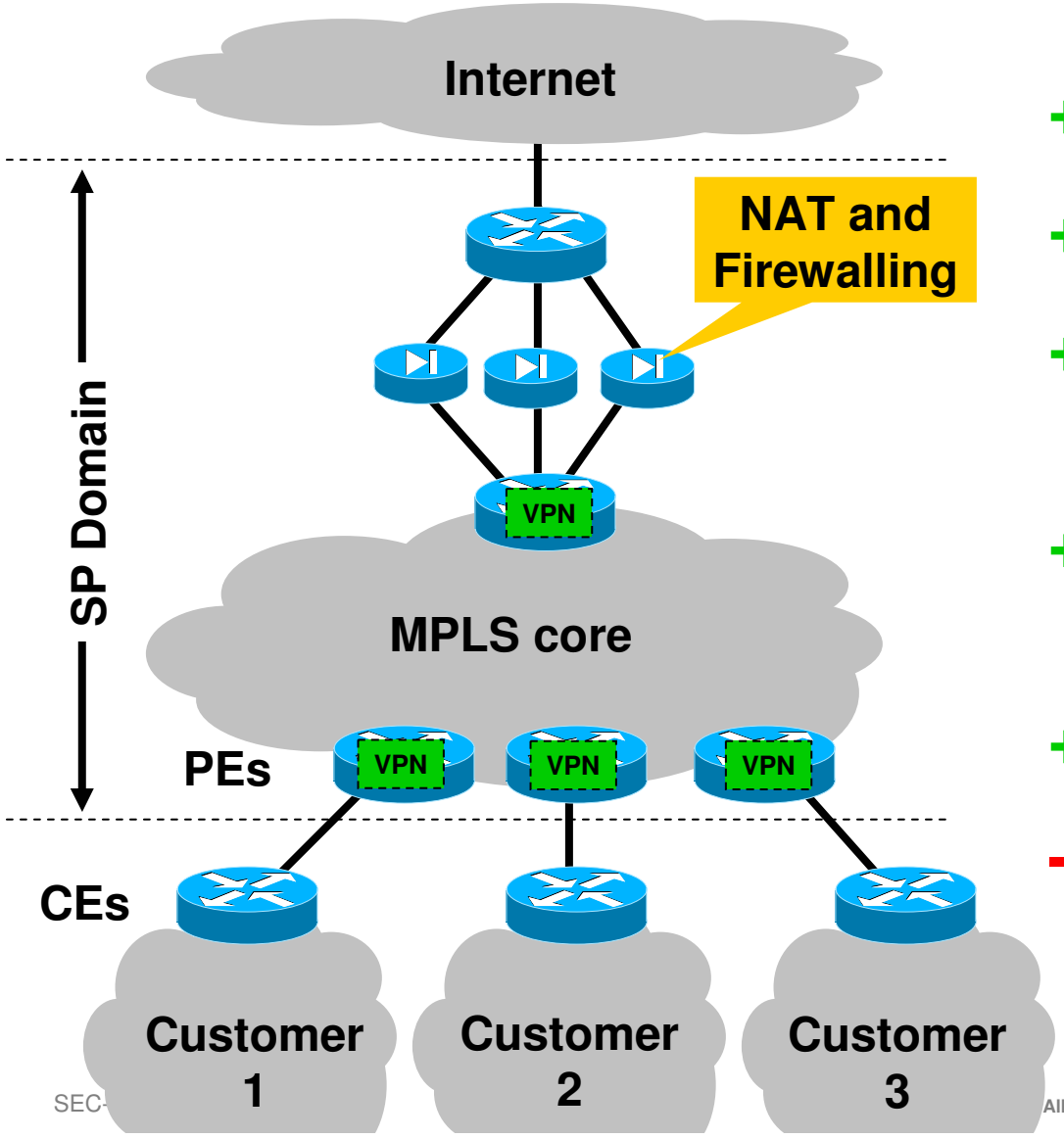
Shared Access Line, CE with VRFs

Cisco.com



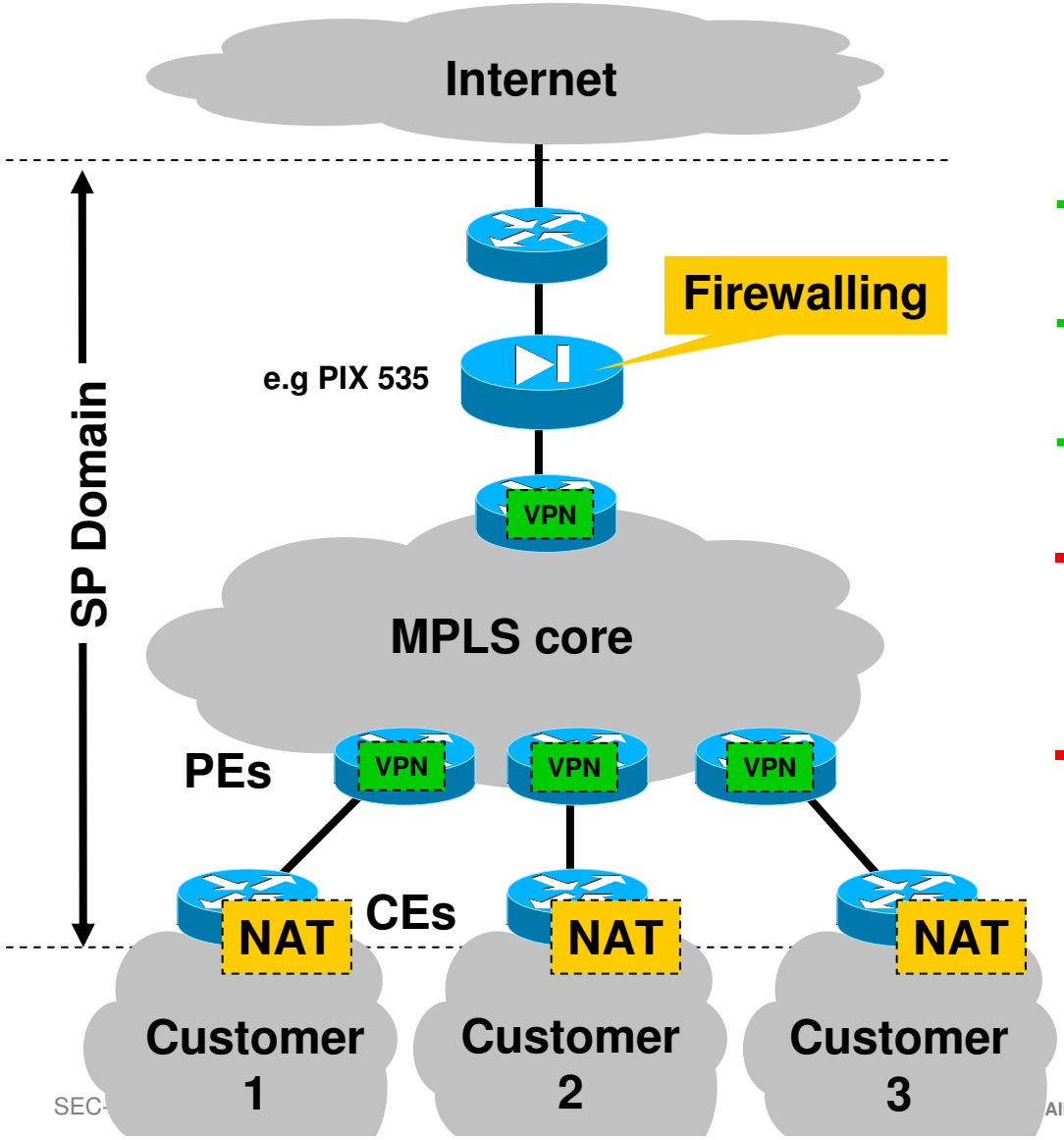
- **Separation:** +++
- **DoS resistance:** + (DoS might affect VPN on PE, line, CE)
- **Cost:** $

Central Firewalling: Option 1: Stacking Firewalls



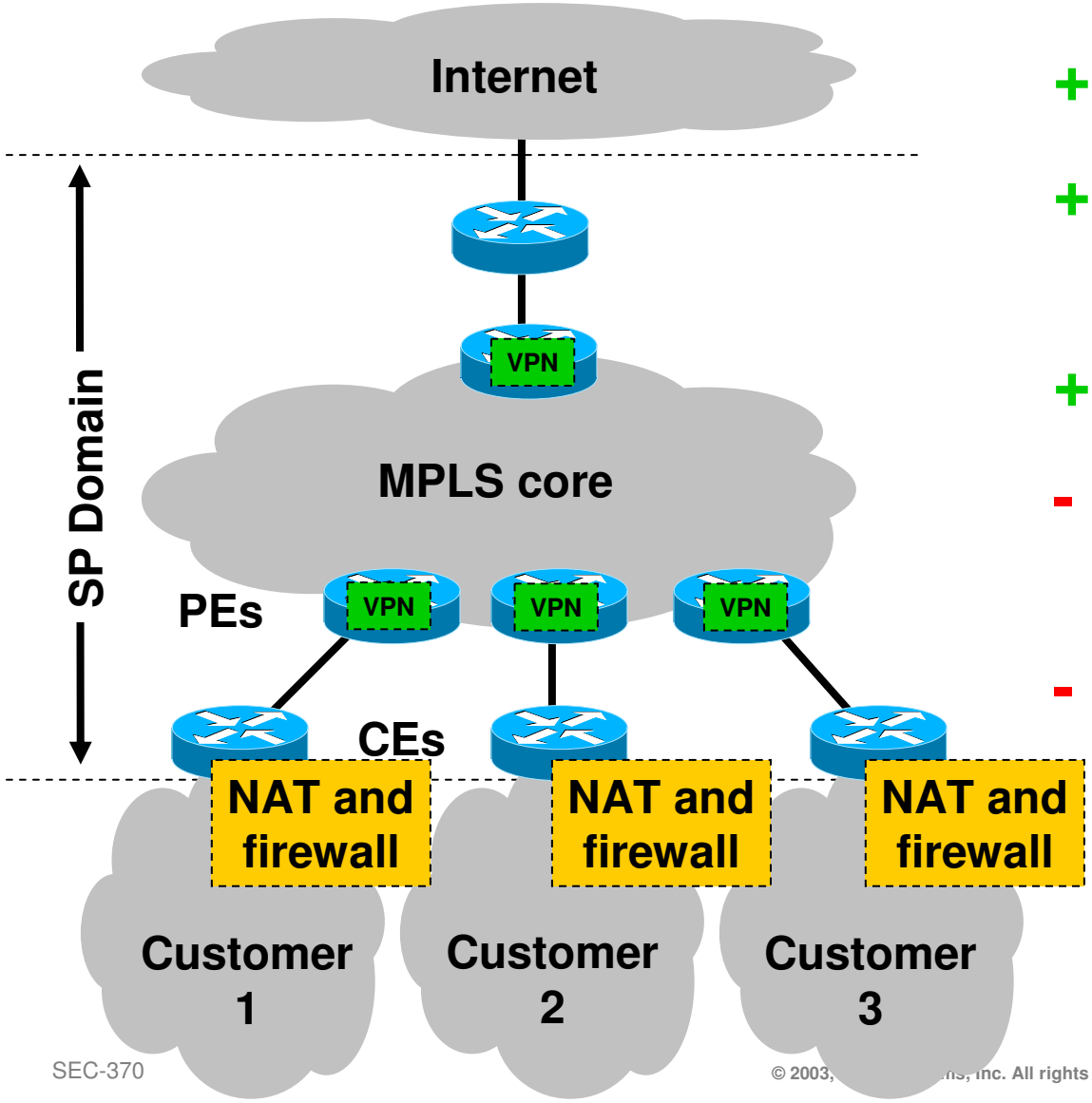
+ Central Management
+ Strong firewalls
+ Customer can choose firewall
+ Different policies per customer possible
+ CEs not touched
- One firewall per customer

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



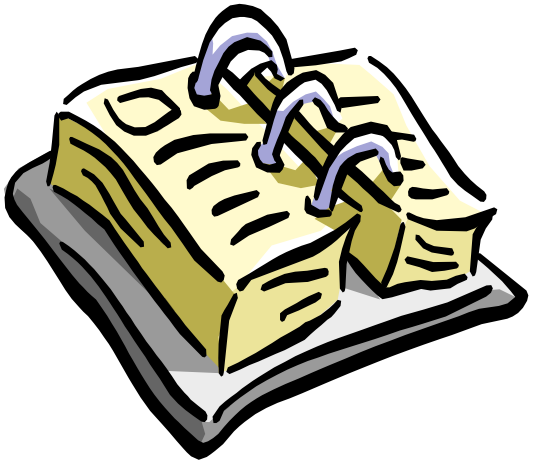
+ Central Management
+ One strong firewall
+ Easy to deploy
- Customer cannot pick his firewall
- CEs need config

Central Firewalling: Option 3: IOS Firewall on CE



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

Agenda



- Analysis of MPLS/VPN Security
- Security Recommendations
- MPLS Security Architectures
  - Internet Access
  - Firewalling Options
- 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