Secure Inter-Provider IP VPNs

Scott Poretsky, Director of QA, Quarry Technologies
sporetsky@quarrytech.com

October 19, 2004

MPLS 2004

QUARRY TECHNOLOGIES

Network Security is a Daily Concern

From: Sean Donelan [sean@donelan.com]

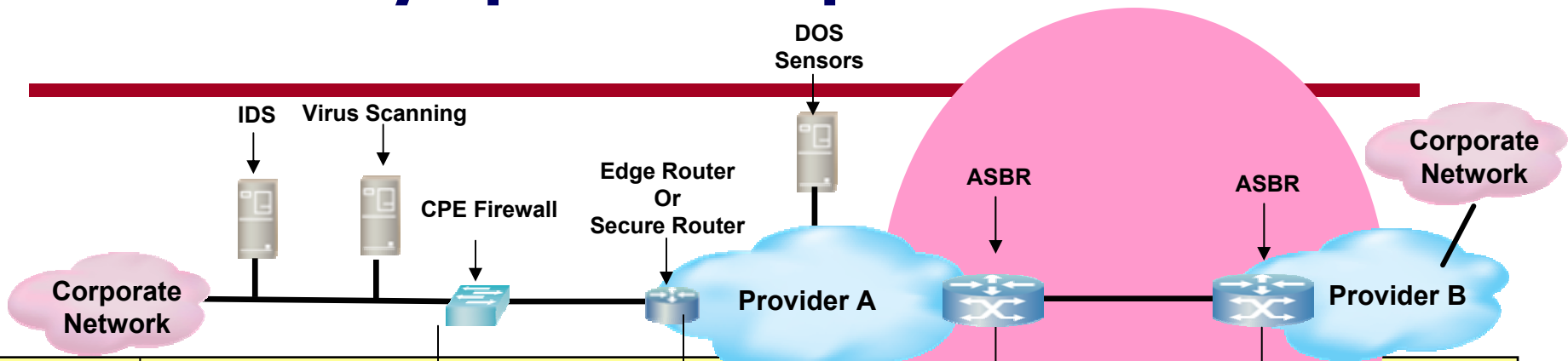
Sent: Tuesday, August 17, 2004 2:39 PM

To: **nanog@merit.edu**

Subject: Re: SYN flood attacks?

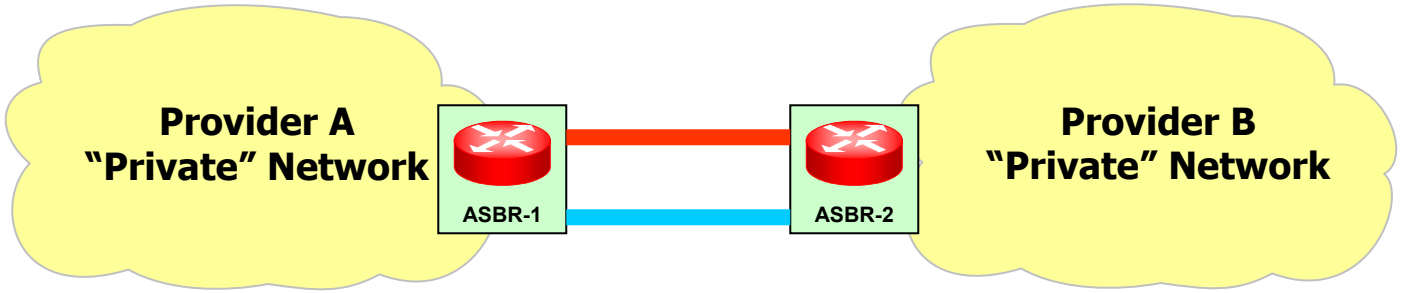
> There are syn flood attacks, icmp attacks, udp attacks, tcp attacks, dns attacks, http attacks, im attacks, ipsec attacks, etc going on every day, all day.

Security Spans multiple boundaries



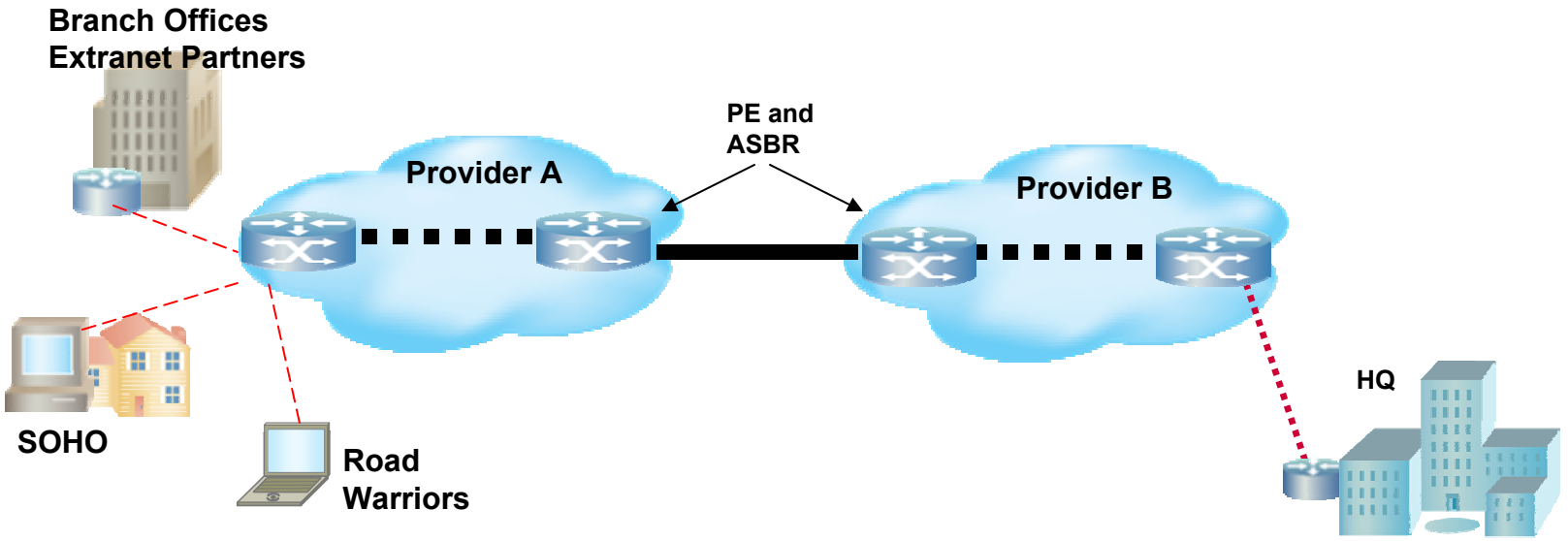
	Enterprise	Last-Mile	VPN Backbone	Inter-Provider MPLS VPN	Partner Network
Function:	**Protect Enterprise Resources**	**Protect Last-Mile Bandwidth**	**Protect Service Provider Network SLAs and VPNs**	**Secure and Control Access Into VPNs**	**Stop Malicious /Unintended Attacks**
Deploy:	- Stateful Packet Inspection - Deep Packet Inspection - Anti-Virus	- ACLs - Transport Layer Firewall - Stateful Packet Inspection - Malicious URL - Deep Packet Inspection - Encryption	- Deep Packet Inspection ACLs - Transport Layer Firewall - Encryption	- ACLs - Transport Layer Firewall - Stateful Packet Inspection - Malicious URL - Deep Packet Inspection - MD-5 for Routing	- Deep Packet Inspection ACLs - Transport Layer Firewall

Inter-Provider Security Considerations



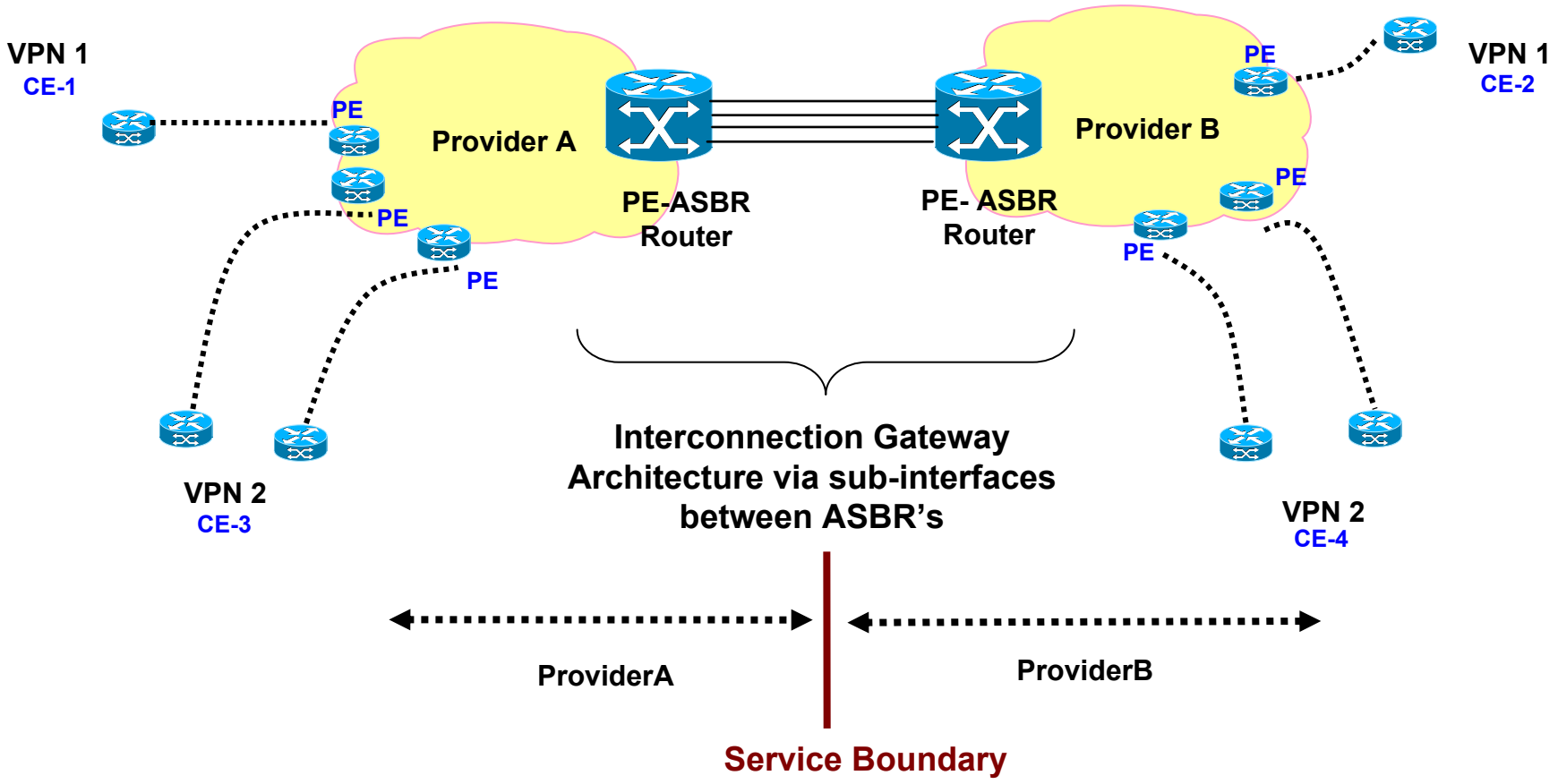
- How "private" are private networks when interconnected with other private networks?
- What amount of control should the partner network be allowed over my network resources?
- How can each Provider retain full control/security over the control protocols and data paths within their network?
- Issues are more acute when TE LSPs are required end-to-end

Inter-Provider IP VPN (In)Security



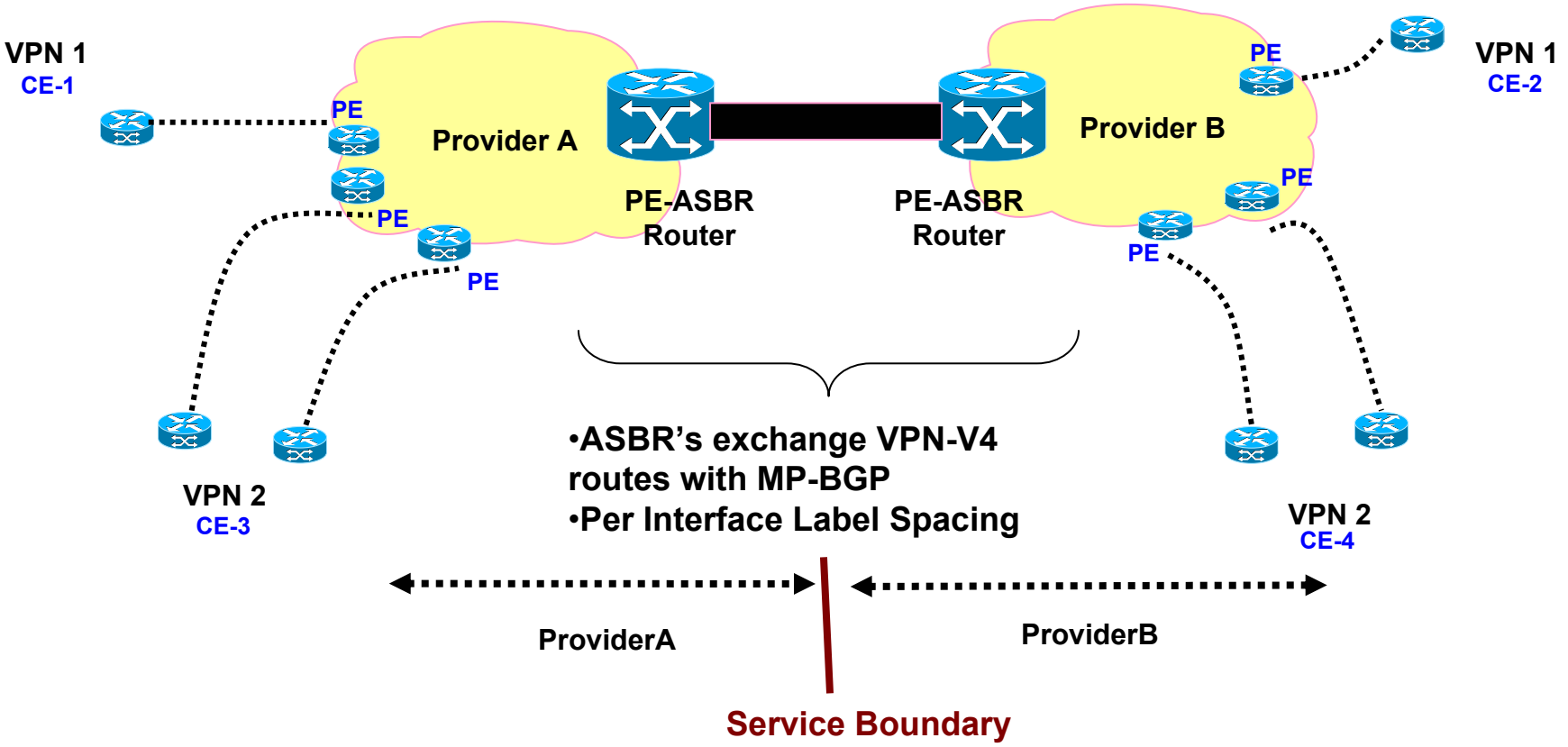
- Control plane vulnerabilities: Solution = MD-5, BGP Filtering, Warnings for approaching VR size limit
- Prone to DoS attacks: Solution = Rate Limiting and Firewall with Deep, Stateful Packet Inspection
- Lack of authentication: Solution = IPsec
- Lack of confidentiality: Solution = IPsec
- Label Spoofing: Solution = Per Interface Label Spacing

Interconnection Option A
Back-to-Back VRs



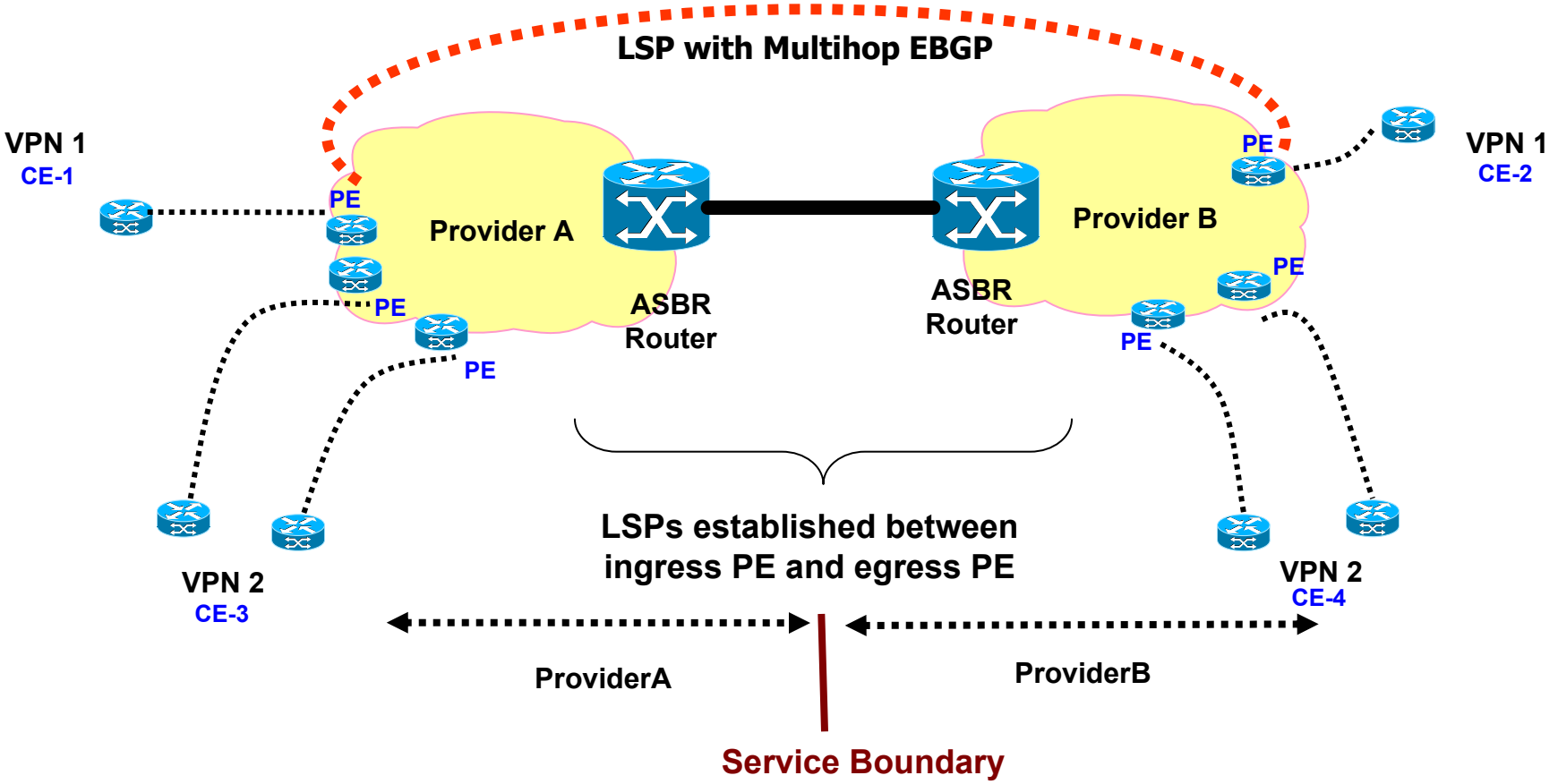
- Security Risks same as any PE-CE relationship
- Routing information between Providers more "secure"
- Data Plane can be constrained on a per VPN basis

Interconnection Option B
MP-eBGP for VPNv4



- Requires an increased level of trust between Providers
- Shared Data Plane across multiple VPNs
- No built-in authentication mechanism for VPN Routes

Interconnection Option C
Multihop MP-eBGP



- Requires Providers to share internal routing information
- Trust and Control issues around setting up E2E LSPs

Secure Inter-Provider VPN Data Plane Requirements

- Requirement: Provider must not be able to flood either the ASBR links to the other Provider
  - Protect EF/Priority traffic
  - Protect bandwidth
    - Overprovision ASBR-ASBR capacity
    - Traffic Engineer ASBR-PE capacity
    - Rate-Limiting: Class-based or RD based
- Requirement: Encrypted customer data
  - IPSec Mapping to MPLS VPN
  - Encrypted MPLS VPNs

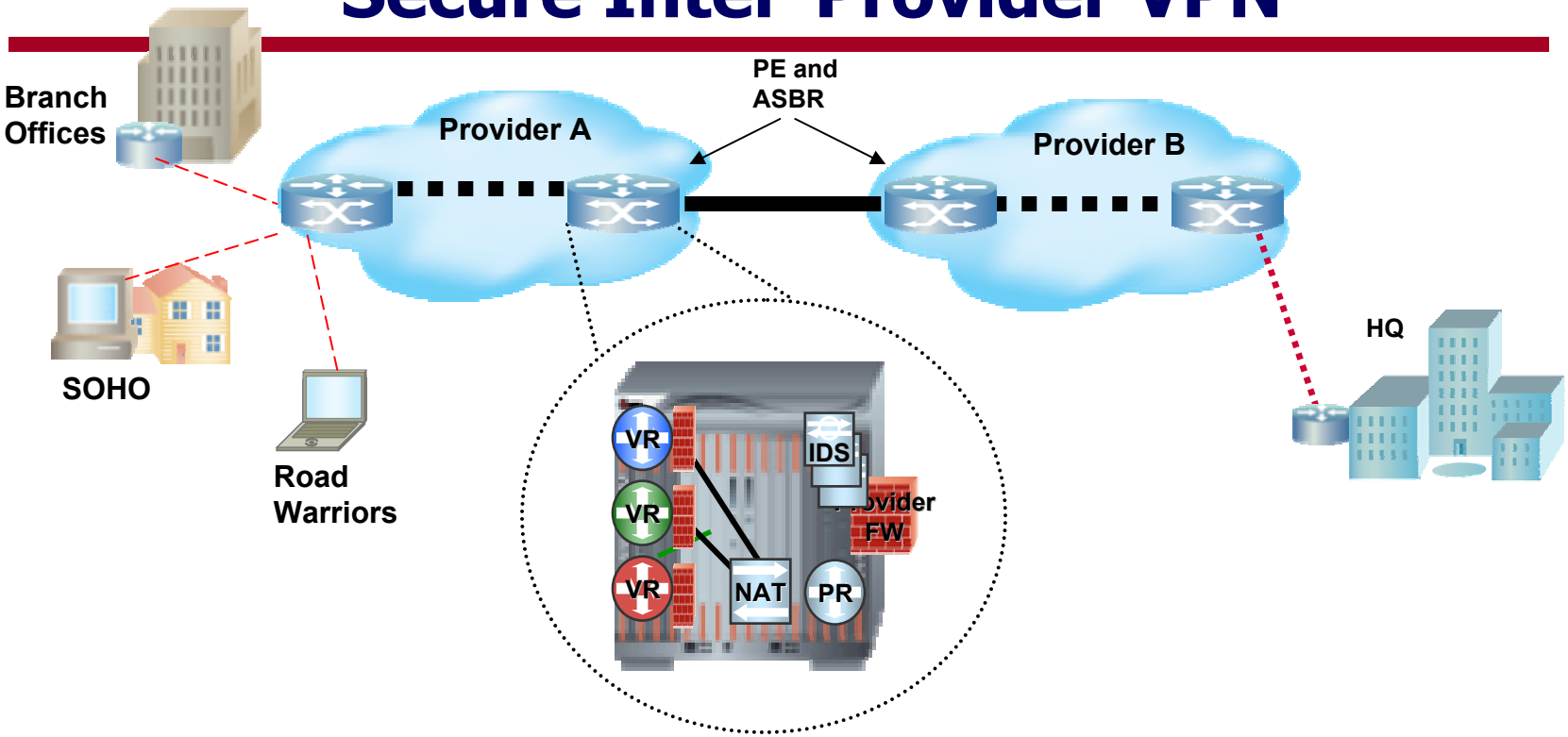
Secure Inter-Provider VPN Control Plane Requirements

- Requirement: Provider A must not be able to affect control plane stability of Provider B (and vice-versa)
- Requirement: Security and Integrity of every Customer VPN must be preserved
  - MD-5 Authenticated VPN-V4 only MP-BGP sessions
  - Max-prefix (desired on a RD basis)
  - Prefix-filtering (wildcards with RD's desired)
  - Policy-server based approach to developing filters

Sample Provider Interconnect Policy Using Option B

- Interconnect interface needs to accept labeled packets only (BGP updates are exception)
  - No IGPs, RSVP, or LDP to be enabled on the interface
- BGP Policy: Outbound
  - Only advertise VPN routes for Provider B customers located on the Provider A infrastructure: achieved using BGP Community match, this includes PE/CE link addresses
- BGP Policy: Inbound
  - Only accept VPN routes for Provider B customers located on the Provider A infrastructure: Provider A will filter based on RD/RT, AS Path and BGP Community as insurance
  - specific prefix filter per route per customer
- Generic BGP Features
  - BGP Dampening, Max Prefix, AS Path filters, MD5 Authentication
- CoS protection
  - Ensure adequate ASBR – ASBR capacity, trend and plan for growth by Class (EF/AF/BE)
  - Ensure that EF class traffic has sufficient "headroom" at an aggregate level (consider rate-limiting as necessary)

Virtual Routers (VRs) for Secure Inter-Provider VPN



- Secure remote-access connectivity into MPLS VPNs
- Secure Internet across Inter-Provider MPLS VPNs
  - NAT/NAPT, Virtualized Firewall, IDS, DOS attack prevention, IPsec VPN

Securing IP VPNs Traffic with IPSec

- End-to-end service with IP and IPsec VPN
  - *IPsec can be deployed across Internet*
  - Across administrative domains
  - Across any MPLS VPN
  - Provides secure remote access for clients and sites

1. IPSec Mapping to MPLS VPN
   - MPLS packet is not IPsec encrypted
   - IPsec enables secure remote access to MPLS core

2. Encrypted MPLS VPNs
   - MPLS VPN tunneled in IP and secured with IPsec www.ietf.org/internet-drafts/draft-ietf-l3vpn-ipsec-2547-03.txt
   - Packets are IPsec encrypted end-to-end through MPLS core
   - Remote access using IPsec provides security off-net

Summary

- Security considerations are important when building Inter-Provider MPLS VPNs
- ASBR to ASBR bandwidth must be managed
- ASBR to PE bandwidth must be protected
- Firewall and Rate Limiting should be deployed on a per VPN basis for customer-specific configurations
- Control Plane needs to be secure
- IPsec may be needed to encrypt customer VPN traffic

Secure Inter-Provider IP VPNs

Scott Poretsky, Director of QA, Quarry Technologies
sporetsky@quarrytech.com

October 19, 2004

MPLS 2004

QUARRY TECHNOLOGIES