



## MPLS VPN Security — An Overview



**Monique Morrow**  
**Michael Behringer**  
**May 2 2007**  
**Future-Net Conference New York**

FutureNet - MPLS Security © 2007 Cisco Systems, Inc. All rights reserved. Cisco Public

1

## 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

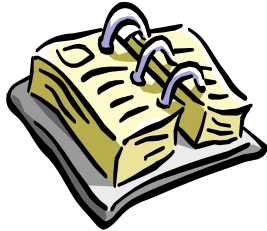


**SP Must Ensure Secure  
MPLS Operations**

FutureNet - MPLS Security © 2007 Cisco Systems, Inc. All rights reserved. Cisco Public

2

## MPLS VPN Security — Agenda



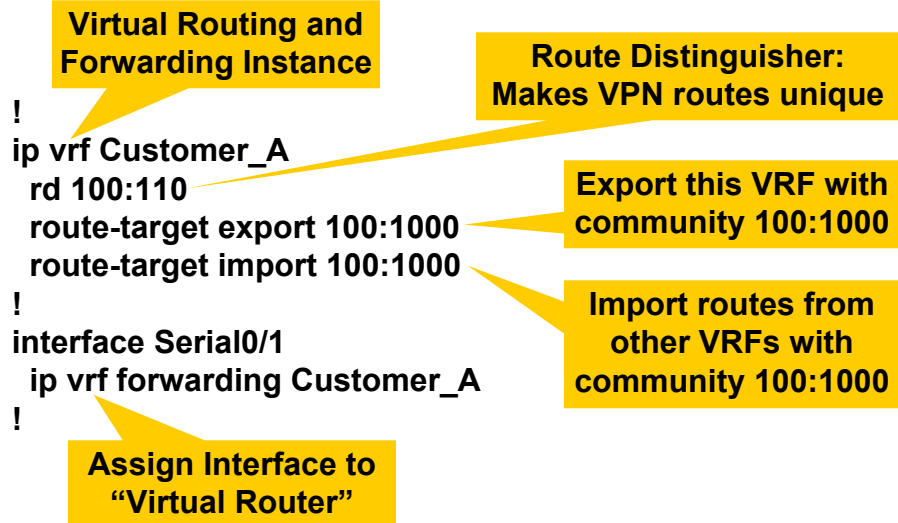
- Analysis of the Architecture
- Secure MPLS VPN Design
  - General Best Practices
- Inter-AS Considerations
- Summary

## Analysis of the MPLS VPN Architecture



(RFC 4364)

## The Principle: A “Virtual Router”



Future MPLS Security © 2003 Cisco Systems, Inc. All rights reserved. Cisco Public

5

## General VPN Security Requirements

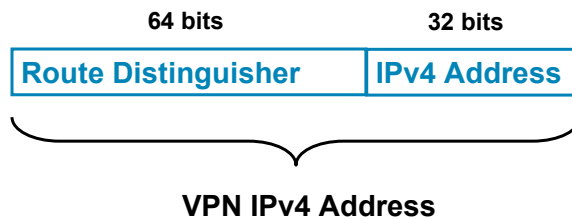
- Address Space and Routing Separation
- Hiding of the MPLS Core Structure
- Resistance to Attacks
- Impossibility of VPN Spoofing

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

Future MPLS Security © 2003 Cisco Systems, Inc. All rights reserved. Cisco Public

6

## Address Space Separation



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

Future of MPLS Security

© 2003 Cisco Systems, Inc. All rights reserved. Cisco Public

7

## 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

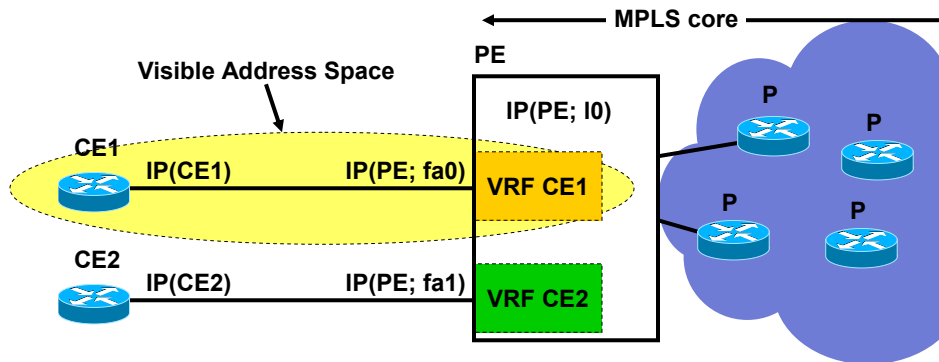
**(For Inter-AS and CsC architectures, see advanced presentation)**

Future of MPLS Security

© 2003 Cisco Systems, Inc. All rights reserved. Cisco Public

8

## Hiding of the MPLS Core Structure



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

Future of MPLS Security © 2007 Cisco Systems, Inc. All rights reserved. Cisco Public

9

## 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

Future of MPLS Security © 2007 Cisco Systems, Inc. All rights reserved. Cisco Public

10

## 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

## Basic RFC 4364 Security: Today's Arguments

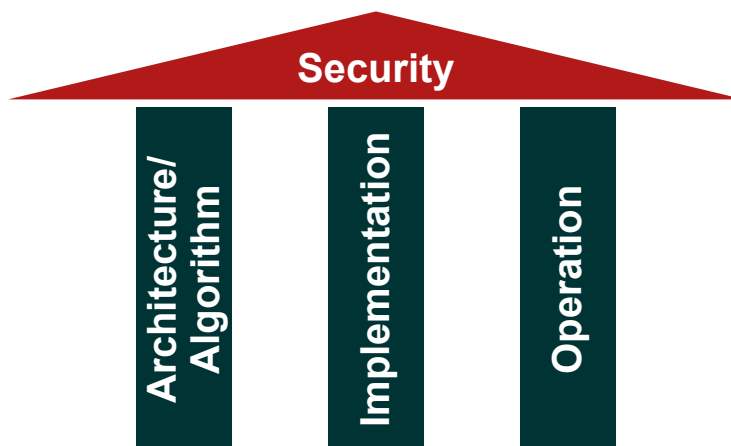
- Can be mis-configured (operation)
  - Routers can have bugs (implementation)
  - PEs can be accessed from Internet, thus intrinsically insecure
  - Floods over Internet can impact VPN traffic
- } True, but same on ATM/FR
- } PEs can be secured, as Internet routers
- } Engineering/QoS

Future of MPLS Security

© 2007 Cisco Systems, Inc. All rights reserved. Cisco Public

13

## Security Relies on Three Pillars

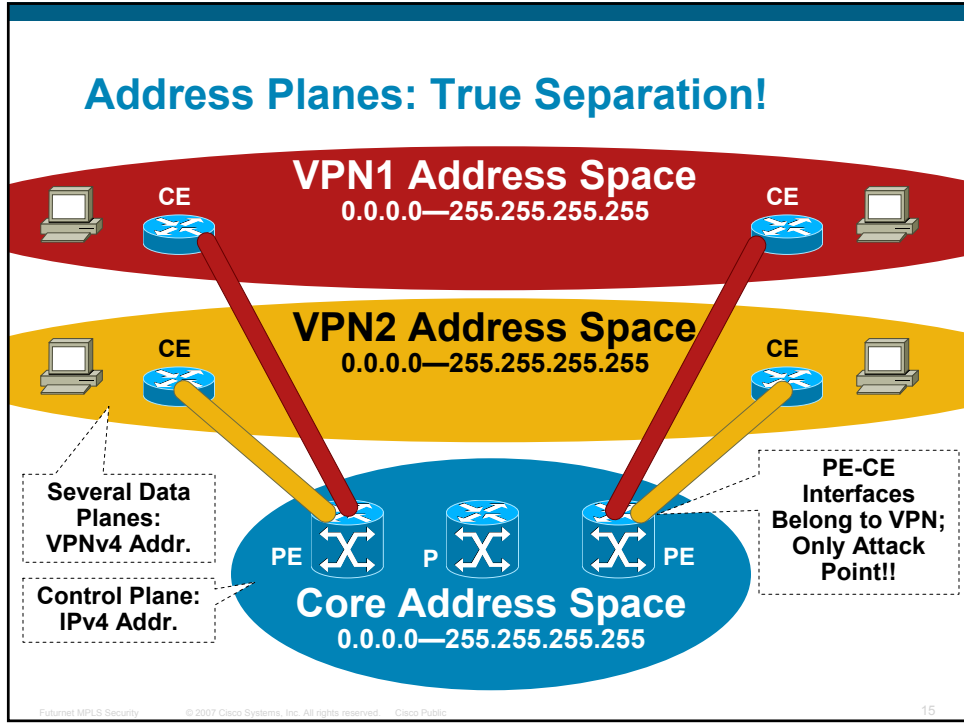


**Break One, and All Security Is Gone!**


Future of MPLS Security

© 2007 Cisco Systems, Inc. All rights reserved. Cisco Public

14



## Secure MPLS VPN Design — General Security Best Practices



Future of MPLS Security | © 2007 Cisco Systems, Inc. All rights reserved. | Cisco Public



## 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:



Still "Open":  
Routing  
Protocol

3. Secure the routing protocol

Neighbor authentication, maximum routes, dampening,...



Only Attack  
Vector:  
Transit Traffic

4. Design for transit traffic

QoS to give VPN priority over Internet

Choose correct router for bandwidth

Separate PEs where necessary



Now Only  
Insider Attacks  
Possible

5. Operate Securely



Avoid Insider  
Attacks

Future MPLS Security

© 2003 Cisco Systems, Inc. All rights reserved. Cisco Public

17

## 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)

Future MPLS Security

© 2003 Cisco Systems, Inc. All rights reserved. Cisco Public

18

## Securing the Core: Infrastructure ACLs

Easy with MPLS!



In MPLS:  
VRF Belongs to  
Customer VPN!

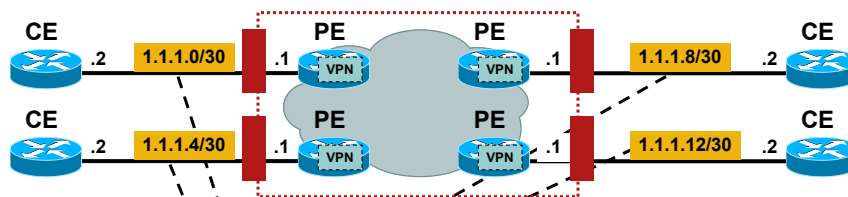
- On PE: “deny ip any <PE VRF address space>”  
Exception: routing protocol from host to host
- Idea: no traffic to PE/P you can't attack
- Prevents intrusions 100%
- DoS: very hard, but traffic over router theoretically enables DoS

Future of MPLS Security

© 2003 Cisco Systems, Inc. All rights reserved. Cisco Public

19

## 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, or ACL with dis-contiguous subnet masks (11111101)

This Is VPN Address  
Space, Not Core!

Future of MPLS Security

© 2003 Cisco Systems, Inc. All rights reserved. Cisco Public

20

## 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
- 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

```
ip vrf red
maximum routes 45 80
```

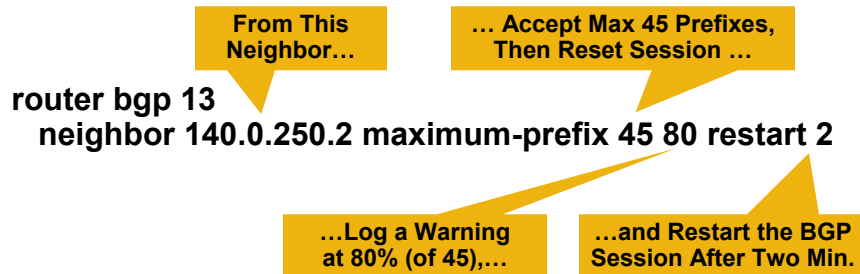
In This VRF...

... Accept Max 45 Prefixes,...

...and Log a Warning at 80% (of 45),...

## 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)



Future MPLS Security

© 2003 Cisco Systems, Inc. All rights reserved. Cisco Public

23

## 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 45  
6d22h: %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

Future MPLS Security

© 2003 Cisco Systems, Inc. All rights reserved. Cisco Public

24

## 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 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...)

## Inter-AS Considerations



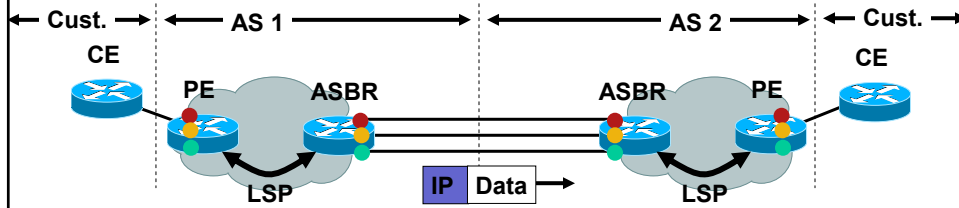
## Inter-AS: The Options

- 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

Future of MPLS Security

© 2007 Cisco Systems, Inc. All rights reserved. Cisco Public

29

## Security of Inter-AS case A

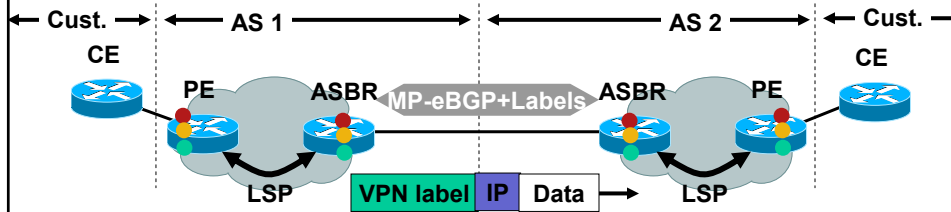
- Static mapping
  - Only IP interfaces
  - SP1 does not “see” SP2’s network
  - And does not run routing with SP2, except within the VPNs
  - Quite secure
- Potential issues:
  - SP 1 can connect VPN connection wrongly (like in ATM/FR)
  - Customer can flood routing table on PE (this is the same issue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

Future of MPLS Security

© 2007 Cisco Systems, Inc. All rights reserved. Cisco Public

30

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



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

Future MPLS Security

© 2007 Cisco Systems, Inc. All rights reserved. Cisco Public

31

## 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)

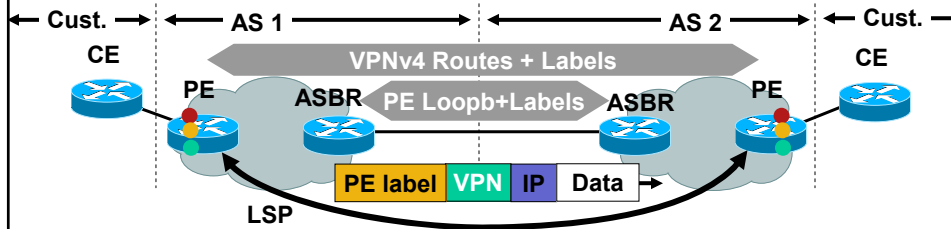
Future MPLS Security

© 2007 Cisco Systems, Inc. All rights reserved. Cisco Public

32



## 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

Future MPLS Security

© 2007 Cisco Systems, Inc. All rights reserved. Cisco Public

33

## 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

Future MPLS Security

© 2007 Cisco Systems, Inc. All rights reserved. Cisco Public

34

## 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

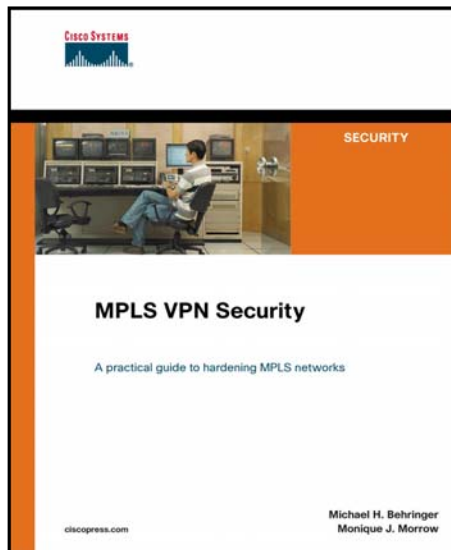
## Summary



## 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](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
- Gartner research note M-17-1953: "MPLS Networks: Drivers Beat Inhibitors in 2003"; 10 Feb 2003

## Q and A



