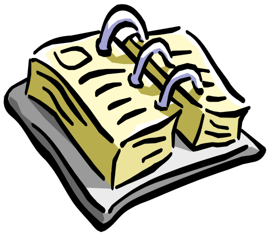
MPLS Virtual Private Network (VPN) Security

An MFA Forum Sponsored Tutorial

Thomas Nadeau
MFA Forum Ambassador
Principle Engineer
Cisco Systems

MPLS VPN Security - Agenda

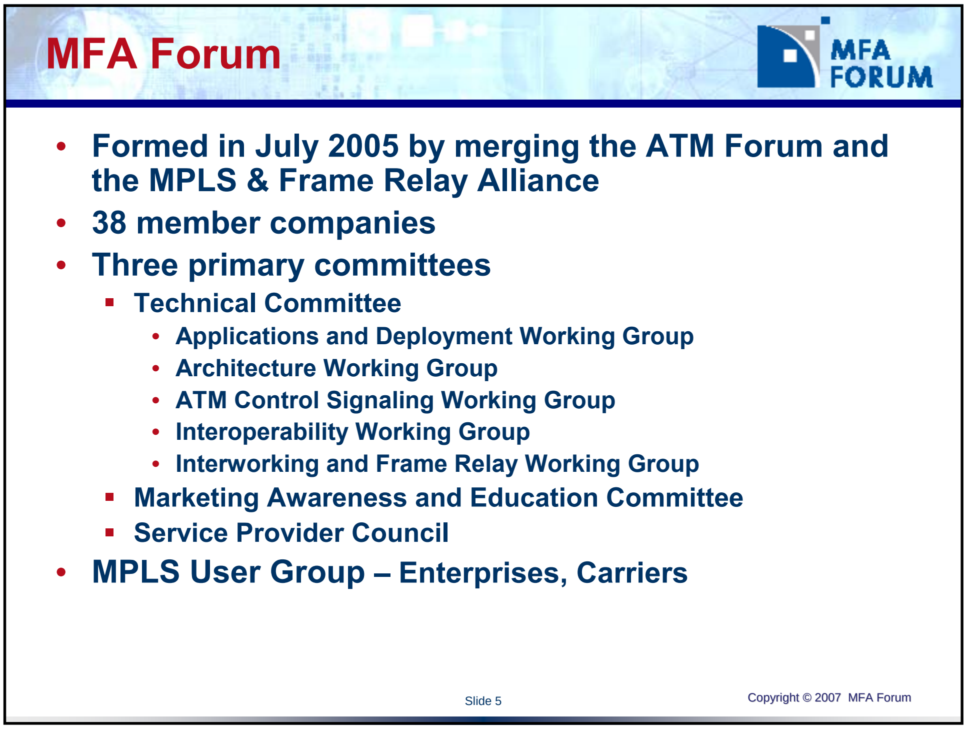


- Introduction
- Analysis of the Architecture
- Secure MPLS VPN Design
  - General Best Practices
  - Internet Access
  - Inter-AS and Carriers’ Carrier
  - Layer 2 VPN Security
- IPsec and MPLS
- Ongoing standardization work
- Summary

Introduction

Mission Statement

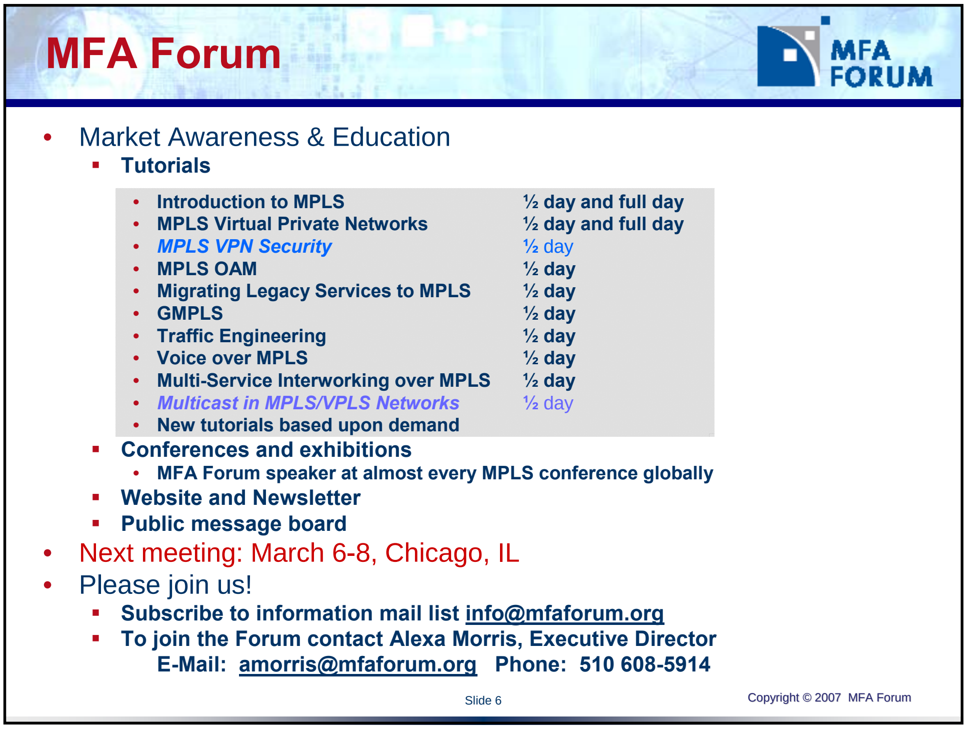
The MFA Forum is an international, industry-wide, nonprofit association of telecommunications, networking, and other companies focused on advancing the deployment of multi-vendor, multi-service packet-based networks, associated applications, and interworking solutions.



MFA Forum

- Formed in July 2005 by merging the ATM Forum and the MPLS & Frame Relay Alliance
- 38 member companies
- Three primary committees
  - Technical Committee
    - Applications and Deployment Working Group
    - Architecture Working Group
    - ATM Control Signaling Working Group
    - Interoperability Working Group
    - Interworking and Frame Relay Working Group
  - Marketing Awareness and Education Committee
  - Service Provider Council
- MPLS User Group – Enterprises, Carriers

Slide 5



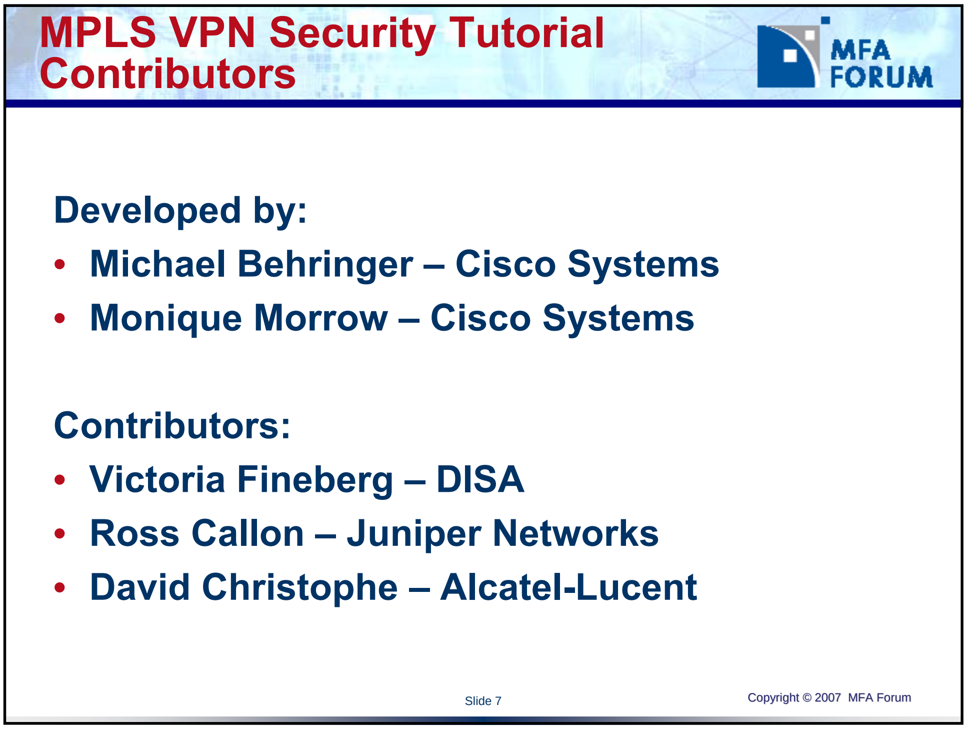
MFA Forum

- Market Awareness & Education
  - Tutorials

Introduction to MPLS	½ day and full day
MPLS Virtual Private Networks	½ day and full day
MPLS VPN Security	½ day
MPLS OAM	½ day
Migrating Legacy Services to MPLS	½ day
GMPLS	½ day
Traffic Engineering	½ day
Voice over MPLS	½ day
Multi-Service Interworking over MPLS	½ day
Multicast in MPLS/VPLS Networks	½ day
New tutorials based upon demand	

  - Conferences and exhibitions
    - MFA Forum speaker at almost every MPLS conference globally
  - Website and Newsletter
  - Public message board
- Next meeting: March 6-8, Chicago, IL
- Please join us!
  - Subscribe to information mail list info@mfaforum.org
  - To join the Forum contact Alexa Morris, Executive Director
    E-Mail: amorris@mfaforum.org Phone: 510 608-5914

Slide 6



MPLS VPN Security Tutorial Contributors

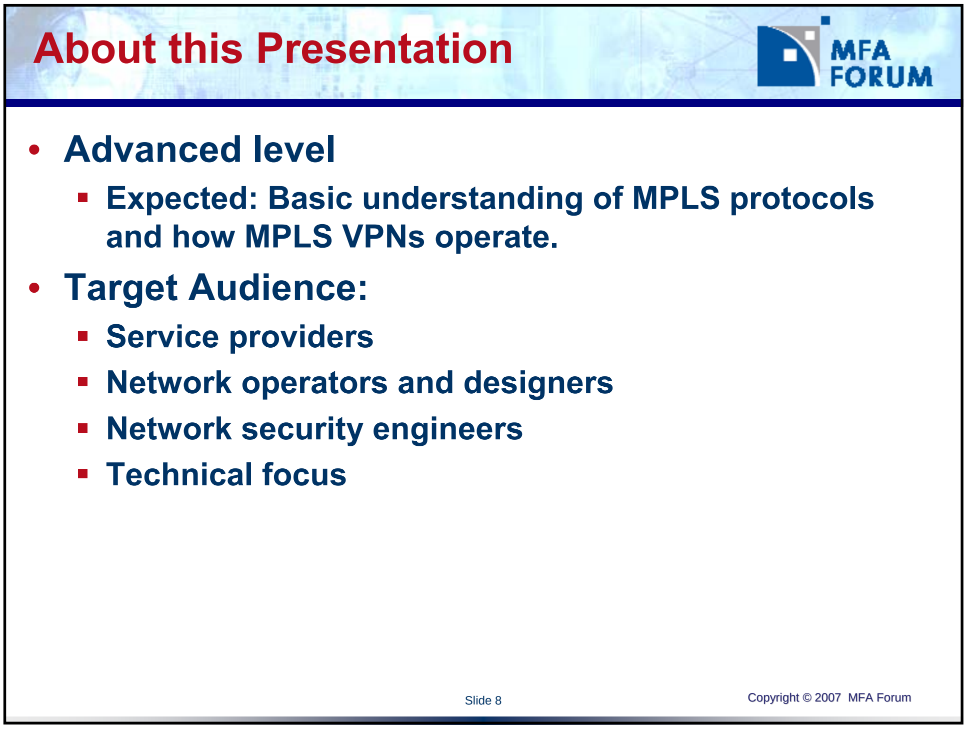
MFA FORUM

Developed by:

- Michael Behringer – Cisco Systems
- Monique Morrow – Cisco Systems

Contributors:

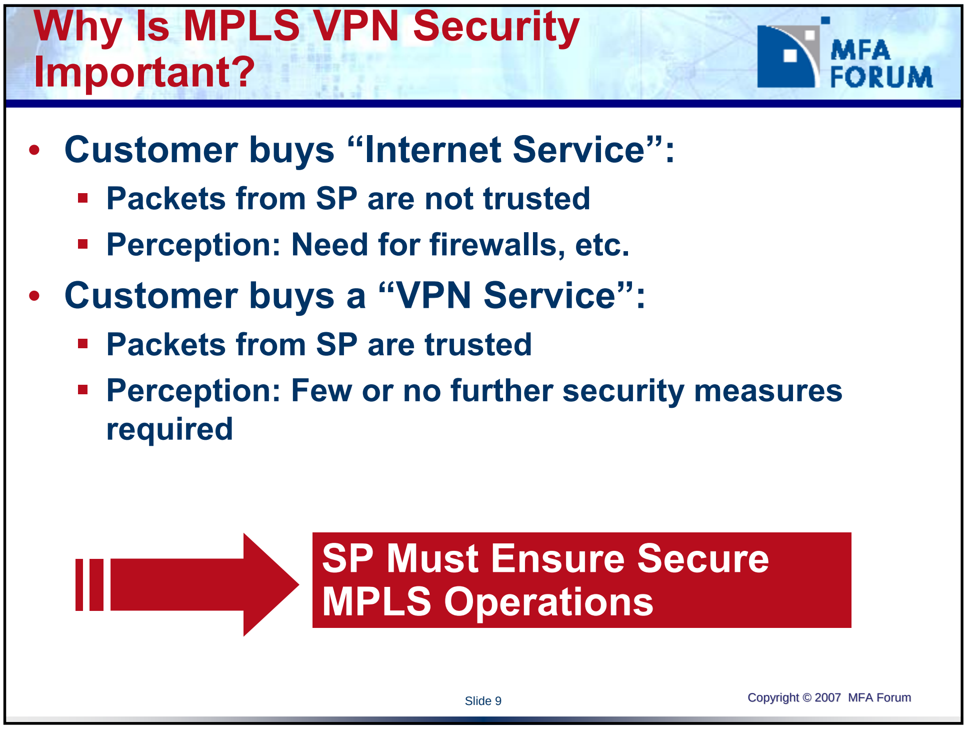
- Victoria Fineberg – DISA
- Ross Callon – Juniper Networks
- David Christophe – Alcatel-Lucent



About this Presentation

MFA FORUM

- Advanced level
  - Expected: Basic understanding of MPLS protocols and how MPLS VPNs operate.
- Target Audience:
  - Service providers
  - Network operators and designers
  - Network security engineers
  - Technical focus

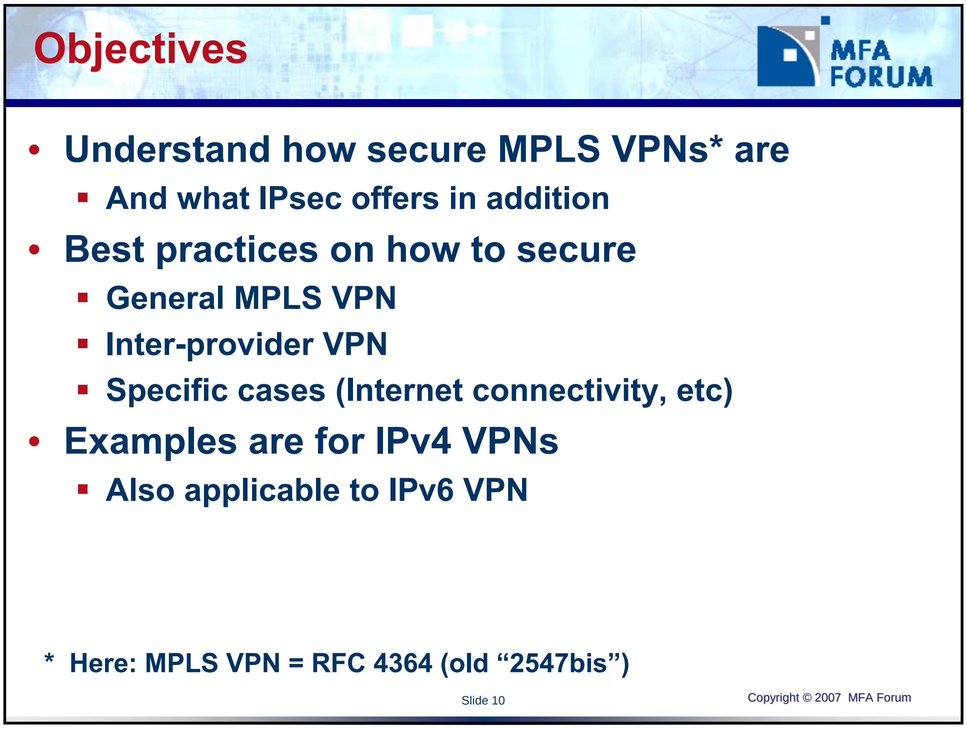


Why Is MPLS VPN Security Important?

- 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: Few or no further security measures required

SP Must Ensure Secure MPLS Operations

Slide 9

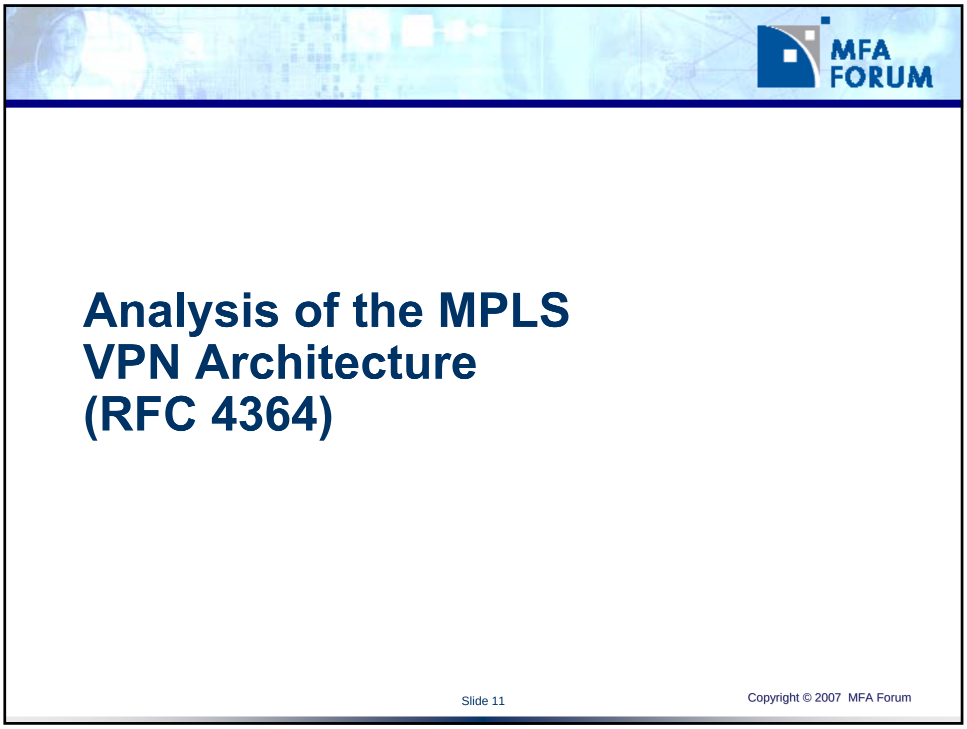


Objectives

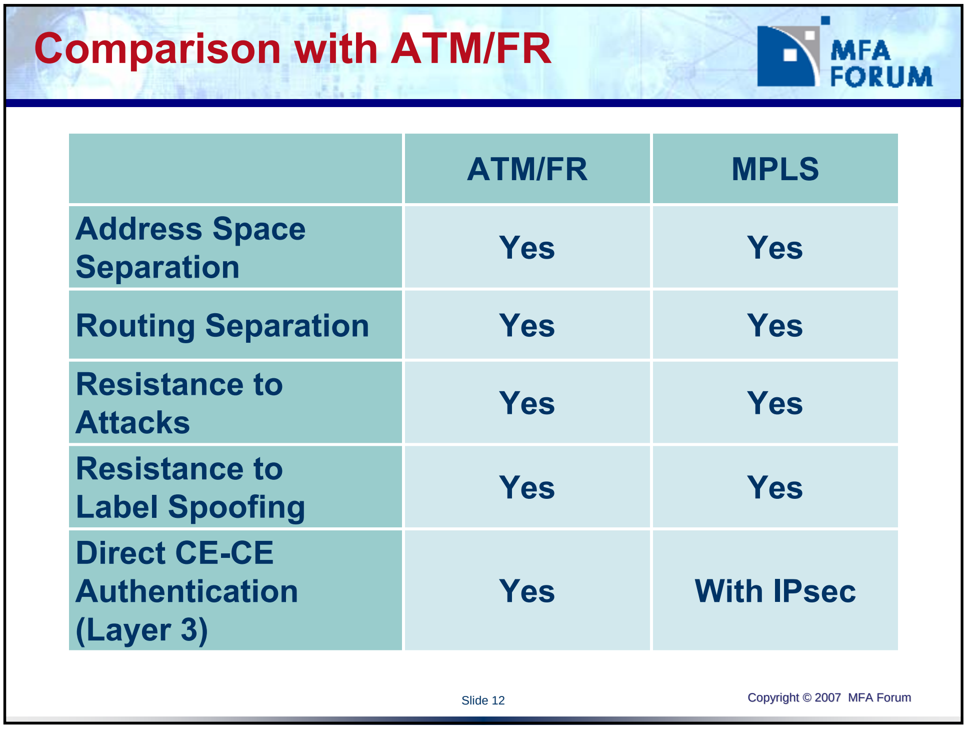
- Understand how secure MPLS VPNs* are
  - And what IPsec offers in addition
- Best practices on how to secure
  - General MPLS VPN
  - Inter-provider VPN
  - Specific cases (Internet connectivity, etc)
- Examples are for IPv4 VPNs
  - Also applicable to IPv6 VPN

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

Slide 10

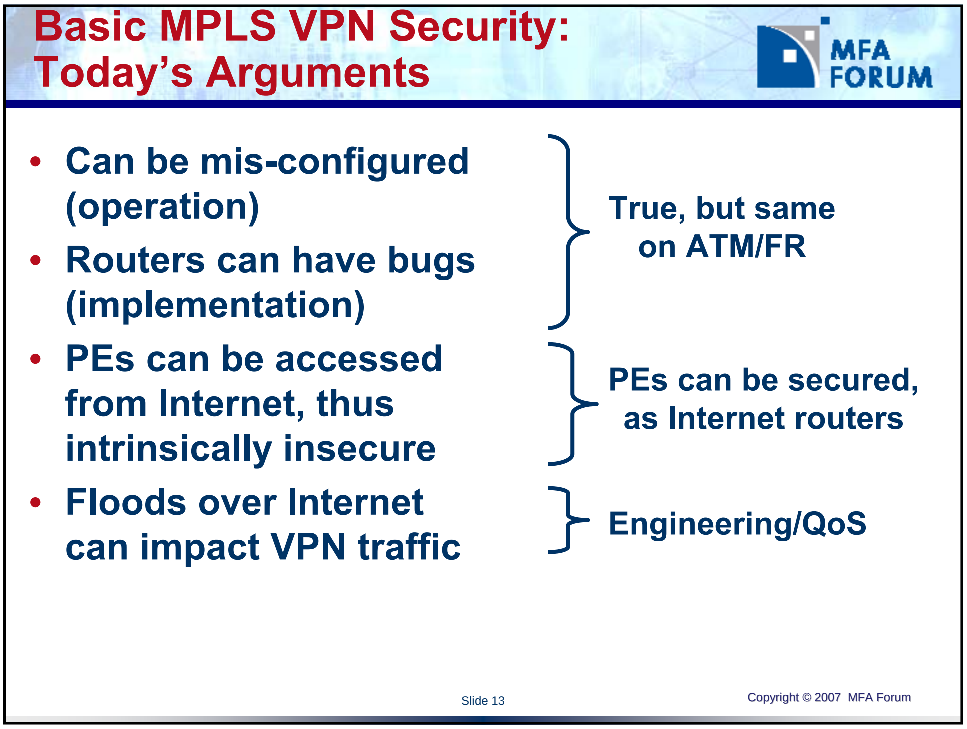


Analysis of the MPLS VPN Architecture (RFC 4364)



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 MPLS VPN Security: Today’s Arguments

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

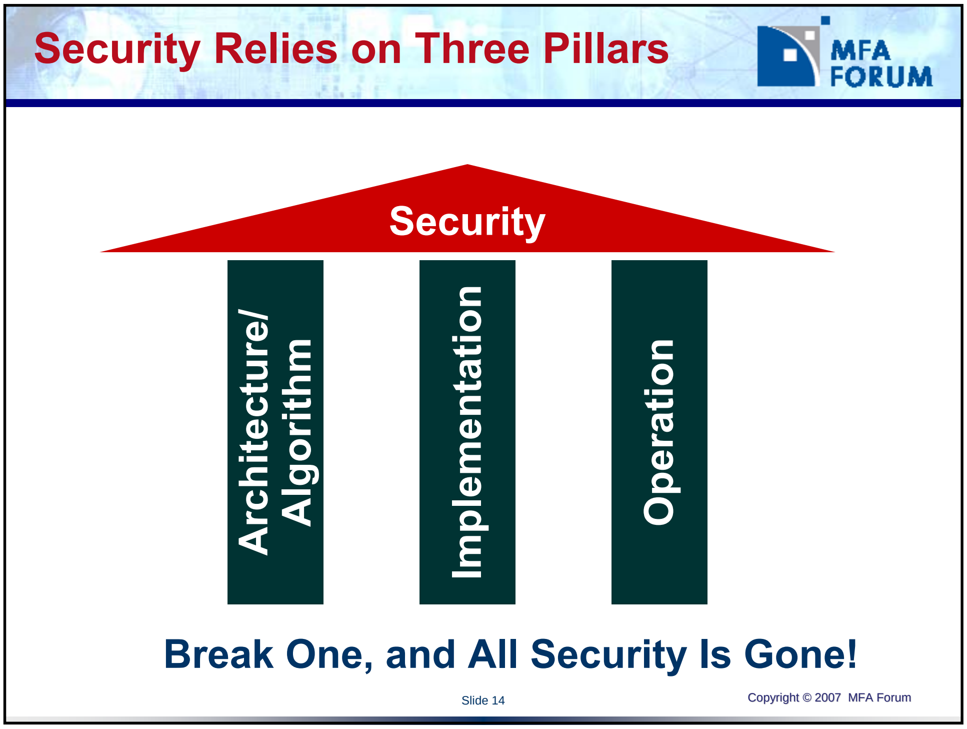
True, but same on ATM/FR

- 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

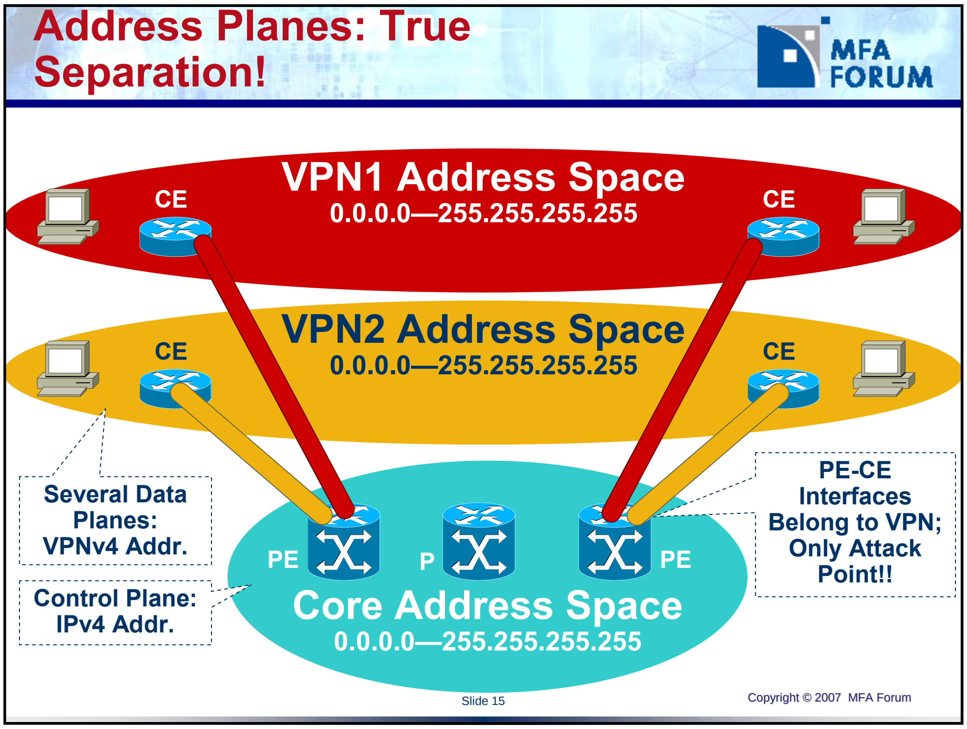
Security

Architecture/ Algorithm

Implementation

Operation

Break One, and All Security Is Gone!



Address Planes: True Separation!

MFA FORUM

VPN1 Address Space
0.0.0.0—255.255.255.255

CE

CE

VPN2 Address Space
0.0.0.0—255.255.255.255

CE

CE

Several Data Planes: VPNv4 Addr.

Control Plane: IPv4 Addr.

PE

P

PE

Core Address Space
0.0.0.0—255.255.255.255

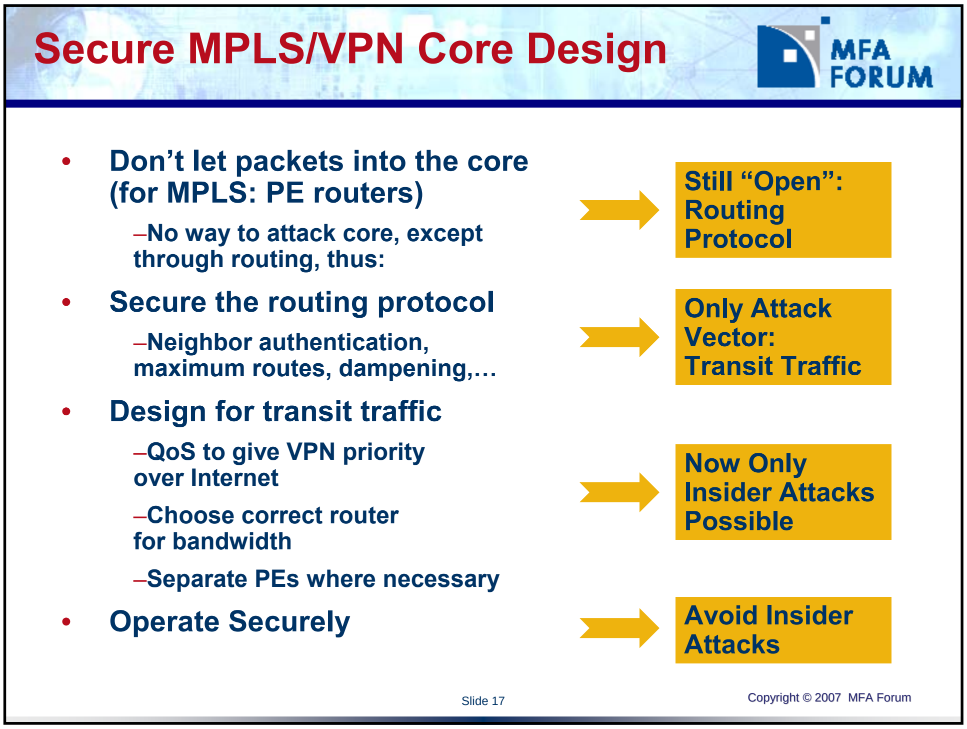
PE-CE Interfaces Belong to VPN; Only Attack Point!!

Slide 15

MFA FORUM

Secure MPLS VPN Design — General Security Best Practices

Slide 16



Secure MPLS/VPN Core Design

- Don’t let packets into the core (for MPLS: PE routers)
  - –No way to attack core, except through routing, thus:
- Secure the routing protocol
  - –Neighbor authentication, maximum routes, dampening,…
- Design for transit traffic
  - –QoS to give VPN priority over Internet
  - –Choose correct router for bandwidth
  - –Separate PEs where necessary
- Operate Securely

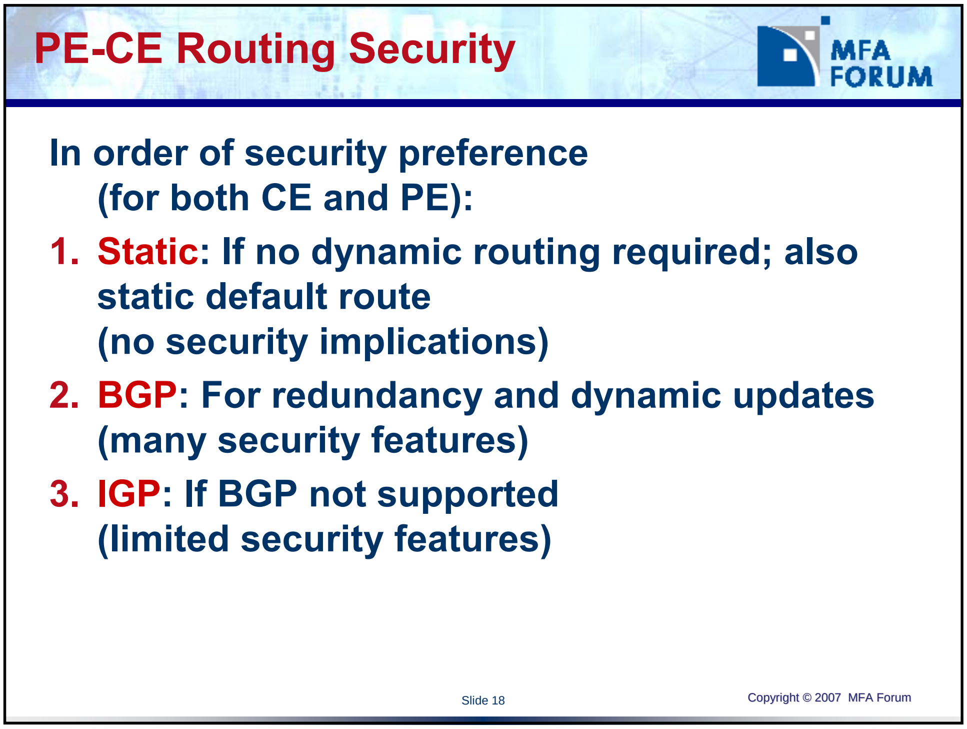
Still “Open”: Routing Protocol

Only Attack Vector: Transit Traffic

Now Only Insider Attacks Possible

Avoid Insider Attacks

Slide 17

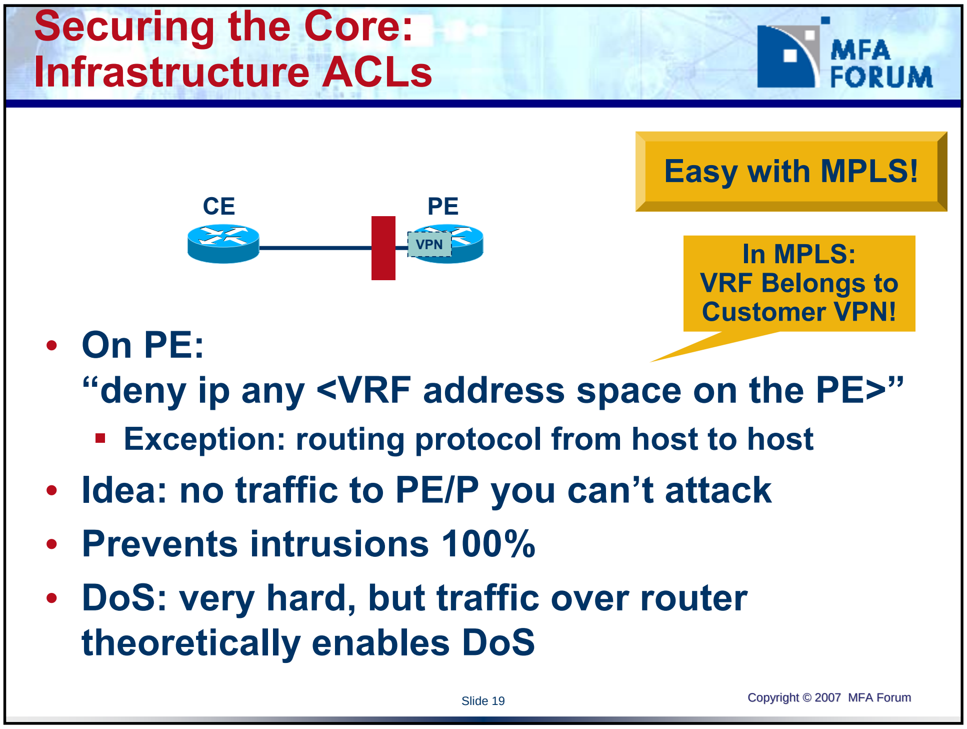


PE-CE Routing Security

In order of security preference
(for both CE and PE):

1. Static: If no dynamic routing required; also static default route
(no security implications)
2. BGP: For redundancy and dynamic updates
(many security features)
3. IGP: If BGP not supported
(limited security features)

Slide 18

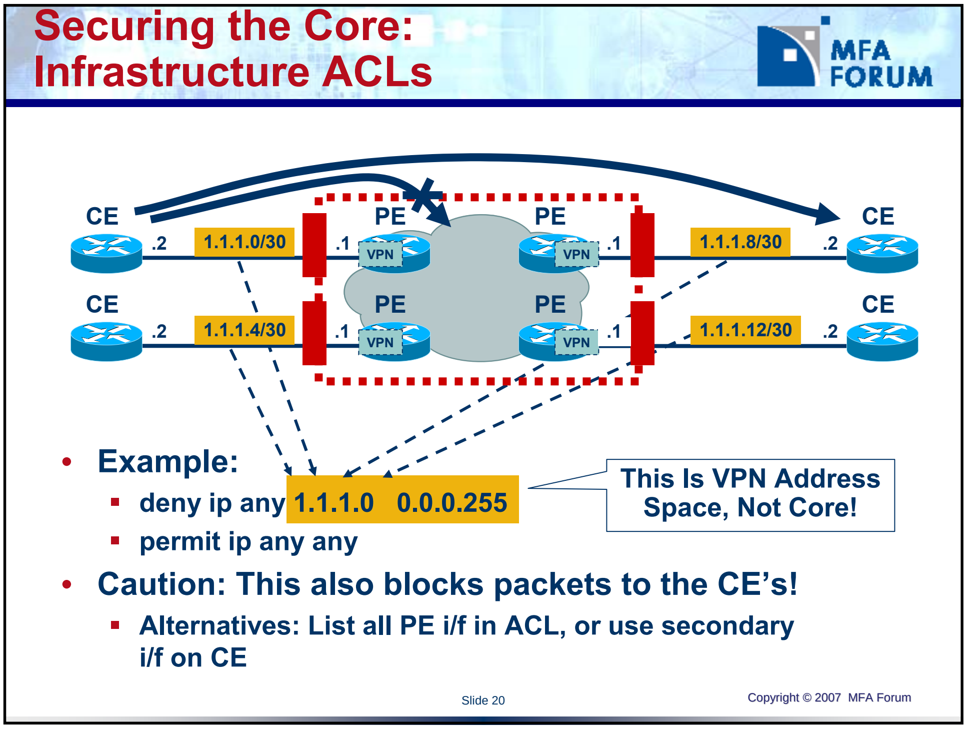


Securing the Core: Infrastructure ACLs

Easy with MPLS!

In MPLS: VRF Belongs to Customer VPN!

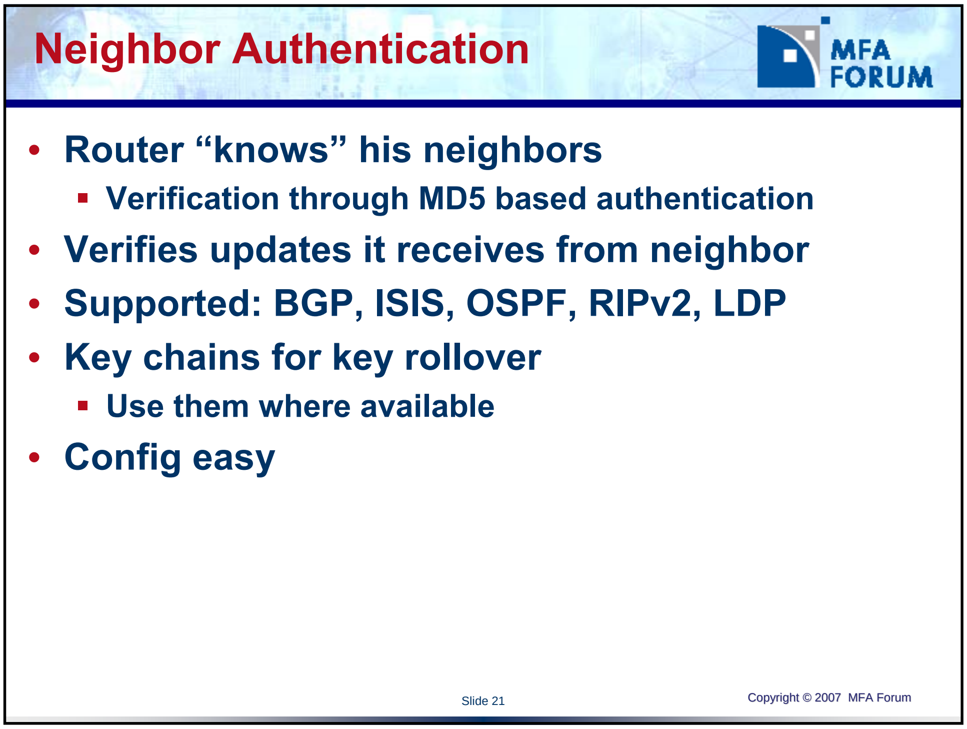
- On PE:
  “deny ip any <VRF address space on the PE>”
  - Exception: routing protocol from host to host
- Idea: no traffic to PE/P you can’t attack
- Prevents intrusions 100%
- DoS: very hard, but traffic over router theoretically enables DoS



Securing the Core: Infrastructure ACLs

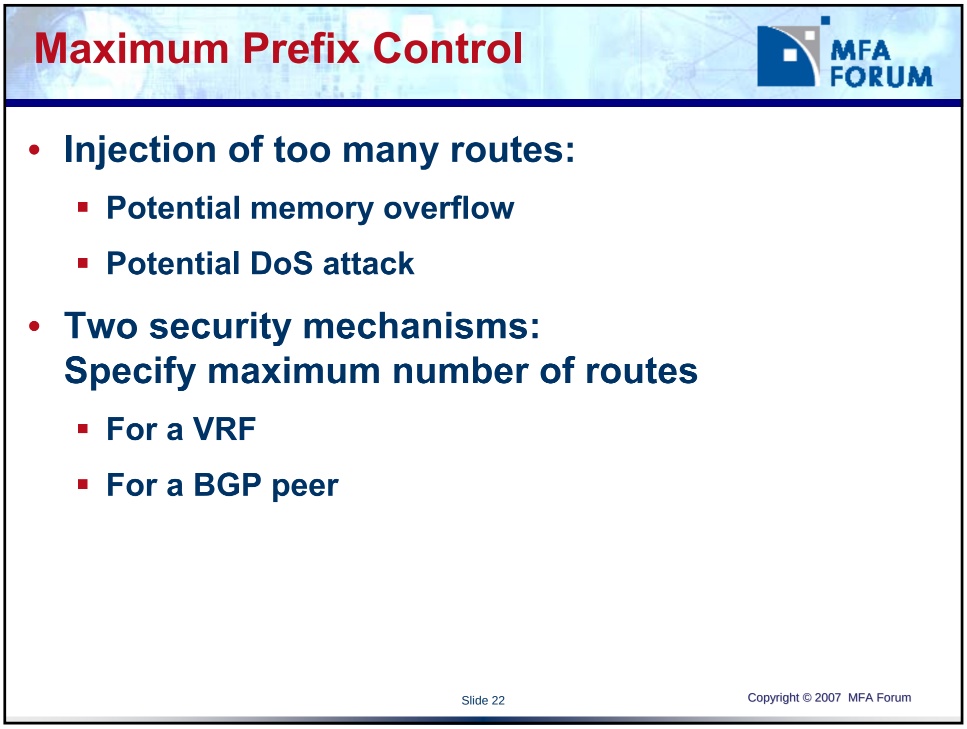
- Example:
  - deny ip any 1.1.1.0 0.0.0.255
  - permit ip any any
- Caution: This also blocks packets to the CE’s!
  - Alternatives: List all PE i/f in ACL, or use secondary i/f on CE

This Is VPN Address Space, Not Core!



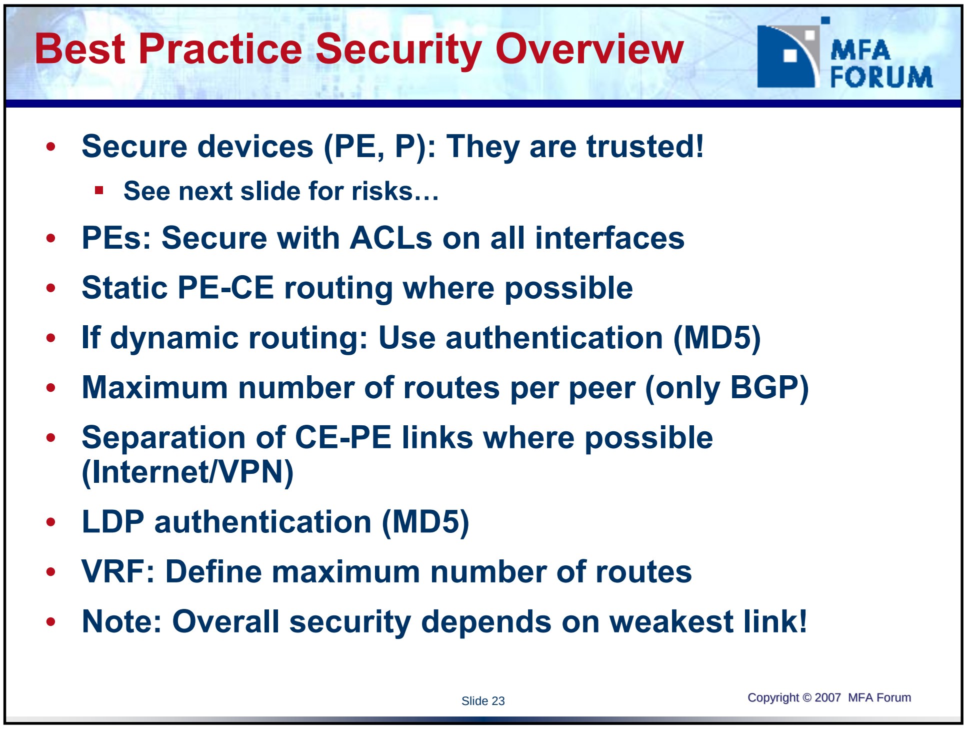
Neighbor Authentication

- Router “knows” his neighbors
  - Verification through MD5 based authentication
- Verifies updates it receives from neighbor
- Supported: BGP, ISIS, OSPF, RIPv2, LDP
- Key chains for key rollover
  - Use them where available
- Config easy



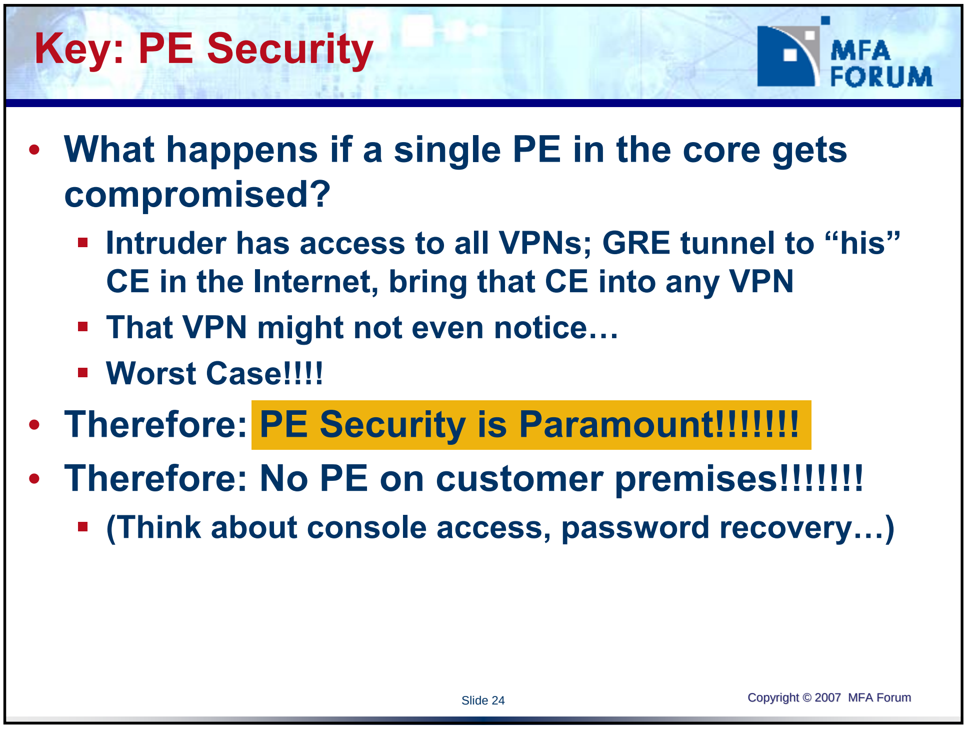
Maximum Prefix Control

- Injection of too many routes:
  - Potential memory overflow
  - Potential DoS attack
- Two security mechanisms:
  Specify maximum number of routes
  - For a VRF
  - For a BGP peer



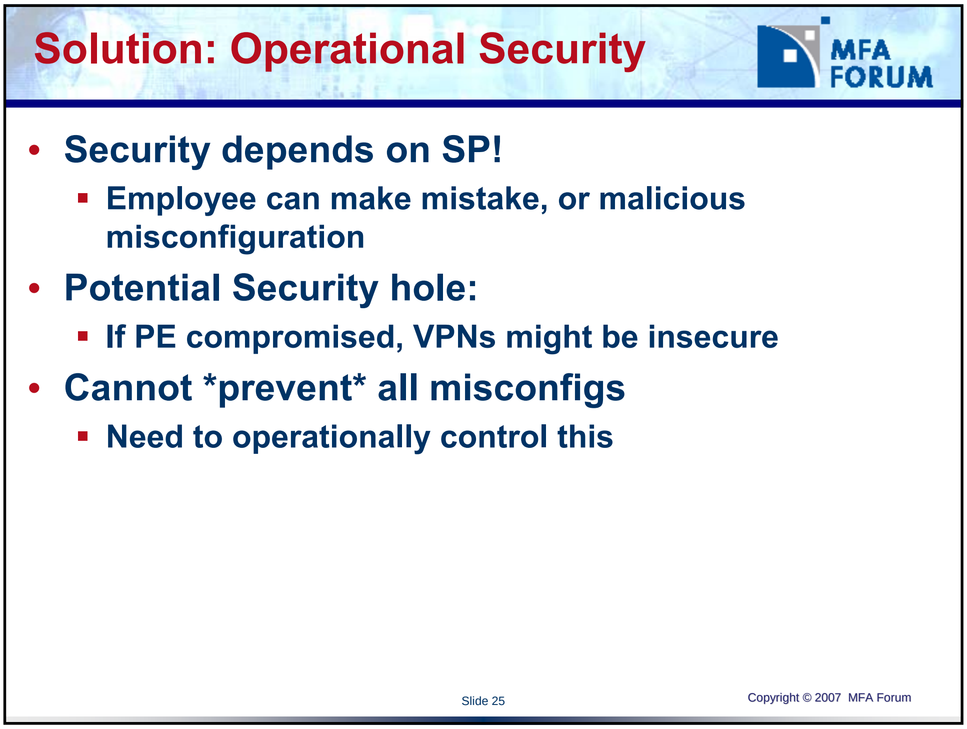
Best Practice Security Overview

- Secure devices (PE, P): They are trusted!
  - See next slide for risks…
- PEs: Secure with ACLs on all interfaces
- Static PE-CE routing where possible
- If dynamic routing: Use authentication (MD5)
- Maximum number of routes per peer (only BGP)
- 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!



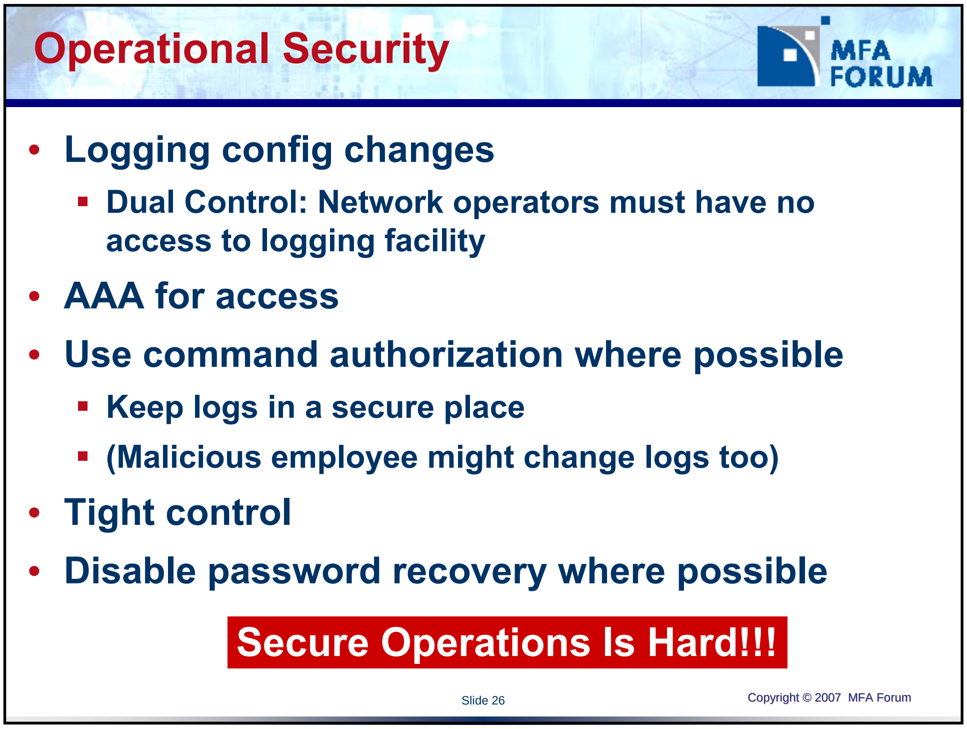
Key: PE Security

- 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…)



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

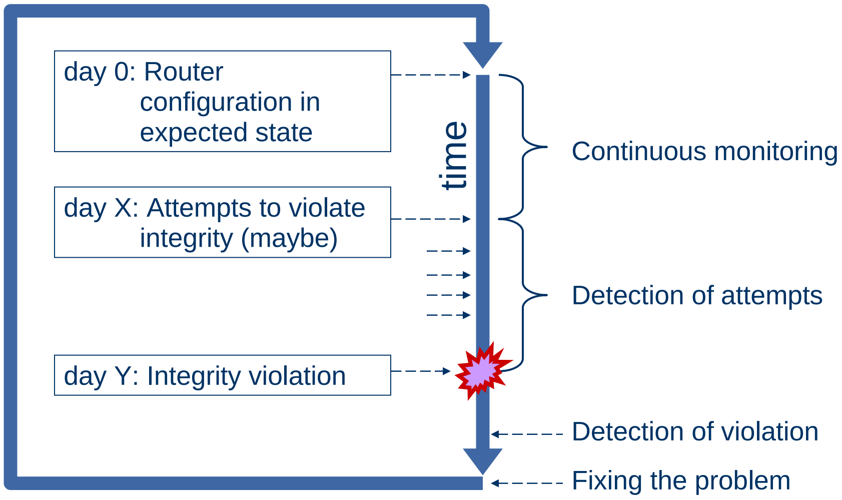


Operational Security

- Logging config changes
  - Dual Control: Network operators must have no access to logging facility
- AAA for access
- Use command authorization where possible
  - Keep logs in a secure place
  - (Malicious employee might change logs too)
- Tight control
- Disable password recovery where possible

Secure Operations Is Hard!!!

Operational Security: The Process



day 0: Router configuration in expected state

day X: Attempts to violate integrity (maybe)

day Y: Integrity violation

Continuous monitoring

Detection of attempts

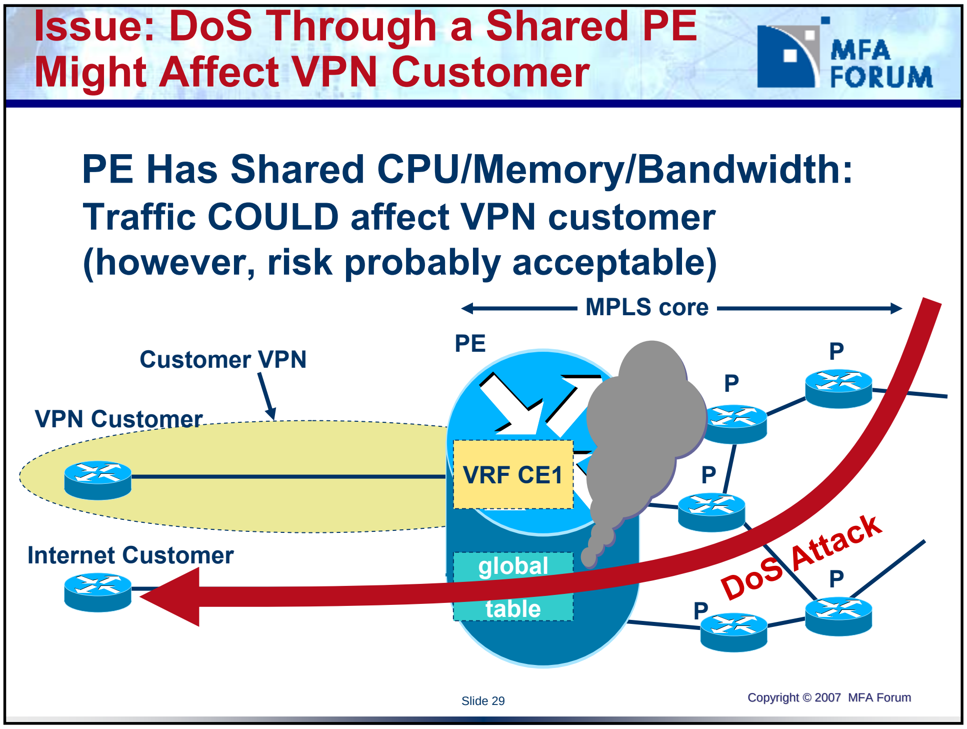
Detection of violation

Fixing the problem

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…



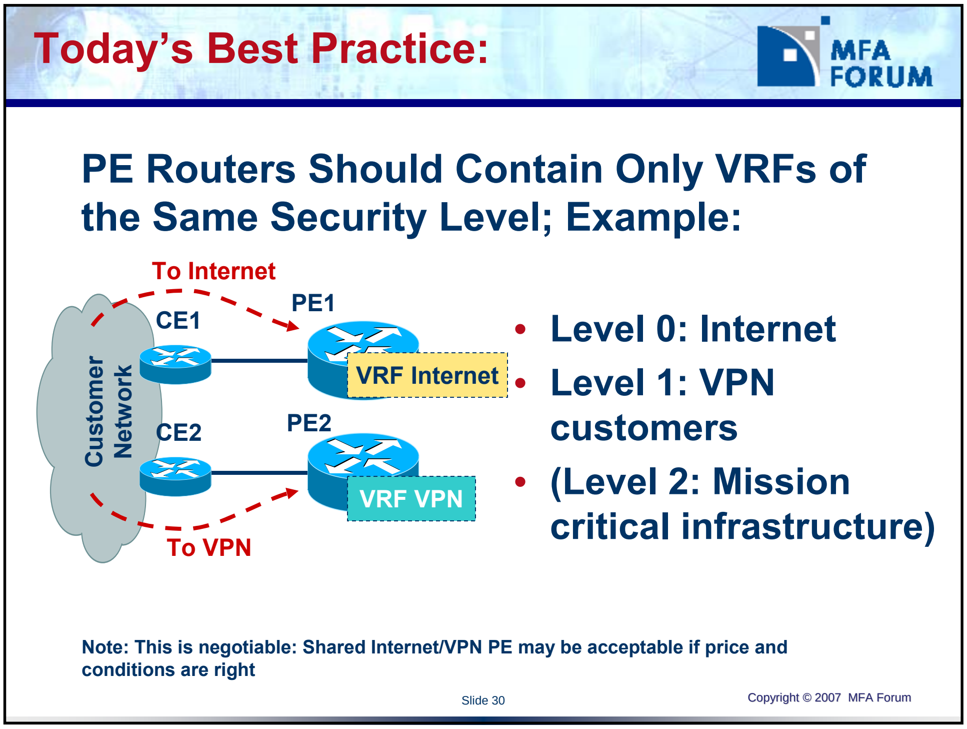
Issue: DoS Through a Shared PE Might Affect VPN Customer

MFA FORUM

PE Has Shared CPU/Memory/Bandwidth:

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

Slide 29



Today's Best Practice:

MFA FORUM

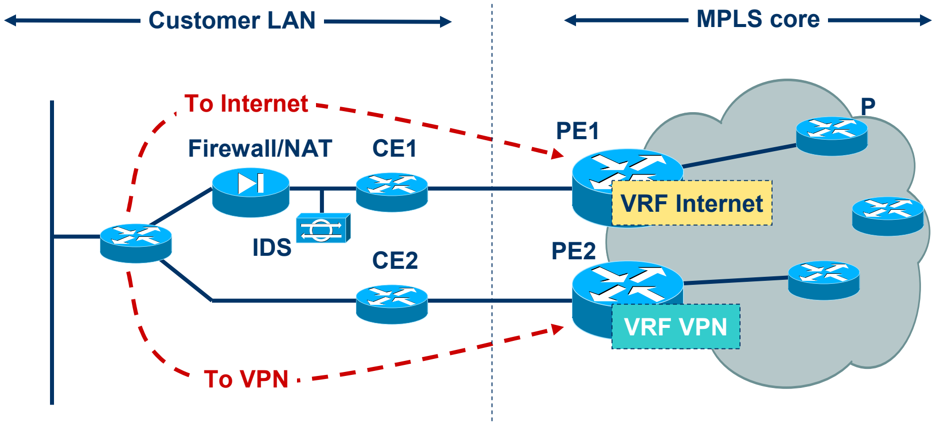
PE Routers Should Contain Only VRFs of the Same Security Level; Example:

- 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

Slide 30

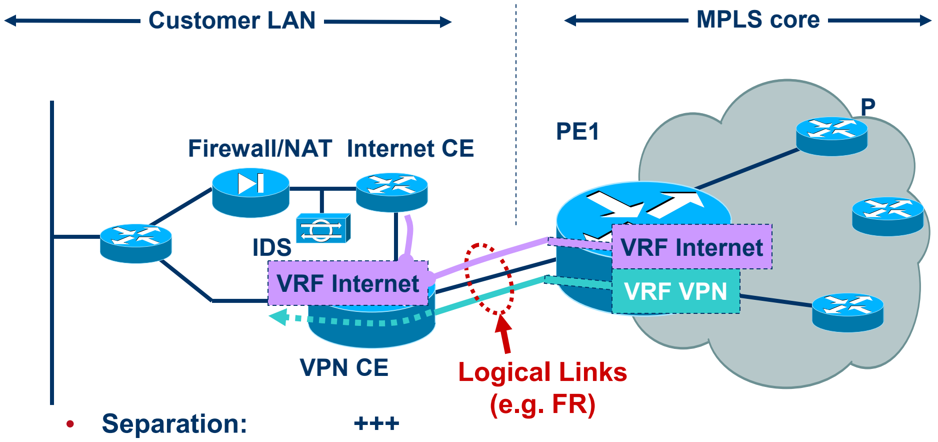
Separate VPN and Internet Access



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

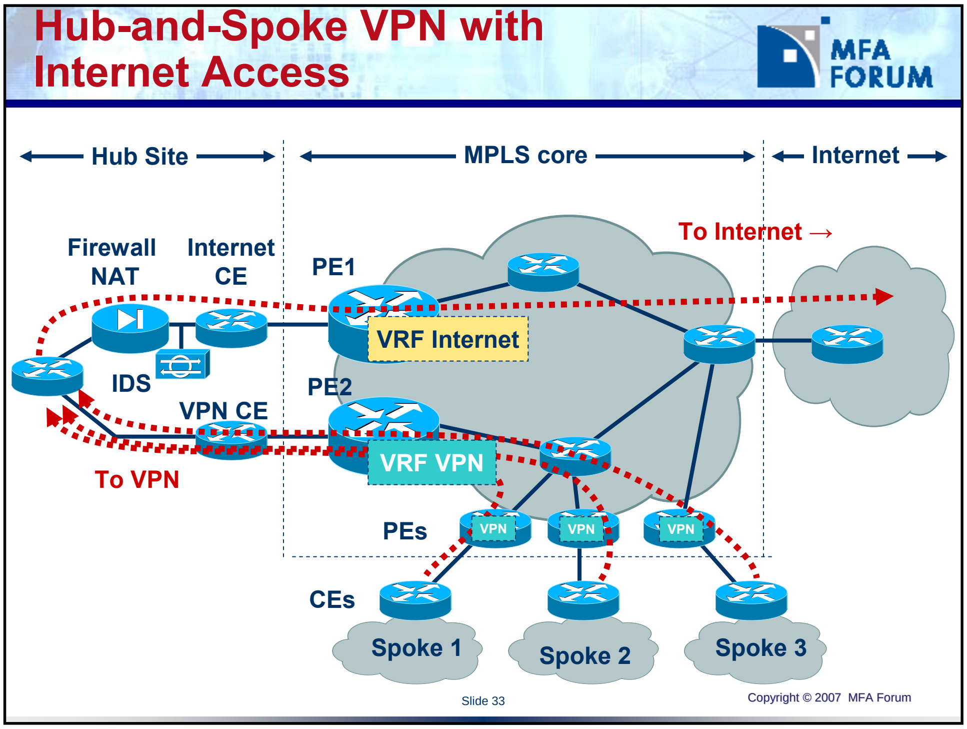
Slide 31

Shared Access Line, CE with VRF Lite



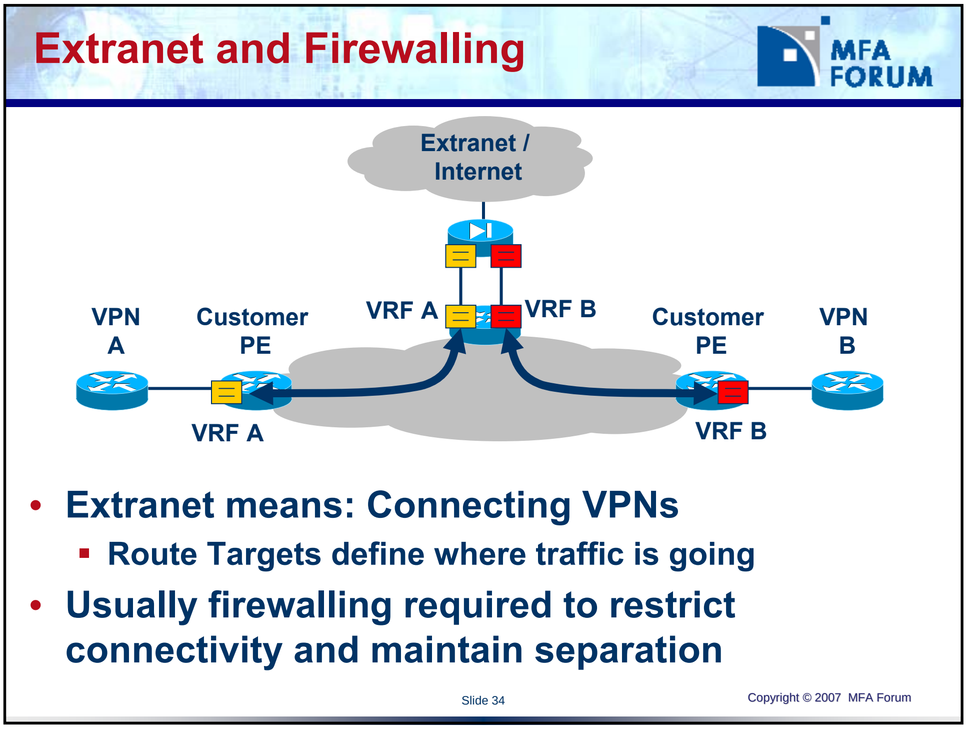
- Separation: +++
- DoS resistance: + (DoS might affect VPN on PE, attachment circuit, CE)
- Cost: $

Slide 32



Hub-and-Spoke VPN with Internet Access

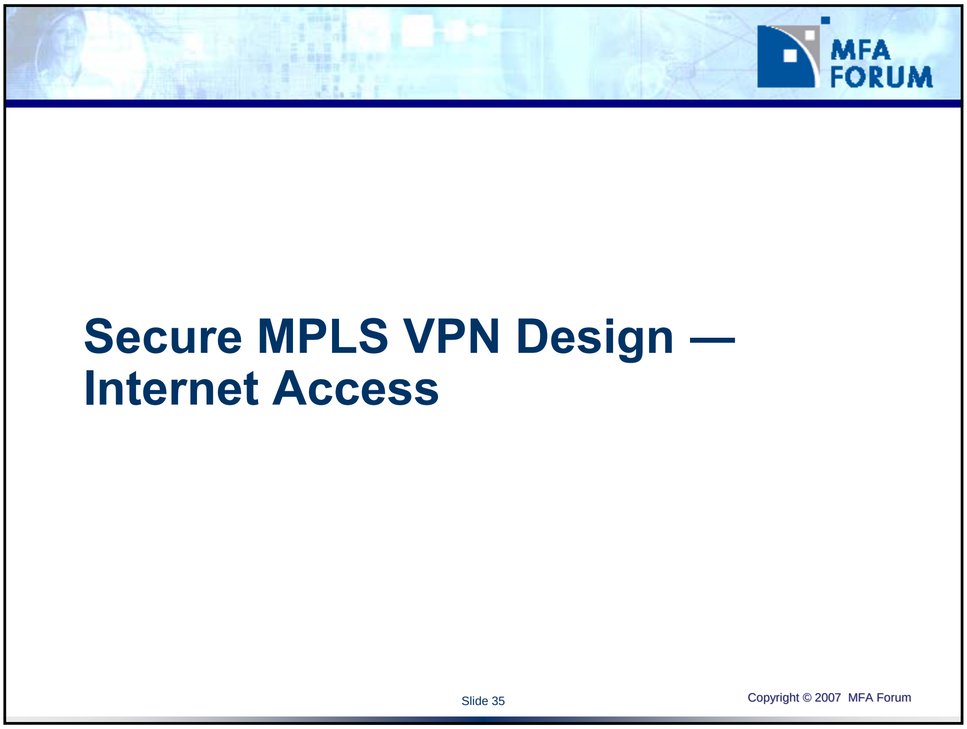
Slide 33



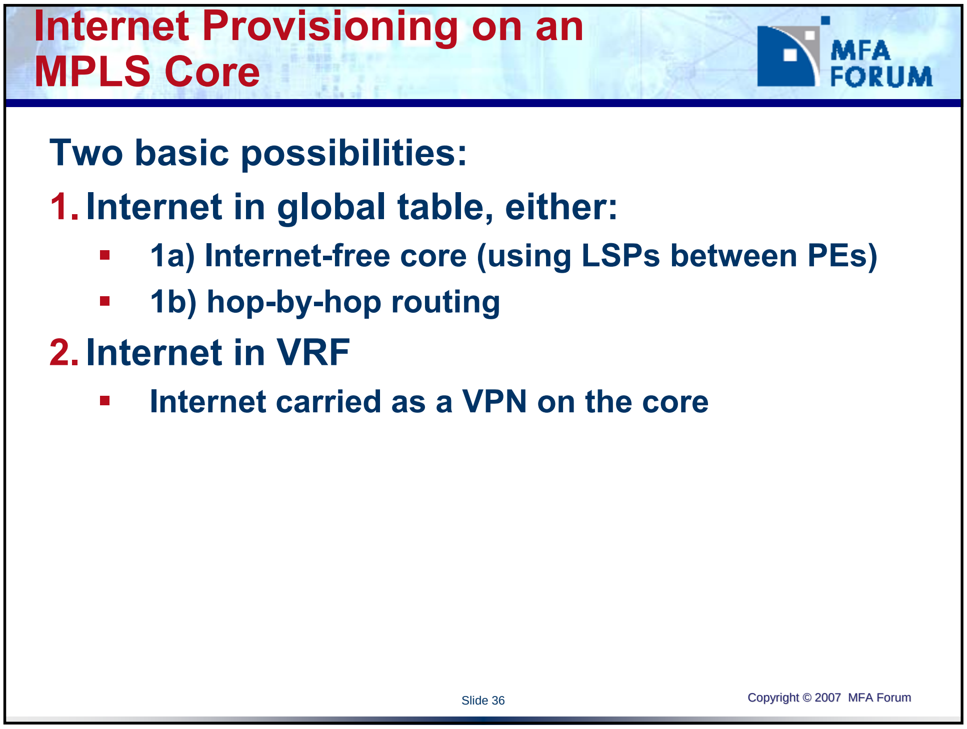
Extranet and Firewalling

- Extranet means: Connecting VPNs
  - Route Targets define where traffic is going
- Usually firewalling required to restrict connectivity and maintain separation

Slide 34



Secure MPLS VPN Design — Internet Access



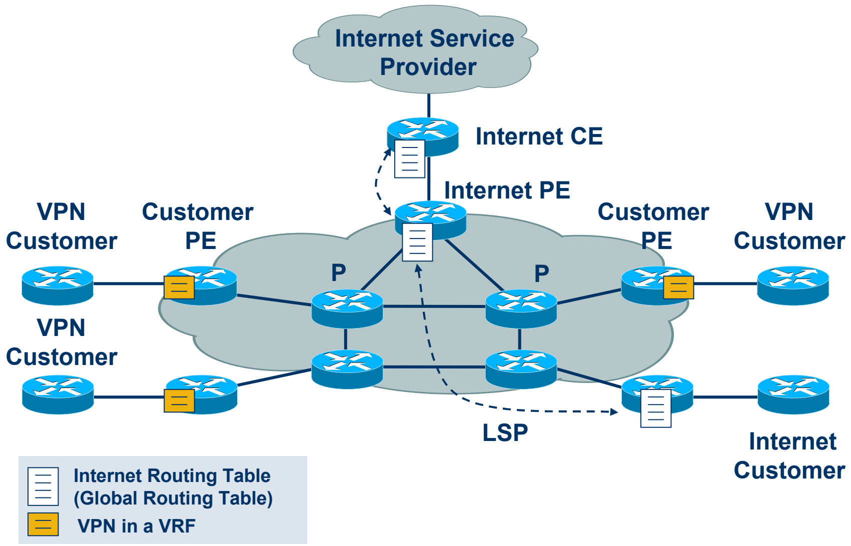
Internet Provisioning on an MPLS Core

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

Internet in Global Routing Table Using LSPs Between PEs

MFA FORUM



Internet in Global Routing Table Using LSPs Between PEs

MFA FORUM

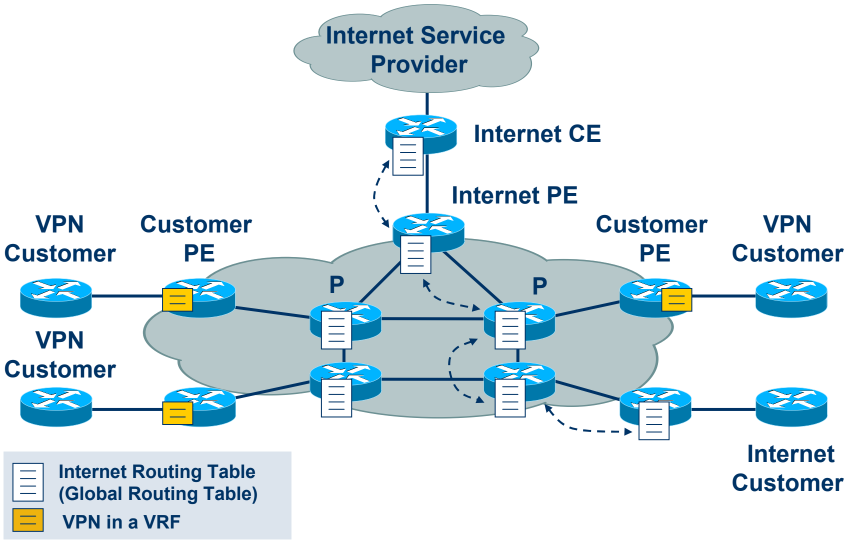
- Default behavior, if Internet in global table!!
  - On ingress PE: BGP next hop: Egress PE loopback
  - Next hop to egress usually has label!
  - LSP is used to reach egress PE
  - P routers do not need to know Internet routes (nor run BGP)
- Security consequence:
  - PE routers are fully reachable 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!

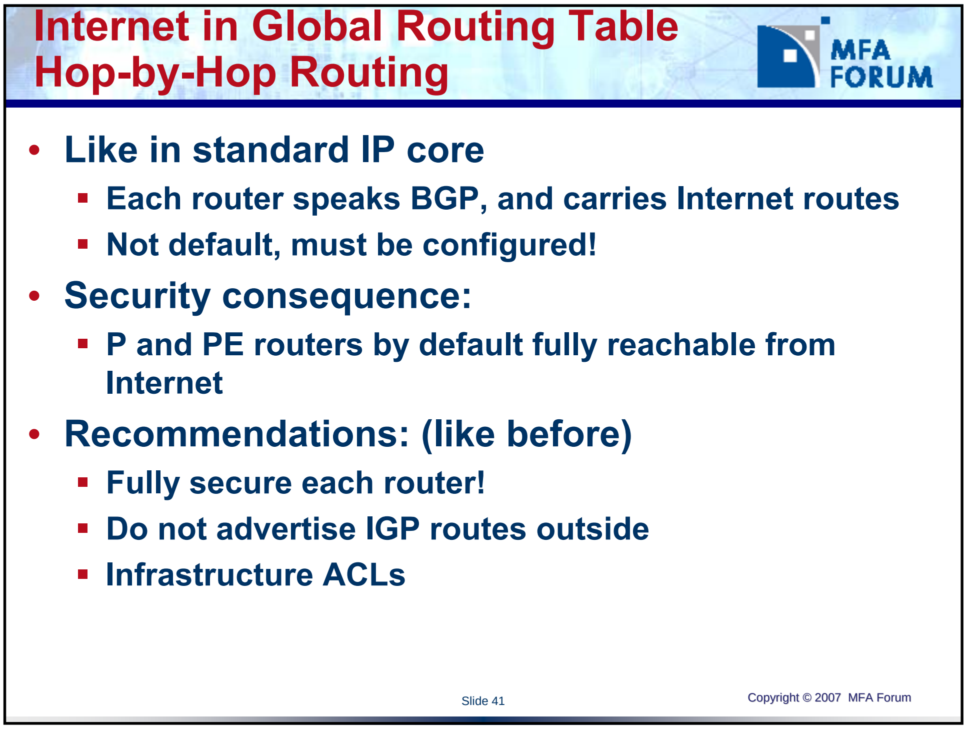
Internet in Global Routing Table Using LSPs Between PEs

Recommendations:

- Fully secure each router!
- Do not advertise IGP routes outside
  - (General 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 Global Routing Table Hop-by-Hop Routing

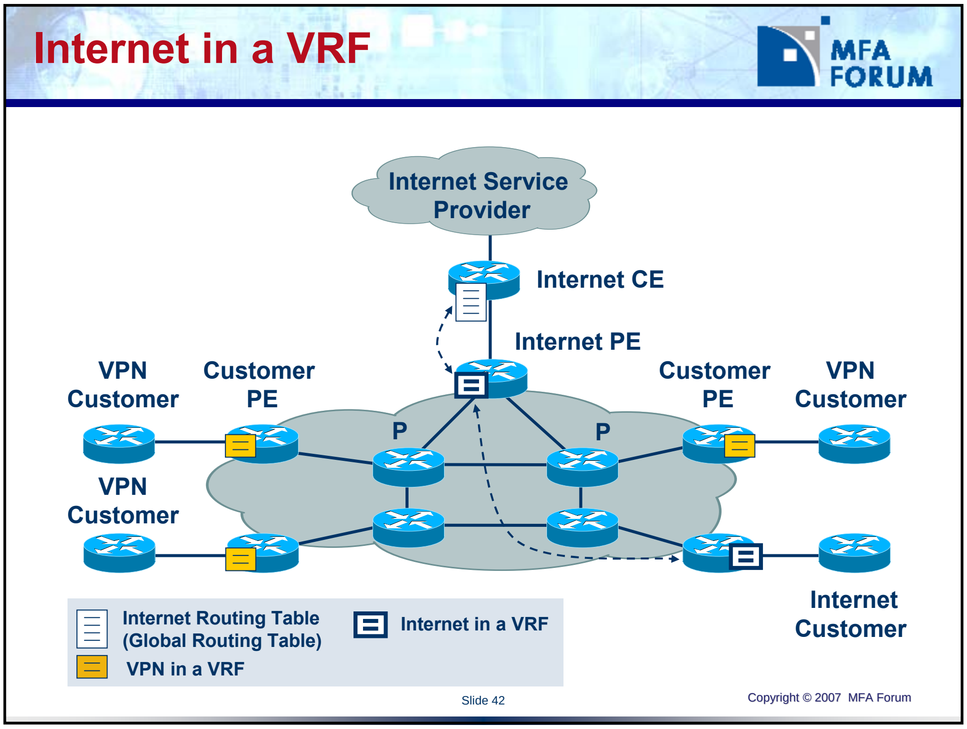




Internet in Global Routing Table Hop-by-Hop Routing

- 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

Slide 41



Internet in a VRF

Internet Service Provider

Internet CE

Internet PE

VPN Customer

Customer PE

P

P

Customer PE

VPN Customer

VPN Customer

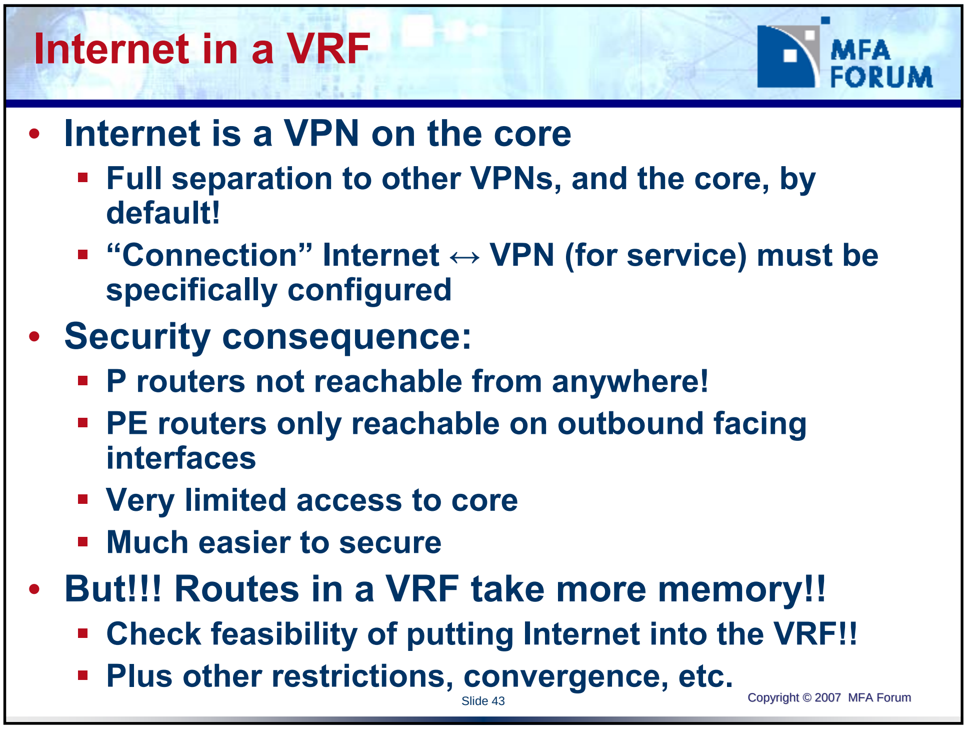
Internet Customer

☰ Internet Routing Table (Global Routing Table)

🟨 VPN in a VRF

⊟ Internet in a VRF

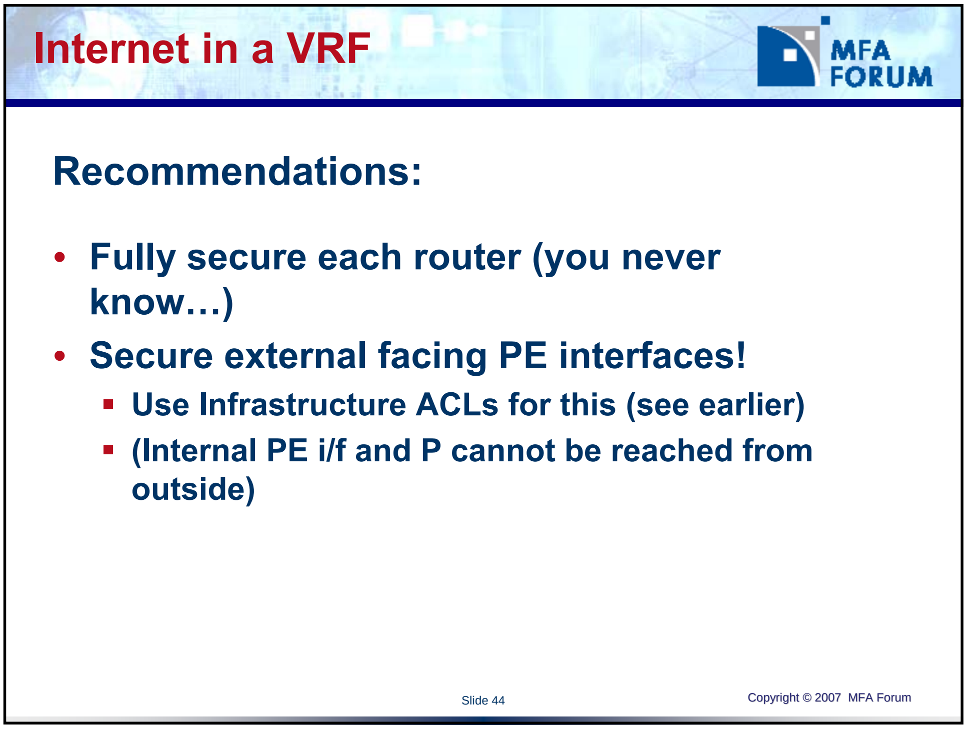
Slide 42



Internet in a VRF

MFA FORUM

- Internet is a VPN on the core
  - Full separation to other VPNs, and the core, by default!
  - “Connection” Internet ↔ 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 access to core
  - Much easier to secure
- But!!! Routes in a VRF take more memory!!
  - Check feasibility of putting Internet into the VRF!!
  - Plus other restrictions, convergence, etc.



Internet in a VRF

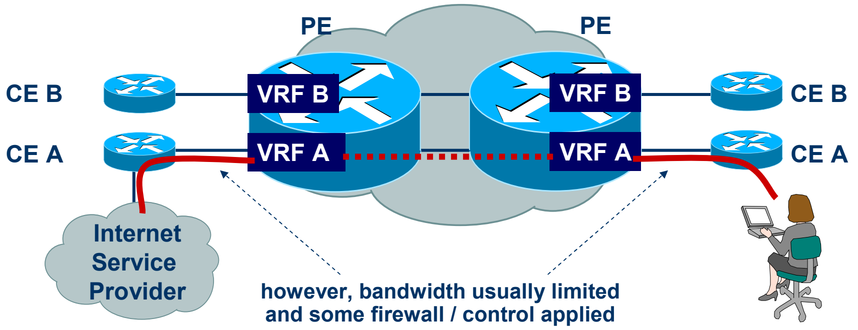
MFA FORUM

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)

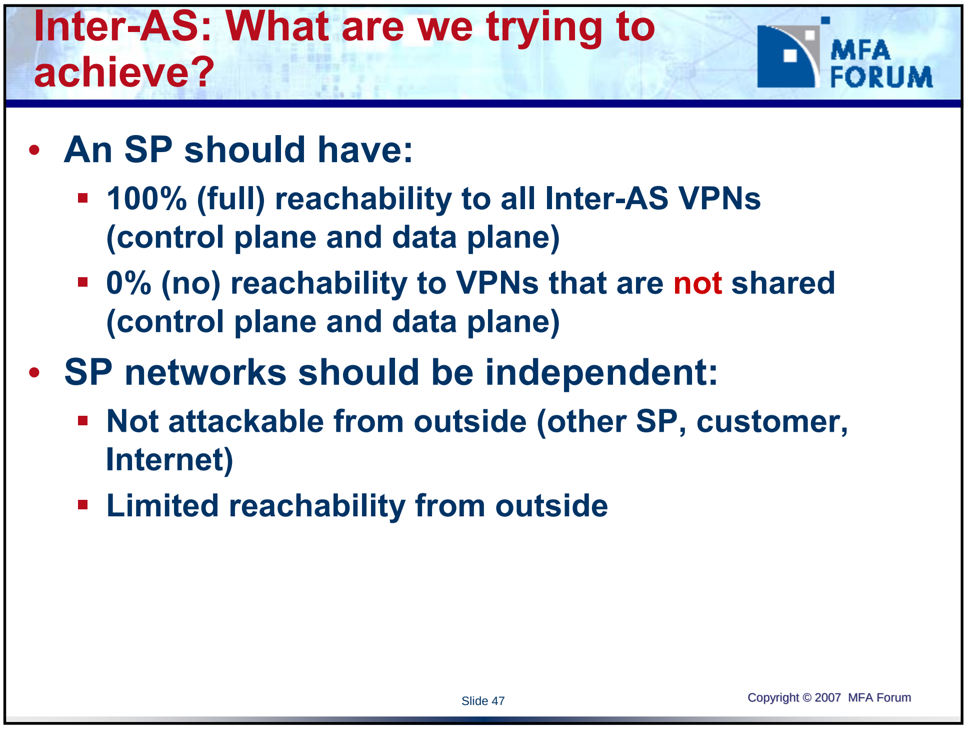
Alternatively: No Internet on the Core

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



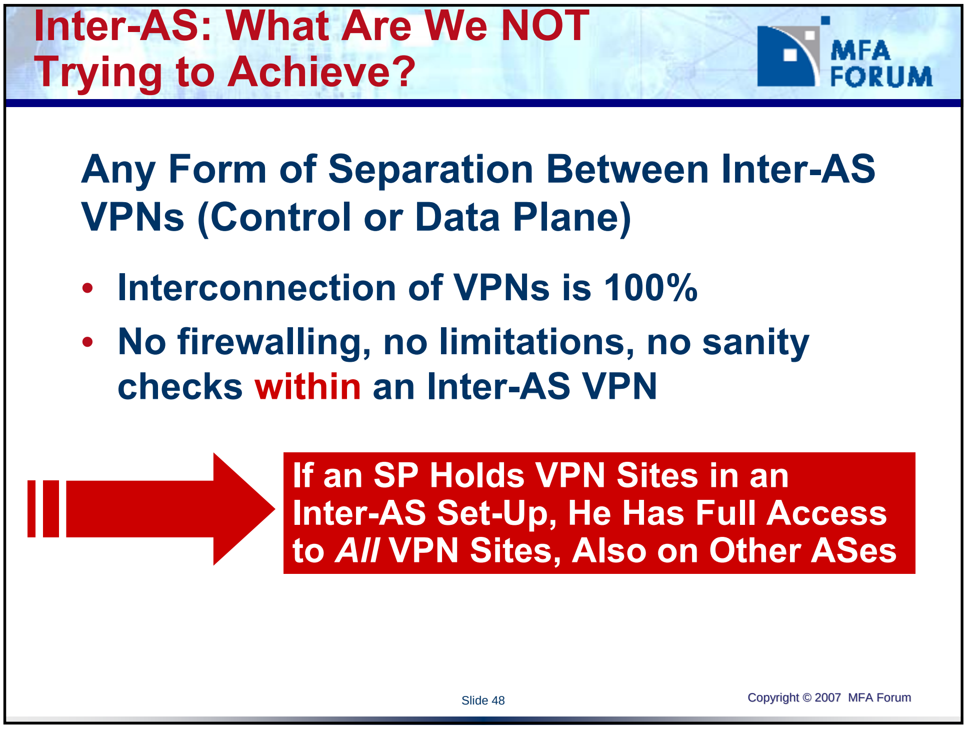
however, bandwidth usually limited and some firewall / control applied

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



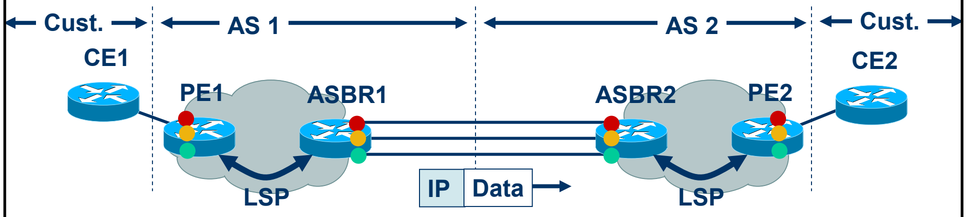
Inter-AS: What Are We NOT Trying to Achieve?

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

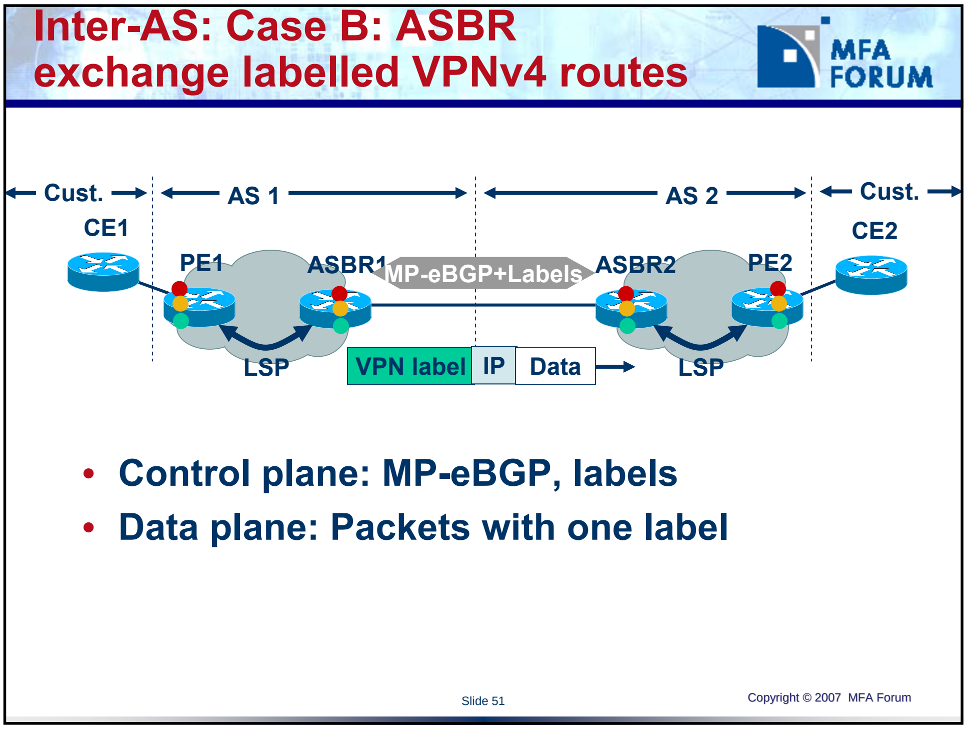
Inter-AS: Case A
VRF-VRF Back-to-Back



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

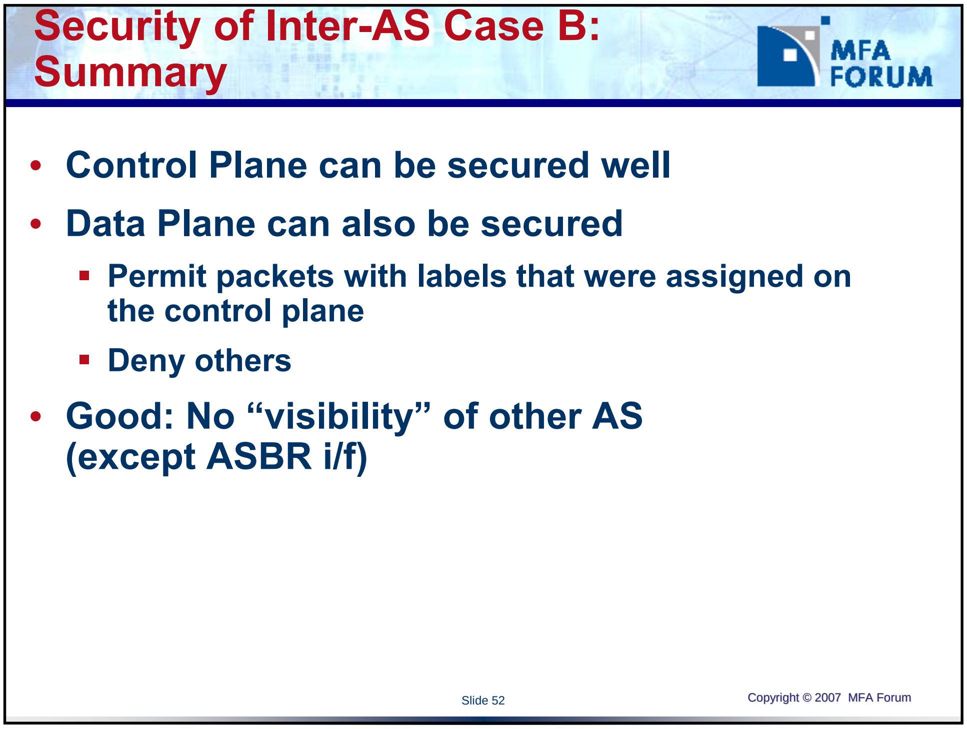
Security of Inter-AS case A

- 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 incorrectly connect VPNs (like in ATM/FR)
  - Customer can flood routing table on PE (this is the same issue as in single-AS; solution: prefix limits)



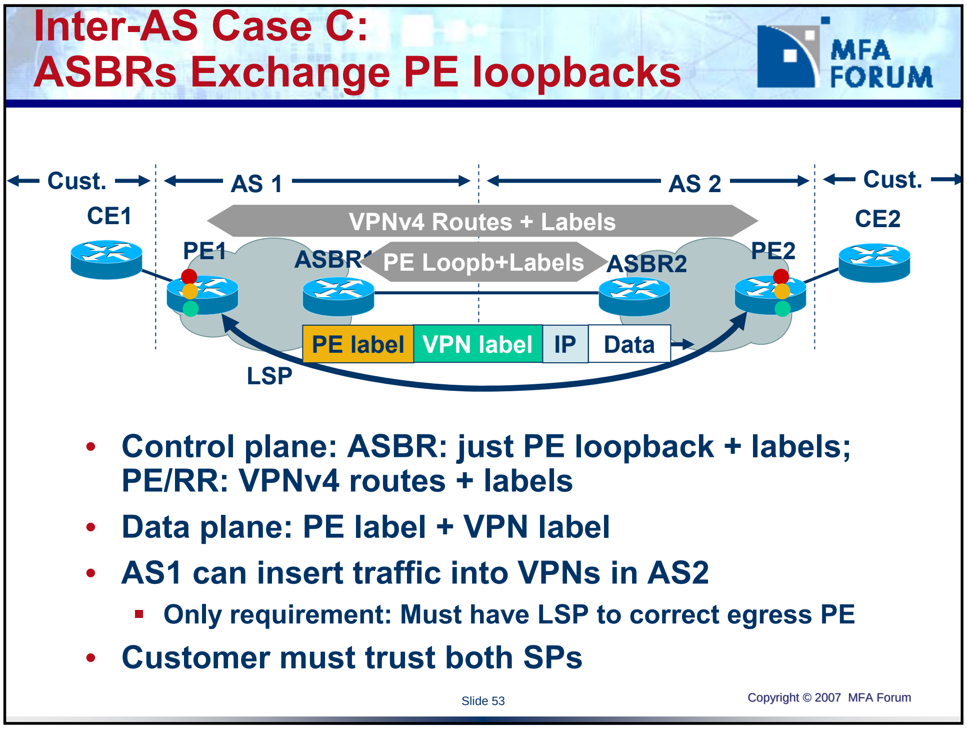
Inter-AS: Case B: ASBR exchange labelled VPNv4 routes

- Control plane: MP-eBGP, labels
- Data plane: Packets with one label



Security of Inter-AS Case B: Summary

- Control Plane can be secured well
- Data Plane can also be secured
  - Permit packets with labels that were assigned on the control plane
  - Deny others
- Good: No “visibility” of other AS (except ASBR i/f)

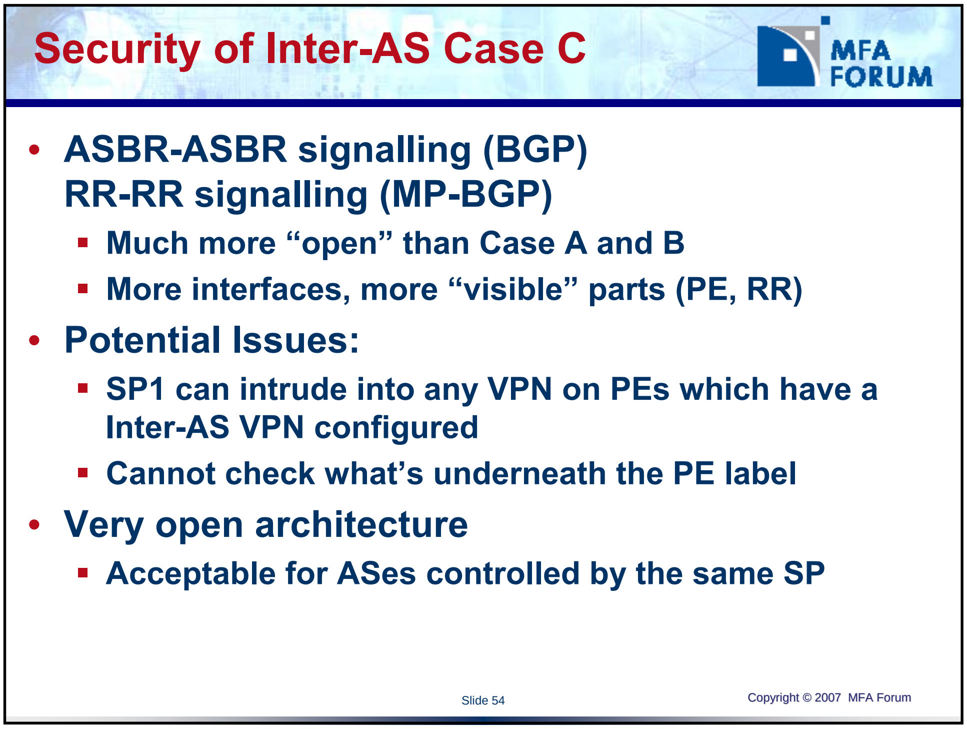


Inter-AS Case C: ASBRs Exchange PE loopbacks

MFA FORUM
Cust.
AS 1
AS 2
Cust.
CE1
CE2
VPNv4 Routes + Labels
PE1
ASBR1
PE Loopb+Labels
ASBR2
PE2
PE label
VPN label
IP
Data
LSP

- 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

Slide 53



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

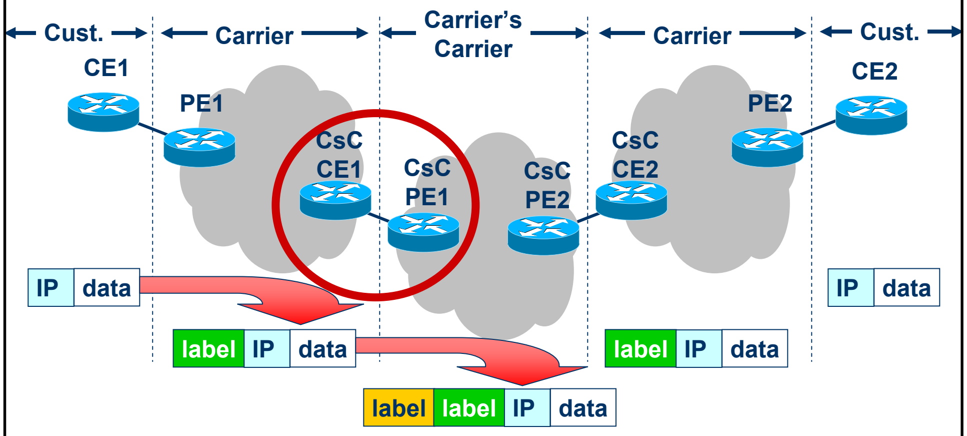
Slide 54

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 flow monitoring
- Case B and C are okay if all ASes are in control of one SP
- Otherwise: Current Recommendation: Use case A

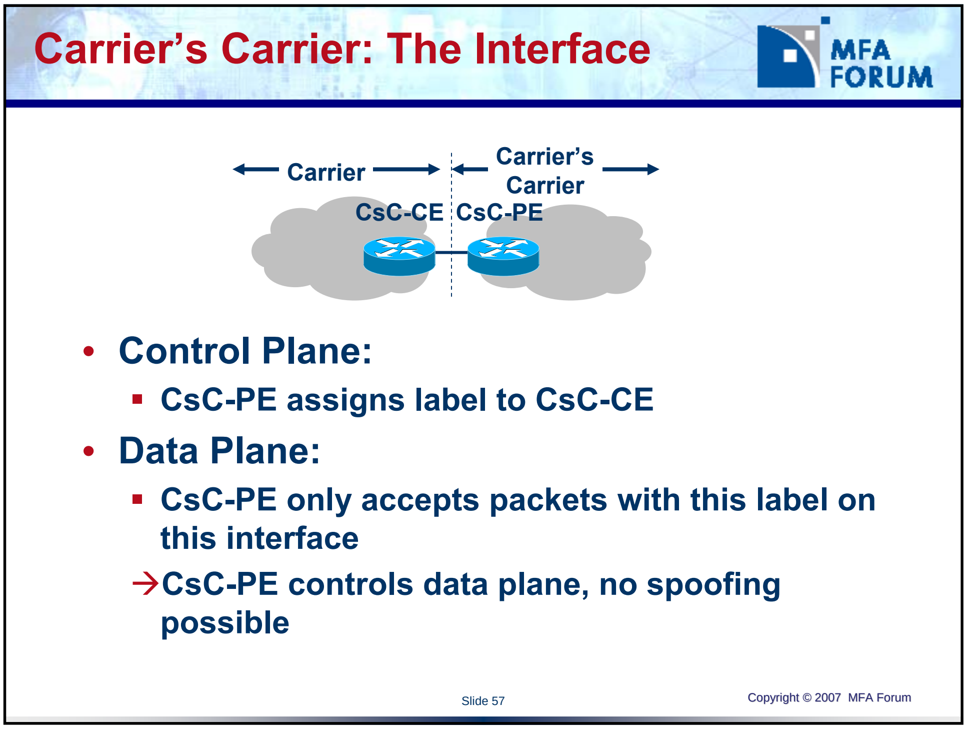
Slide 55

Carrier's Carrier



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

Slide 56



Carrier's Carrier: The Interface

MFA FORUM

Carrier

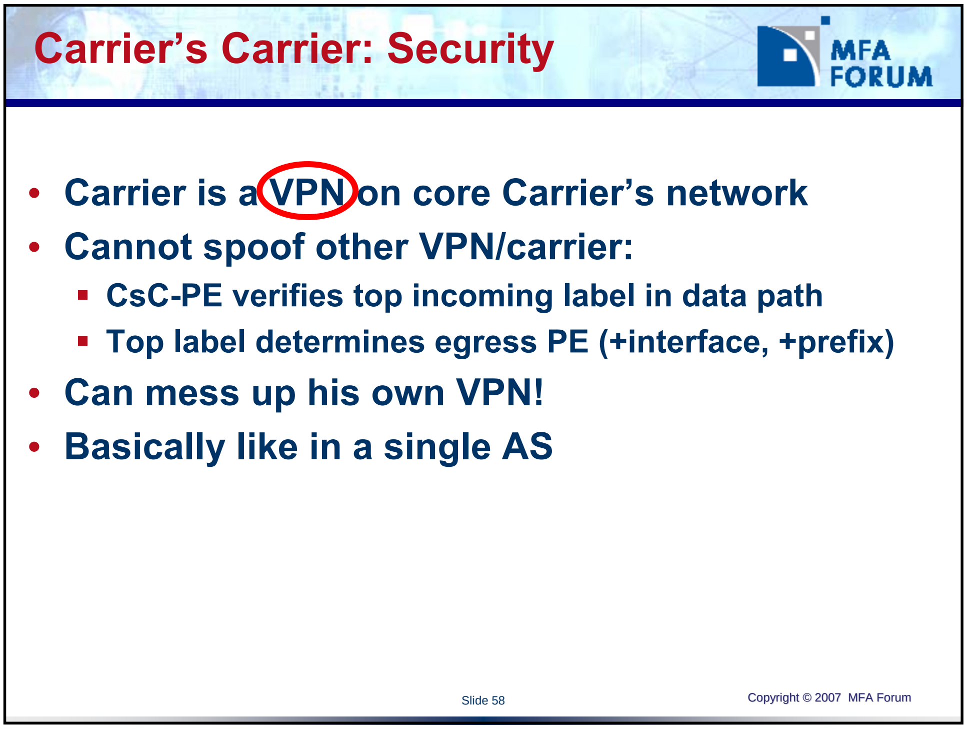
Carrier's Carrier

CsC-CE CsC-PE

- Control Plane:
  - CsC-PE assigns label to CsC-CE
- Data Plane:
  - CsC-PE only accepts packets with this label on this interface

  →CsC-PE controls data plane, no spoofing possible

Slide 57



Carrier's Carrier: Security

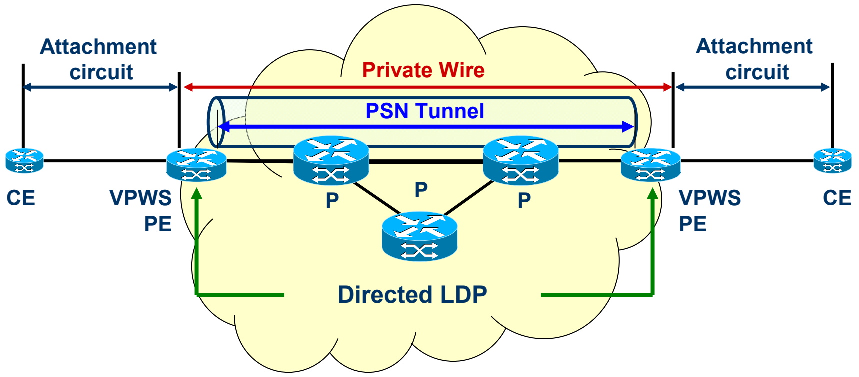
MFA FORUM

- Carrier is a VPN on core Carrier's network
- Cannot spoof other VPN/carrier:
  - CsC-PE verifies top incoming label in data path
  - Top label determines egress PE (+interface, +prefix)
- Can mess up his own VPN!
- Basically like in a single AS

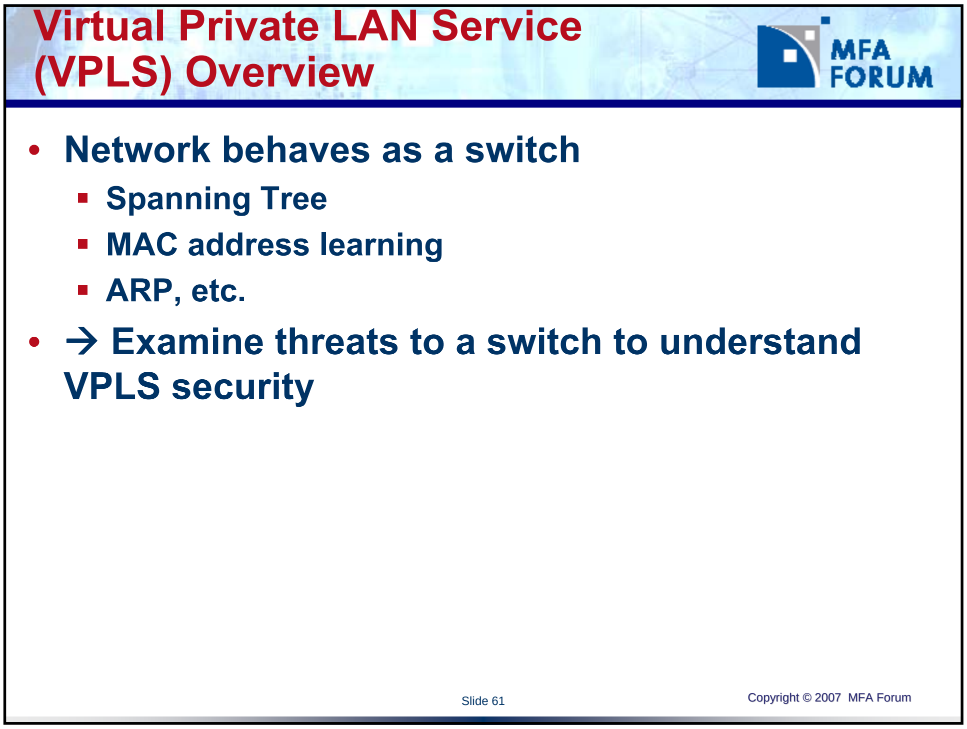
Slide 58

L2VPN Security

Virtual Private Wire Service (VPWS) Overview

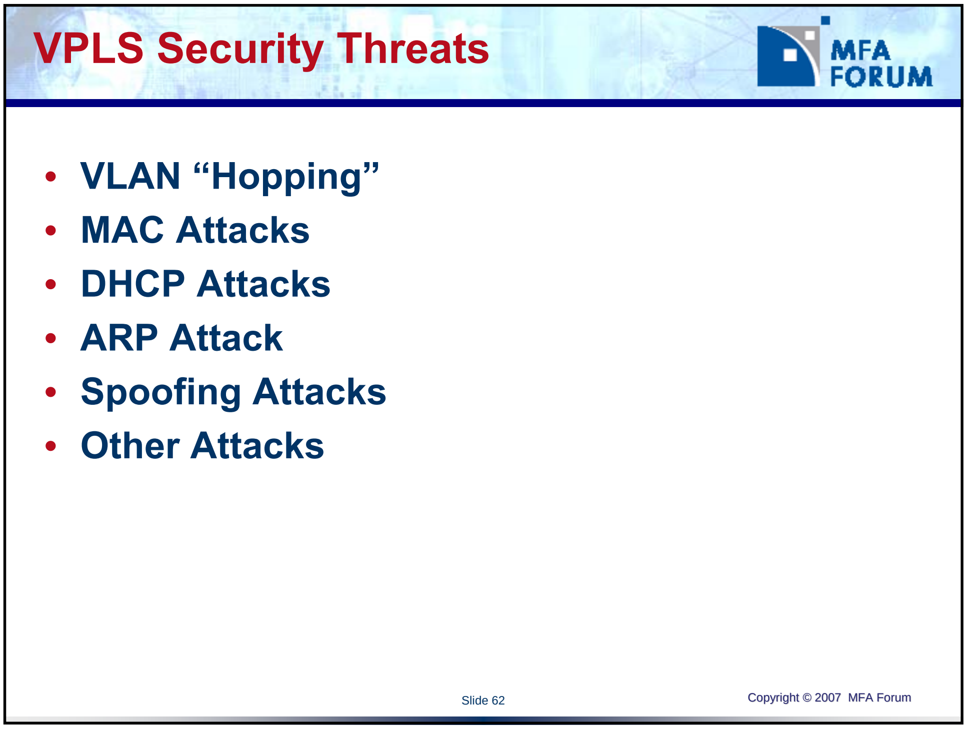


- In VPWS: Packets coming in on one side, are blindly forwarded to the other. → Low security exposure



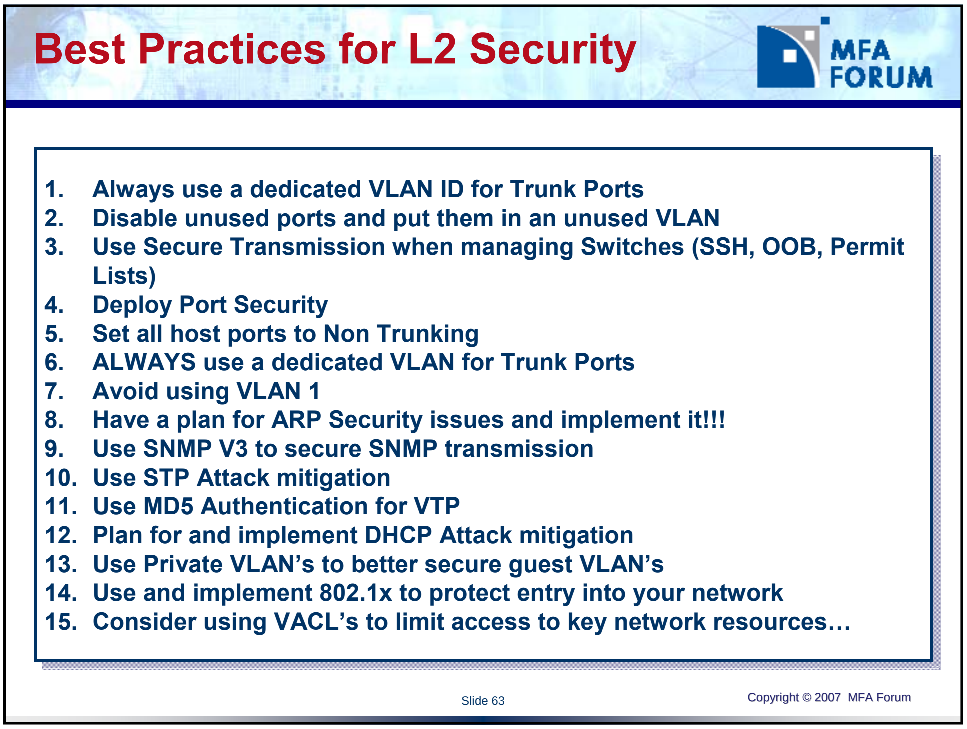
Virtual Private LAN Service (VPLS) Overview

- Network behaves as a switch
  - Spanning Tree
  - MAC address learning
  - ARP, etc.
- → Examine threats to a switch to understand VPLS security



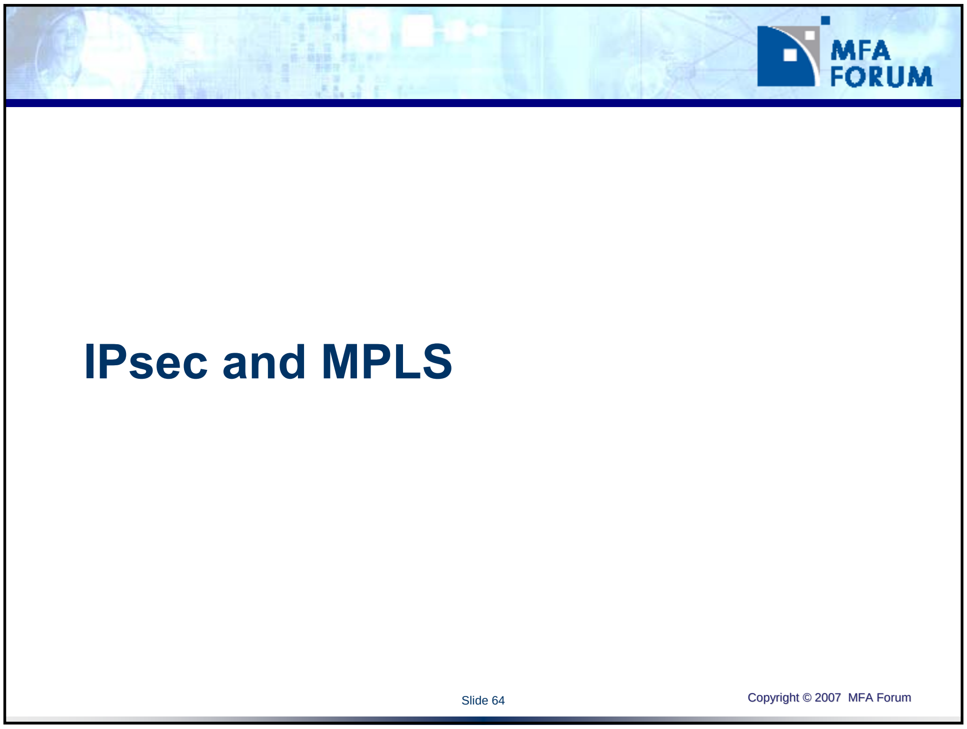
VPLS Security Threats

- VLAN “Hopping”
- MAC Attacks
- DHCP Attacks
- ARP Attack
- Spoofing Attacks
- Other Attacks



Best Practices for L2 Security

1. Always use a dedicated VLAN ID for Trunk Ports
2. Disable unused ports and put them in an unused VLAN
3. Use Secure Transmission when managing Switches (SSH, OOB, Permit Lists)
4. Deploy Port Security
5. Set all host ports to Non Trunking
6. ALWAYS use a dedicated VLAN for Trunk Ports
7. Avoid using VLAN 1
8. Have a plan for ARP Security issues and implement it!!!
9. Use SNMP V3 to secure SNMP transmission
10. Use STP Attack mitigation
11. Use MD5 Authentication for VTP
12. Plan for and implement DHCP Attack mitigation
13. Use Private VLAN's to better secure guest VLAN's
14. Use and implement 802.1x to protect entry into your network
15. Consider using VACL's to limit access to key network resources…



IPsec and MPLS

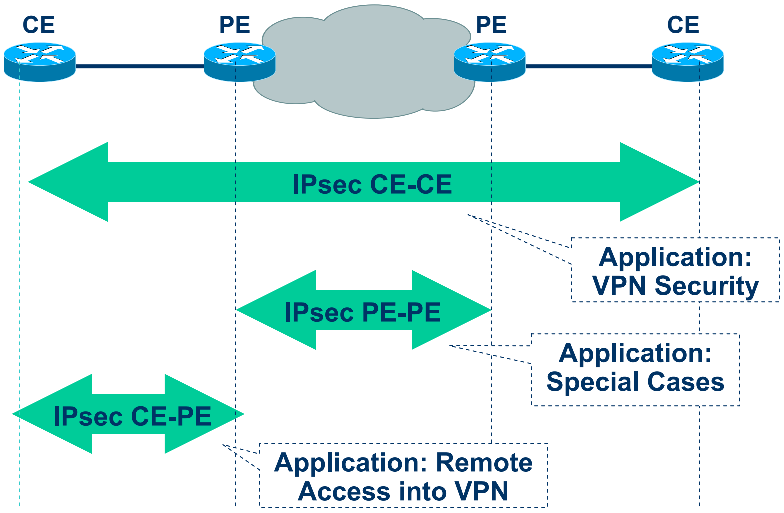
Use IPsec If You Need:

- Encryption of traffic
- Direct authentication of CEs
- Integrity of traffic
- Replay detection

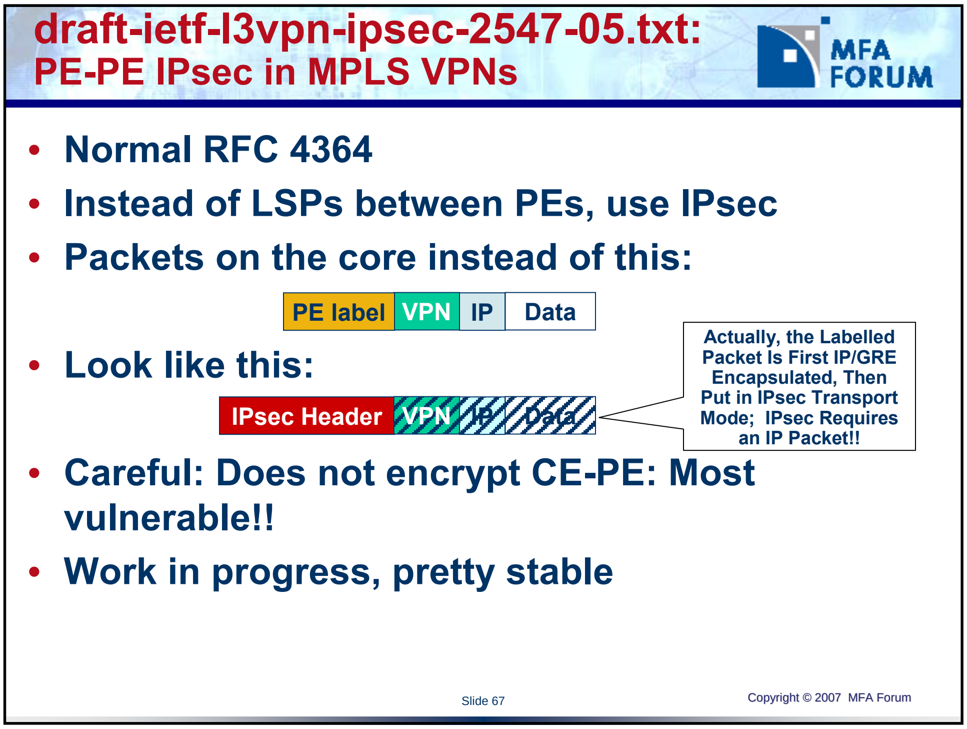
- Or: If you don’t want to trust your ISP for traffic separation!

Slide 65

Where to Apply IPsec


CE
PE
PE
CE
IPsec CE-CE
Application: VPN Security
IPsec PE-PE
Application: Special Cases
IPsec CE-PE
Application: Remote Access into VPN

Slide 66



draft-ietf-l3vpn-ipsec-2547-05.txt: PE-PE IPsec in MPLS VPNs

MFA FORUM

- Normal RFC 4364
- Instead of LSPs between PEs, use IPsec
- Packets on the core instead of this:

PE label	VPN	IP	Data

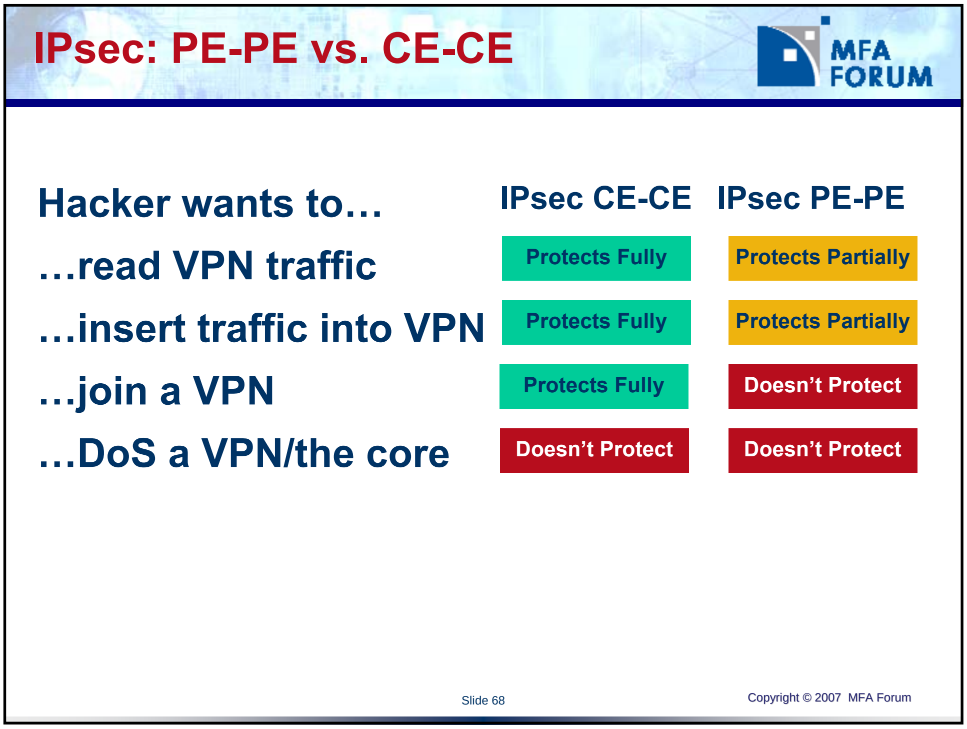
- Look like this:

IPsec Header	VPN	IP	Data

Actually, the Labelled Packet Is First IP/GRE Encapsulated, Then Put in IPsec Transport Mode; IPsec Requires an IP Packet!!

- Careful: Does not encrypt CE-PE: Most vulnerable!!
- Work in progress, pretty stable

Slide 67



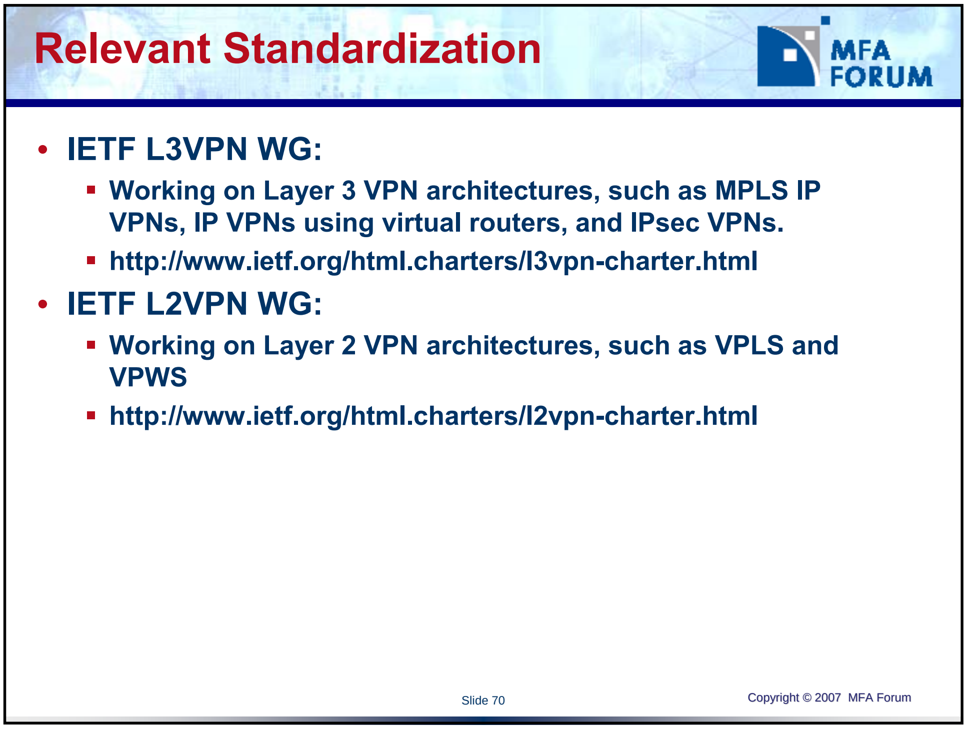
IPsec: PE-PE vs. CE-CE

MFA FORUM

Hacker wants to…	IPsec CE-CE	IPsec PE-PE
…read VPN traffic	Protects Fully	Protects Partially
…insert traffic into VPN	Protects Fully	Protects Partially
…join a VPN	Protects Fully	Doesn't Protect
…DoS a VPN/the core	Doesn't Protect	Doesn't Protect

Slide 68

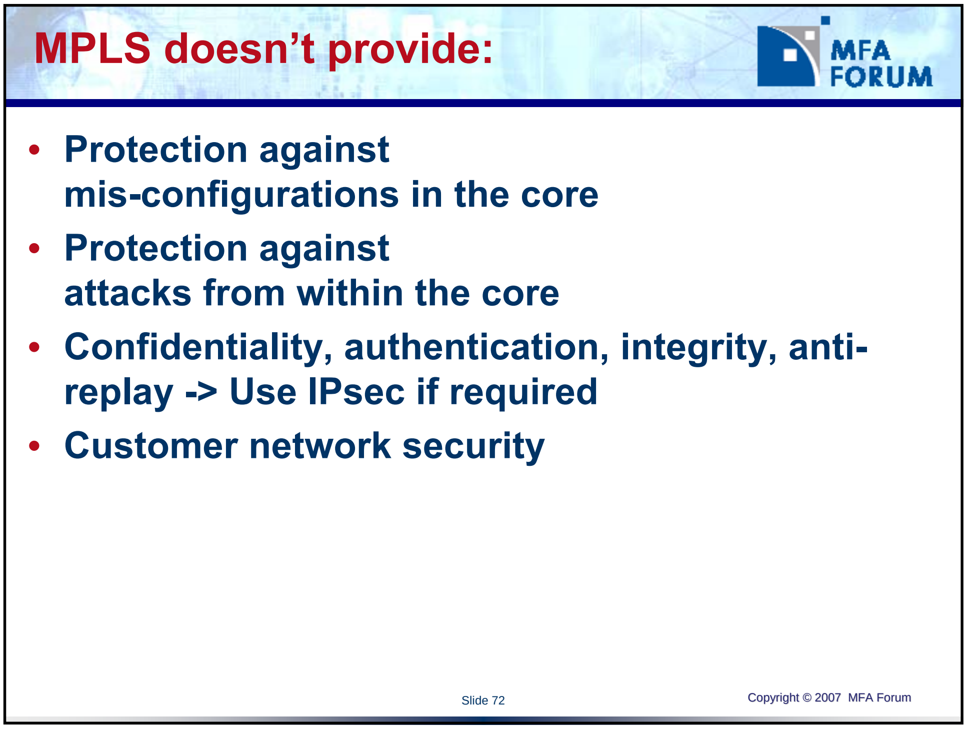
Ongoing Standardizations Work



Relevant Standardization

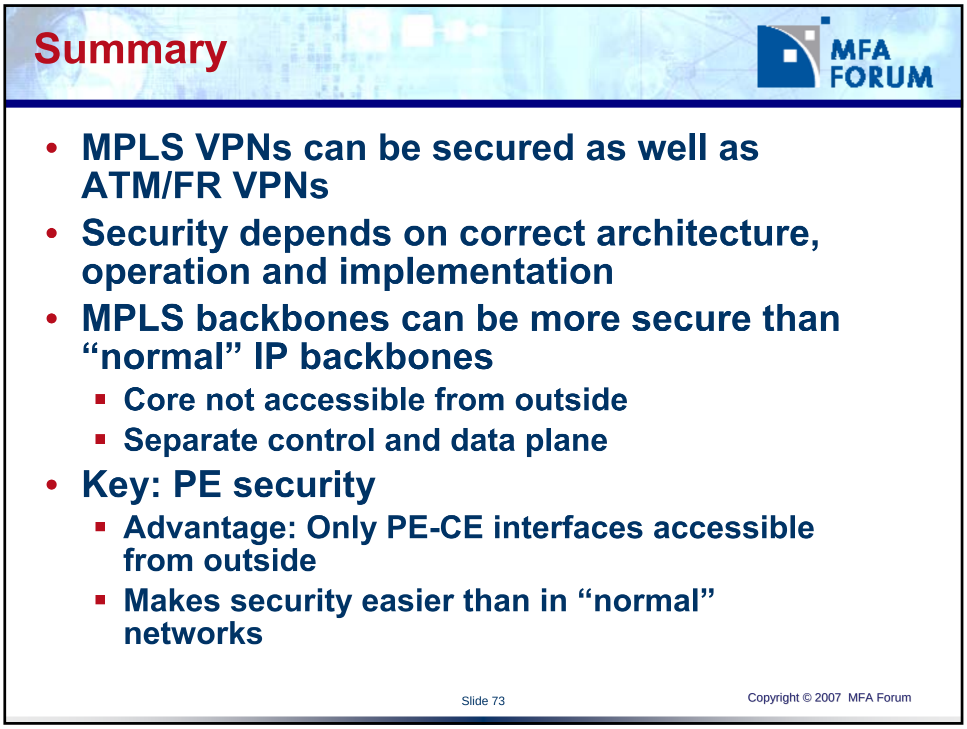
- IETF L3VPN WG:
  - Working on Layer 3 VPN architectures, such as MPLS IP VPNs, IP VPNs using virtual routers, and IPsec VPNs.
  - http://www.ietf.org/html.charters/l3vpn-charter.html
- IETF L2VPN WG:
  - Working on Layer 2 VPN architectures, such as VPLS and VPWS
  - http://www.ietf.org/html.charters/l2vpn-charter.html

Summary



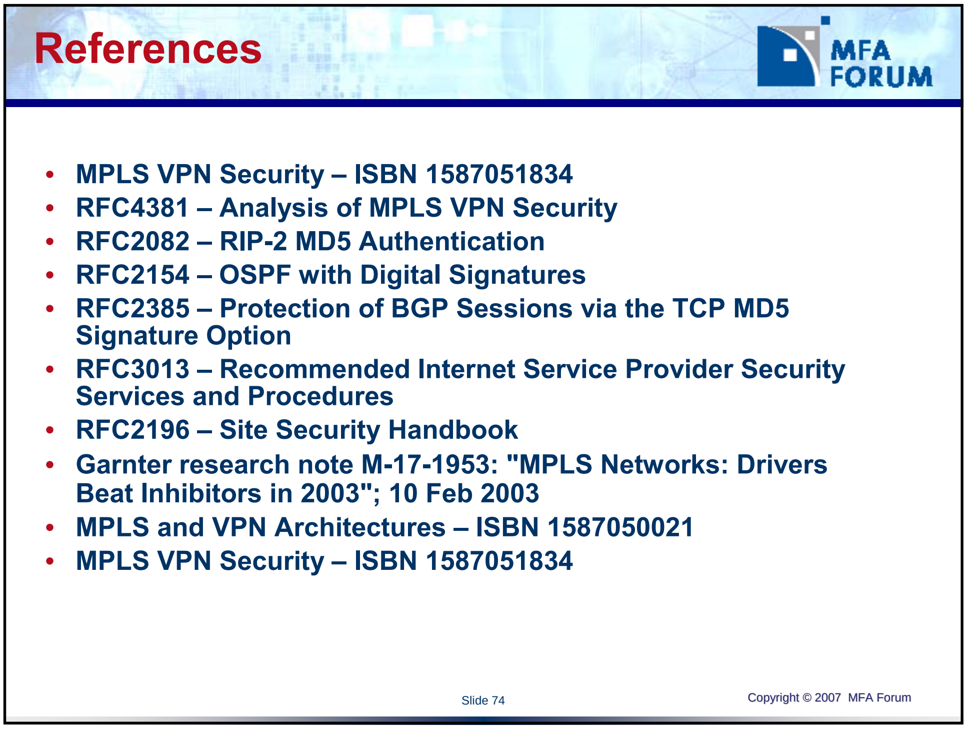
MPLS doesn't provide:

- 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 architecture, 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



References

- MPLS VPN Security – ISBN 1587051834
- RFC4381 – Analysis of MPLS VPN Security
- RFC2082 – RIP-2 MD5 Authentication
- RFC2154 – OSPF with Digital Signatures
- RFC2385 – Protection of BGP Sessions via the TCP MD5 Signature Option
- RFC3013 – Recommended Internet Service Provider Security Services and Procedures
- RFC2196 – Site Security Handbook
- Garnter research note M-17-1953: "MPLS Networks: Drivers Beat Inhibitors in 2003"; 10 Feb 2003
- MPLS and VPN Architectures – ISBN 1587050021
- MPLS VPN Security – ISBN 1587051834

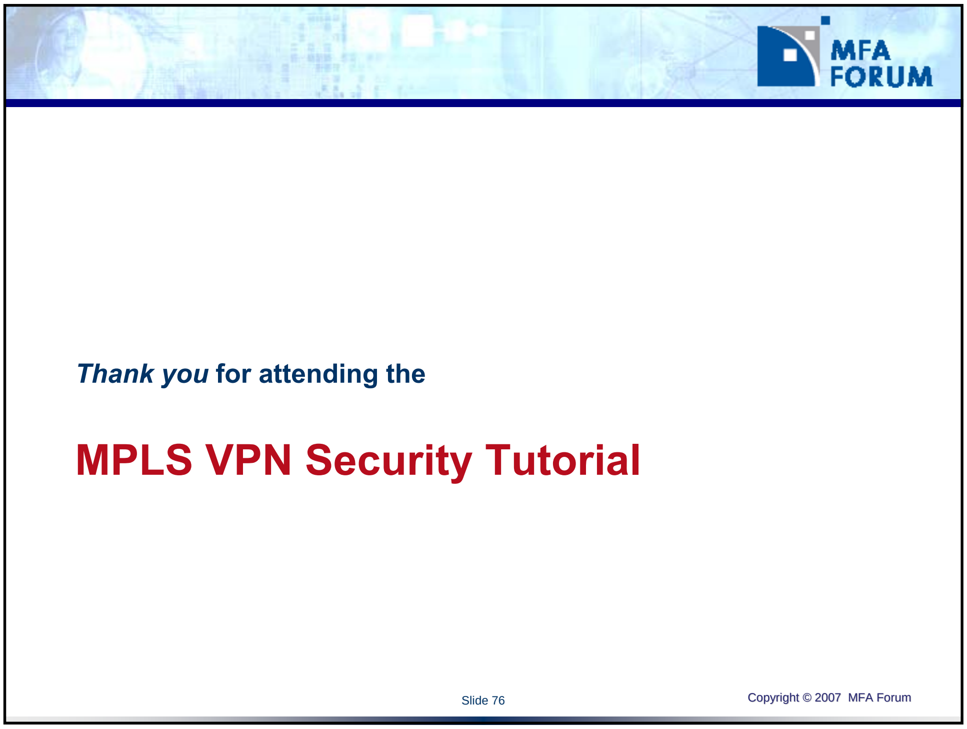
For More Information. . .

- http://www.mfaforum.org
- http://www.ietf.org
- http://www.itu.int
- http://www.mplsrc.com

For questions, utilize the MFA Forum Message Board

Website: http://www.mfaforum.org/board/

Slide 75



***Thank you* for attending the**

MPLS VPN Security Tutorial

Slide 76