Introduction to Provider-Based IPSec VPNs
Session SEC-120

Agenda

• Overview IPSec Services
• What Is Needed to Manage a VPN?
• Management Issues
• Performance Monitoring for the VPN
Managed CPE-Based IPsec VPNs

- Secure site-to-site connectivity
- Topology
  - Full mesh
  - Hub and spoke
  - Partial mesh
- Dial clients, fixed wireless, CPE* IPsec tunnels
- Management software to manage CPE's

*CPE—Customer Premise Equipment

Managed Network Based IPsec

- VPN concentrator terminates tunnels at provider edge
- Multiple customer tunnels terminate in a routing table and are mapped to outgoing core logical interface
- Tunnels aggregated in the core
- In some cases customer to concentrator not secure
- Management software to manage concentrators
Intranet VPN

- Intranet over shared IP infrastructure
- Remote sites with connectivity to corporate
- Possibly full mesh
- Hub and spoke with no branch office communication

Extranet VPN

- Extend corporate services to partners, suppliers
- Shared IP infrastructure
- Topology hub and spoke
- Secure hub site
IPSec Management Overview

What Is Needed to Manage a VPN Service

- **Inventory**
  - Discovery of devices and device parameters
  - Customer sites, CPE or concentrators and policy information

- **VPN activation**
  - Create, modify, decommission a service
  - Configure parameters and schedule activation
  - Secure connectivity to network devices

- **Audit or verify the VPN service**
  - Verify the VPN is functional

- **Performance monitoring**
  - Determine and monitor service level agreements (SLA) parameters for the VPN
Components of a VPN Service

- Select devices for VPN service
- Policies
  - IKE and IPSec policies for the VPN translated to device specific policies
  - Determine interesting traffic to enter tunnel
- Authentication
  - Shared secret generation or certificate support
- Topology
  - Full mesh, hub and spoke, partial mesh
- Routing over VPN
  - Campus at VPN site and routing exchange
  - Load balancing and fail over

Policy Details

- IKE policies
  - Shared secret or RSA signature
  - DES or 3DES encryption
  - Hash algorithm SHA or MD5
  - IKE lifetime
  - IKE keepalive support
  - Support for Diffie-Hellman Group 1, 2, 5, 7

- IPSec policies
  - AH MD5-HMAC, SHA-HMAC, none
  - ESP authentication MD5-HMAC, SHA-HMAC, none
  - ESP encryption DES, 3DES, null cipher, none
  - Compression LZS, none
  - IPSec lifetime support in Kb or seconds
  - Perfect forwarding secrecy
Typical IOS Commands Needed

- An ordered list of IKE proposals [IKE policies]
- Shared secrets
  - Auto-generate shared secret keys per tunnel
- SA lifetimes
- IKE keepalive
- Crypto map
  - An ordered list of IPSec proposals [transform sets]
  - Crypto ACL—Protect interesting traffic
  - Remote peers
  - Apply crypto map to interface

Routing Provisioning

- Encrypted GRE tunnels
  - IGP may be running at customer site
  - Route exchange to other CPEs’ customer sites using GRE
  - Transport mode

- IPSec
  - Static routes to other CPEs’
  - Internet access on secure I/f
  - Tunnel mode
Management Issues

How Is Configuration Made Easy?

• Provisioning system will generate VPN IOS commands automatically
• Schedule and activate VPN service using management system
• Automate topology creation, hub and spoke, full mesh and partial mesh
• Modification and change of VPN without error
• Decommission VPN—roll back
• Automate failover site provisioning
• Create topology views of the VPN
How Do We Automate Provisioning of Service?

- Smart configuration engine
- Provisioning by modeling IOS commands
  - Attribute-based provisioning
    - Accurately create service based on current network configuration—avoid conflicts
    - Detect problems before provisioning
  - Operator has no need for extensive IOS knowledge

Just in Time Provisioning Mechanism

- Telnet or SSH to CPE's
- Upload current configuration
  - Validates operator input
  - Creates configuration
- Download and activate

Management Network/NOC
Scalable Service Creation

- Scalable provisioning engine
  Distributed and multi-threaded Telnet/SSH gateway server for activation
- Automatically generate shared secret for large number of tunnels
  Full mesh of CPE(CPE-1)/2, 100 CPE = 4950 tunnels
  Reasonable time is 30 minutes or less
  Large number of crypto map entries per device
- Scalable and secure using SSH or IPSec tunnel
- API to drive a flow-thru process without GUI

Distributed Telnet Gateway Server (TGS) Provisioning

Large Set of VPH Service Requests

Generic Transport Layer Server

Split Telnet Requests into Smaller Bundles Based on Threads of GTL

Partition Bundle Allocate to TGS1 and Provision

Partition Bundle Allocate to TGS2 and Provision

Service Provider Network
Verification of VPN Service

- Auditing verifies VPN is functioning
  - Audit per customer
  - Audit per VPN
  - Audit per tunnel
  - Audits are normally scheduled periodically
- Audit IOS configuration
  - Collect configuration
  - Verify provisioned VPN IOS commands line by line
- Audit routing
  - Collect routing table
  - Verify routing tables (used for GRE tunnels)

VPN Service States

- FAILED DEPLOY
  - Download Failed
  - REQUESTED Service
  - Bad Service Request
  - INVALID

- PENDING
  - Download OK

- FAILED AUDIT
  - State Chance by Provisioning
  - State Chance by Audit

- DEPLOYED Config OK
  - DEPLOYED
  - Config OK

- LOST Missing Config

- BROKEN No Routing
  - FAILED
  - AUDIT

- CLOSED
  - State Chance by Provisioning
  - State Chance by Audit

  State Chance by Audit

  State Chance by Provisioning
Typical Provisioning and Audit Flow

Select Customer and CPE's for VPN

Choose Topology
• Full mesh
• Hub and spoke

Select Predefined IKE and IPSec Policy
Select Routing

• View tunnels
• Verify end points
• Satisfied all OK

• Translate inputs to IOS commands
• PROVISION commands

• Schedule periodic audits
• View audit reports

VPN Performance Monitoring
Service Level Agreement Monitoring

- SLA metrics measured
  - Response time
  - Availability
  - Jitter
  - Packet loss
  - Threshold violations

* SA Agent is IOS Service Assurance Agent

Service Level Agreement (SLA) Monitoring

- Create Service Assurance Agent probes
- Periodic collection of SAA MIB for SLA statistics

  Possible probes:
  - ICMP echo
  - TCP connect
  - UDP echo
  - HTTP
  - DNS
  - DHCP
  - Voice jitter (packet loss monitoring)
SAA Probe Possibilities

- SAA probes within the tunnel
  - SAA probes are periodically sending packets
  - Keep tunnel up
  - Actual IPSec tunnel delay and packet loss

- SAA outside the tunnel
  - Tunnel will not remain Up
  - Statistics demonstrating site-to-site IP network delay and packet loss not per tunnel

SLA Network Statistics

- Customer statistics per VPN tunnel or outside tunnel
  - Monitor customer is within SLA for packet delay
  - Monitor customer is within SLA for packet loss
  - Per Class of Service packet delay and loss

- Provision SAA probes to produce traps
  - Timeout trap
  - Connectivity loss trap
  - Threshold trap

- Interface statistics collection
- QOS MIB statistics collection
Managing Configuration

- Collect router configuration periodically
- Use config-change trap to indicate what devices in the network need to be collected
- Version control and archive of configuration files in case of router failure
- Download console to apply any router configuration
- Just-in-time provisioning involves upload of configuration file so database in sync with network after provisioning

Cisco VPN Management Offering

VPN Solution Center (VPNSC)

- Cisco’s service management platform for multiple IP VPN technology offerings
  - Service Provider Class VPN Management Application
    - Release 2.0 FCS March 2001
    - Provisioning and Auditing
    - Key Management
    - SLA Monitoring
    - Open Service Provider API’s
- Information about software:
- Documentation URL:
Introduction to Provider-Based IPSec VPNs
Session SEC-120

Please Complete Your Evaluation Form
Session SEC-120