



시스코 통합 보안 솔루션



Nov 2007

시스코 시스템즈 코리아

목차

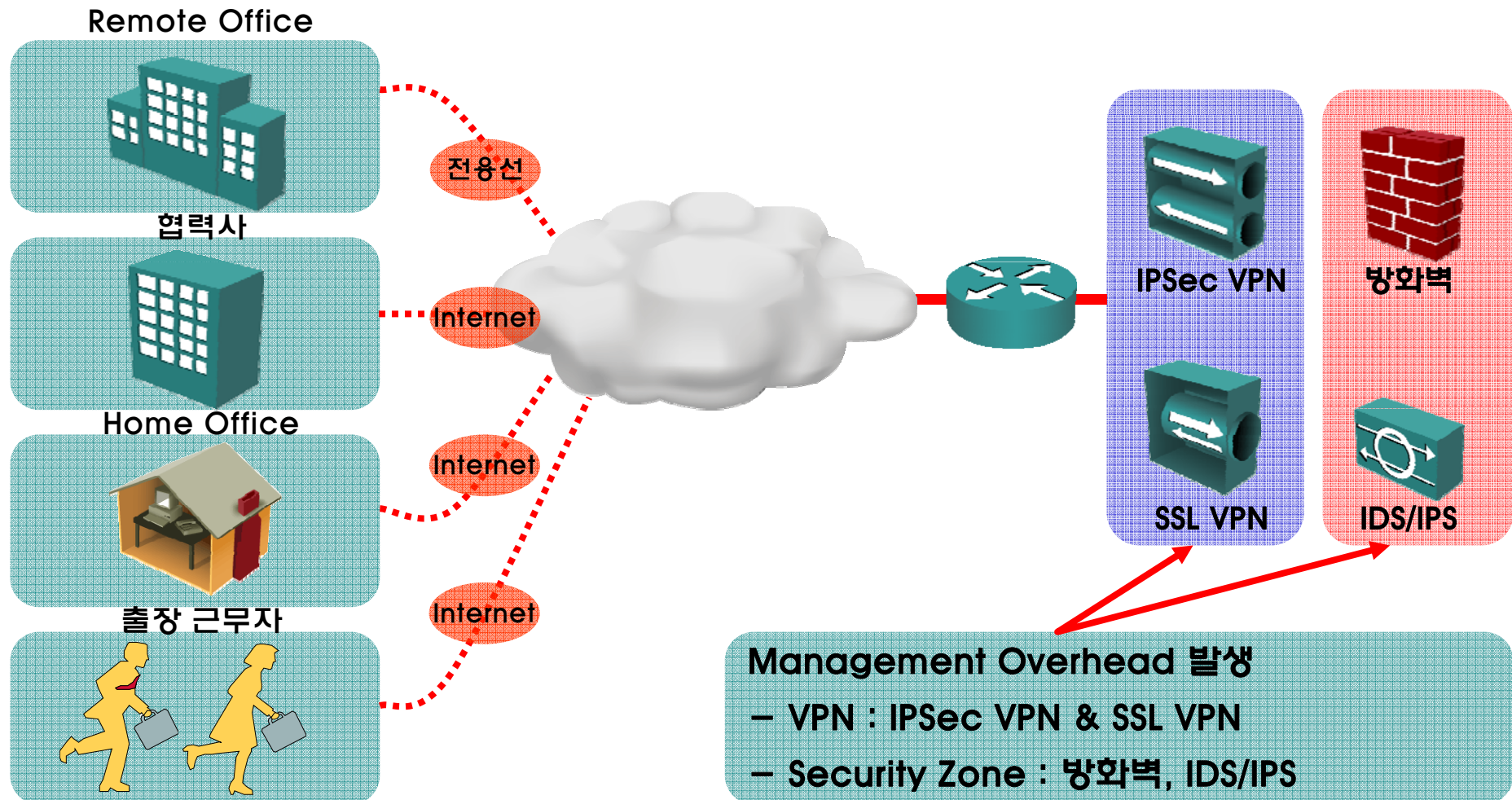
- 통합 보안 장비의 필요성
- 통합 보안 장비 기능 소개
- 통합 보안 장비 제품 소개
- 결론

통합 보안 장비의 필요성



왜 통합 보안 장비인가?

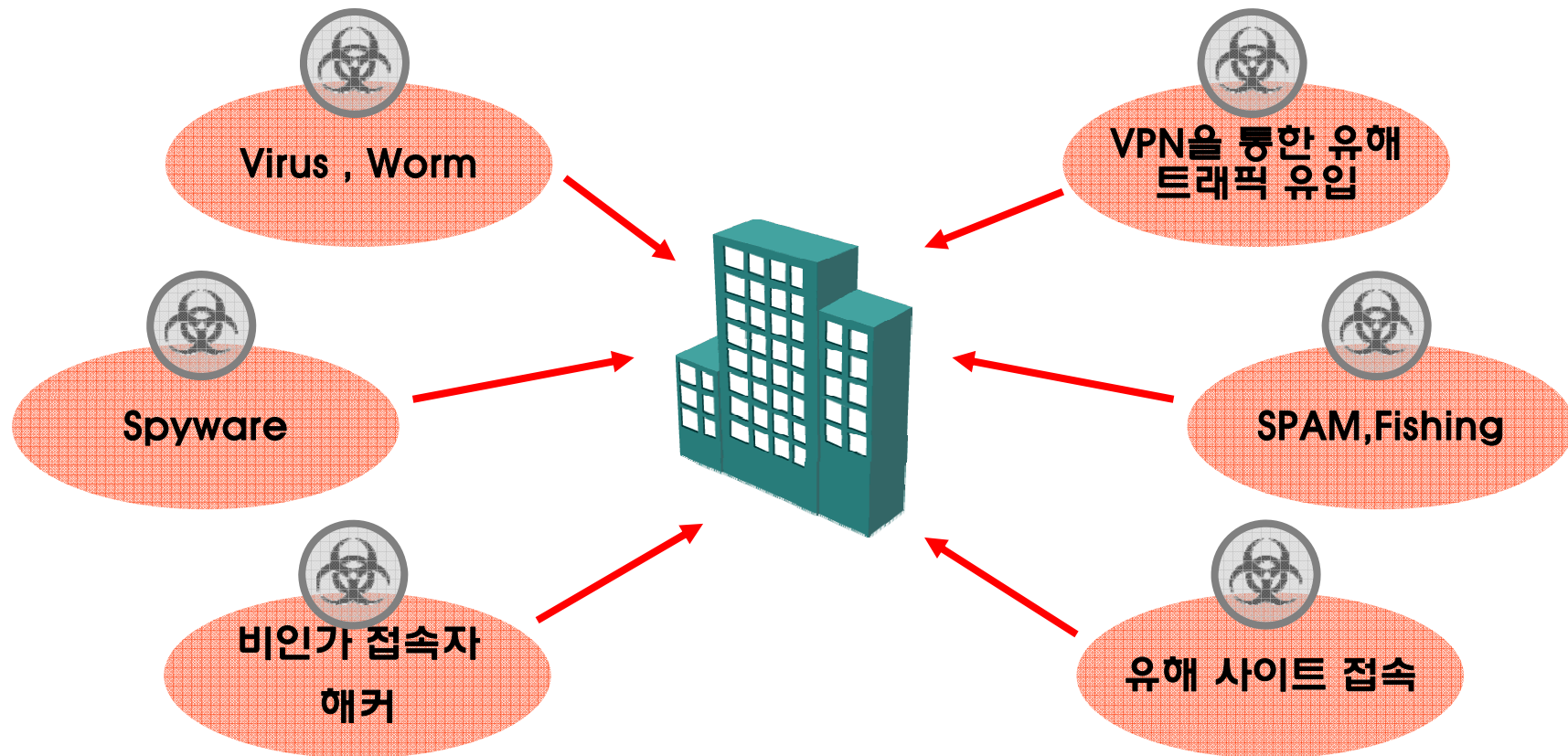
Internet 기반의 Business 증가 - 생산성 향상, 새로운 비즈니스 기회 창출



왜 통합 보안 장비 인가?

보안 위협의 다양성

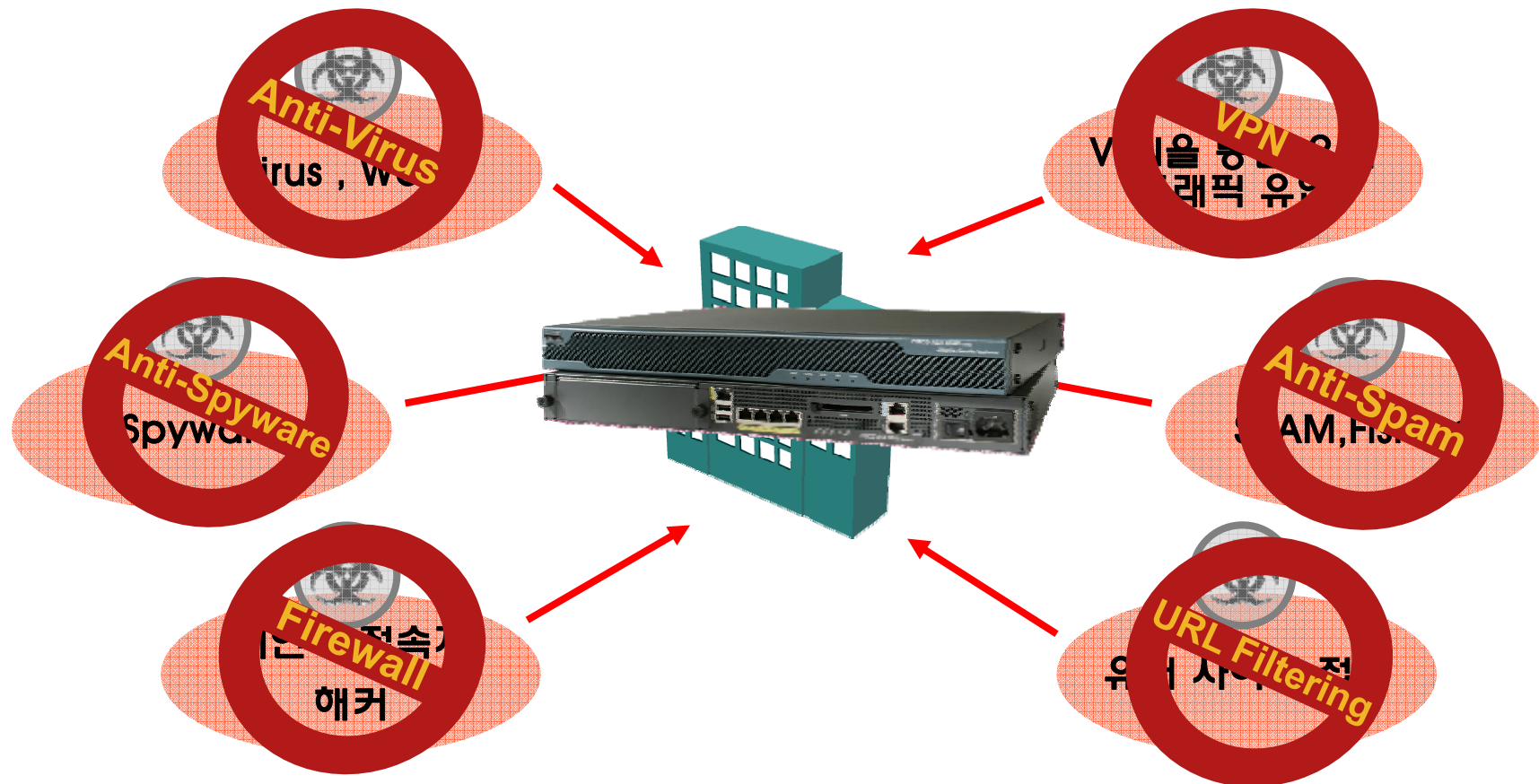
보안 위협의 증가로 인한 Internet 기반의 비즈니스 서비스 중단 가능성...



왜 통합 보안 장비인가?

다양한 위협으로부터 강력한 보안 서비스 요구

다양한 위협에 대비한 통합 장비 기반의 강력한 보안 서비스



ASA 5500 통합 보안 장비

- 기능 소개



업계에서 가장 다양한 통합 보안 서비스 제공

ASA 5500 통합 보안 장비

Market 검증 기술



방화벽 기술
Cisco PIX / FWSM




IDS/IPS 기술
Cisco IPS



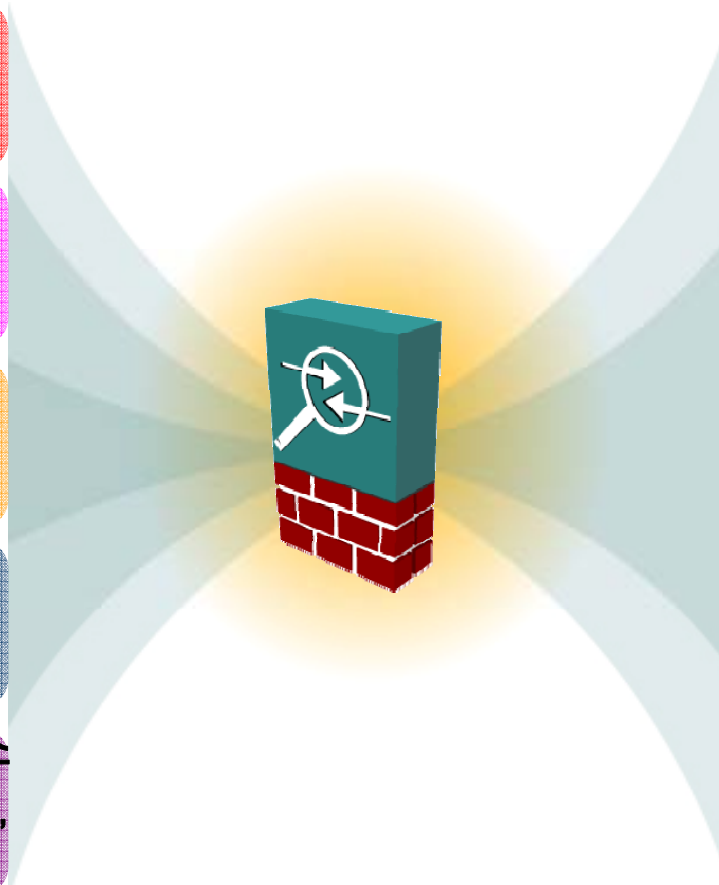
Virus Wall
Trend Micro A.V



VPN 기술
VPN 3000



지능형 네트워크서비스
QoS, IPv6, RIP, OSPF,
EIGRP, PIM



적응형 위협 방어 기술



Application 보안
App Inspection
기반 보안 구현



Anti-X 방어
Virus, Worm, Spam,
Phishing, Spyware,
URL Filtering...



Network 억제, 제어
Traffic 제어
지능형 방어



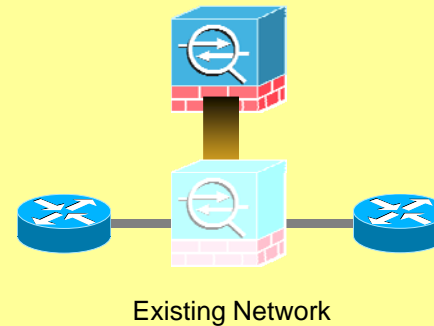
Secure 접속
SSL VPN 동시지원
IPSec VPN

ASA 5500 통합 보안 장비 – Firewall

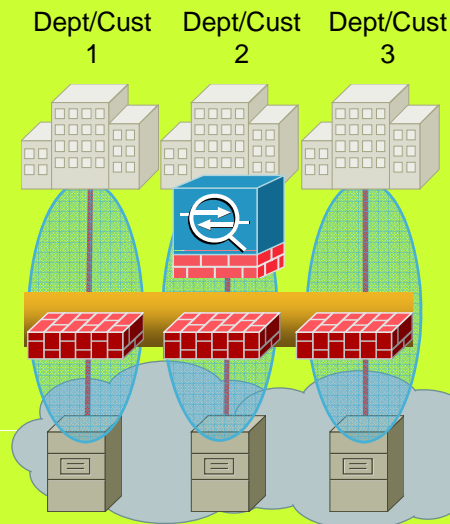
다양한 Firewall 기능 제공

- 확장성 있는 보안 서비스 제공
- 방화벽과 IPS 서비스에 대한 손쉬운 관리
- 신속하고 손쉬운 보안 적용을 위한 Transparent firewall 제공
 - 기존 네트워크에 IP 주소 변경 없이 적용 가능
 - 신규 어플리케이션 등에 따른 내부 Firewall 또는 보안 영역에 손쉽게 적용
- 저렴한 비용으로 확장성 있는 virtual firewalls 제공
 - 장비의 통합 및 각개 영역별 분리 가능
 - 개별적인 보안 정책 및 관리 지원

Transparent Firewall



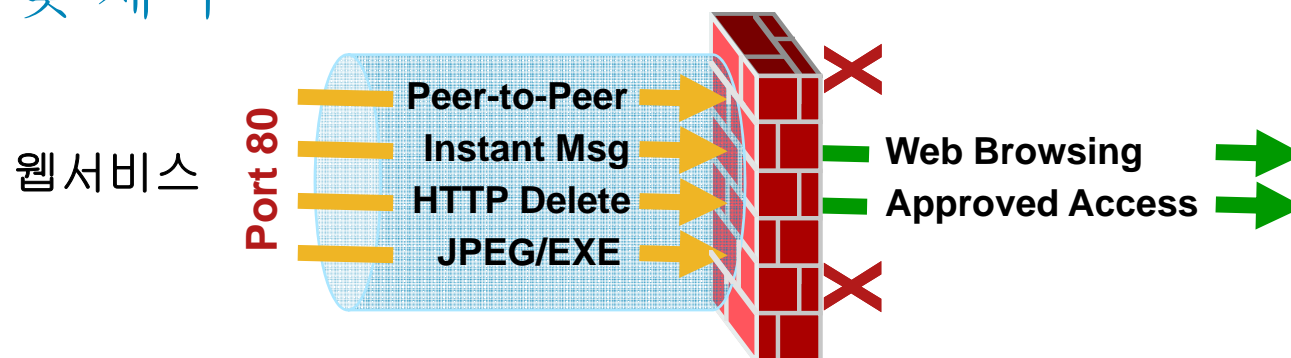
Virtual Firewall



ASA 5500 통합 보안 장비 – Firewall

진화된 어플리케이션 검사 및 제어

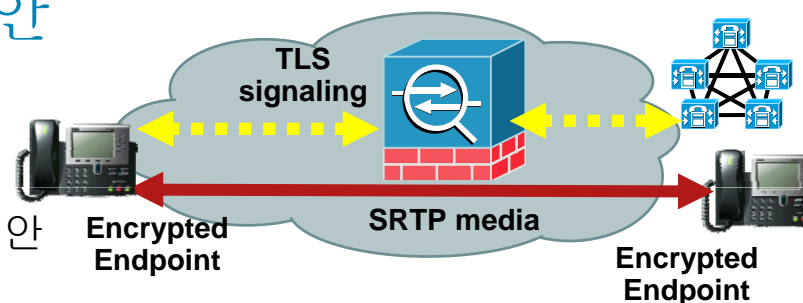
- **Web, SMTP 등** 어플리케이션 영역까지의 패킷 검사 및 제어



▪ Voice 및 멀티 미디어 서비스 보안

차세대 통합 네트워크를 위한 강화된 보안

- 향상된 H.323, SIP, MGCP, RTSP, 그리고 fragmentation / segmentation 지원으로 선두 VoIP 보안 제공

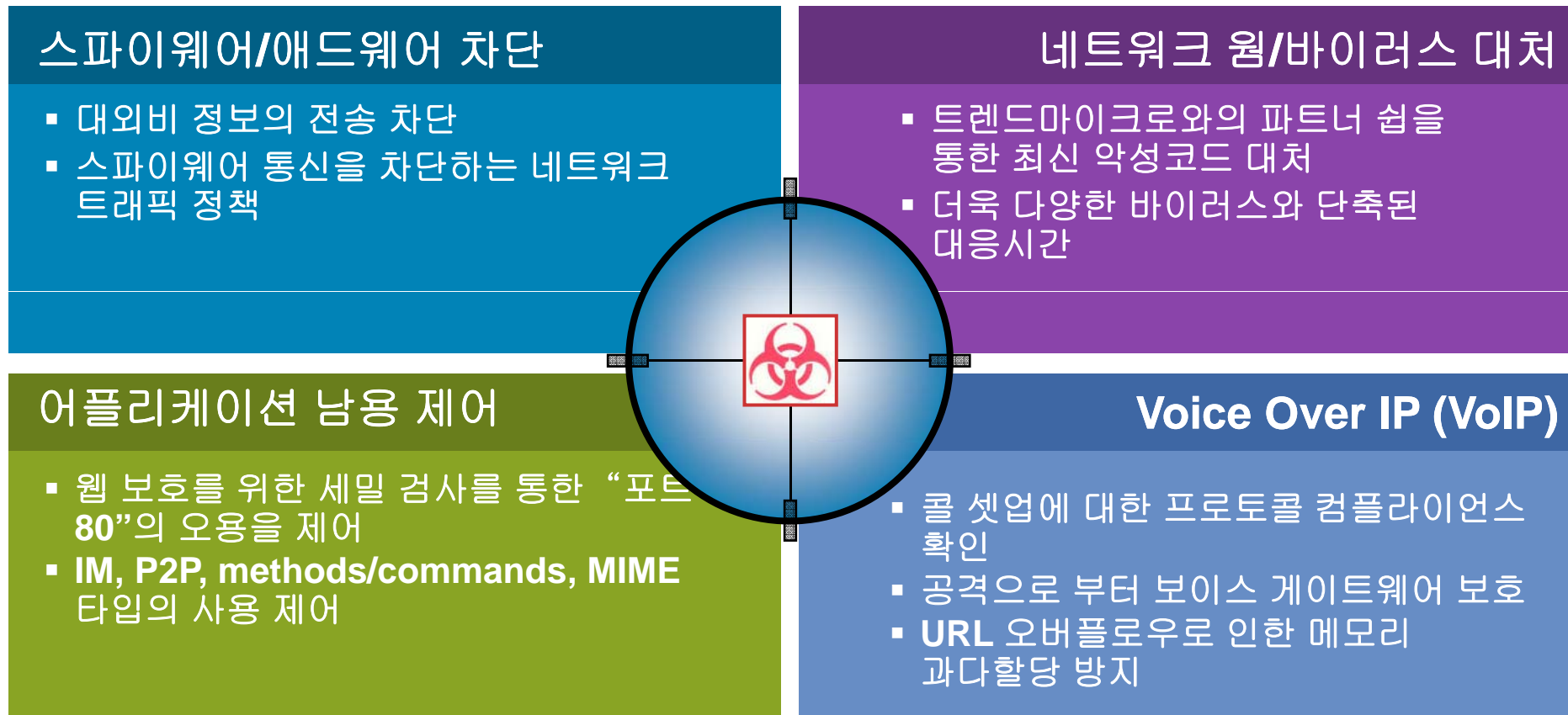


- 지연에 민감한 프로토콜에 대한 최우선 순위의 QoS 지원

- SRTP/TLS 등 암호화된 시스코 voice/video 통신에 대한 보안 제공

ASA 5500 통합 보안 장비 – IPS/Content Security

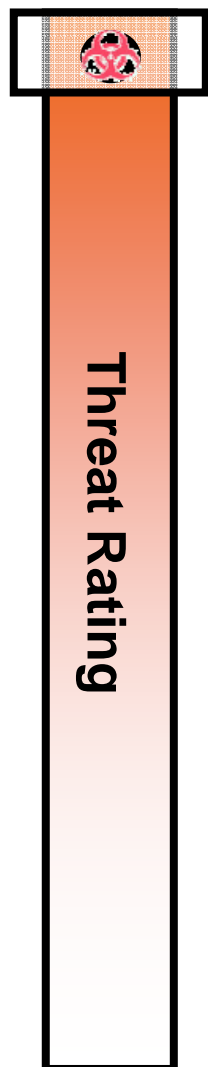
Multi-Vector Threat Identification



광범위한 공격 및 Malware 방어

ASA 5500 통합 보안 장비 - IPS

위협관리기반의 보안 정책 적용



- + 얼마나 위협적 공격인가?
- + 오탐일 가능성은 얼마인가?
- + 공격대상에 대한 해당 공격의 유효성은?
- + 공격대상에 대한 자산의 중요성은?

= Risk Rating

Drives Mitigation Policy



Customizable Risk Rating Thresholds :

0 < RR < 35
35 < RR < 85
85 < RR < 100

Alarm
Alarm & Log Packets
Drop Packet

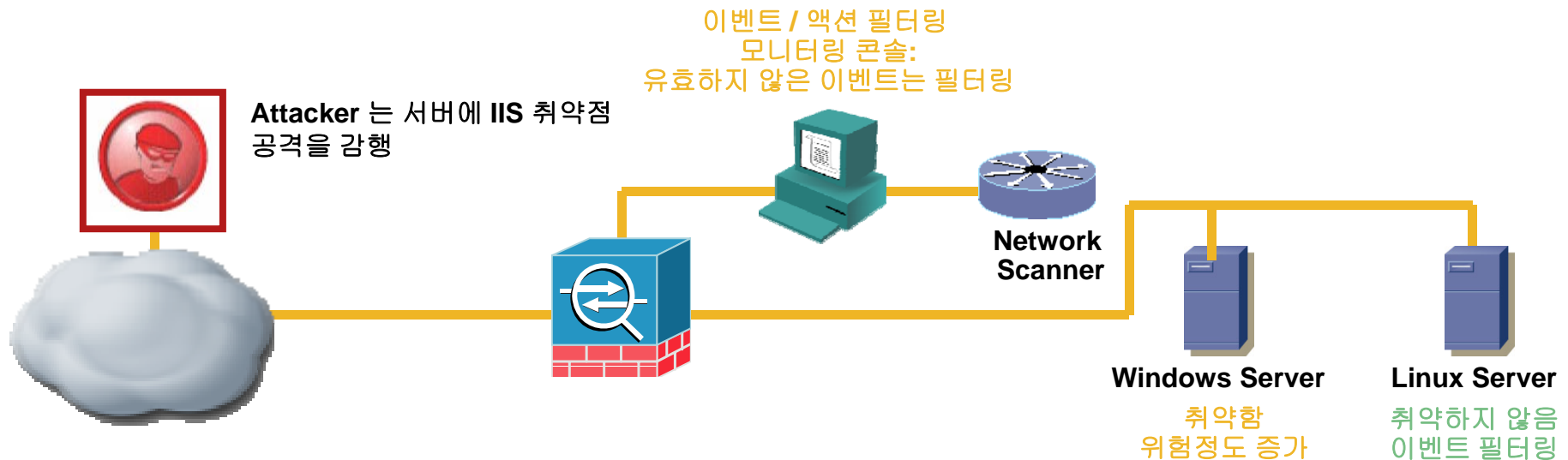
Result: 공격의 정확한 위험성 분석 값 산출 → 정밀한 탐지 및 차단

ASA 5500 통합 보안 장비 - IPS

공격 유효성 검증기능

- 공격 대상에 대한 공격의 유효성에 따라 대응방법 재정의
- 공격 유효성 판단 방법
 - 공격발생시 대상에 대한 OS 및 취약점 확인
 - 기 입력된 OS 정보에 따라 탐지/차단에 대한 예외설정
- 공격의 유효성에 따른 동적인 위협정도 조정

Result: 공격의 상황에 따른 최적의 대응 방안 적용

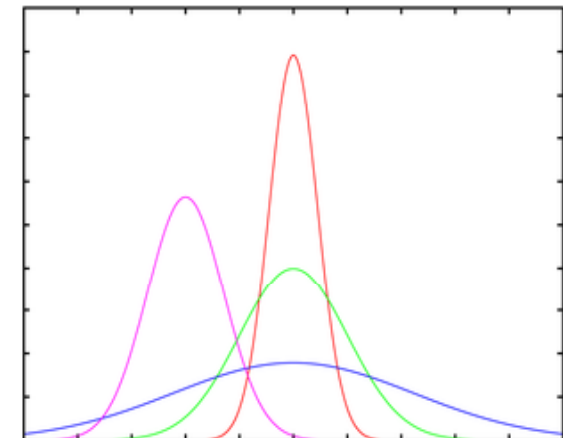
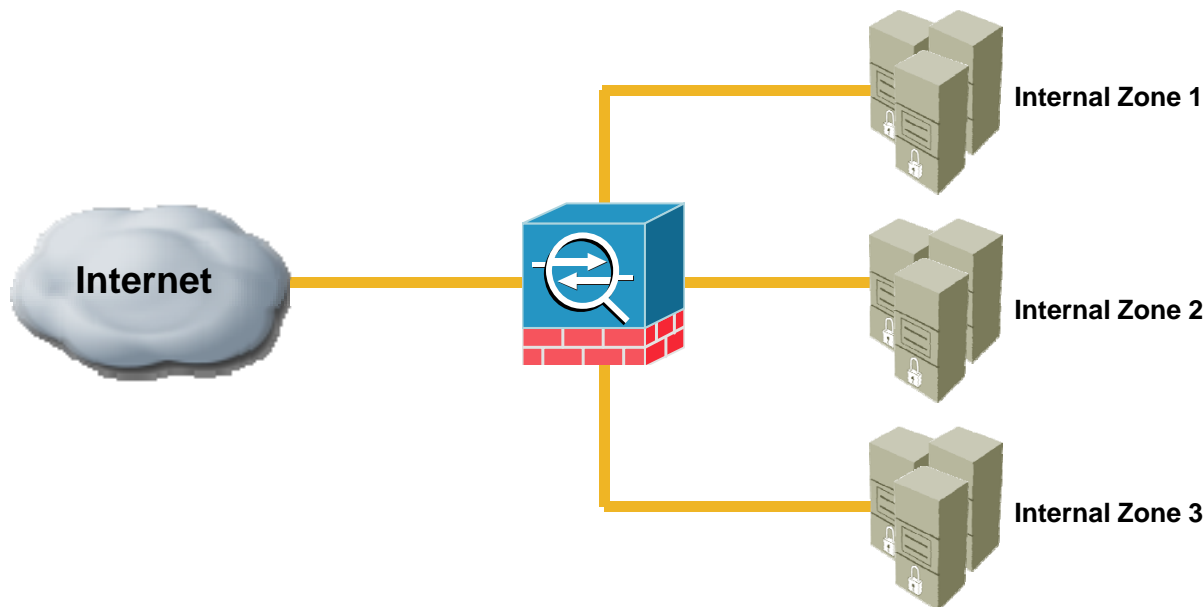


ASA 5500 통합 보안 장비 - IPS

제로데이 공격 방어

- 비정상 행위 분석 기능을 이용한 알려지지 않은 공격 차단
- 평상시 네트워크의 사용패턴을 학습
- 비정상적인 패턴의 트래픽 발생시 자동 탐지 및 정책 기반의 차단

Result: Signature 개발 전의 공격에 대한 탐지 및 차단



보호대상 네트워크의
프로토콜 타입별 정상적인
사용 패턴/통계 그래픽화

ASA 5500 통합 보안 장비 – Content Security

Anti-X

위협 형태



Unauthorized Access



Intrusions and Attacks



Insecure Comms.



Viruses

Spyware



Malware

Phishing



Spam

Inappropriate URLs

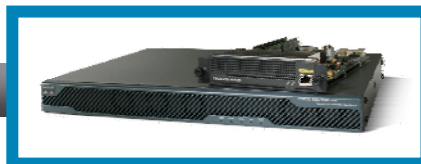


Identity Theft

Offensive Content

NEW Anti-X Service Extensions

Cisco ASA 5500 with CSC-SSM



Granular Policy Controls

Comprehensive Malware Protection

Advanced Content Filtering

Integrated Message Security

Easy to Use

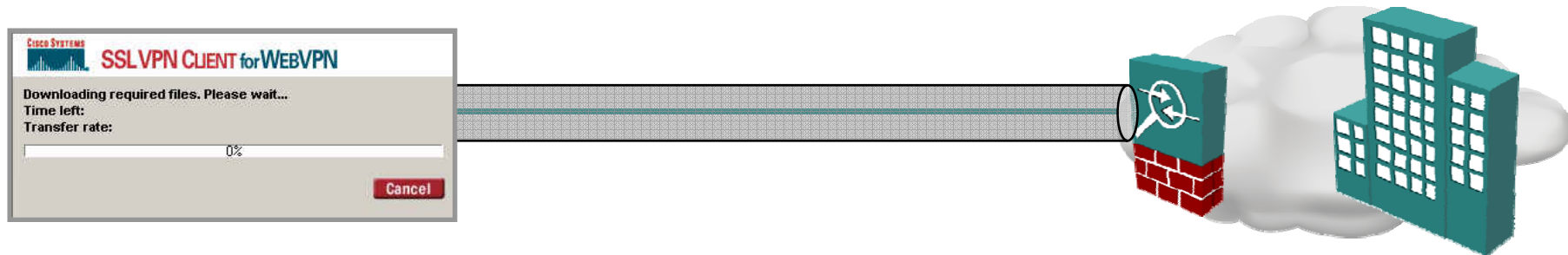
방어

Resource and Information Access Protection

- Hacker Protection
- Client Protection
- DDoS Protection
- Protected Email Communication
- Protected Web Browsing
- Protected File Exchange
- Unwanted Visitor Control
- Audit and Regulatory Assistance
- Non-work Related Web Sites
- Identity Protection

ASA 5500 통합 보안 장비 – SSL VPN

Full Network Access 기능 제공



Tunnel Mode 기반의 SSL VPN Service 제공

- 단일 플랫폼에서 IPsec 과 같은 SSL VPN 서비스를 제공

손쉬운 관리 및 설치

- IPsec 과 달리 Client 자동 설치 및 구성 환경 배포 가능

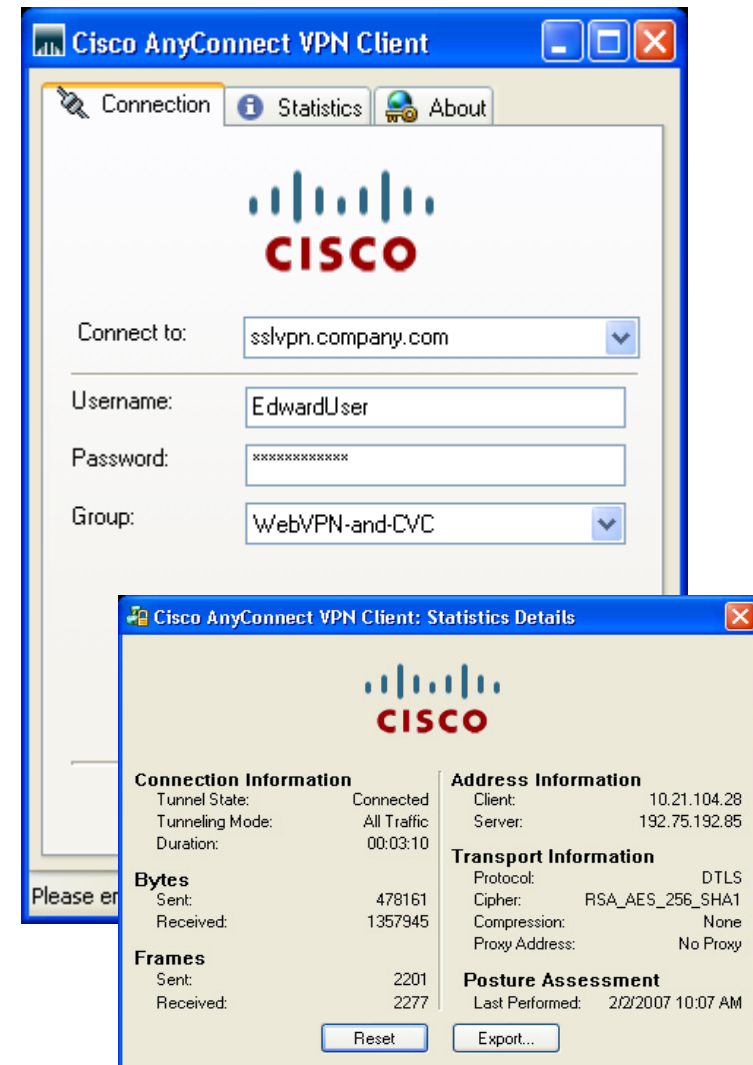
SSL VPN Service의 가장 빠른 구현

- 빠른 설치 및 배포, 작은 설치 용량, LAN 과 같은 구성 환경 제공

ASA 5500 통합 보안 장비 – SSL VPN

Full Network Access 기능 – Cisco AnyConnect

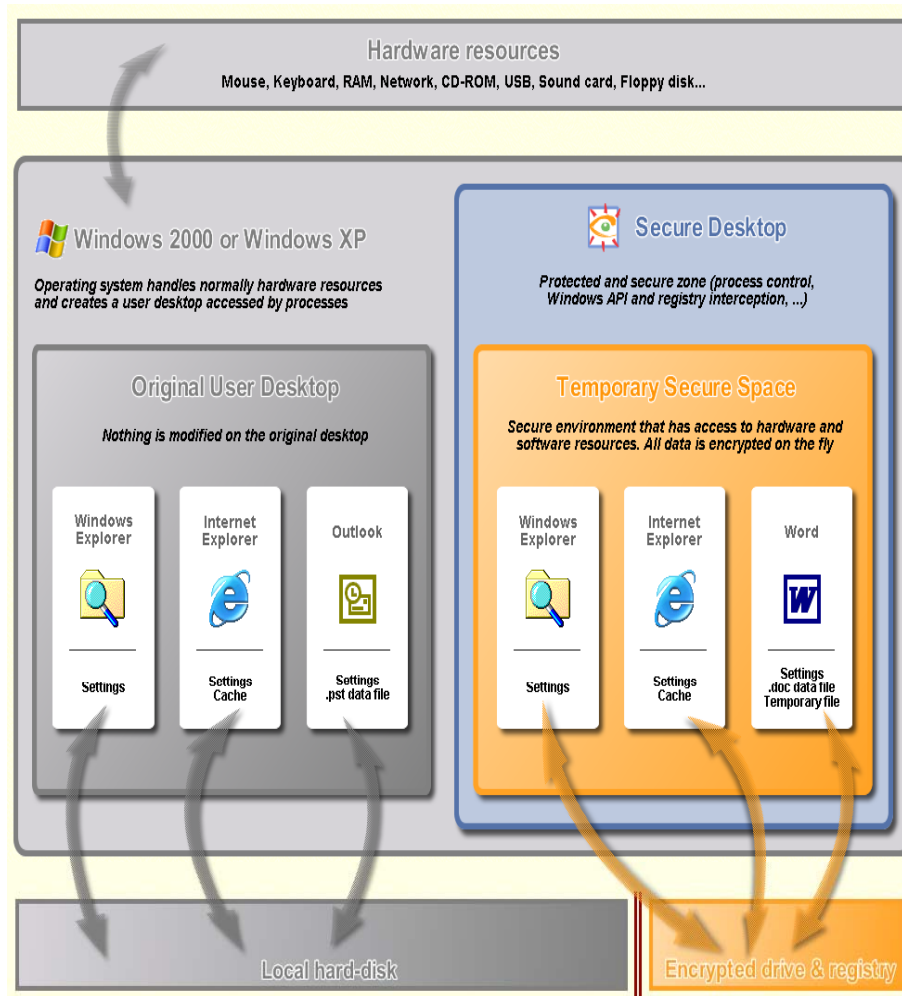
- 차세대 **VPN client**로써, 대부분의 플랫폼을 지원함
 - Windows Vista 32-bit, Windows XP 32-bit and 64-bit, and Windows 2000
 - Mac OS X 10.4 (Intel and PPC)
 - Intel-based Linux
 - Windows Mobile 5 Pocket PC Edition
- 웹포탈 연결 후 자동 설치 및 독립된 인스톨프로그램 설치 기능
- 윈도우 로그인 전 **SSL VPN** 연결 기능
- **Voice, Video** 등 지연 전송률에 민감한 트래픽 조정 기능(DTLS)



ASA 5500 통합 보안 장비 – SSL VPN

Cisco Secure Desktop 기능 제공

- 신뢰성 높지 않은 PC 기반 사용시 적용.
- SSL VPN 사용시 CSD를 통한 Data 각종 정보 암호화



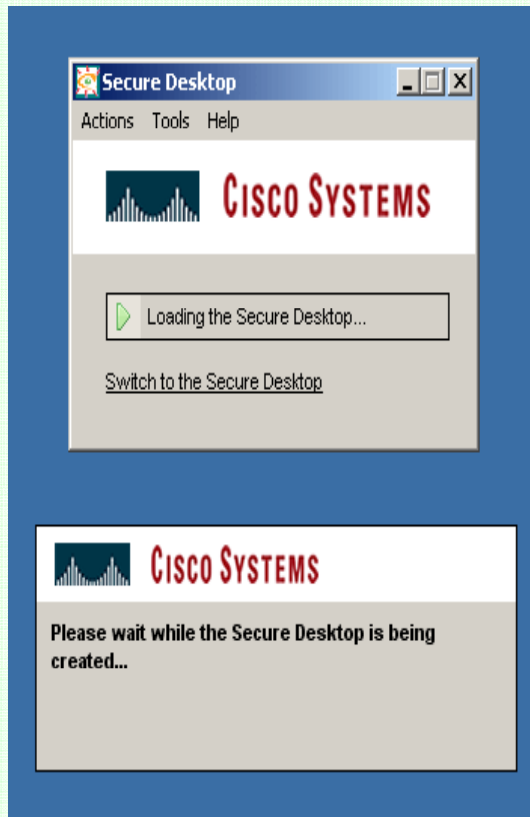
CSD 주요 특징

- 자동 설치 배포
관리자의 구성에 따라 자동 배포 가능
- 자원 활용의 극대화
CSD 설치 후에도 모든 PC 자원 활용 가능
- 강력한 제어
모든 Application 과 행위들은 CSD에 의해 제어 받음
- Data 사용 후 안심 종료
CSD 설치 이후 사용 되는 Data의 쓰기 삭제는 모두 암호화되어 PC 사용 환경 신뢰성 크게 증가

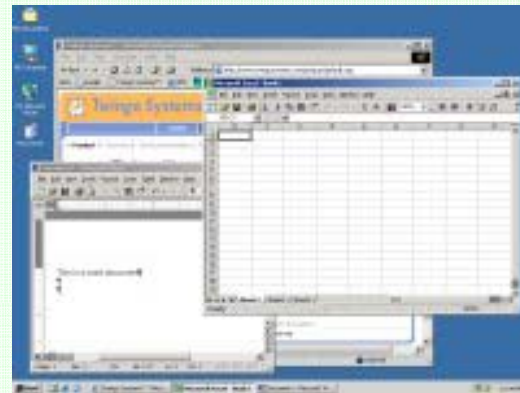
ASA 5500 통합 보안 장비 – SSL VPN

Cisco Secure Desktop 기능 제공

CSD 동작 화면

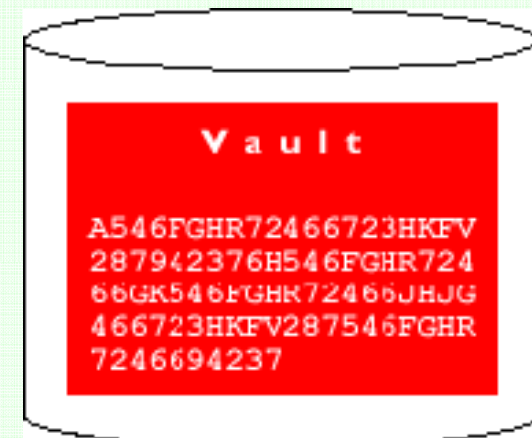


CSD 사용하지 않을 경우



Browser history:
www.competitor.com/jobs
www.etrade.com/myportfolio
Webmail message:
employee evaluation
trade secret
Word document:
attorney_letter.doc
Excel Spreadsheet
Salaries.xls
Sales forecast.xls

CSD 사용시 Data 암호화



기업 내부의 Server

PC 방 / 공항/ 역사 / 호텔 공용 PC

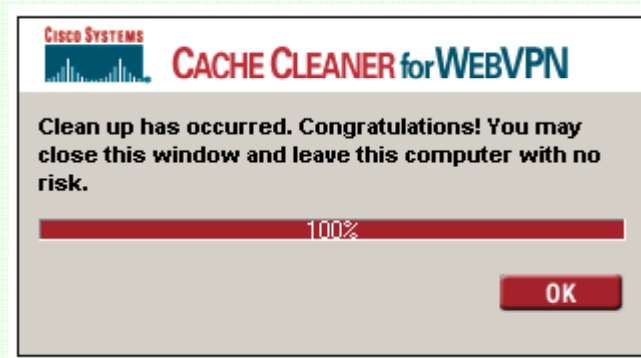
ASA 5500 통합 보안 장비 – SSL VPN

Cisco Secure Desktop 기능 제공

CSD 안심 종료 서비스

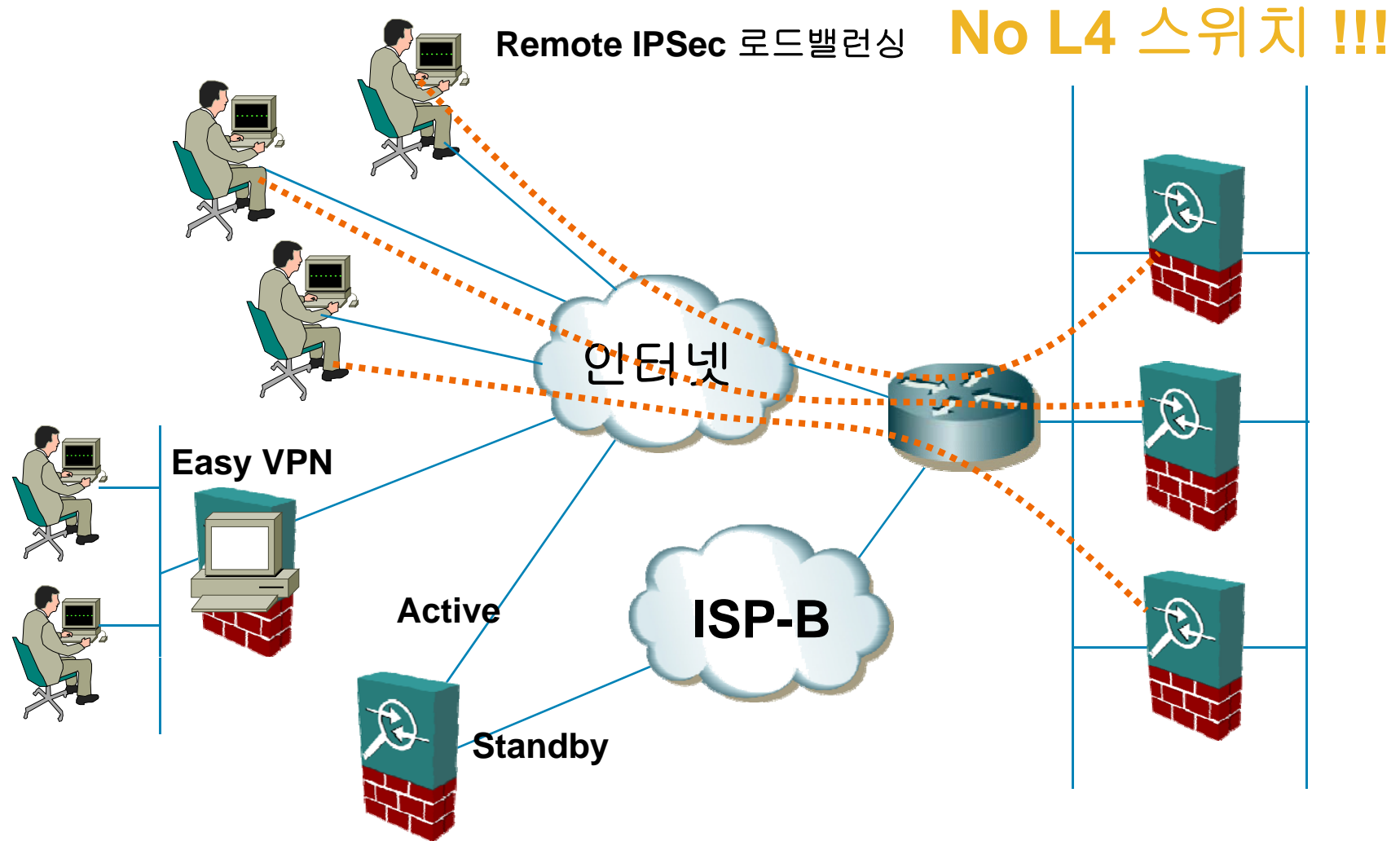
안심 종료 서비스 제공

- **Cookies** 삭제
- **History** 삭제
- **Cache** 삭제
- **Passwords** 삭제



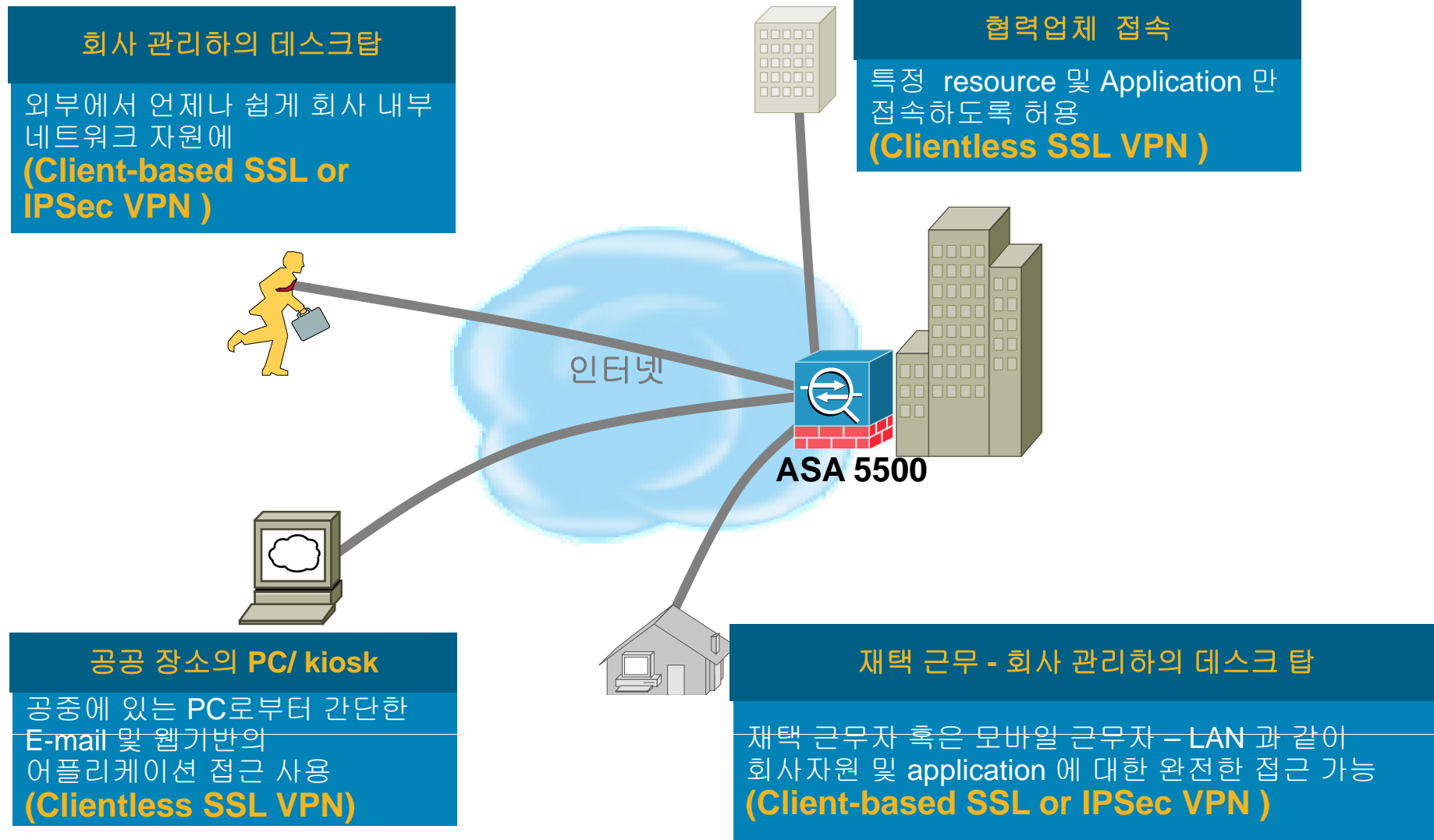
ASA 5500 통합 보안 장비 – IPSec VPN

다양한 IPSec VPN feature



ASA 5500 통합 보안 장비 – IPSec/SSL VPN

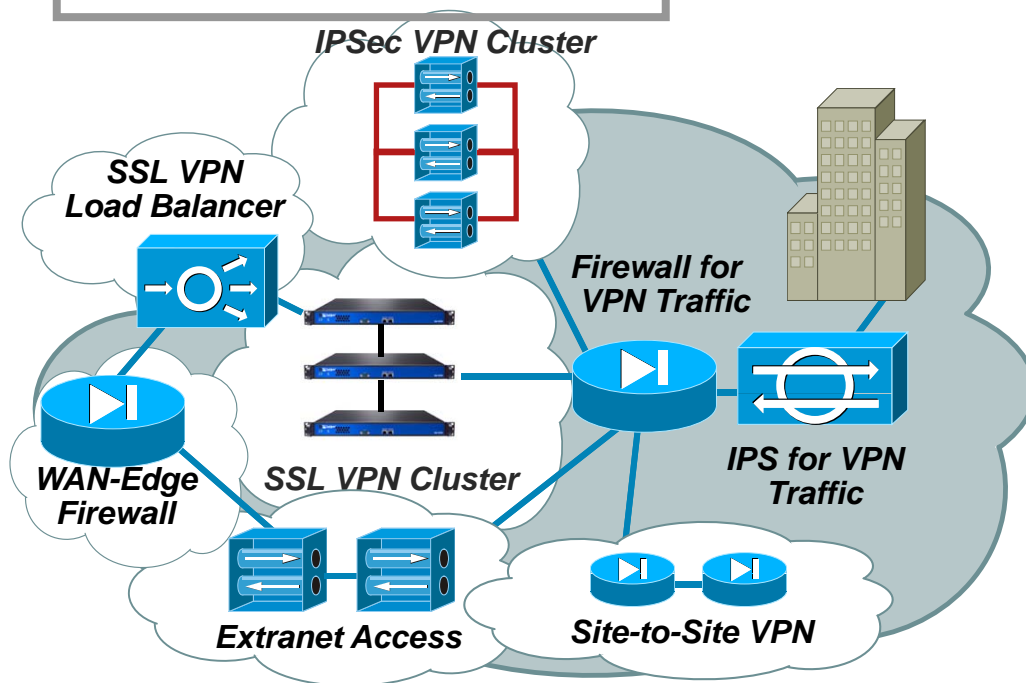
IPSec 및 SSL VPN 서비스 동시 지원



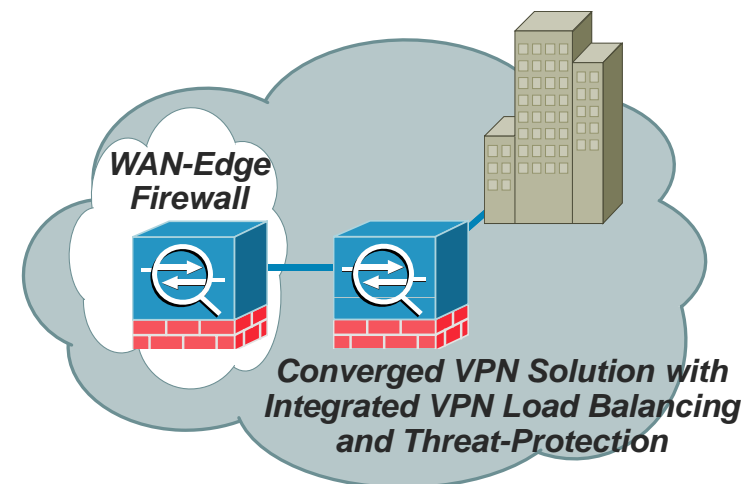
ASA 5500 통합 보안 장비 – IPSec/SSL VPN

비용효과적인 VPN 네트워크 구성

일반적인 **SSL VPN** 도입 환경



Cisco SSL VPN 도입 환경:
Less Equipment Required



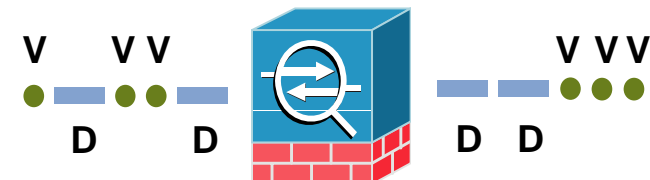
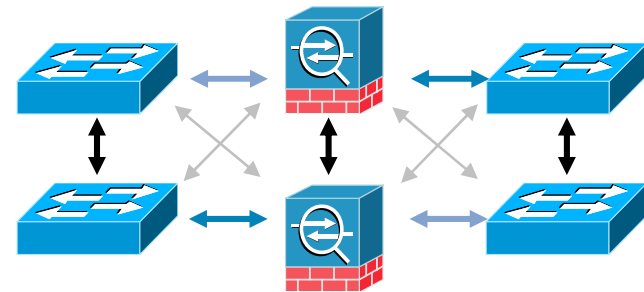
ASA VPN Solution Delivers:

- 통합 VPN 서비스 제공 – remote access(Ipsec,SSL), extranet and site-to-site VPN
- 모든 VPN 트래픽에 대한 방화벽/IPS 을 통한 통합 보안 위협 관리 제공
- 자체 로드밸런싱 기능으로 VPN 네트워크에 대한 저비용의 확장성 및고가용성 제공
- 쉬운 운영을 통한 단독/통합 관리 솔루션 제공

ASA 5500 통합 보안 장비 - 지능형 네트워크 서비스

Routing 및 QoS

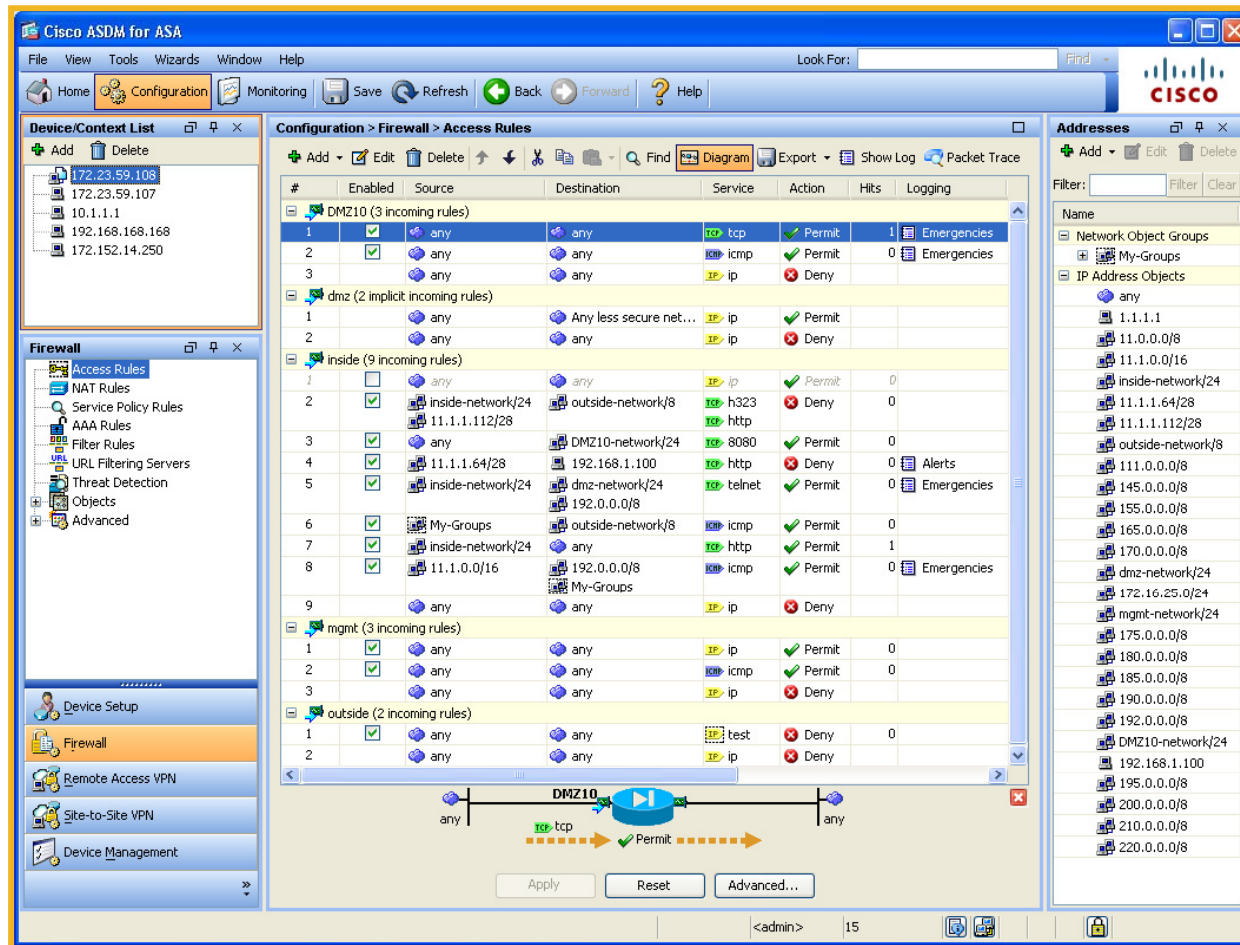
- **EIGRP** , OSPF 및 RIPv2 라우팅 지원
- 지연에 민감한 트래픽의 처리를 위한 **QoS** 트래픽 우선순위 제공 (라우터의 LLQ)
- IPv4/IPv6 하이브리드 네트워크 환경을 위한 IPv6 지원
- PIM sparse mode **멀티캐스트** 지원
- TCP,UDP 및 ICMP 등의 다양한 프로토콜을 간단한 **Object** 그룹으로 관리



Quality of Service

ASA 5500 통합 보안 장비 - 관리

ASDM - Built-In 된 Web UI를 이용한 직접 설정 및 모니터링



- 새로운 인터페이스

➔MS-Outlook 과 유사한 제공으로 쉽게 접근 및 사용 가능

- drag-and-drop and in-place editing

➔ 정책 편집 단순화

- 사용자 정의 인터페이스 제공

➔ 운영에 적합한 인터페이스로의 최적화

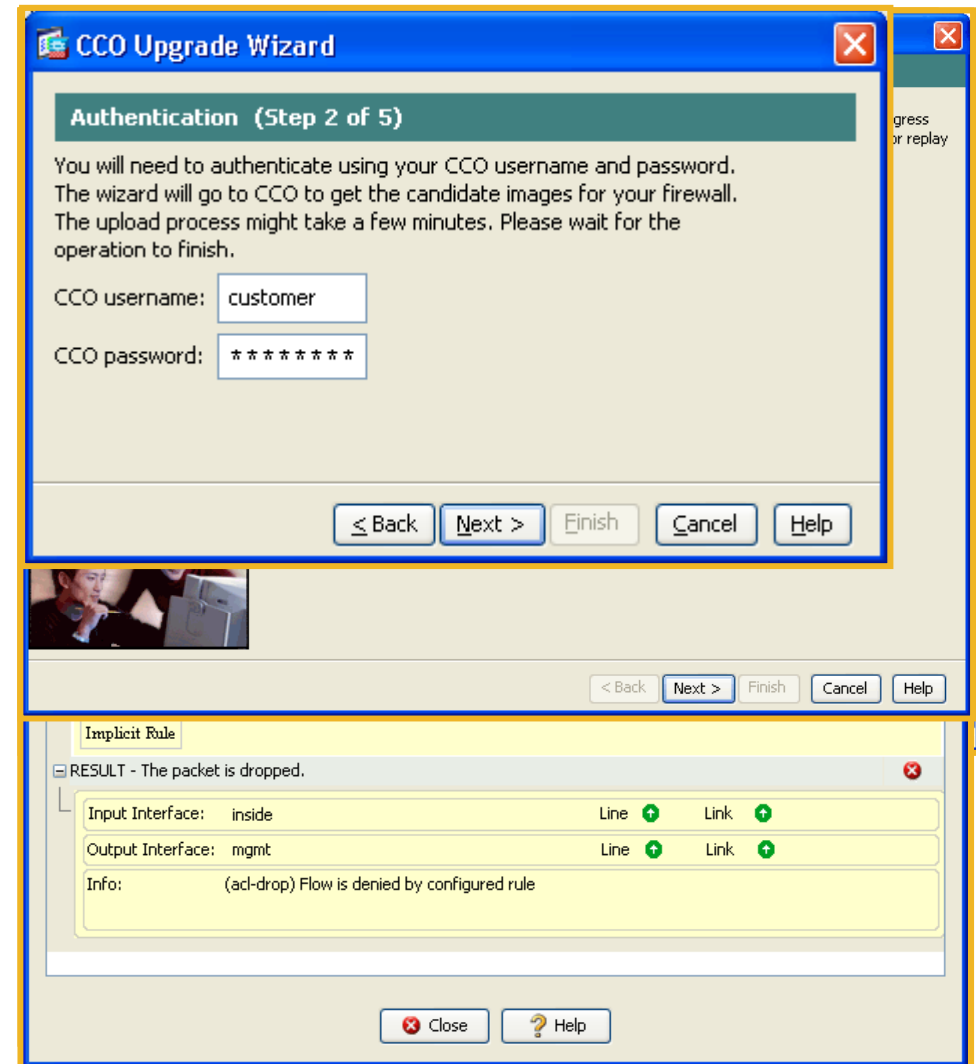
- Firewall Dashboard 제공

- Firewall 룰 테이블의 실시간 ACL hitcount 제공

ASA 5500 통합 보안 장비 - 관리

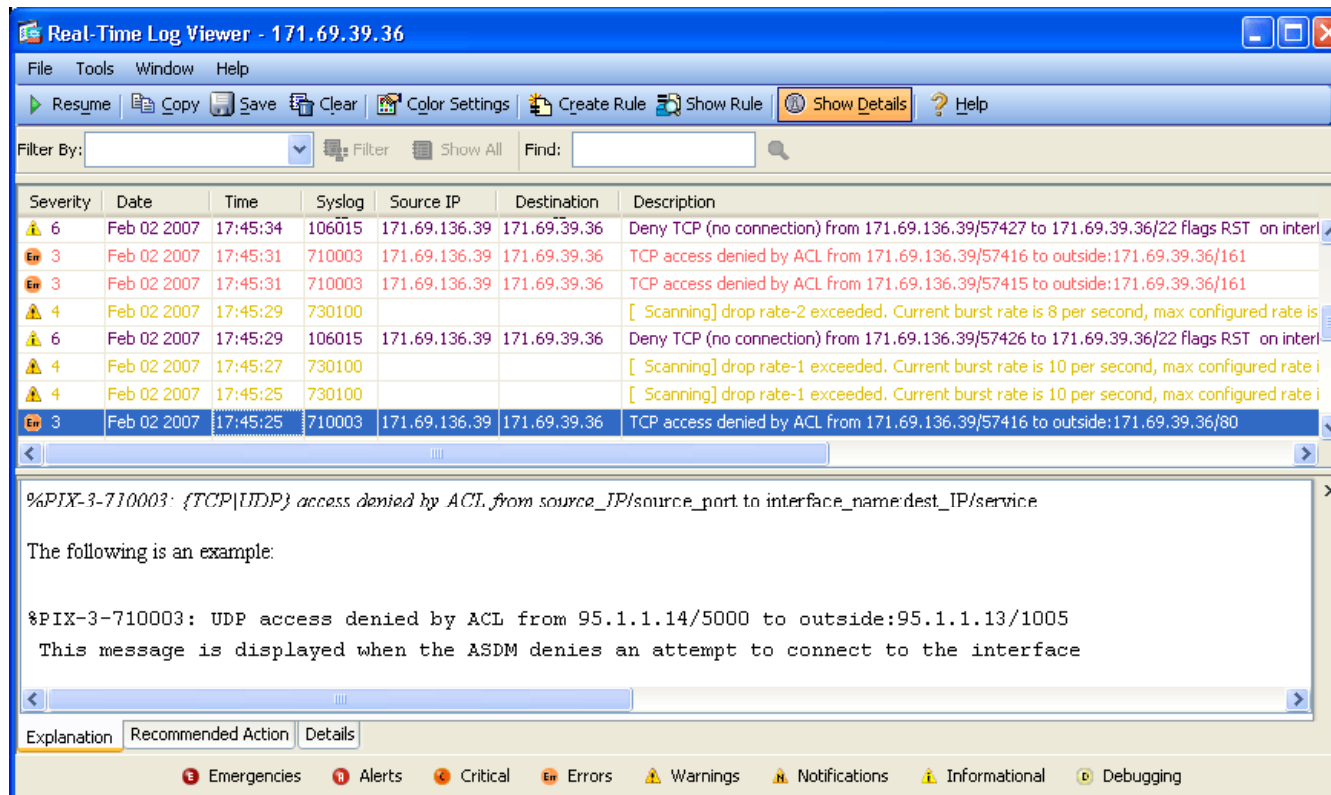
ASDM - 기능 하이라이트

- Redesigned interface
- Security Dashboards
- Packet Tracer
- Packet Capture Wizard
- Software Upgrade Wizard



ASA 5500 통합 보안 장비 - 관리

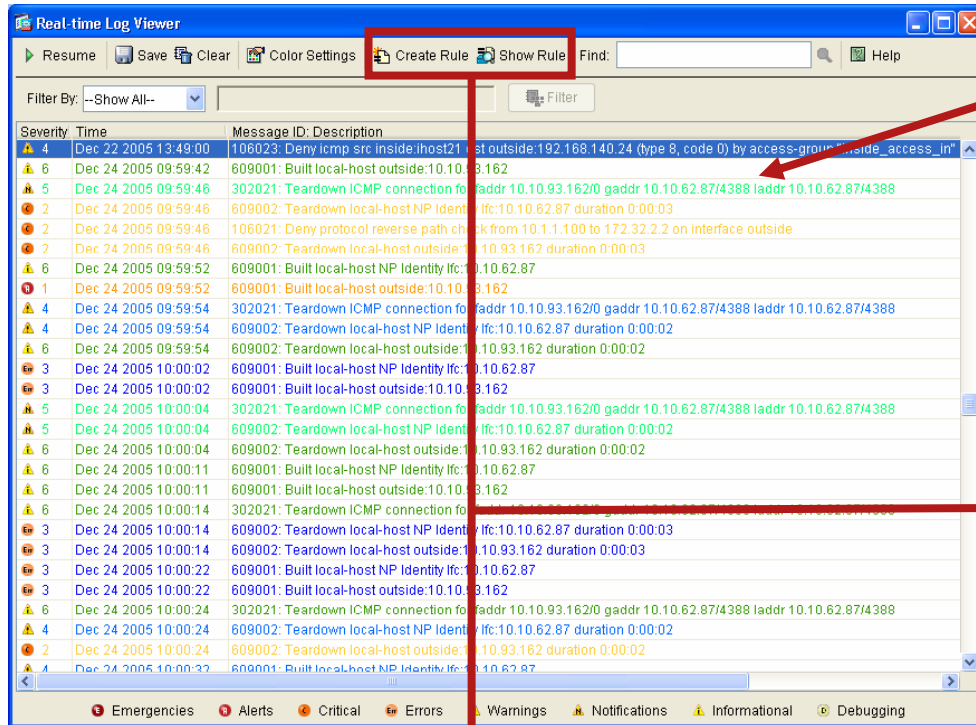
ASDM - Real-Time Syslog Viewer



- 구조화된 실시간 모니터링 뷰어 기능 제공
- coloring of events
→ 중요이벤트 모니터링 가시화
- real-time interpretation of log messages, with
→ 각 로그 메시지에 대한 설명 제공, 직관성 증대

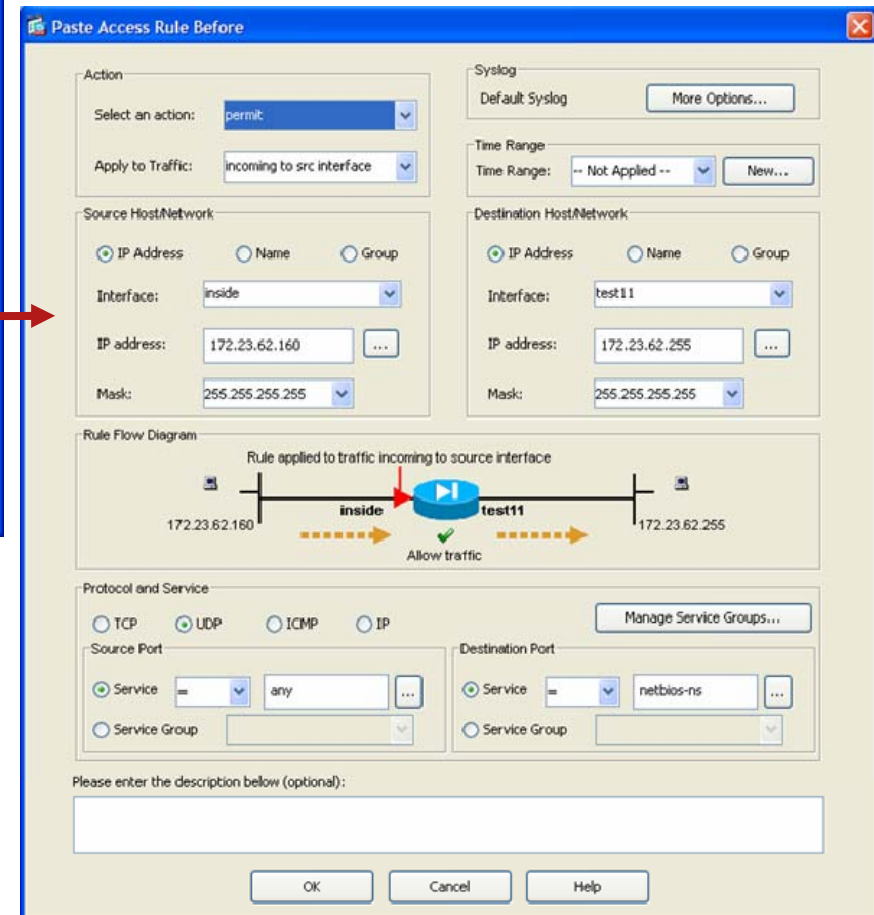
ASA 5500 통합 보안 장비 - 관리

ASDM-손쉬운 Firewall 보안 정책 편집



각 **ACL**의 라인마다 **Unique No** 부여
→ 발생한 이벤트 확인 가시화

실시간으로 발생하는 이벤트와 관련된
보안정책을 직접 편집 또는 추가 가능



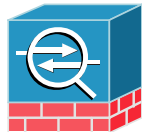
ASA 5500 통합 보안 장비






- 제품 소개



ASA 5500 통합 보안 장비 - 제품 소개

ASA 5500 Series Product Lineup



	Cisco ASA 5505	Cisco ASA 5510	Cisco ASA 5520	Cisco ASA 5540	Cisco ASA 5550
					
대상 시장	재택 근무, 지방 사무소, 소기업	중소 규모	일반 기업	중.대형 기업	대기업
성능 최대 방화벽 성능 최대 방화벽 + IPS 성능 최대 IPSec VPN 성능 최대 IPSec/SSL VPN Peers	150 Mbps Future 100 Mbps 25/25	300 Mbps 300 Mbps 170 Mbps 250/250	450 Mbps 375 Mbps 225 Mbps 750/750	650 Mbps 450 Mbps 325 Mbps 5000/2500	1.2 Gbps N/A 425 Mbps 5000/5000
Platform Capabilities 최대 동시 연결 세션수 최대 초당 연결 세션수 Packets/Second (64 byte) 기본 인터페이스 VLANs 지원 고가용성 지원	10,000/25,000 3,000 85,000 8-port FE switch 3/20 (trunk) Stateless A/S (Sec Plus)	50,000/130,000 6,000 190,000 5 FE 50/100 A/A and A/S (Sec Plus)	280,000 9,000 320,000 4 GE + 1 FE 150 A/A and A/S	400,000 20,000 500,000 4 GE + 1 FE 200 A/A and A/S	650,000 28,000 600,000 8 GE + 1 FE 250 A/A and A/S

ASA 5500 통합 보안 장비 - 제품 소개

H/W 구성

4개의 10/100/1000
RJ45 기가비트 포트

1개의 10/100 관리 포트*
(일반 포트도 설정 가능)

부가 서비스를 위한 확장 슬롯
(ex: IPS)

얇고 고성능의
1 Rack Unit (RU) 디자인

저장 디스크 없는 구조로
고 가용성 제공

현장에서 교체할 수 있는 단일
AC 또는 DC 전원 공급 장치



2개의 USB 2.0 포트
(향후 사용: Credentials,
Failover, 등등)

소프트웨어, 설정, 로그 등의
저장을 위한 컴팩트플래시 메모리

콘솔과 AUX 포트

5개의 상태 LEDs (전원,
상태, Active, VPN, Flash)

ASA 5500 통합 보안 장비 - 제품 소개

확장 슬롯 모듈

IPS Security Services Module (AIP SSM)



- IPS 및 IDS 서비스 제공
- 두가지 모델 제공 : SSM-10 and SSM-20
- IPS 기준 450 Mbps 성능
- 손쉬운 탈/장착
- 10/100/1000 out-of-band management port
- ASA 5510, 5520 및 5540 에서 지원

Content Security Services Module (CSC SSM)



- Anti-X 서비스 지원
(anti-virus, anti-spyware, anti-spam, anti-phishing, URL filtering, and more)
- 두가지 모델 제공 : SSM-10 and SSM-20
- Anti-virus 및 anti-spyware 서비스는 사용자 수 및 추가 옵션에 따른 라이선스
- ASA 5510, 5520 및 5540 에서 지원

4-Port GE Services Module (4GE SSM)

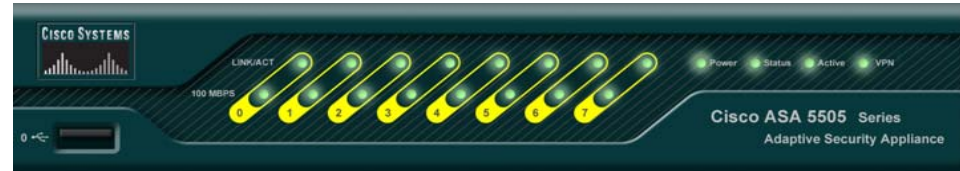


- 유연한 네트워크 구성을 위한 4개의 SFP 포트 및 4개의 10/100/1000 포트 제공
- 8개 포트중 4개포트까지 혼합하여 선택 사용 가능
- ASA 5510, 5520 및 5540 에서 지원

ASA 5500 통합 보안 장비 - 제품 소개

Cisco ASA 5505 Adaptive Security Appliance - 차세대 SOHO 용

소규모 기업 또는 지사 사무실 및
재택 근무자를 위한 차세대 통합 보안
솔루션



고성능의 시장에서 검증된 보안 서비스

- 응용프로그램 Inspection 및 Control 서비스
- Site-to-Site VPN/Cisco Easy VPN Server/Remote IPSec VPN 지원
- SSL VPN 지원
- object tracking 및 failback 기능을 이용하여 Dual ISP 지원
- Hardware failover, PPPoE, dynamic DNS 등!

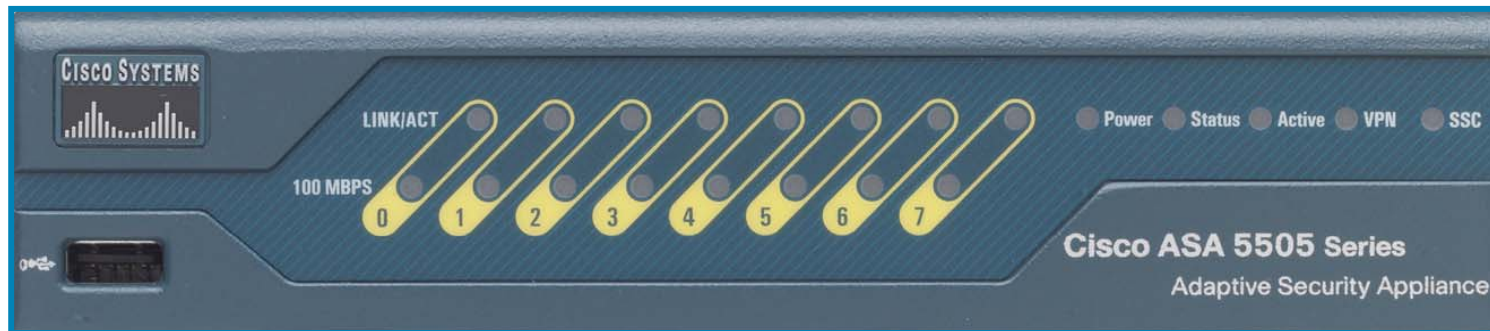
Platform 하이라이트

- Compact desktop form-factor
- Integrated VPN acceleration
- 8 x 10/100 ports with flexible port grouping
- VLANs: Home/Business/Outside
- Support for true DMZ & trunking
- Power over Ethernet (802.3af) ports for IP phones, external Wireless APs, etc.
- USB 2.0 ports for future use
- Wall and rack mountable
- Convection cooling (no fan)

ASA 5500 통합 보안 장비 - 제품 소개

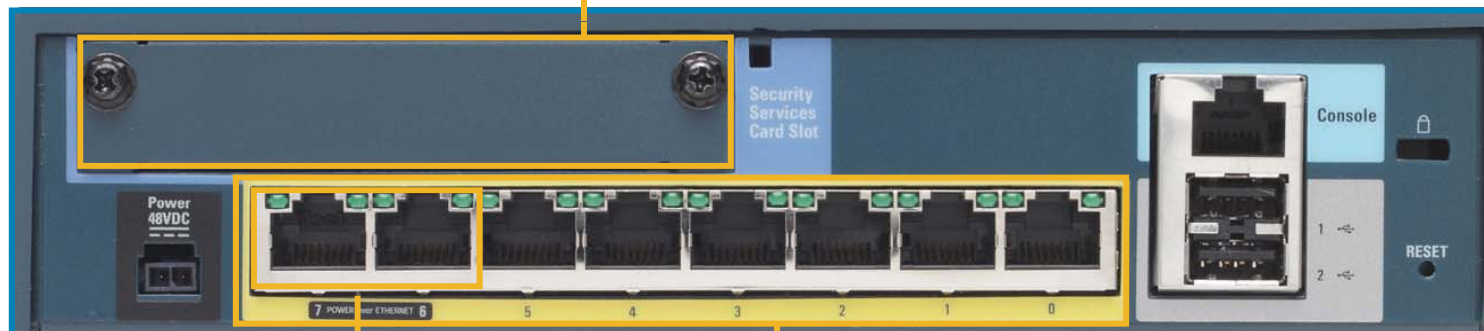
Cisco ASA 5505 Adaptive Security Appliance

전면부



향후 사용을 위한 확장 슬롯

후면부

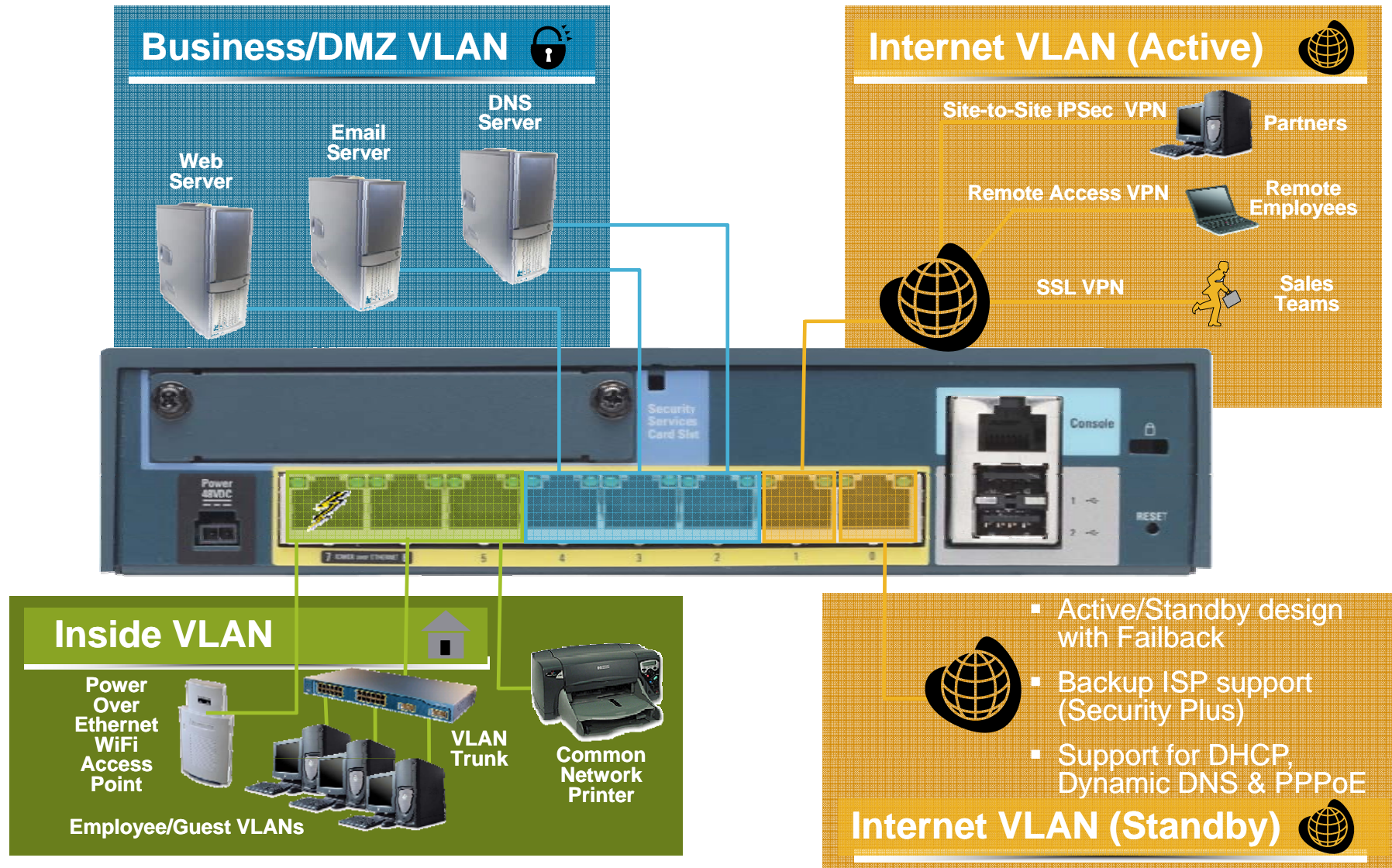


P Phones, Wi-Fi Access, Points, Video Surveillance 등을 위한 두 개의 Power over Ethernet (PoE) 포트 지원

8-Port 10/100 Fully Configurable Switch with VLAN Support

ASA 5500 통합 보안 장비 - 제품 소개

Cisco ASA 5505 Adaptive Security Appliance - 구성 디자인



결론



통합 보안 장비 ASA 5500 요약

업계 최고의 가장 이상적인 통합 보안 장비

- ▶ 하나의 장비에서 방화벽, IPSec VPN, SSL VPN, IPS/IDS, Anti-x 방어 기능 제공

높은 신뢰성의 통합 보안 장비

- ▶ 보안 시장 점유율 1위의 검증된 보안 기술을 바탕으로 한 통합 보안 기술 구현

강력한 네트워킹 서비스의 통합 보안 장비

- ▶ 라우팅 프로토콜, 멀티캐스트, QoS, 로드밸런싱 등 업계 1위의 라우터/스위치의 지능형 네트워크 서비스 기능 구현으로 유연한 디자인 구성 가능



