MPLS VPN Security in Service Provider Networks

Peter Tomsu

Michael Behringer

Monique Morrow

About this Presentation

- Advanced level

  "… advanced MPLS concepts and architectures."

- Target Audience:

  Service provider!!

  Network operators and designers

  Technical focus

Why Is MPLS VPN Security Important?

- Customer buys “Internet Service”:
  - Packets from SP are not trusted
  - Perception: Need for firewalls, etc.
- Customer buys a “VPN Service”:
  - Packets from SP are trusted
  - Perception: No further security required

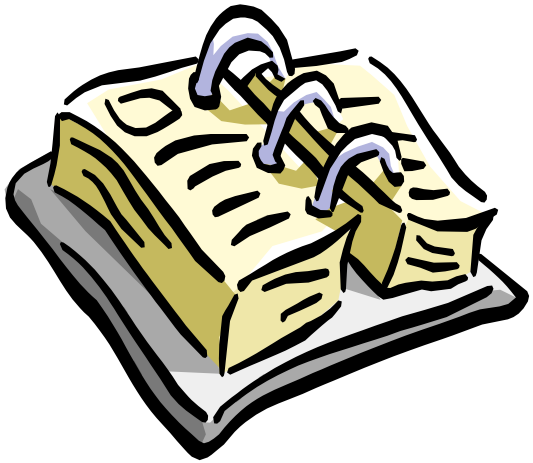
SP Must Ensure Secure MPLS Operations

Objectives

- Understand how secure MPLS VPNs* are
  - And what IPsec offers in addition
- Best practices on how to secure
  - General MPLS VPN deployments
  - Inter-provider VPN
  - Specific cases (Internet, etc)

*** Here: MPLS VPN = RFC 4364 (old RFC 2547bis)**

MPLS VPN Security _ Agenda



- Analysis of the Architecture
- Secure MPLS VPN Design
  - General Best Practices
  - Internet Access
  - Inter-AS and CsC
- IPsec and MPLS
- Outlook
- Summary

Analysis of the MPLS VPN Architecture

(RFC 4364)

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

Basic RFC 4364 Security: Today's Arguments

- Can be mis-configured (operation)
- Routers can have bugs (implementation)

True, but same on ATM/FR

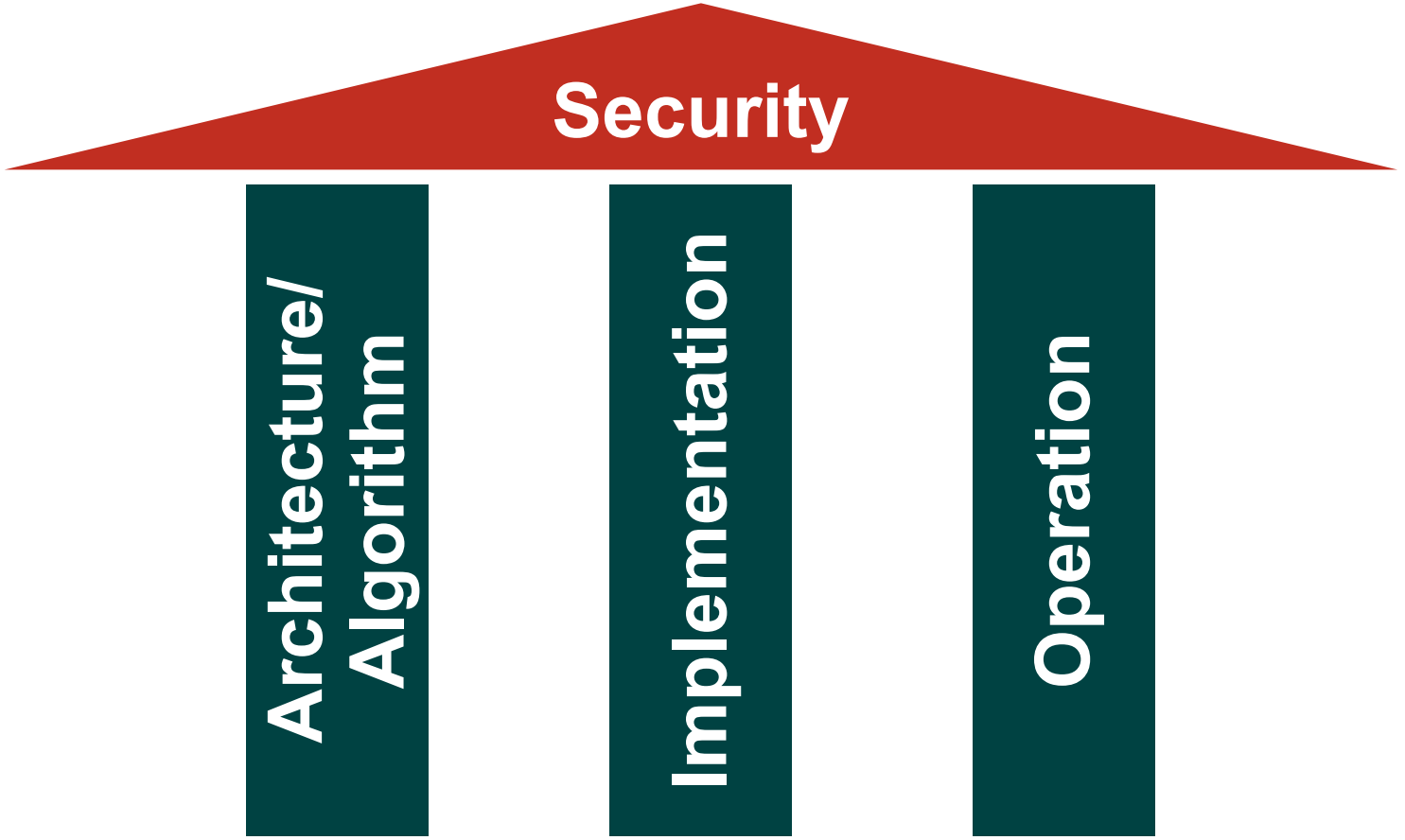
- PEs can be accessed from Internet, thus intrinsically insecure

PEs can be secured, as Internet routers

- Floods over Internet can impact VPN traffic

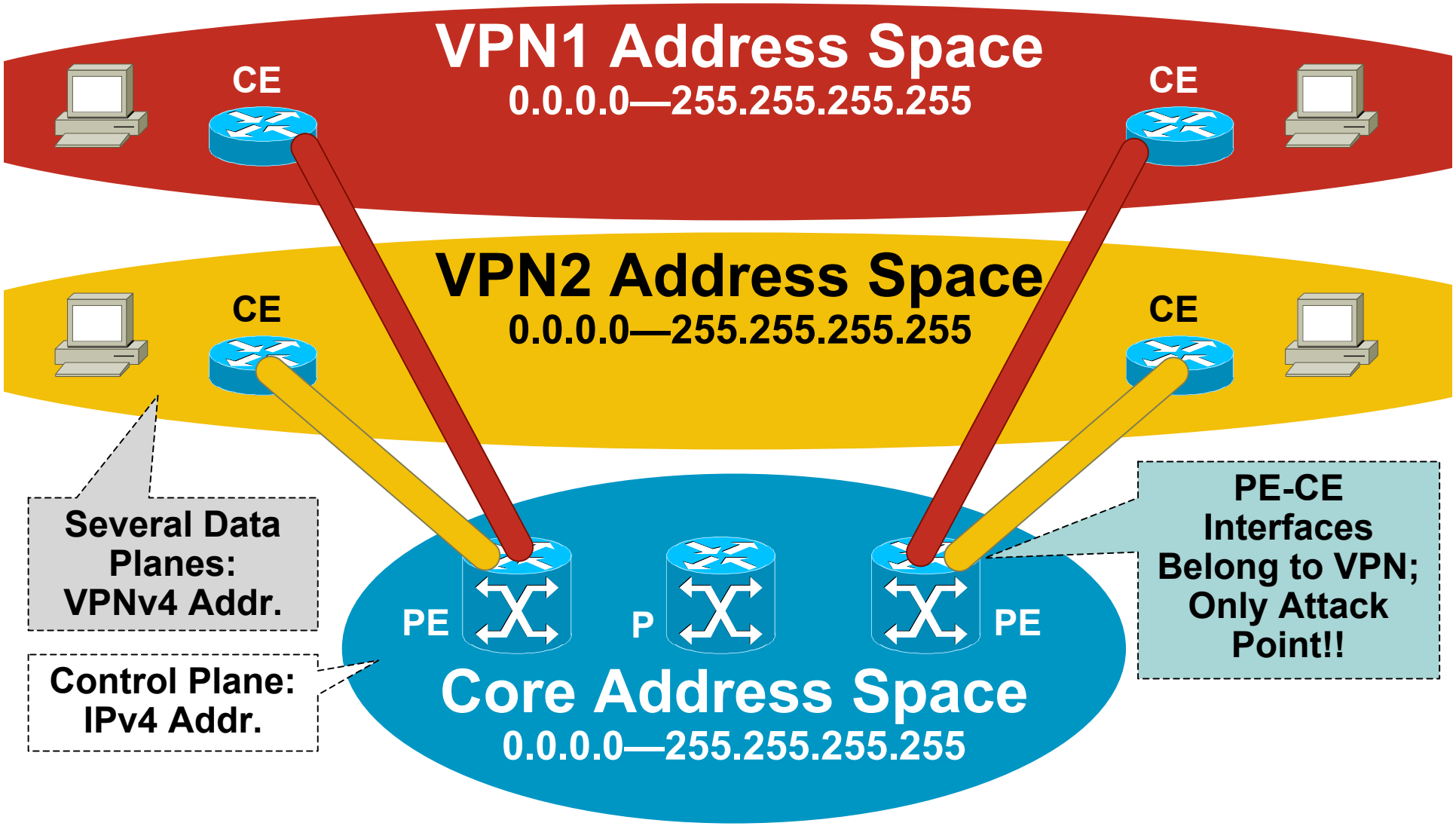
Engineering/QoS

Security Relies on Three Pillars



Break One, and All Security Is Gone!

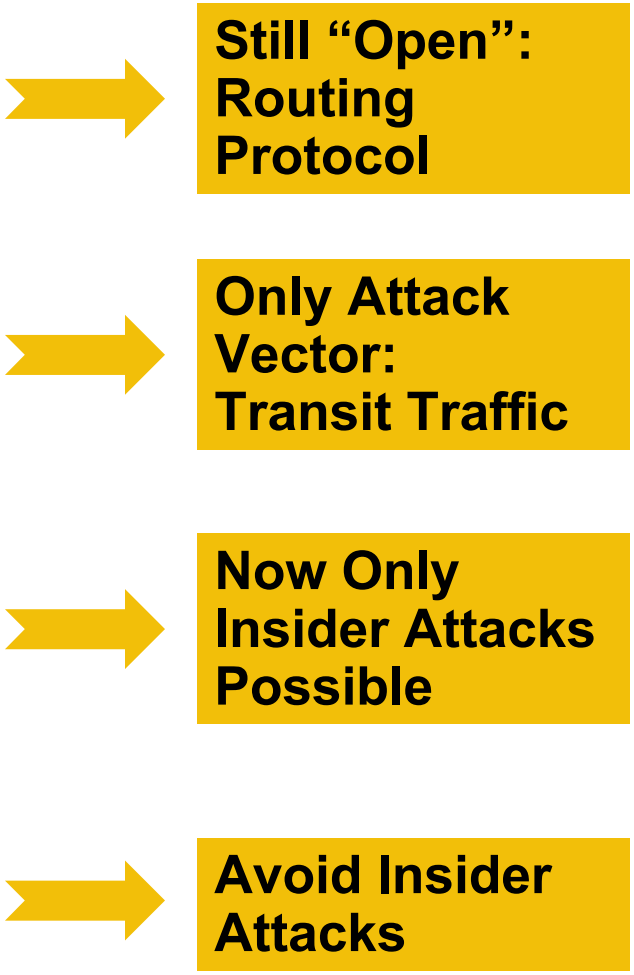
Address Planes: True Separation!



Secure MPLS VPN Design _ General Security Best Practices

Secure MPLS/VPN Core Design

1. Secure each router individually
2. Don't let packets into (!) the core
   - No way to attack core, except through routing, thus:
3. Secure the routing protocol
   - Neighbor authentication, maximum routes, dampening,…
4. Design for transit traffic
   - QoS to give VPN priority over Internet
   - Choose correct router for bandwidth
   - Separate PEs where necessary
5. Operate Securely



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. **IGPs**: If BGP not supported
   (limited security features)

Securing the Core: Infrastructure ACLs

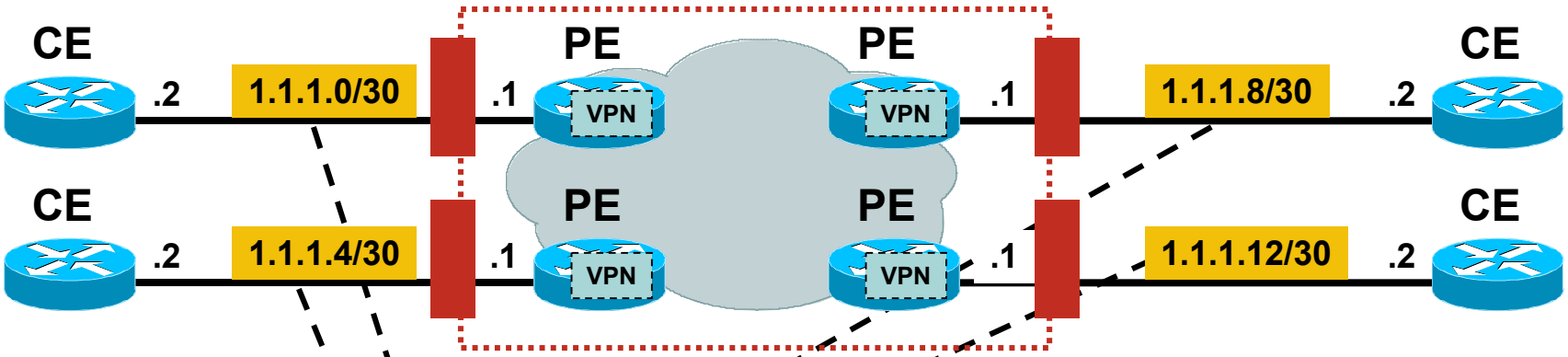
Easy with MPLS!

In MPLS: VRF Belongs to Customer VPN!

- On PE: “deny ip any <PE VRF address space>”

  Exception: routing protocol from host to host
- Idea: no traffic to PE/P you can’t attack
- Prevents intrusions 100%
- DoS: very hard, but traffic over router theoretically enables DoS

Securing the Core: Infrastructure ACLs



- Example:

  deny ip any 1.1.1.0 0.0.0.255

  permit ip any any

This Is VPN Address Space, Not Core!

- Caution: This also blocks packets to the CE's!

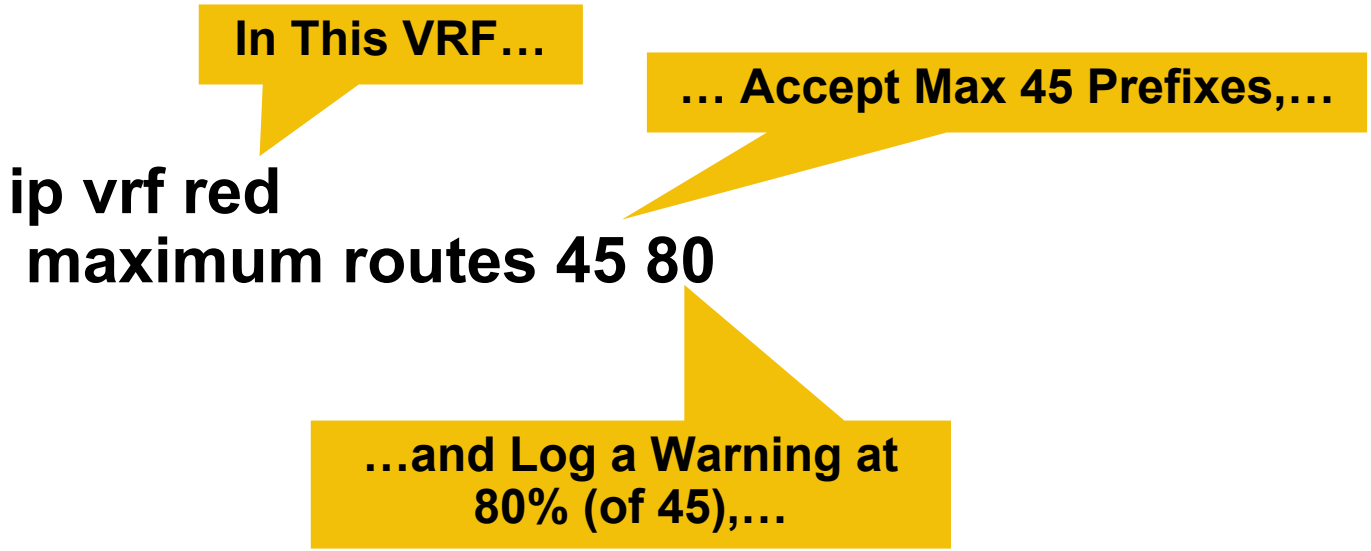
  Alternatives: List all PE i/f in ACL, or use secondary i/f on CE, or ACL with dis-contiguous subnet masks (11111101)

Neighbor Authentication

- Router “knows” his neighbors
  - Verification through shared MD5 secret
- Verifies updates it receives from neighbor
- Supported: BGP, ISIS, OSPF, EIGRP, RIPv2, LDP
- Key chains supported for ISIS, EIGRP, RIP
  - Use them where available
  - Easier key roll-over
  - Support for LDP key chains soon
- Config easy

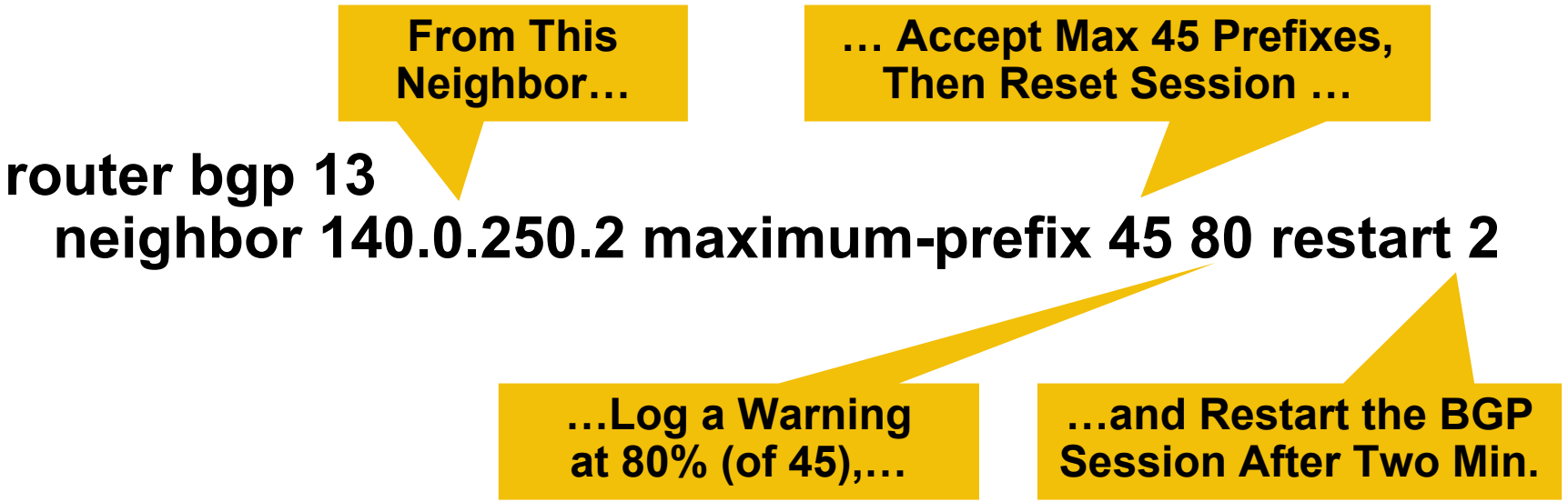
VRF Maximum Prefix Number

- Injection of too many routes:
  - Potential memory overflow
  - Potential DoS attack
- For a VRF: Specify the maximum number of routes allowed



Control of Routes from a BGP Peer

- Injection of too many routes:
  - Potential memory overflow
  - Potential DoS attack
- Control with “maximum prefix” command
  - (under the BGP neighbor definition)



Control of Routes from a BGP Peer: Logging

6d22h: %BGP-4-MAXPFX: No. of prefix received from 140.0.250.2 (afi 2) reaches 37, max 45

6d22h: %BGP-3-MAXPFXEXCEED: No. of prefix received from 140.0.250.2 (afi 2): 46 exceed limit 456d22h: %BGP-5-ADJCHANGE: neighbor 140.0.250.2 vpn vrf VPN_20499 Down BGP Notification sent

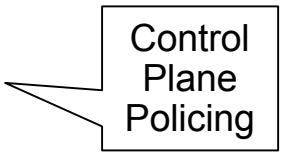
6d22h: %BGP-3-NOTIFICATION: sent to neighbor 140.0.250.2 3/1 (update malformed) 0 bytes FFFF FFFF FF

Best Practice Security Overview

- Secure devices (PE, P): They are trusted!

  See next slide for risks…

- PEs: Secure with ACLs on all interfaces; CoPP



- Static PE-CE routing where possible
- If routing: Use authentication (MD5)
- Maximum number of routes per peer (only BGP)
- Separation of CE-PE links where possible (Internet/VPN)
- LDP authentication (MD5) (key chains to be supported soon)
- VRF: Define maximum number of routes
- Note: Overall security depends on weakest link!

Key: PE Security

- What happens if a single PE in the core gets compromised?
  - Intruder has access to all VPNs; GRE tunnel to “his” CE in the Internet, bring that CE into any VPN
  - That VPN might not even notice…
  - Worst Case!!!!
- Therefore: PE Security is Paramount!!!!!!!
- Therefore: No PE on customer premises!!!!!!!
  - (Think about console access, password recovery…)

No Service Password-Recovery

- Different implementations
  - When password recovery → erase NVRAM
  - Password recovery impossible (really!)
- Where available: Use It!
- This makes it hard to intrude into a PE, even with physical access!

Solution: Operational Security

- Security depends on SP!
  - Employee can make mistake, or malicious misconfiguration
- Potential Security hole:
  - If PE compromised, VPNs might be insecure
- Cannot *prevent* all misconfigs
  - Need to operationally control this

Operational Security

- Logging config changes; automated audits

  Dual Control: Network operators must have no access to logging facility

  See also: Router Security Audit (12.0(27)S, 12.2(18)S)
- AAA for access
- CLI views or AAA for command authorization

  Keep logs in a secure place

  (Malicious employee might change logs too)
- Tight control
- No service password-recovery where available

Secure Operations Is Hard!!!

MPLS VPNs are Quite Secure

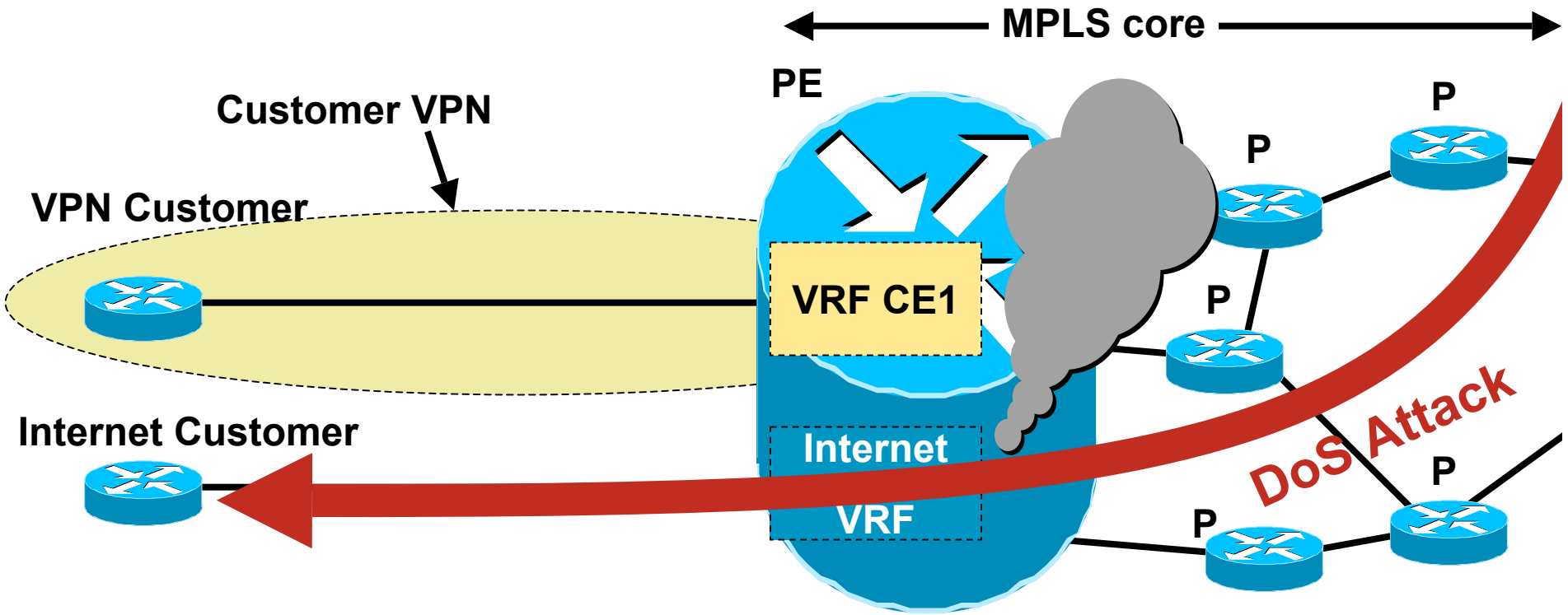
- Perfect Separation of VPNs
  - No intrusions possible
- Perfect Separation of the Core from VPNs
  - Again, no intrusions possible

But there is one remaining issue…

The Issue: DoS Through a Shared PE Might Affect VPN Customer

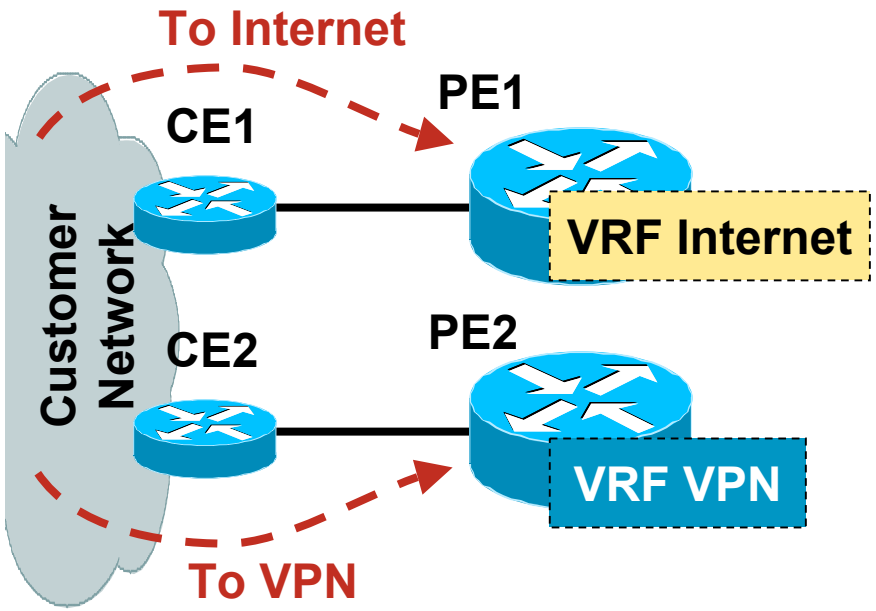
PE Has Shared CPU/Memory/Bandwidth:

Traffic COULD affect VPN customer
(however, risk probably acceptable)



Today's Best Practice: MPLS VPN Security Recommendation:

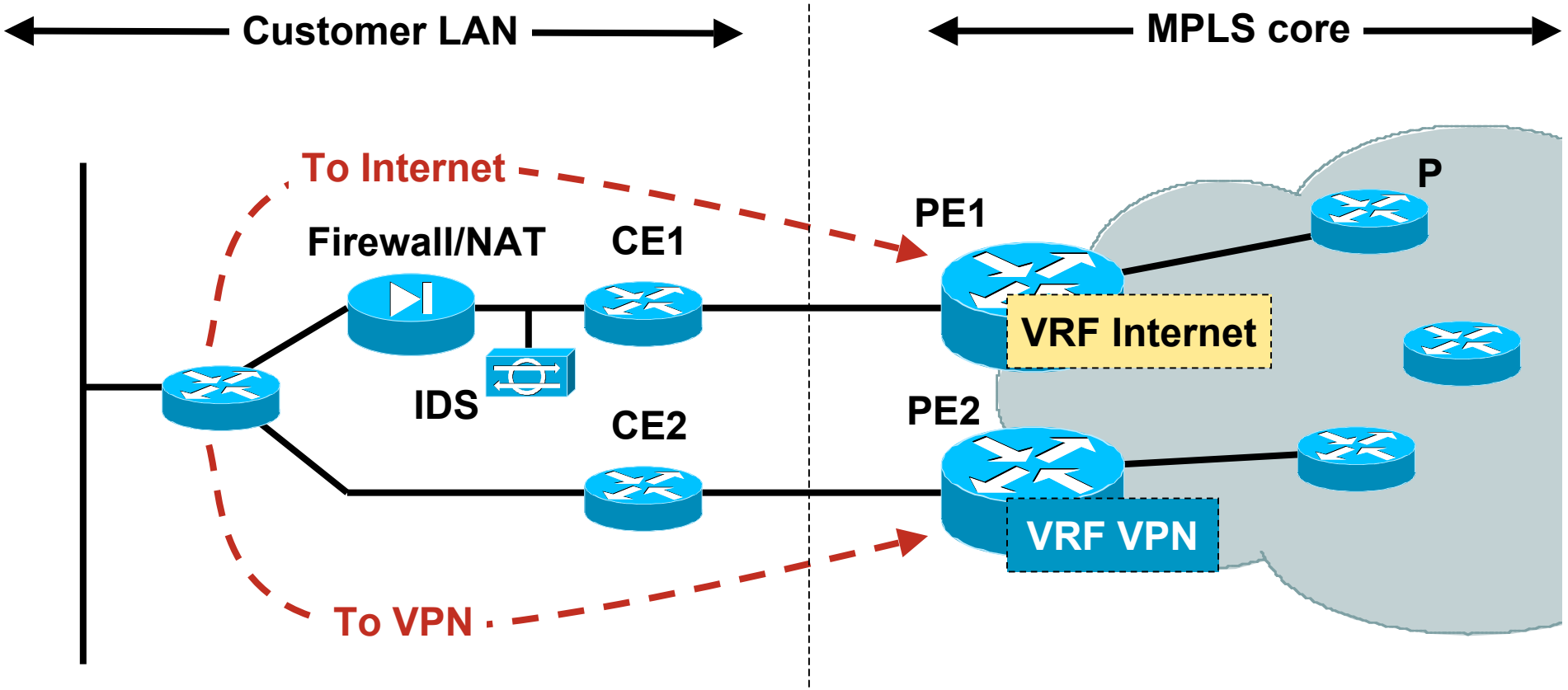
PE Routers Should Contain Only VRFs of the Same Security Level; Example:



- Level 0: Internet
- Level 1: VPN customers
- (Level 2: Mission critical infrastructure)

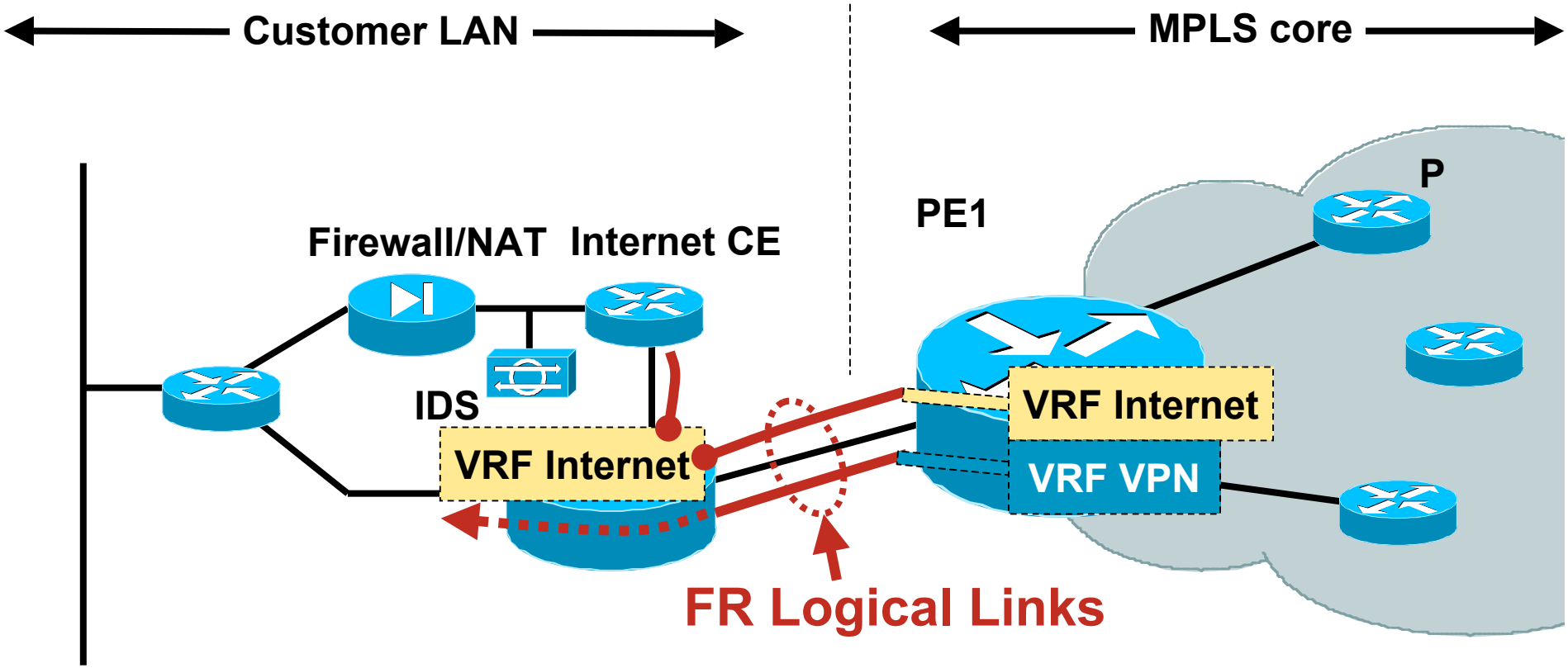
Note: This is negotiable: Shared Internet/VPN PE may be acceptable if price and conditions are right

Separate VPN and Internet Access



- Separation: +++
- DoS resistance: +++
- Cost: $$$ (two lines and two PEs: expensive!)

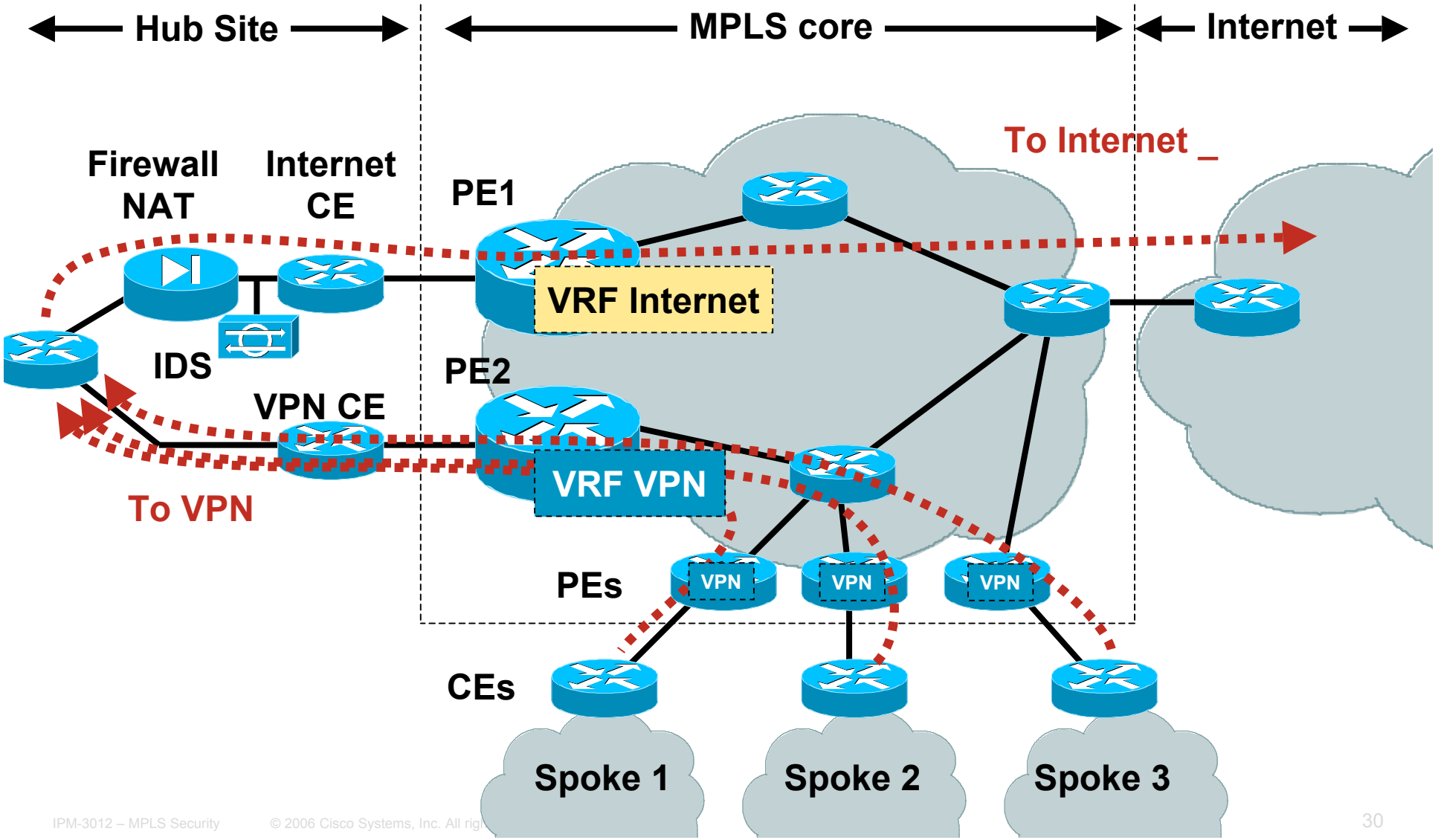
Shared Access Line, CE with VRF Lite



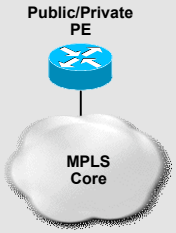
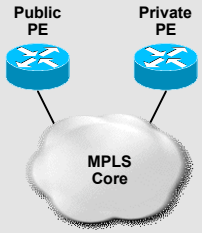
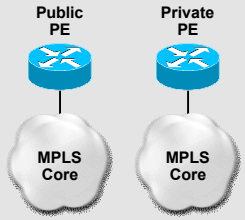
- Separation: +++
- DoS resistance: + (DoS might affect VPN on PE, line, CE)
- Cost: $

Note: CE config more complex here!

Hub-and-Spoke VPN with Internet Access

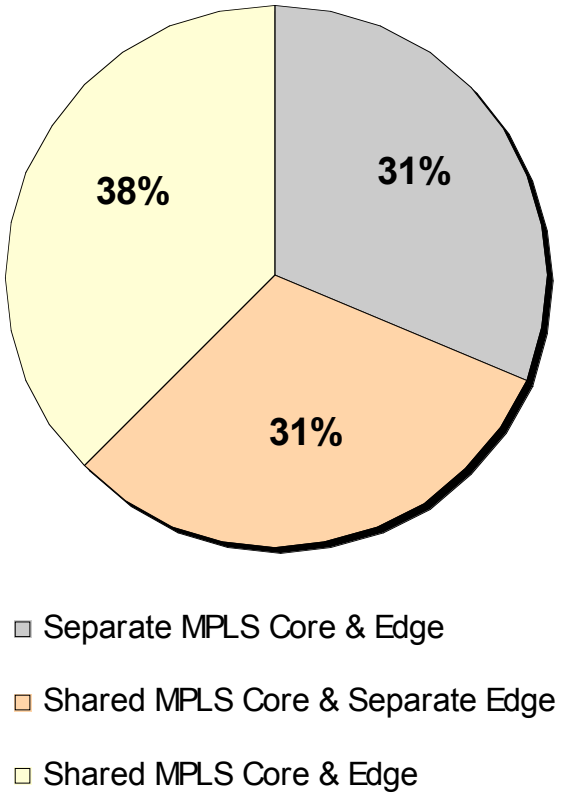


MPLS Deployment Scenarios

	Shared MPLS Core & Edge	Shared MPLS Core & Separate Edge	Separate MPLS Core & Edge
			
MPLS Core Network	• Single MPLS core for both public IP and private VPN traffic • Optional BGP/Internet free core	• Single MPLS core for both public IP and private VPN traffic • Optional BGP/Internet free core	• Separate MPLS cores for public IP and private VPN traffic • Optional BGP/Internet free core
MPLS Edge Network	• PE routers terminate both public IP and private VPN connections	• Dedicated PE routers used for termination of public IP and private VPN connections	• Dedicated PE routers used for termination of public IP and private VPN connections

Current MPLS Deployments

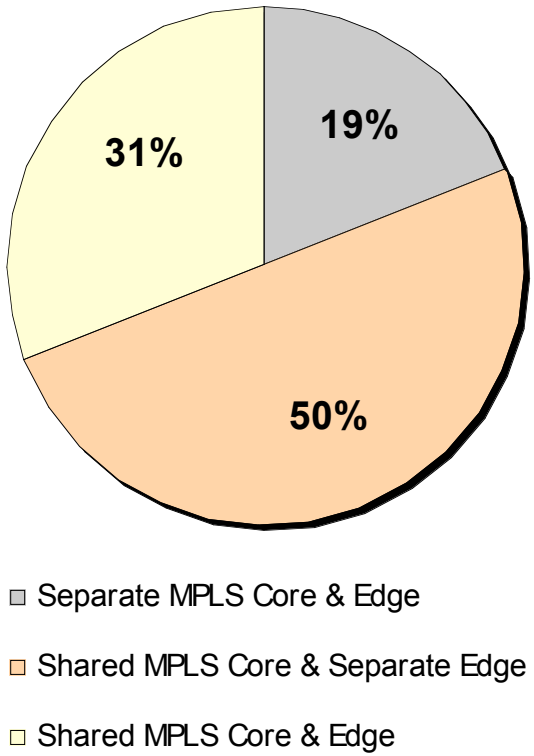
- Internal survey of key SP customers on deployment of public and private MPLS services
  - Separate MPLS core & edge
  - Shared MPLS core & separate edge
  - Shared MPLS core & edge
- No common MPLS deployment preference
  - Balanced distribution of various MPLS deployment scenarios



Source: Internal 2006 MPLS Security Survey by Michael Behringer.

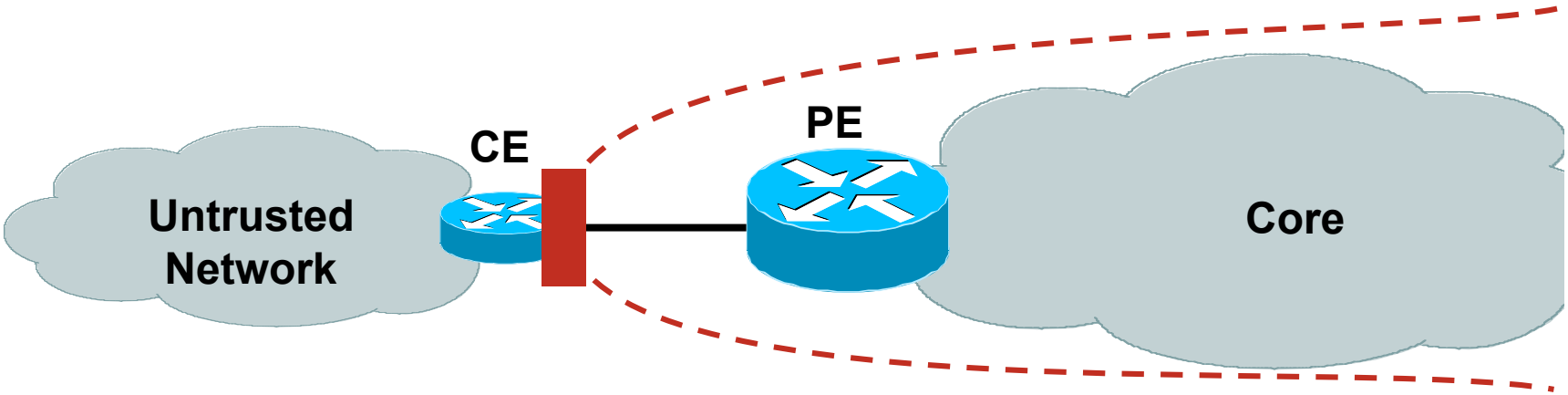
Future MPLS Deployment Plans

- Future MPLS deployment plans indicate increasing network consolidation
  - Increasing number of shared MPLS core deployments
- Common MPLS core for public and private services
- Migration of both public and private services onto single MPLS edge



Source: Internal 2006 MPLS Security Survey by Michael Behringer.

Alternative Model for Securing PEs



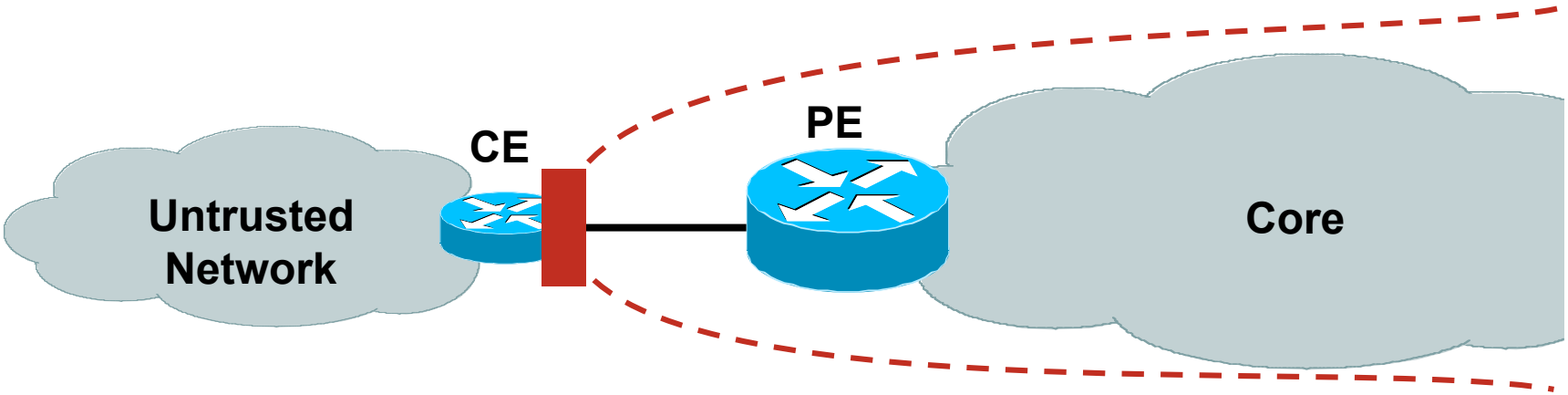
- Block packets to PE (actually, entire core!) **on CE (!)**
- Core not attackable from “outside”

  (Attacks with transit traffic still theoretically possible)

BUT: CE must be trusted !!!

Can we really assume that???

How Can We Trust the CE?



- Goal: No unauthorised change / bypass of CE config
- Strong CE security (basic router security)
- No service password-recovery
  - Prevents config access through console/aux ports
- Some form of authentication
  - Protects against another device being used instead of CE
  - PPPoX, routing authentication (but then routing required)

Secure MPLS VPN Design _ Internet Access

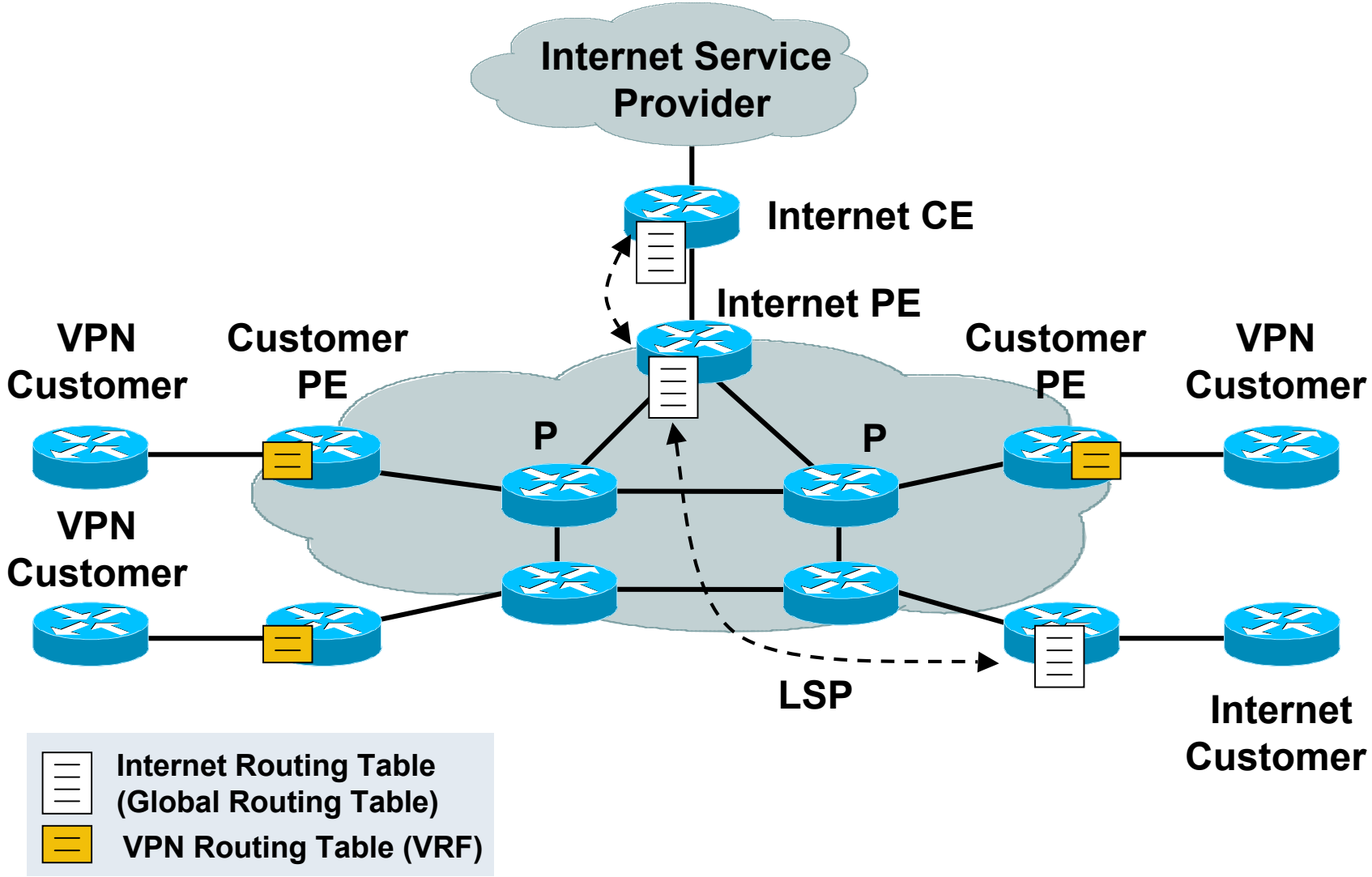
Internet Provisioning on an MPLS Core

Two basic possibilities:

1. Internet in global table, either:
   - 1a) Internet-free core (using LSPs between PEs)
   - 1b) hop-by-hop routing
2. Internet in VRF
   - Internet carried as a VPN on the core

This is the “default”!!!

Internet in the Global Routing Table Using LSPs Between PEs



Internet in the Global Routing Table Using LSPs Between PEs

- Default behavior, if Internet in global table!!
  - On ingress PE: BGP next hop: Egress PE loopback
  - Next hop to egress usually has label!
  - LSP is used to reach egress PE
  - P routers do not need to know Internet routes (nor run BGP)
- Security consequence:
  - PE routers are fully reachable from Internet, by default (bi-directional)
  - P routers are also by default reachable from Internet; but only uni-directional, they don't know the way back!

Internet in the Global Routing Table Using LSPs Between PEs

Recommendations:

- Fully secure each router!
- Do not advertise IGP routes outside

  (This is a general security recommendation for all cores!)

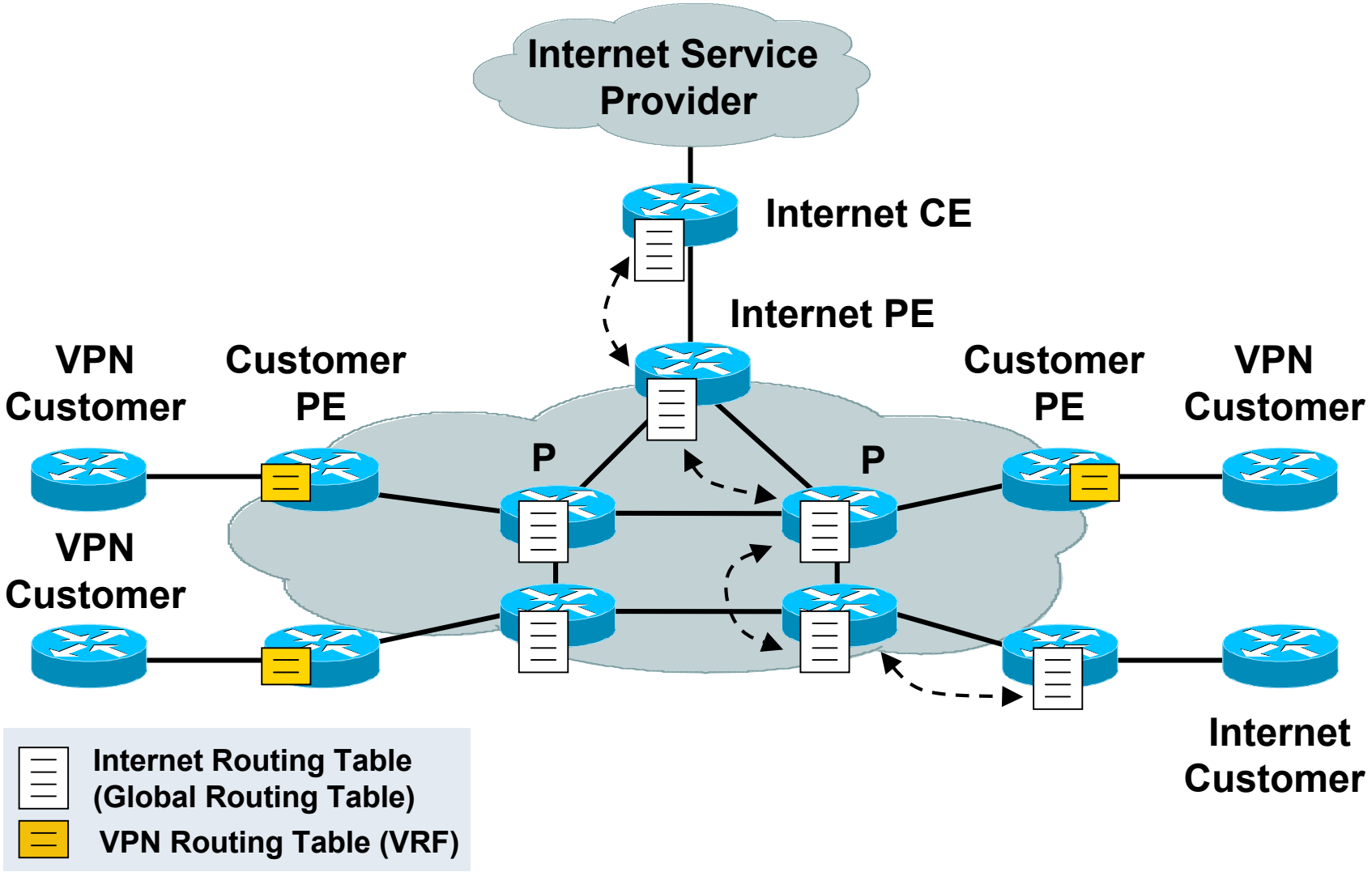
  P routers not reachable (unless someone defaults to you)

  PE routers not reachable (possible exception: Peering PE)
- Infrastructure ACLs to block core space:

  Additional security mechanism

  Even if someone defaults to you, he cannot reach the core

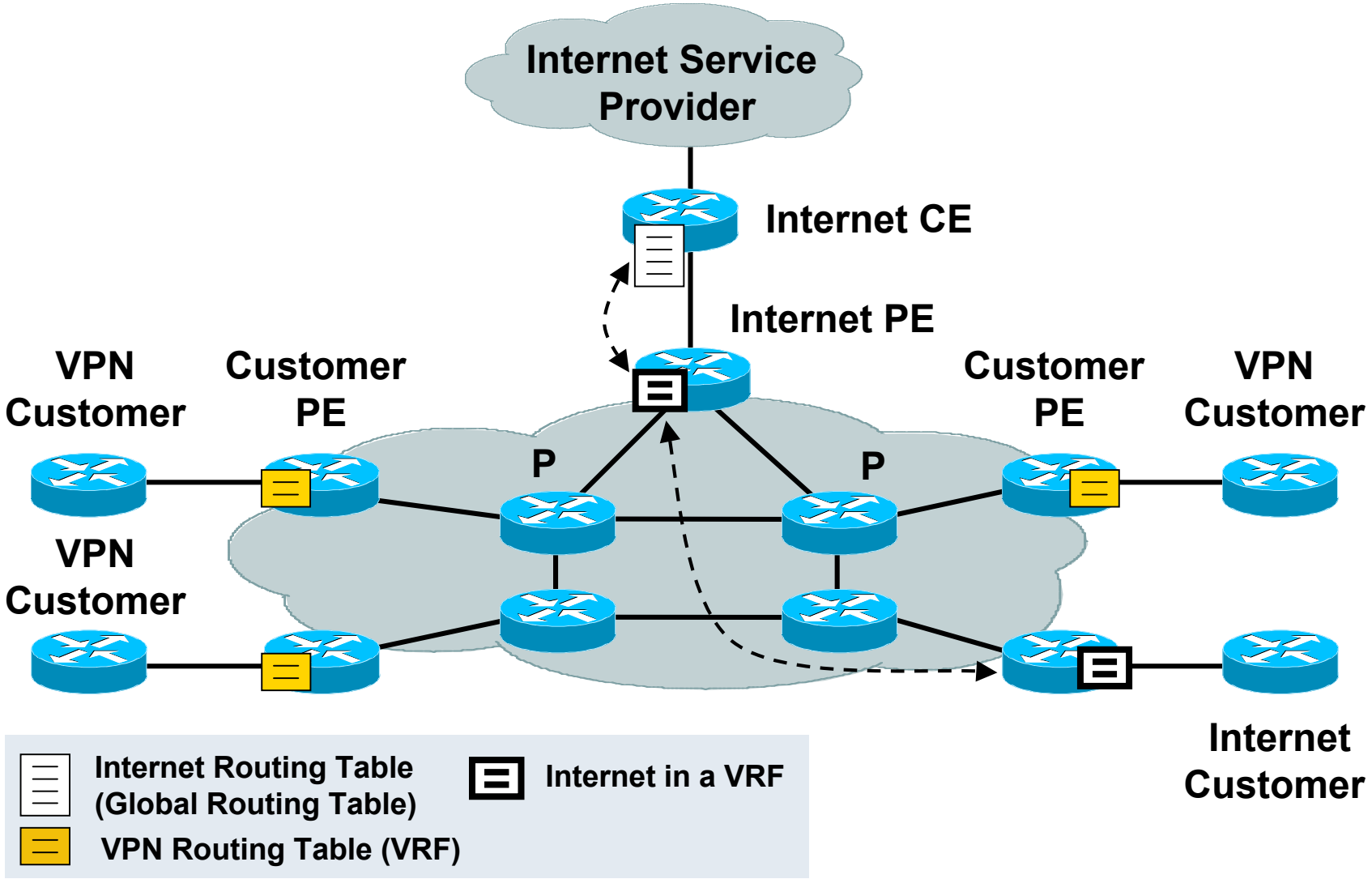
Internet in the Global Routing Table Hop-by-Hop Routing



Internet in the Global Routing Table Hop-by-Hop Routing

- Like in standard IP core
  - Each router speaks BGP, and carries Internet routes
  - Not default, must be configured!
- Security consequence:
  - P and PE routers by default fully reachable from Internet
- Recommendations: (like before)
  - Fully secure each router!
  - Do not advertise IGP routes outside
  - Infrastructure ACLs

Internet in a VRF



Internet in a VRF

- Internet is a VPN on the core
  - Full separation to other VPNs, and the core, by default!
  - “Connection” between Internet and a VPN (for service) must be specifically configured
- Security consequence:
  - P routers not reachable from anywhere!
  - PE routers only reachable on outbound facing interfaces;
  - Very limited
  - Much easier to secure
- But!!!
  - Routes in a VRF take more memory!!
  - Convergence times increase

These are serious issues!

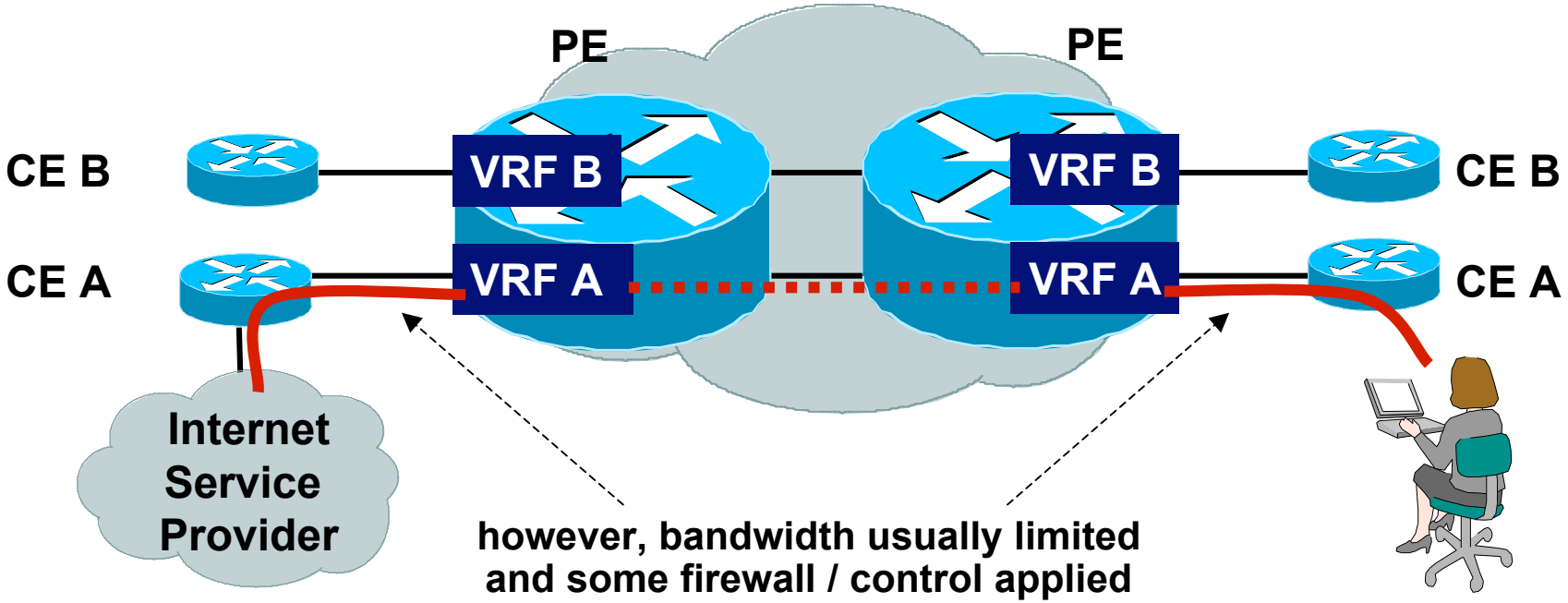
Internet in a VRF

Recommendations:

- Fully secure each router (you never know…)
- Secure external facing PE interfaces!
  - Use Infrastructure ACLs for this (see earlier)
  - (Internal PE i/f and P cannot be reached from outside)

Alternatively: No Internet on the Core

- Pure MPLS VPN service considered “most secure”
- But what about:



Secure MPLS VPN Design _ Inter-AS and CsC

Inter-AS: What are we trying to achieve?

- An SP should have:

  100% (full) reachability to all Inter-AS VPNs
  (control plane and data plane)

  0% (no) reachability to VPNs that are **NOT** shared
  (control plane and data plane)

- SP networks should be independent:

  Not attackable from outside (other SP, customer, Internet)

  Limited reachability from outside

Inter-AS: What Are We NOT Trying to Achieve?

Any Form of Separation Between Inter-AS VPNs (Control or Data Plane)

- Interconnection of VPNs is 100%
- No firewalling, no limitations, no sanity checks within an Inter-AS VPN

If an SP Holds VPN Sites in an Inter-AS Set-Up, He Has Full Access to *All* VPN Sites, Also on Other ASes

Inter-AS: The Options

- Option A

  VRF back to back;

  IP interface

- Option B

  ASBRs exchange labelled VPN prefixes;

  labelled interface

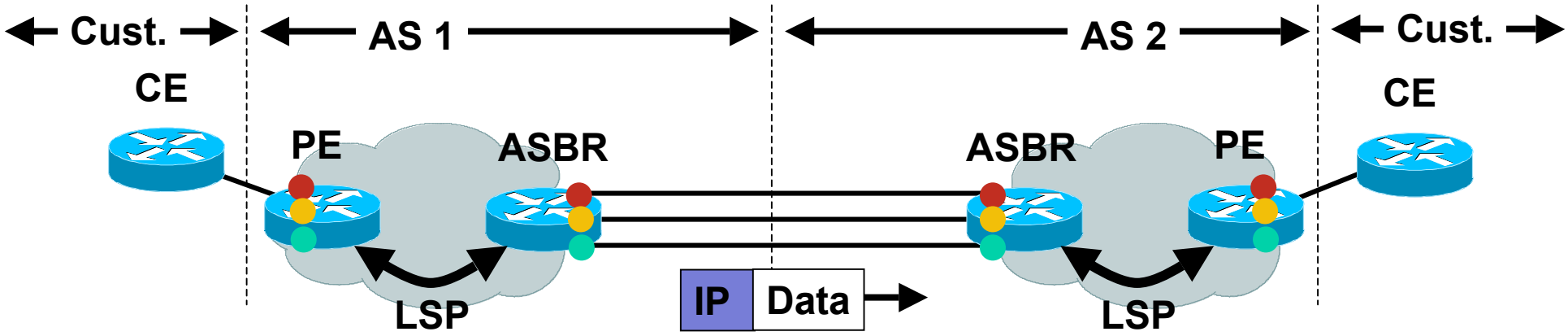
- Option C

  ASBRs don't hold VPN information - only RRs do;

  labelled interface

ASBR: Autonomous System Border Router
RR: Route Reflector
VRF: Virtual Routing and Forwarding instance

Inter-AS: Case A
VRF-VRF Back-to-Back

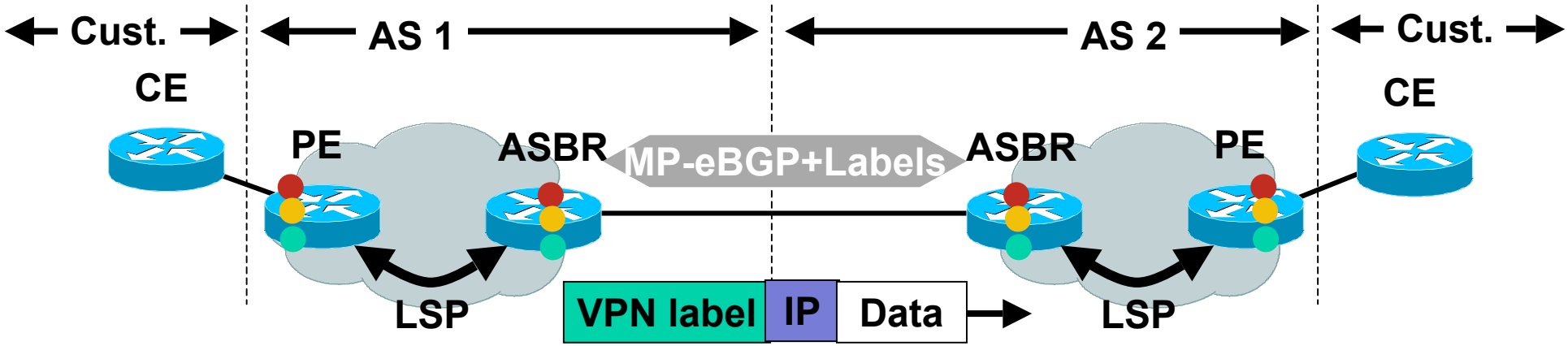


- Control plane: No signalling, no labels
- Data plane: IPv4 only, no labels accepted
- Security: as in RFC 2547 (single-AS)
- SPs are completely separated

Security of Inter-AS case A

- Static mapping
  - Only IP interfaces
  - SP1 does not “see” SP2’s network
  - And does not run routing with SP2, except within the VPNs
  - → Quite secure
- Potential issues:
  - SP 1 can connect VPN connection wrongly (like in ATM/FR)
  - Customer can flood routing table on PE (this is the same issue as in RFC 2547 (single-AS); solution: prefix limits)

Inter-AS: Case B
ASBRs Exchange Labeled VPNv4 Routes



- Control plane: MP-eBGP, labels
- Data plane: Packets with one label
- Labeled packets at interface
  - Lookup in LFIB
  - But not checked, thus spoofing possible!

Security of Inter-AS Case B: Summary

- Control Plane can be secured well
- Data Plane has some security issues:

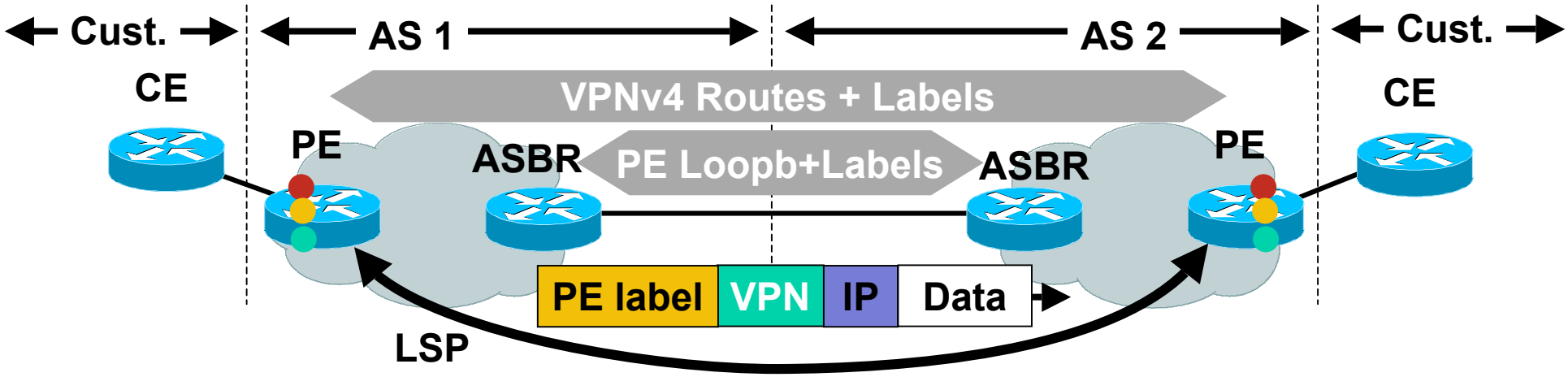
  Label is not checked today (since i/f in global table)

  Labelled packets on any MPLS i/f will be forwarded if LFIB entry exists
- Potential Issues:

  Insertion of traffic into non-shared VPNs
  (uni-directional only)
  (requires compromised/faulty ASBR, remote exploit not possible)

  All global i/f on an ASBR share the same LFIB, thus might affect third parties
- Good: No “visibility” of other AS (except ASBR i/f)

Inter-AS Case C: ASBRs Exchange PE loopbacks



- Control plane: ASBR: just PE loopback + labels; PE/RR: VPNv4 routes + labels
- Data plane: PE label + VPN label
- AS1 can insert traffic into VPNs in AS2

  Only requirement: Must have LSP to correct egress PE
- Customer must trust both SPs
- More scalable, but worse for security!

Security of Inter-AS Case C

- ASBR-ASBR signalling (BGP)
  RR-RR signalling (MP-BGP)
  - Much more “open” than Case A and B
  - More interfaces, more “visible” parts (PE, RR)
- Potential Issues:
  - SP1 can intrude into any VPN on PEs which have a Inter-AS VPN configured
  - Cannot check what’s underneath the PE label
- Very open architecture
  - Acceptable for ASes controlled by the same SP

Inter-AS Summary and Recommendation

- Three different models for Inter-AS
  - Different security properties
  - Most secure: Static VRF connections (case A), but least scalable
- Basically the SPs have to trust each other
  - Hard/impossible to secure against other SP in this model
  - But: Can monitor with **MPLS aware NetFlow (!!)**
- Okay if all ASes in control of one SP
- Current Recommendation: Use case A

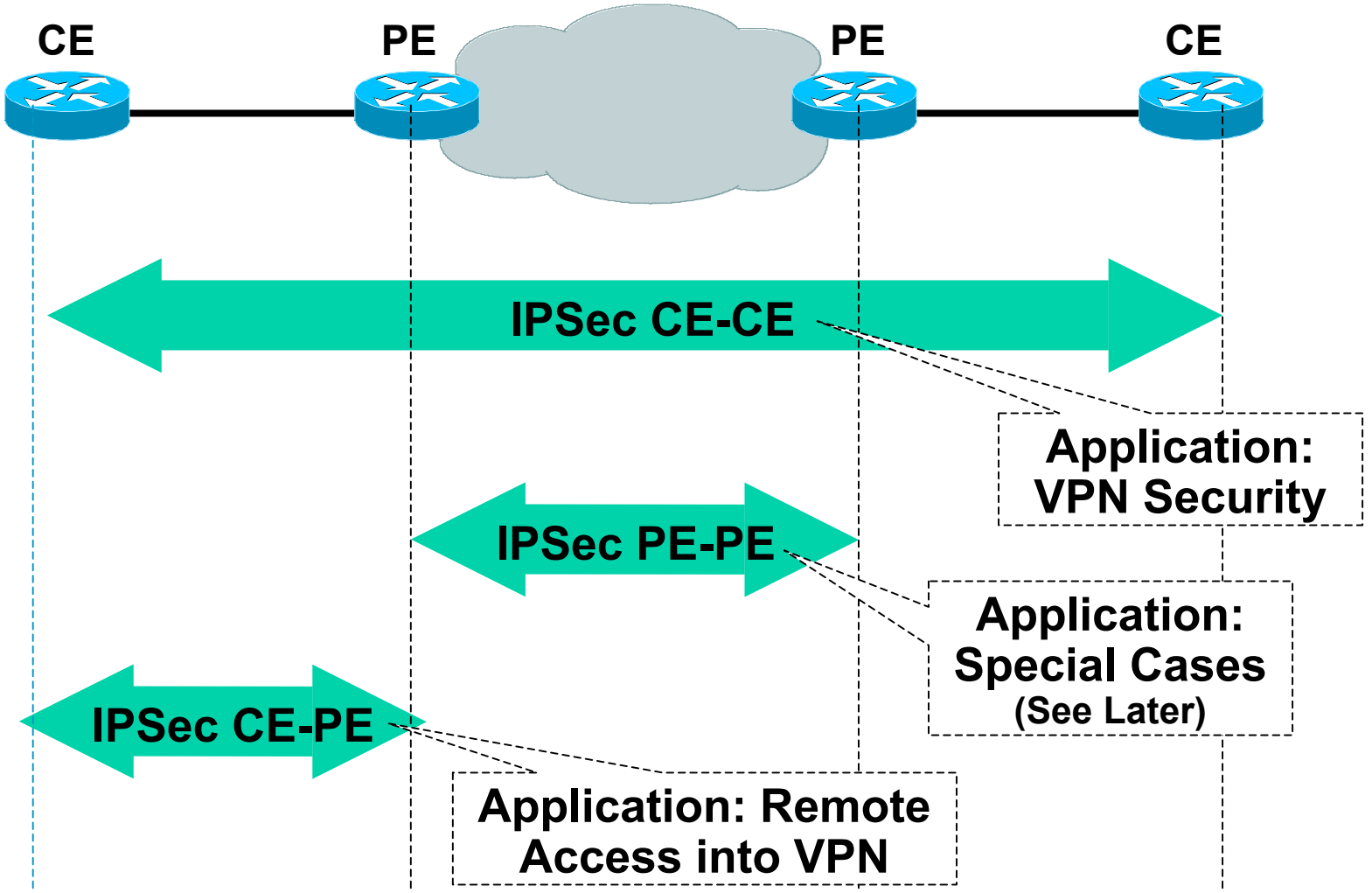
IPsec and MPLS

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!

Where to Apply IPSec



How to Establish IPSec: Options

- Option 1: Static IPSec
  - Pre-configure static IPSec tunnels
  - Works, but does not scale well
- Option 2: Dynamic Cryptomap/ Tunnel Endpoint Discovery
  - Scaling improvements over 1).
- Option 3: DMVPN
  - Dynamic tunnel establishment
  - Easy to configure and maintain
  - Some scaling issues
- Option 4: GET VPN
  - Easy to configure and maintain
  - Scales well

Dynamic Multipoint VPN

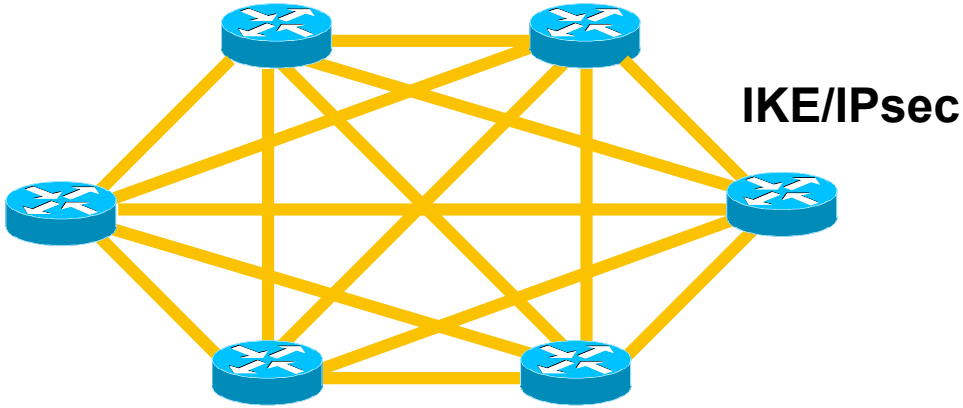
Group Encrypted Transport

launched Dec 2006

GET VPN: IPsec Made Easy!

Traditional IPsec:

- n^2 Problem (scalability)



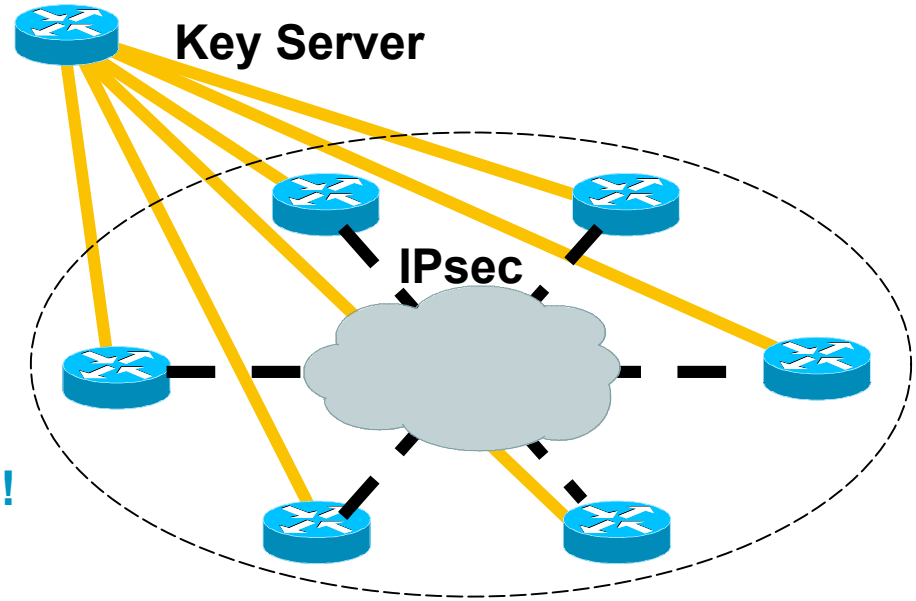
GET VPN:

- 2 Security Associations

- to the key server (~IKE)

- to the group (IPsec)

Only 1 group association needed!



Outlook

What We Are Working On

- GET VPN: Platform support
- PE Security:
  - Control Plane Protection (VRF aware)
  - General router security improvements
- LDP and Routing:
  - Better MD5 key management (eg LDP key chains)
  - LDP lossless key change
- Many more features…

Summary

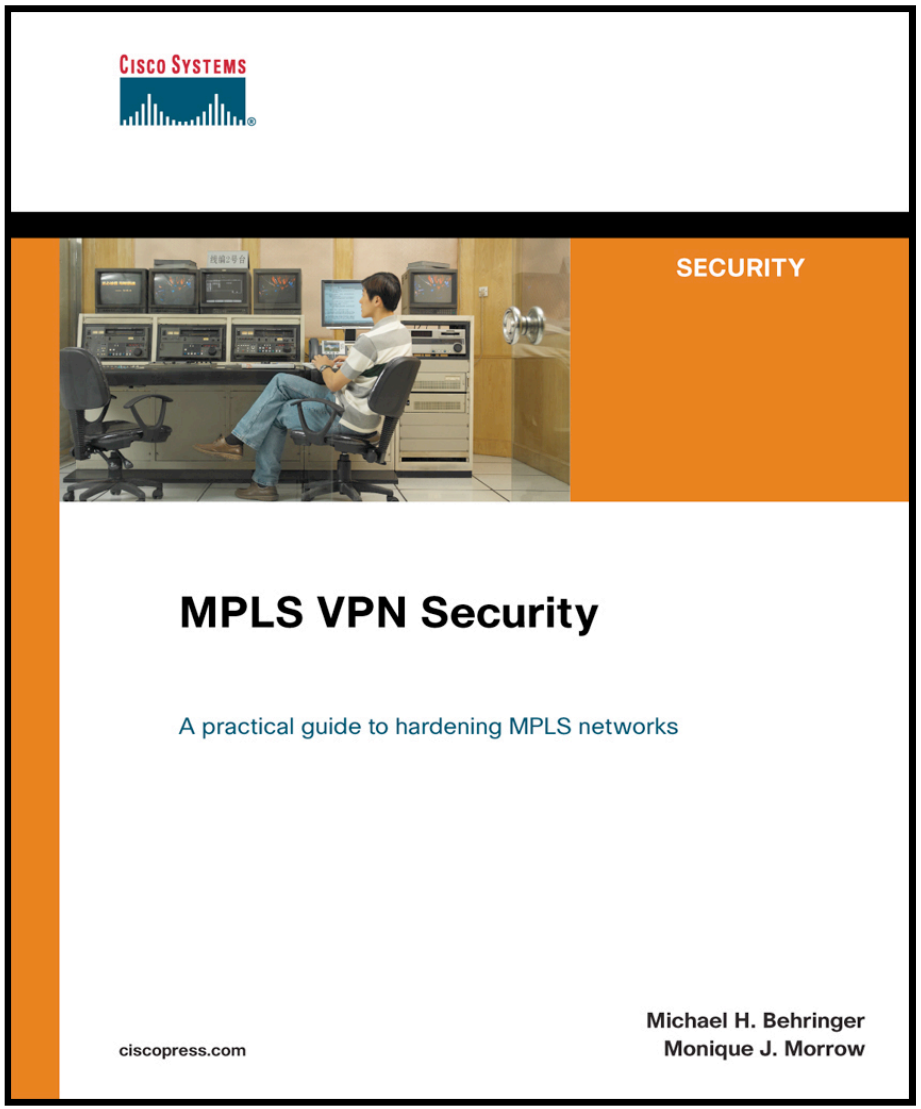
MPLS doesn’t provide:

- 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

Summary

- MPLS VPNs can be secured as well as ATM/FR VPNs
- Security depends on correct operation and implementation
- MPLS backbones can be more secure than “normal” IP backbones
  - Core not accessible from outside
  - Separate control and data plane
- Key: PE security
  - Advantage: Only PE-CE interfaces accessible from outside
  - Makes security easier than in “normal” networks

For More Information: "MPLS VPN Security"



Authors:
Michael Behringer
Monique Morrow

Cisco Press,
ISBN: 1587051834

Published June, 2005

Additional Information

- MPLS Security White Paper:

  http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/mxinf_ds.htm
  Analysis of the security of the MPLS architecture

- RFC on MPLS VPN Security:

  http://www.ietf.org/rfc/rfc4381.txt

- Miercom MPLS test report:

  http://www.mier.com/reports/cisco/MPLS-VPNs.pdf
  Practical tests show that MPLS is secure

- Garnter research note M-17-1953: "MPLS Networks: Drivers Beat Inhibitors in 2003"; 10 Feb 2003

Q and A