Introduction to Virtual Private Network (VPN) Management

Session 2608
Introduction to VPN Management

Agenda

• VPN Overview
  Types and Benefits
  Management Challenges

• VPN Management Challenges and Solutions
  Site-to-Site
  Remote Access

• Summary and Conclusions

VPN Overview

Extending Classic WAN and Dialup Networks
**VPN Types and Benefits**

- **Intranet VPN**
  - Low Cost, Tunneled Connections with Rich VPN Services (IPsec and QoS) to Ensure Reliable Throughput
  - Cost Savings and New Applications

- **Extranet VPN**
  - Extends WANs to Business Partners
  - New Applications and Business Models

- **Remote Access VPN**
  - Secure, Scalable, Encrypted Tunnels Across a Public Network
  - Cost Savings

**VPN Components**

- Routers, concentrators, firewalls
- Desktop client software
- Management tools
- Supporting servers (AAA, DNS, DHCP, etc.)
Site-to-Site VPN Topologies

- New technologies introduced by VPNs
  - Tunneling
  - IP security (IPSec)
  - Generic Routing Encapsulation (GRE)

Site-to-Site VPN Management Challenges

- Security configuration
- Connectivity and reliability
- Status and performance monitoring—including faults and events
- Scalability—devices
Remote Access VPN Topology

- New technologies introduced by VPNs
  - Tunneling
    - Point-to-Point Tunneling Protocol (PPTP)
    - Layer 2 Tunneling Protocol (L2TP)
    - IP security (IPSec)

Remote Access VPN Management Challenges

- Security configuration
- Connectivity and reliability
- Usage auditing—session status including faults and events
- Scalability—users
VPN Management

Site-to-Site Challenges and Components

What Are the Top Concerns?

• Overall security and data integrity
  How to configure and maintain end-to-end
• Connectivity and reliability
  How to maintain and monitor end-to-end
• Session monitoring
  How to monitor and troubleshoot end-to-end
• Scalability
  How to support maintain network and services growth
Site-to-Site VPN Management Challenges Security

- Tunnel configuration (establishing peers)
  - IPSec (authentication: MD5, SHA; encryption: DES, 3DES, RC4)
  - GRE (multicast and broadcast support)
- Configuring supporting services
  - Authentication (AAA, certificate, directory)
  - Timing/NTP servers—utilized by certificates
  - Access Control Lists (ACLs) and firewalling
- Relevant concerns
  - Be aware of services you need to pass: (i.e., IKE/ISAKMP utilizes UDP port 500, PPTP utilizes TCP port 1723; NTP uses UDP port 123, IPSec AH uses UDP port 51, IPSec ESP uses UDP port 50)
  - Configuration complexity varies based on VPN model (i.e., hub-and spoke vs. meshed)
  - Verifying certificate duration
  - Combining IPSec and NAT
Site-to-Site VPN Management Challenges Security

- Security device configuration solution example
  - IPSec tunnel configuration per device:
    - Tunnel templates (IKE, auth and encryption)
    - Creating cryptomaps and crypto ACLs

- Security policy configuration solution example
  - Tunnel/IKE templates
  - Tunnel Policies

Site-to-Site VPN Management Challenges Connectivity

- Includes throughput, response time, latency and availability
  - Across the shared VPN infrastructure (Internet and/or multiple SPs)
  - Must utilize real-time and historical data (e.g., Top N reports—longest downtime, highest throughput, most failures)
  - Requires alarm and events (syslog hosts, SNMP Trap recipients) with user-defined notification methods

- Relevant concerns
  - Ownership—within the enterprise, an SP or between partner vendors
  - High-availability—parallel paths, redundant routers
  - Verifying and maintaining tunnel and service connectivity (Layer 2–7)
Site-to-Site VPN Management Challenges Connectivity

- Traditional WAN connectivity management:
  - Interfaces, IP addresses and netmasks, routing
  - Management via CLI, embedded web interfaces or centralized console
  - Existing/traditional troubleshooting methods may include ICMP 'pings' and traceroute

- VPN connectivity management:
  - Requires an end-to-end network and services connectivity view
  - Still requires centralized console and basic configuration tools
  - Support for quality of service (QoS)—optimizes bandwidth
  - Peer-to-peer configuration (TED, IKE 'keep alives')
  - Requires embedded device functionality (e.g., SAA in Cisco IOS®)

Network Service Level Verification
QoS Network Policy Configuration
Per-Device Traffic Class Configuration

Service Level Troubleshooting
Network Service Level Verification
Per-Device Traffic Class Monitoring
Site-to-Site VPN Management
Challenges Session Monitoring

- Monitoring tunnel status and performance
  - Session status and duration
  - Session failures
  - Policy and service status
  - Alarms and events required

- Ability to effectively monitor and log device and network events

- Relevant concerns
  - Monitoring is dependent on successfully establishing tunnels
  - Encrypted tunnels hide application layer information
  - Secure management access to network devices
  - Response/repair time thresholds (internal vs. outsourced)

Site-to-Site VPN Management
Challenges Session Monitoring

- Traditional WAN session management:
  - Device-level monitoring via CLI or central console
  - Probes and device instrumentation are typically utilized
  - Standard MIBs (MIB II, RMON)
  - Syslogs, SNMP Traps—must configure event recipients
  - Real-time and long-term monitoring used to provide reports

- VPN session management:
  - Similar to traditional WAN monitoring, but...
  - LAN/WAN probes are not as effective due to data encryption
  - Enhanced device instrumentation is required
    - Draft MIBs (IPSec, IKE)
    - Proprietary MIBs (Policy Map MIB)

Implications

Central Site
Company A
Remote Site
POP
SP/Internet
DSL
Cable
VPN
Site-to-Site VPN Management Challenges Session Monitoring

- IPSec MIBs
- Internet drafts (‘works in progress’)
  - IKE Monitoring MIB
    - Defines monitoring and status information when the IKE protocol is used to create IPSec SAs; it does not provide policy information
  - IPSec Flow MIB
    - Provides IPSec monitoring and troubleshooting functionality
    - Provides traps reporting operational failures during the setting up, tearing down and normal lifetime of IPSec tunnels
    - Does not present in-depth low level debugging and diagnostic support
- Cisco proposed MIB: IPSec Policy Map MIB
  - An appendix to the IPSec Flow MIB
  - Maps the IPSec entities created dynamically to the policy entities that caused them
  - Two basic MIB components: IKE tunnel-to-policy mapping table and IPSec tunnel-to-policy map table

Site-to-Site VPN Management Challenges Scalability

- Support and maintenance of network and services growth
- Network devices
  - Two sites up to 1,000s of sites
  - Device interfaces
  - Device performance (tunneling/encryption is CPU intensive)
- Services
  - Tunnels
    - Topology dependent (meshed vs. hub-and-spoke vs. hybrid)
    - Up to 10,000s of tunnels
  - Firewalls and ACLs
  - QoS
- Relevant concerns
  - Reliability and speed of configuration process (minimize down time)
  - Security Association (SA) setup rate, max. SAs, encryption performance
Site-to-Site VPN Management Challenges Scalability

- Traditional WAN scalability management:
  - Management solution will most likely change as the network grows.
  - Small installations (typically, < 10 devices): device-centric tools.
  - Larger installations (typically, 10s to 1000s of devices): network-wide tools.
  - Hierarchy/distributed approach (distributed servers and consoles).

- VPN scalability management:
  - Similar to traditional WAN scalability issues but with additional concerns:
    - Security session mgmt (e.g., key lifetimes, encryption strength, hash algorithms, PFS).
    - Larger installations may consider policy-based tools.
    - Product extensibility (APIs, XML access, etc.) for customization.

Implications

Remote Access Challenges and Components
Remote Access VPN Management Challenges

What Are the Top Concerns?

- Overall user security management
  Establishing secure tunnels
  Ease and reliability of VPN client configuration
- Connectivity and reliability
  How to configure and maintain user connectivity
- Usage auditing
  How to monitor and troubleshoot user session activity
- Scalability
  How to support and maintain large number of users

Remote Access VPN Management Challenges—Security

- Tunnel configuration (establishing peers)
  PPTP (authentication: PAP, MSCHAP; encryption: MPPE (40-bit, 128-bit))
  L2TP (authentication: PAP, CHAP; encryption: not available)
- Configuring supporting services
  Similar to site-to-site services, but user authentication is imperative
  User Authentication (AAA, certificate, directory)
    RADIUS, TACACS+, Windows NT domain, security server
    (e.g., SecureID) for One-Time-Passwords (OTP), LDAP, Certificate Authority
  Addressing (client-based, DHCP, DNS, pools-mode configuration)
- Relevant concerns
  Configuration complexity varies based on user scale
  Consistency in user security parameter configuration -> policy
  Verifying certificate duration
Remote Access VPN Management Challenges—Security

Access security management:
- Management typically via CLI, embedded web interfaces or centralized console
  - Focused on the NAS
- Device authentication (e.g., PAP, CHAP)
- User authentication configuration (e.g., RADIUS, Win NT)
- ACLs

VPN security management:
- Similar to access scenario, but add:
  - Two phase authentication (devices/pre-shared/certs) and user authentication (e.g., AAA)
  - Encryption configuration (IPSec)
  - Additional client software
  - Configuration of VPN user ‘policies’

Remote Access with Enhanced Clients

Enhanced client
- Policy-based, auto-configuration and access
- Cisco client provided for Win/NT 95 and 98 environments

VPN router
- Full tunneling compatibility
- PPTP and IPSec/L2TP
- Digital certificate authentication
- Third-party authentication
- User and group policies
Remote Access VPN Management Challenges—Connectivity

- Includes throughput, response time, latency, and availability
  - User-to-user and user-to-server
  - Similar basic connectivity concerns as site-to-site scenario

- Relevant concerns
  - Must scale to thousands of concurrent users
  - Connectivity is through Internet and/or service provider(s)
  - User location is variable/unknown
  - To manage connectivity services, must manage per-client service-level agreements (SLAs), anytime, anywhere

Remote Access VPN Management Challenges—Connectivity

- Access connectivity management:
  - Management focused on the access server(s) via CLI or centralized console
  - Management of modem connections and pools
  - At the PoP and Enterprise

- VPN user connectivity management:
  - Similar to access scenario, but add a VPN router at the enterprise
  - User connectivity is established typically through several SPs
  - An user-to-user/server connectivity view is required
Remote Access VPN Management Challenges—Connectivity

- User-based service-level monitoring solution example
- Utilizes combination of centralized console, embedded device functionality and client software:
  - Software installed on VPN clients (i.e., IP InSight Client)
  - IP InSight Client checks DNS for CGI and server
  - Script configures which IP InSight management server to report to
  - Service reports are then available to track throughput, latency, etc.
- Supports end-to-end monitoring through SPs

Remote Access VPN Management Challenges—Usage Auditing

- Must track user activity throughout the network
  - Active/inactive sessions
  - Session failures
  - Session duration and throughput
  - Data transferred/session
- Relevant concerns
  - Remote users location can vary
  - Recovery methods
  - Usage tools should also be provided by (managed) service provider
Remote Access VPN Management Challenges—Usage Auditing

• Access WAN usage auditing:
  Management typically focused on the authentication server (e.g., AAA)
  Management via a centralized console
    AAA console
    SNMP MIBs may also be utilized within the NAS
  Used for billing and accounting and planning purposes

• VPN usage auditing:
  Similar to access scenario, but add a VPN router at enterprise
  Auditing user sessions at the VPN router is most efficient
    Via SNMP MIBs or CLI/web views

Implications

Remote Access VPN Management Challenges—Usage Auditing

• Remote access VPN usage monitoring example:
  Monitoring established connections at VPN router
    Active/inactive sessions
    Session duration, throughput, etc.
  Web-based status and performance reports
  Secure Sockets Layer (SSL) provides secure access to reports
Site-to-Site VPN Management Challenges—Scalability

- Support and maintenance of user growth
- Network users
  100s sites up to 1,000s of users
  Up to 10,000s of tunnels
- Relevant concerns
  User connectivity is typically through multiple service providers
  Users are geographically dispersed
  Reliability and speed of configuration process is imperative (minimize down time)
  IS staffing and expertise must increase accordingly with network growth

Remote Access VPN Management Challenges—Scalability

- Access WAN scalability management:
  Management solution will change as the number of network users grows
  Small deployments (typically, up to 100s users): device-centric tools
  Larger deployments (typically, 1000s–10,000s of users): network-wide tools
- VPN scalability management:
  Similar to access WAN scalability issues with additional concerns:
  Larger deployments may consider policy-based user configuration and monitoring tools
  Security policy updates -> operational model
  Certificate Authority deployment

Implications
Cisco VPN Management Solutions

Overview

VPN Management Solutions

- Cisco provides VPN management solutions to support VPN deployments
  - Connectivity and reliability across a shared network
    - CiscoWorks2000: Service Management Solution
    - CiscoWorks2000: Routed WAN Management Solution
    - QoS Policy Manager
  - Security configuration end-to-end
    - Cisco Secure Policy Manager
    - Cisco VPN 3000 Concentrator Manager
    - Cisco Secure Access Control Server (ACS)
  - Usage and session monitoring
    - Cisco VPN 3000 Monitor
  - Scalability
    - CiscoWorks2000 Solutions
    - Cisco Secure Policy Manager
    - Cisco VPN 3000 Monitor and Concentrator Manager
Introduction to VPN Management
Summary and Conclusions

• VPNs introduce additional management challenges beyond those in traditional WAN and dial-up environments
  Connectivity and reliability across a shared network
  Service-level monitoring provides an end-to-end view
  Security configuration end-to-end
  Tunnel configuration via policies and templates
  User access policies
  Usage and session monitoring across a shared network
  Depends upon device instrumentation provided for centralized monitoring
  Scalability to support 1000s of users, devices and services
  Must consider the operational model required for effective management

• An effective VPN management solution is an essential component for deploying scalable, economic VPNs

• Cisco provides VPN management solutions to address the above challenges

Reference Information
Networkers 2000 Sessions

• Introduction to VPNs (#2400)
• Introduction to Security (#2500)
• Introduction to Service-Level Management (#2601)
• Deploying Remote Access VPNs (#2401)
• Deploying Secure Networks (#2502)
• Deploying QPM in an Enterprise (#2606)
• Advanced IPSec Deployment Scenarios (#2402)
• Advanced Topics in Enterprise VPNs and PKI (#2403)
Reference Information
RFCs/Internet Drafts

• IPSec Documents
  RFC 2401: Security Architecture for the Internet Protocol
  RFC 2406: IP Encapsulating Security Payload (ESP)
  RFC 2408: Internet Security Association Key Management Protocol (ISAKMP)
  RFC 2409: The Internet Key Exchange (IKE)

• PPTP/L2TP Documents
  RFC 2661: Layer Two Tunneling Protocol (L2TP)
  RFC 2637: Point-to-Point Tunneling Protocol (PPTP)
  RFC 2118: Microsoft Point-to-Point Compression (MPPC) Protocol
  Internet Draft: Microsoft Point-to-Point Encryption (MPPE) Protocol (draft-ietf-pppext-mppe-04.txt)

Reference Information
Web Resources

• IPSec Web Resources
  Cisco TAC’s IPSec page:
  General information:
  Internet engineering task force:
  IP Security Working Group:

• PPTP/L2TP Web Resources
  PPTP information:
  http://infodeli.3com.com/infodeli/tools/remote/general/pptp/pptp.htm
  http://www.microsoft.com/ntserver/commserv/techdetails/default.asp
  L2TP information:
  http://www2.dgsys.com/~lkh/TechInfo/L2TP_PPP.html
  Internet engineering task force:
  Point-to-Point Protocols Extensions working group:
Introduction to Virtual Private Network (VPN) Management

Session 2608

Please Complete Your Evaluation Form

Session 2608