

Enterprise Challenges

Interop May 2004

Agenda

- ◆ Network of tunnels
- ◆ Risk-IT interaction
- ◆ Storage internetworking
- ◆ Network admission control
- ◆ Management of complexity

Network of Tunnels

- ◆ Problem/challenge space
 - Abstraction creating a network of tunnels, not interfaces
 - IPSec, GRE and nested (today)
 - Troubleshooting visibility
 - Deep packet inspection visibility
 - Appliances - F/W, IDS, SLB, cache
 - Services - web services, XML routing, P2P and prohibited
 - NMS tools

- ◆ Drivers
 - Private line replacement
 - Privacy
 - L3 Mobility

- ◆ Possible solution approaches
 - NMS tools and sniffers can natively understand tunnels
 - Crypto transparently built into hardware
 - GRE alternatives for routing domain and segmentation

Risk-IT interaction

◆ Problem/challenge space

- Changing network design goals and reference architectures
 - Core network segmentation - GRE, VRF-Lite, MPLS, ACL+VLAN
 - e-Commerce/DMZ segmentation – pVLAN, growing layers
 - Metro – high-speed encryption, Fiber channel?
- L3 data encryption
 - Creating a network of tunnels
- Routing to enforce SEC
- Privacy and archive of email and chat

◆ Drivers

- Privacy of customer data
- Core network segmentation based on data classification, transaction zones
- e-Commerce/DMZ horizontal and vertical segmentation
- Compliance regulations

◆ Possible solution approaches

- Routing to enforce SEC – new thinking needed (network access control)
- Crypto transparently built into hardware

Storage internetworking

◆ Problem/challenge space

- Creating Fiber-channel switched internetworks
- Increasingly inserting the IP network between servers and storage
 - CAS, iSCSI
- Metro, WAN design impacted by remote vaulting of data
 - via IP transport (“synchronous” IP, FCIP)
 - Fiber channel over the network
- Troubleshooting visibility

◆ Drivers

- Cost, efficiency – expanded access to centralized storage arrays
- Data life cycle management – virtualization
- Compliance, BCP increasing off-site data instances and archiving

◆ Possible solution approaches

- Storage arrays and switches use IP transport for mirroring/vaulting
- Union (or at least visibility) of storage network into enterprise NMS

Network admission control

◆ Problem/challenge space

- Emerging 802.1x, still immature
 - desktop client agents - Bad
 - desktop HIDS - Bad
- Enforcement via core network segmentation is complex
 - GRE, VRF-Lite, MPLS, ACL+VLAN
- Security policy server (Radius) also immature (Cisco ACS !?)
- MAC locking is the current alternative

◆ Drivers

- Risk – “know your endpoints”
- Changing work environment - employee mobility, contractor, guest
- Mobility computing – endpoints can be wireless, PDA, etc.

◆ Possible solution approaches

- Access control implicit in the network instead of “segmentation”
- Client challenge/response better defined

Management of complexity

- ◆ Problem/challenge space
 - Virtualized infrastructure (root cause virtual / physical?)
 - Abstracted network of tunnels, not interfaces
 - Troubleshooting visibility
 - Business service views on segmented networks
 - Network application overlays

- ◆ Drivers
 - Storage, wireless, IPT, cellular dual-mode, multi-cast
 - Security risk
 - Autonomic, on-demand provisioning
 - Higher expectations, management visibility

- ◆ Possible solution approaches
 - Wireless and wired behavior the same
 - Unify visualization and emerging correlation capabilities
 - Discovery tools aware of network topologies