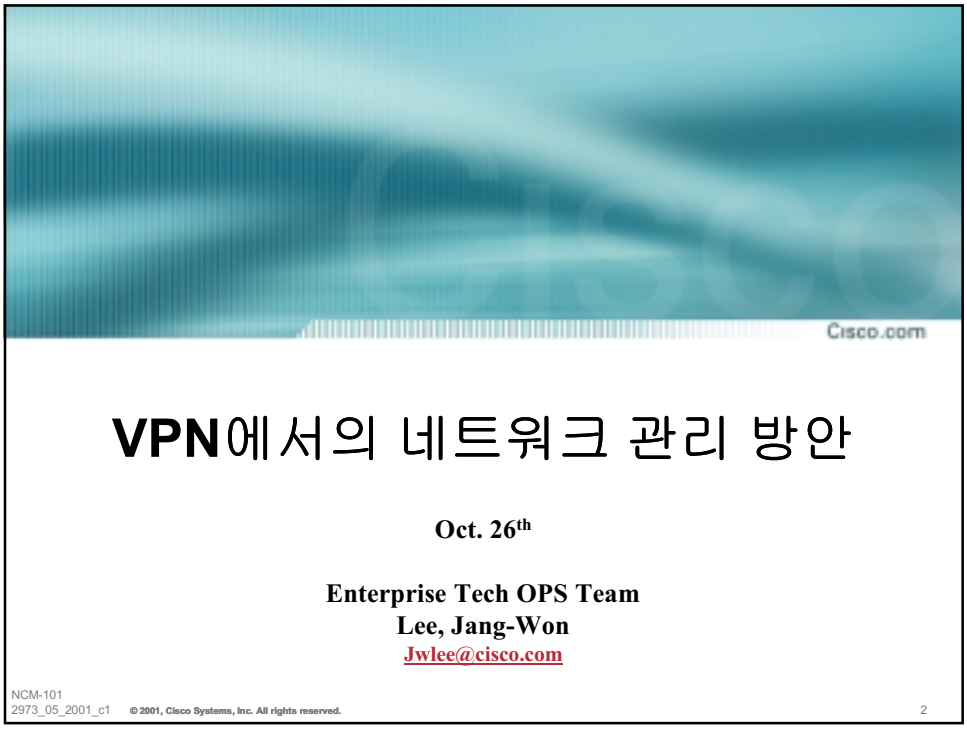
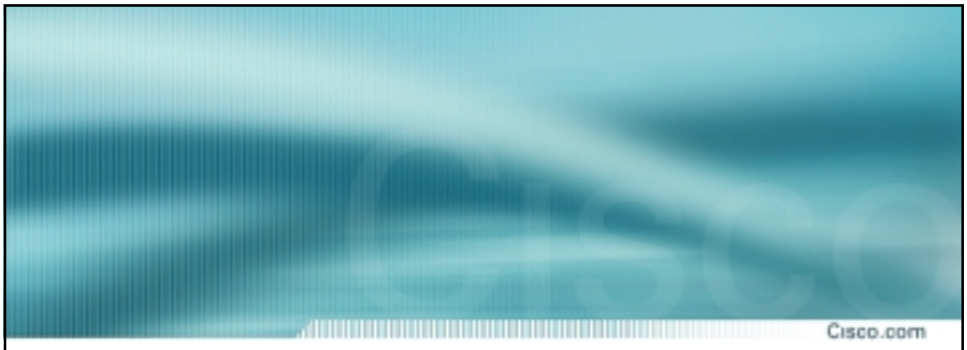


Agenda

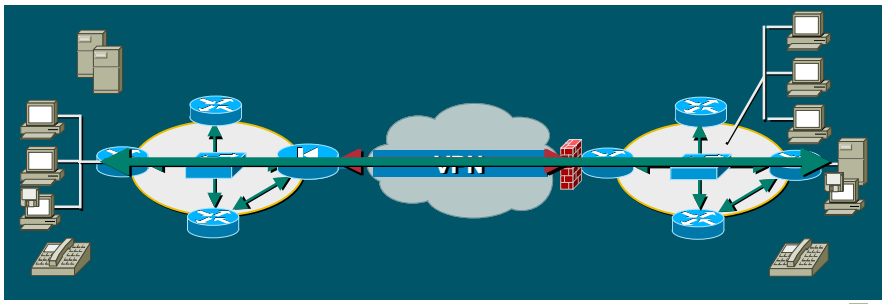
Cisco.com

- **VPN Management** 개요
- **VPN Management** 기능 분석
- 사례분석
- **Ciscoworks 2000** 제품소개



VPN Management 기능 분석

VPN Management 요구사항



- Controls network access by configuring access points
- Protects the flow of sensitive information by provisioning IPSec VPNs to encrypt the data
- Protects from malicious network attacks using intrusion detection sensors

5

VPN Management 요구사항

고려해야 할 요인 ?

- 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

6

VPN Management 요구사항 - Security

Cisco.com

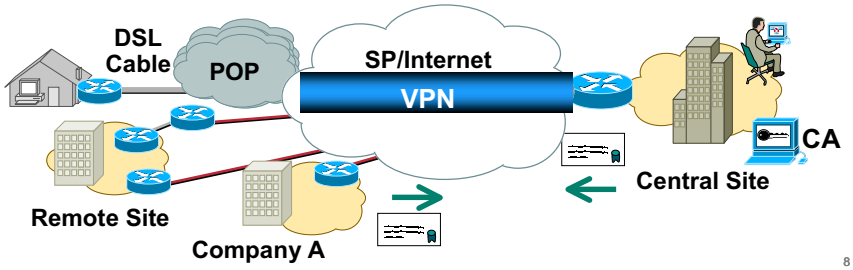
- **Tunnel configuration (establishing peers)**
  - IPSec (authentication: MD5, SHA; encryption: DES, 3DES, RC4)
  - GRE (multicast and broadcast support)
- **Configuring supporting services**
  - Authentication (AAA, certificate, directory)
  - Timing/NTP servers—utilized by certificates
  - Access 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

7

VPN Management 요구사항 - Security

Cisco.com

- **Traditional WAN security management:**
  - Management via CLI, embedded web interfaces or centralized console
  - ACL/firewall configuration
  - Typically, no authentication and encryption technologies utilized
- **VPN security policy management:**
  - Multidevice configuration via centralized console
    - Configures access lists, tunnel methods, SAs/lifetime, crypto maps, interfaces
    - Configure packet authentication using pre-shared keys or certs
    - Certificate authorities: server mgmt, device enrollment and revocation lists
  - Implications

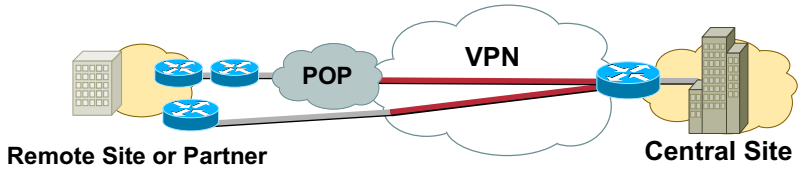


8

VPN Management 요구사항 - Connectivity

Cisco.com

- 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)

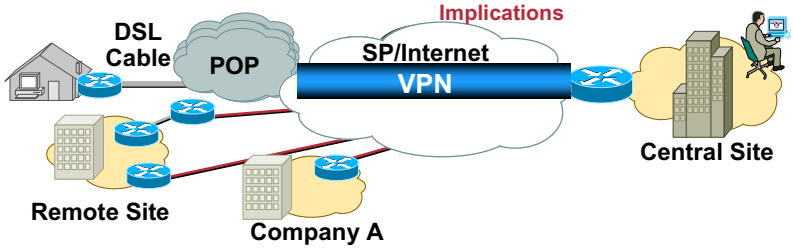


9

VPN Management 요구사항 - Connectivity

Cisco.com

- 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®)
  - Implications



10

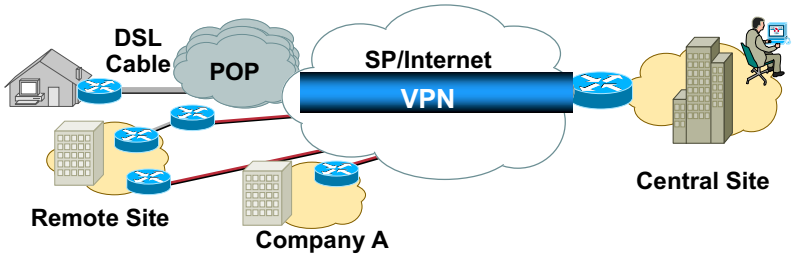
VPN Management 요구사항 - Session Monitoring

- 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)

11

VPN Management 요구사항 - 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



12

VPN Management 요구사항 - Scalability

Cisco.com

- 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
  - Firewalling and ACLs
  - QoS
- Relevant concerns
  - Reliability and speed of configuration process (minimize down time)
  - Security Association (SA) setup rate, max. SAs, encryption performance

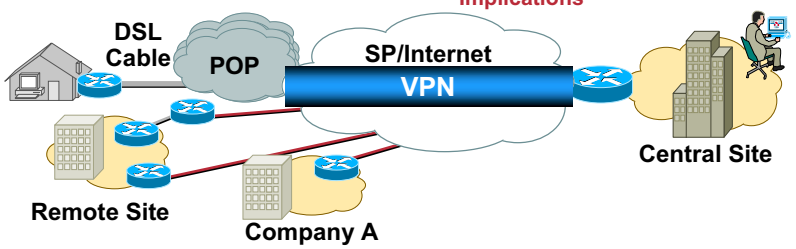
13

VPN Management 요구사항 - Scalability

Cisco.com

- 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



14

Cisco.com

사례 분석

사례 1: IPSec VPN

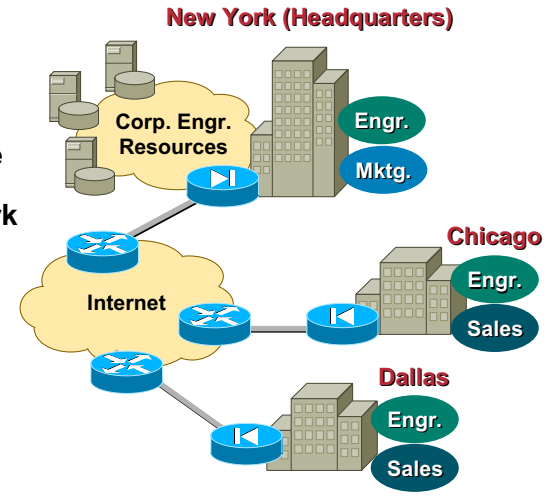
Cisco.com

- 환경

  Site-to-site VPN links HQ to remote branches across Internet/SP network

- 목적

  To monitor VPN service delivery to ensure consistent availability



관리 대상

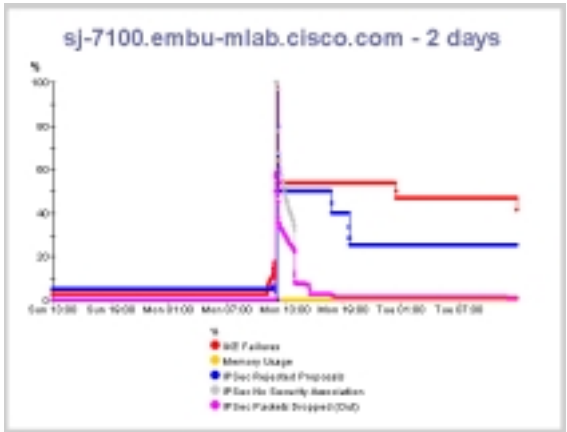
Cisco.com

- **Router resources**
  - **CPU**
  - **Memory**
  - **Active tunnels/sessions**
- **Throughput**
- **Failures**
  - **Key management**
  - **Data management**

17

What Happened Here? – VPN Monitor

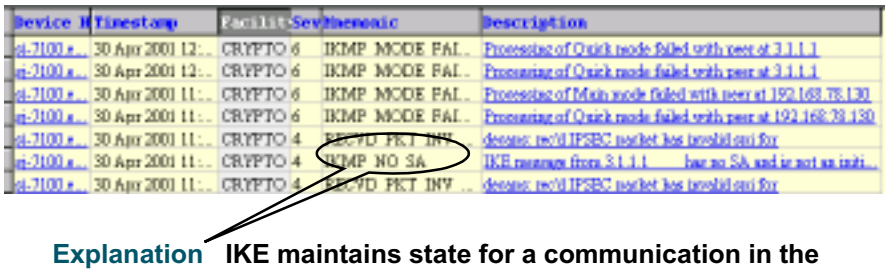
Cisco.com



Tunnel Type	Remote EndPoint	Local Network	Remote Network	User Name	Connect Time	Packets (In)	Packets (Out)	Octets (In)	Octets (Out)
LAN-to-LAN	2.1.1.1	192.168.77.0/26	102.1.1.0/24	N/A	0 days 17:20	421	421	70944	70184
LAN-to-LAN	3.1.1.1	192.168.77.0/26	103.1.1.0/24	N/A	0 days 17:20	905	905	139896	139864

18

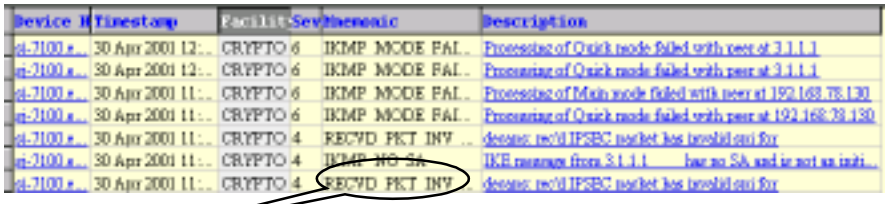
Check Syslog



Explanation IKE maintains state for a communication in the form of security associations; no security association exists for this packet and it is not an initial offer from the peer to establish one; this situation could denote a denial of service attack

Recommended Action Contact the remote peer's administrator

Check Syslog



Explanation A received IPSEC packet specifies an SPI that does not exist in the security association database (SADB); this may be a temporary condition resulting from slight differences in the aging of SAs between the IPSEC peers, or because the local SAs have been cleared; it may also be caused by bogus packets being sent by the IPSEC peer; some might consider this a hostile event

Recommended Action If the local SAs have been cleared, the peer may not know this; in this case, if a new connection is established from the local router, the two peers may reestablish successfully; if the problem occurs for more than a brief period, either attempt to establish a new connection or contact the peer's administrator

Check Syslog

Cisco.com

Device I	Timestamp	Facility	Sev	Mnemonic	Description
ci-7100.e...	30 Apr 2001 12:..	CRYPTO	6	IKMP_MODE_FAI..	Processing of Quick mode failed with peer at 3.1.1.1
ci-7100.e...	30 Apr 2001 12:..	CRYPTO	6	IKMP_MODE_FAI..	Processing of Quick mode failed with peer at 3.1.1.1
ci-7100.e...	30 Apr 2001 11:..	CRYPTO	6	IKMP_MODE_FAI..	Processing of Main mode failed with peer at 192.168.78.130
ci-7100.e...	30 Apr 2001 11:..	CRYPTO	6	IKMP_MODE_FAI..	Processing of Quick mode failed with peer at 192.168.78.130
ci-7100.e...	30 Apr 2001 11:..	CRYPTO	4	RECVD_PKT_INV ..	decaps: rec'd IPSEC packet has invalid spi for
ci-7100.e...	30 Apr 2001 11:..	CRYPTO	4	IKMP_NO_SA	IKE message from 3.1.1.1 has no SA and is not an initi...
ci-7100.e...	30 Apr 2001 11:..	CRYPTO	4	RECVD_PKT_INV ..	decaps: rec'd IPSEC packet has invalid spi for

Quick Mode failure

Explanation Negotiation with the remote peer failed

Recommended Action If this situation persists contact the remote peer

Main Node failure

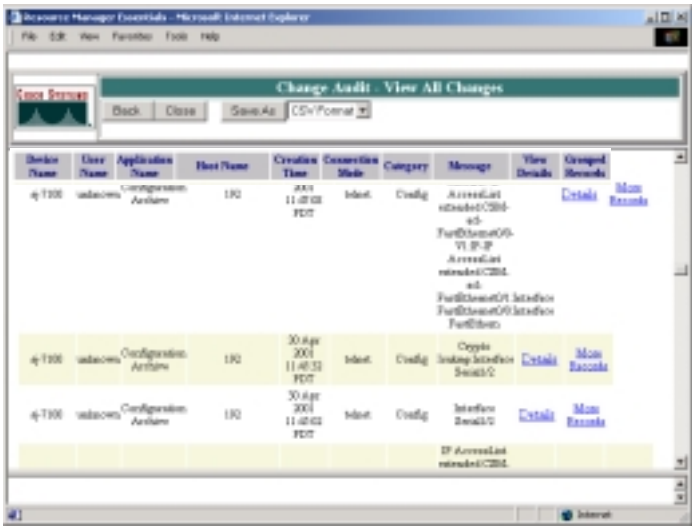
Explanation Negotiation with the remote peer failed

Recommended Action If this situation persists contact the remote peer

21

Config 변화 검사

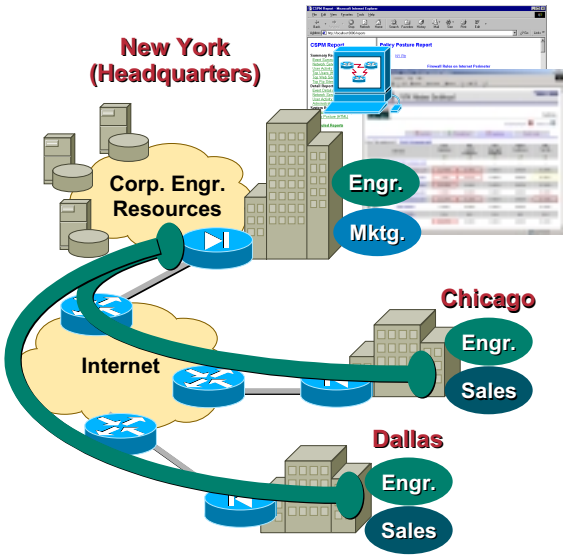
Cisco.com



22

Service Monitoring Applications

- CSPM
  - Policy auditing and monitoring
  - Near-real time event data
- CWVMS
  - System, throughput, failures and events
  - Threshold violations
  - Real-time graph of key VPN parameters
  - Tunnel drill-downs



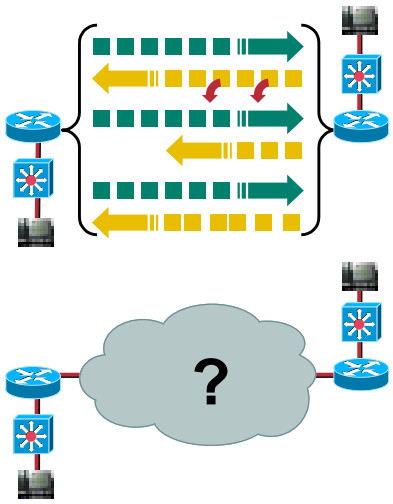
사례 2: VoIP

- 환경
  - Government agency with distributed offices using VoIP to reduce telephony charges
  - Wants ability to objectively monitor and report on voice quality in network
  - Voice QoS affected by Network QoS: when former detected, need to examine latter

VoIP의 일반적인 문제점

Cisco.com

- Typical QoS problems
  - Packet Loss
  - Excessive Delay
  - Excessive Jitter
- Core problems do not always show evidence on edges
- Need means to inject at edges, track ingress to egress

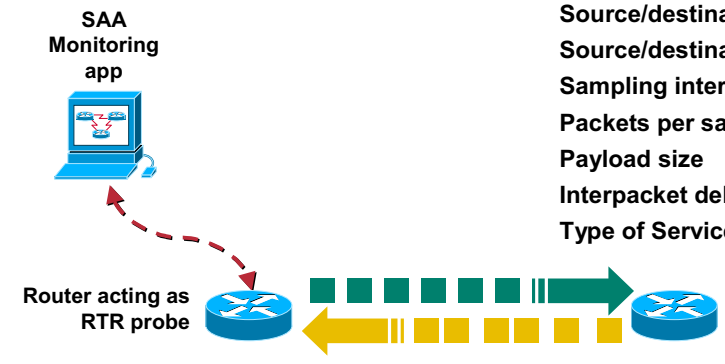


25

Service Assurance Agent Jitter Probes

Cisco.com

- Parameters
  - Source/destination devices
  - Source/destination ports
  - Sampling interval
  - Packets per sample
  - Payload size
  - Interpacket delay
  - Type of Service



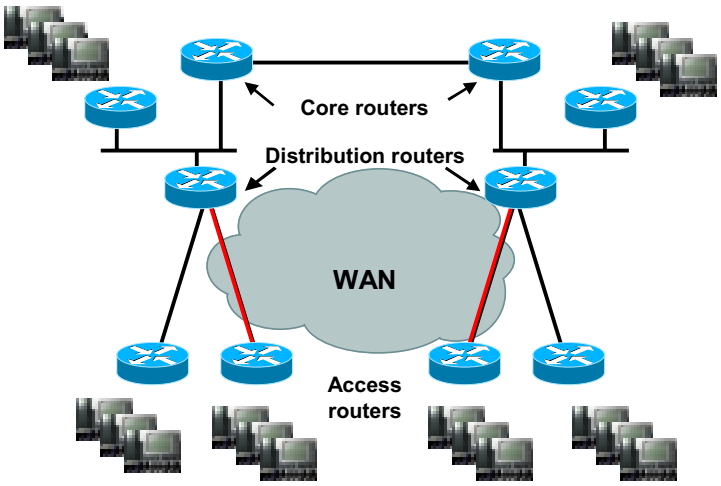

```
rtr 1
 type jitter dest-ipaddr 5.0.0.1 dest-port 99
rtr schedule 1 life 10000000 start-time now
ntp server 6.0.0.2
```

```
(config)#rtr responder
```

26

SAA Deployment—Coverage

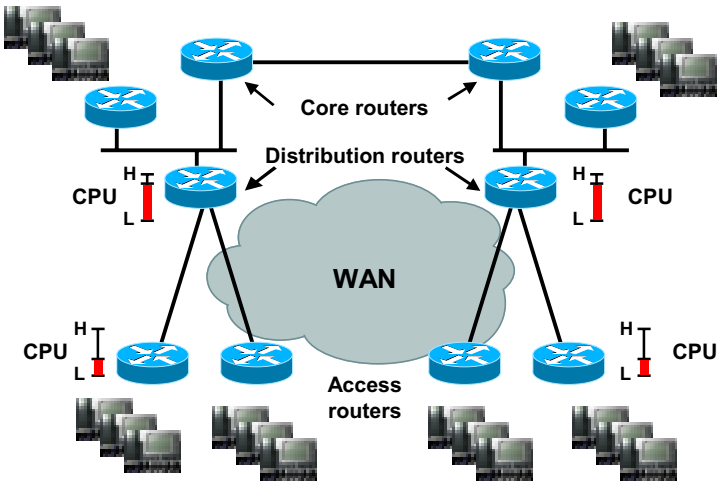
Cisco.com



27

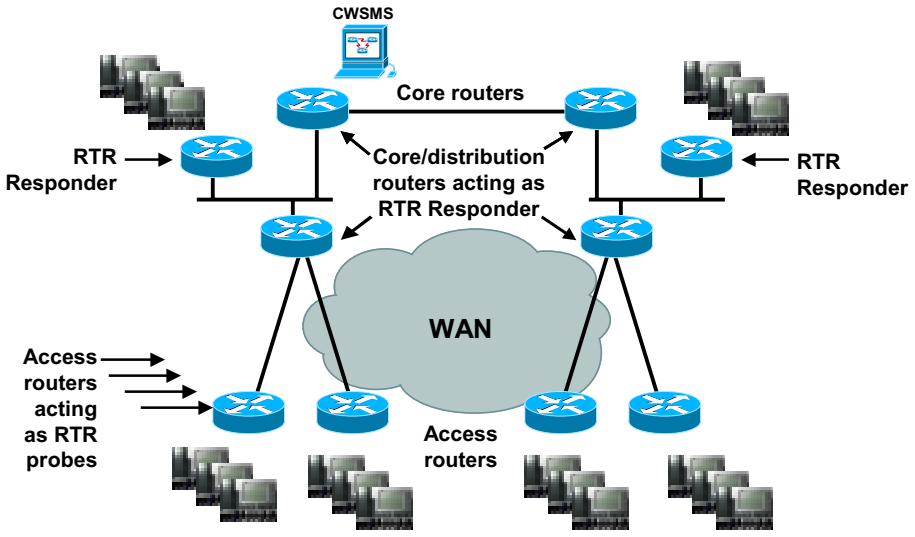
SAA Deployment—CPU Impact

Cisco.com



28

Deployment—Probes and Responders



29

QoS 고려사항

- **Probe traffic must have same QoS as real voice traffic**
- **LLQ or RTP Priority configurations on the router may need to be adjusted so that traffic from the RTR probes is subject to strict priority queuing**

Example:

```
class-map VoiceRTP
  match access-group name IP-RTP
policy-map 192Kbps_site
  class VoiceTRP
  priority 110

ip access-list extended IP-RTP
  deny ip any any fragments
  permit udp <from> <mask> range 16384 32768 <to> <mask> range 16384 32768
precedence critical
  permit udp any any eq 20000 precedence critical
  permit udp any eq 20000 precedence critical
```

30

Tracking 결과

Cisco.com

- Define SLAs paralleling service guarantees
- View trends, threshold status
- APIs to access data for individual uses

31

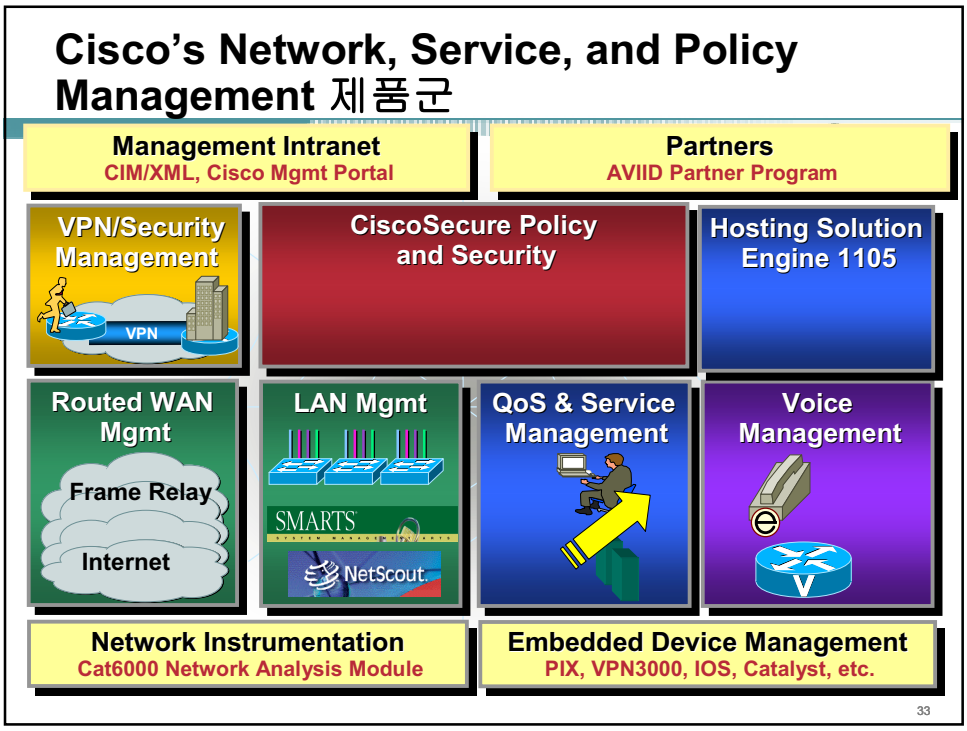
Cisco.com

Ciscoworks 2000 제품소개

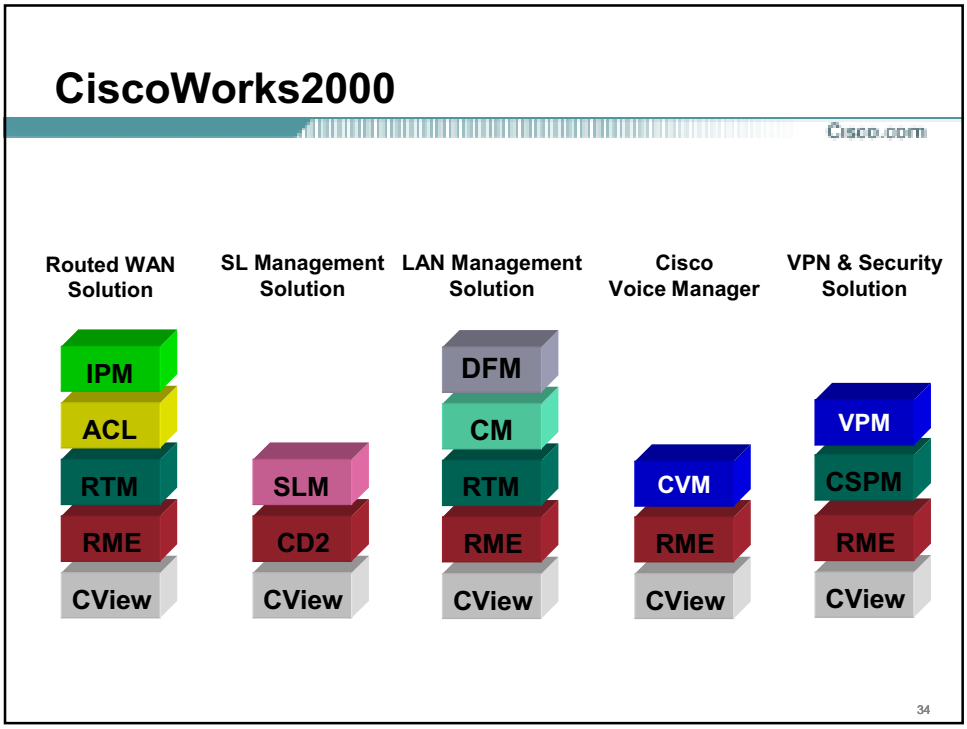
NCM-101
2973_05_2001_c1

32

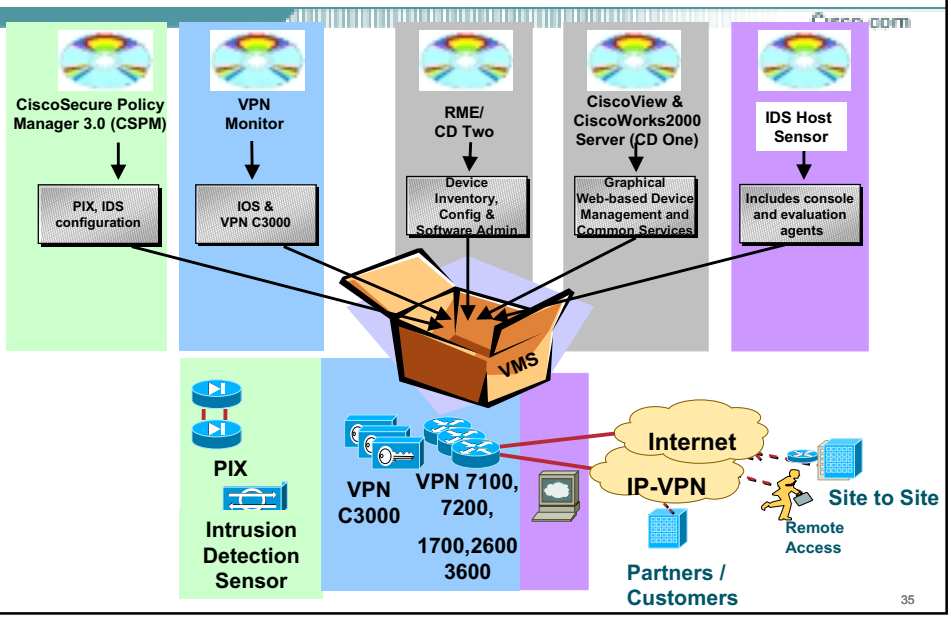
Cisco's Network, Service, and Policy Management 제품군



CiscoWorks2000



VPN/Security Management Solution



35

VMS 구성요소

- **VPN Monitor**
  - –Collects stores and reports on L2TP, PPTP remote access and IPSec based site to site VPN's configured on Cisco VPN Concentrator 3000 series, Cisco 7100 series VPN routers or Cisco 7200 series routers.
- **Cisco Secure Policy Manager (CSPM)**
  - –Defines and enforces security policies on Cisco Secure PIX firewalls, and reporting and alerting of intrusions when Cisco Secure Intrusion Detection System (IDS) devices are deployed.
- **Resource Manager Essentials (RME)**
  - –Provides the operational management features required by enterprises. Software distribution, change audit and authorization, device inventory and credentials management and Syslog analysis for problem solving and notification of VPN and Security operational problems.
- **CiscoView**
  - –Provides WAN managers with browser access to real-time device status, operational and configuration functions.
- **CiscoWorks2000 Management Server (CD-One)**
  - –Provides the common database, web, and desktop services used to integrate with other Cisco and third party tools.
- **CiscoWorks2000 Inventory Services (CD Two)**
  - –VMS provides an installation option for customers wishing to only install the inventory administration tools of RME. Inventory Services tracks the network devices, reporting hardware and software characteristics and provides device credentials management.

36

특성 및 효과

Cisco.com

- **Software Planning**
  - **Reduced cost of network operation**
- **VPN Reports**
  - **Optimize performance, improved availability**
- **VPN Monitor Dashboard**
  - **Focus operation support**
  - **Isolate device and connection bottlenecks**
- **Enforce and Monitor Security Policy**
  - **Protect Business assets**

37

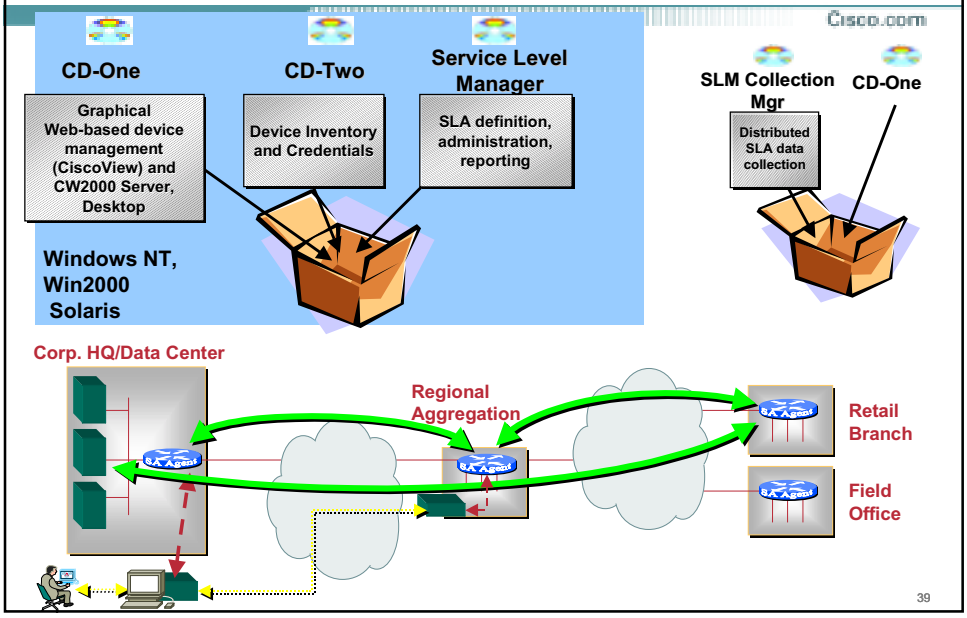
주 대상 고객

Cisco.com

- **Education, Retail Services, Dealerships**
- **Lots of Remote Branch's**
- **Small, Medium and Large**
- **Reduce Remote Access Costs**
- **Deploying B to B, Concerned with Security**
- **Cisco Device**
  - **VPN C3000, VPN 7100, 7200**
  - **PIX Firewall, IDS**

38

Service Management Solution



39

특성 및 효과

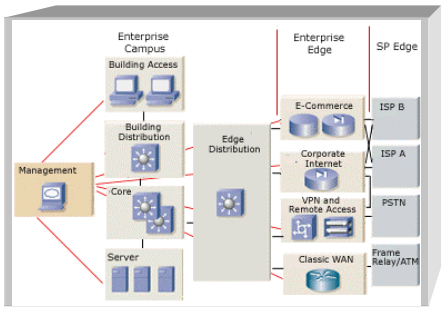
- **Business Drivers**
  - Reduce WAN/telecom costs
  - Increase service quality
  - Evaluate effectiveness of new technology
- **Problems Addressed**
  - Verification of delivered service levels
  - Network's ability to support new services
  - Lack of standards in SLAs

40

주 대상 고객

Cisco.com

- Enterprises w/ VPNs, outsourced services, or whose IT is measured by SLAs
- Broadband Access providers
- ISPs
- Managed service providers



Works with virtually all Cisco IOS devices running 12.0(5)T, or the 12.1 IOS trains.

You know you're looking at a good target customer if…

- They provide or consume managed services
- Use/plan to use VoIP, video, VPN, QoS, SLAs

41

CISCO SYSTEMS

EMPOWERING THE INTERNET GENERATION℠

NCM-101
2973_05_2001_c1

42