고성능 10기가 방화벽 및 통합 위협관리 시스템

김용호 (yonghkim@cisco.com)

Cisco Systems Korea

목 차

- 고성능 10G 방화벽
- 통합위협관리(UTM) 솔루션
- 결론

고성능 10G 방화벽

인터넷을 통한 The Human Network의 도래

Changing the Way We Live, Work, Play, and Learn

인터넷을 기반으로 한 비즈니스 모델의 발전

협업을 위한 다양한 인터넷기반 S/W의 발전

데이터와 음성의 통합

온라인 트랜잭션

Rich Media

Social Networking

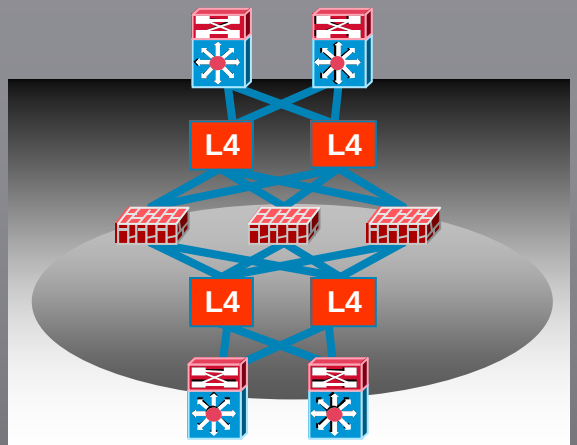
개인 블로그 및 WiKi

주문형 비디오의 활성화

무선기반의 모빌리티 환경

웹 2.0

고성능 방화벽에 대한 새로운 요구사항



syslog 302013 TCP connection creation
syslog 302015 UDP connection creation
syslog 302017 GRE connection creation
syslog 302020 ICMP connection creation
syslog 302015 UDP connection creation

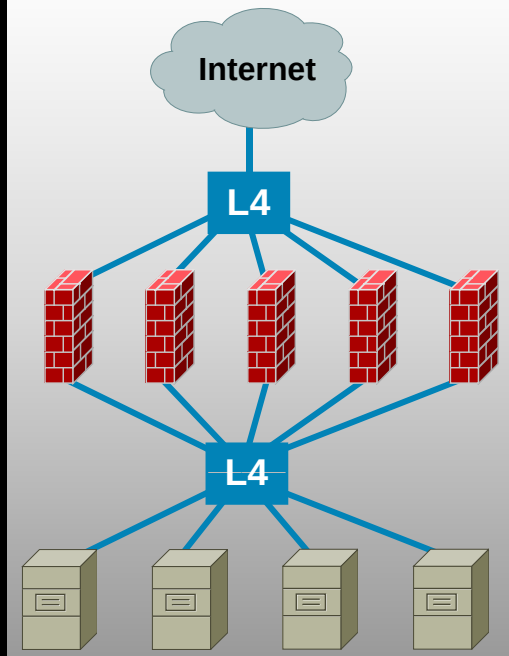
고성능, 고속

유연한 구성

효율적인관리

High-End 방화벽 시장의 현실

과거구성형태



- 대당 1~2Gbps
- Multi-Giga 방화벽 구성을 위한 LB
- LB Switch 성능의 한계 때문에 더 이상의 확장 불가

공급업체별 10G Firewall 출시

네트워크 보안 솔루션 업계 '10G' 속도경쟁 가속
상반기중 10기가 방화벽, IPS, 통합보안 신제품 잇단 출시

"올해부터는 10기가비트다."

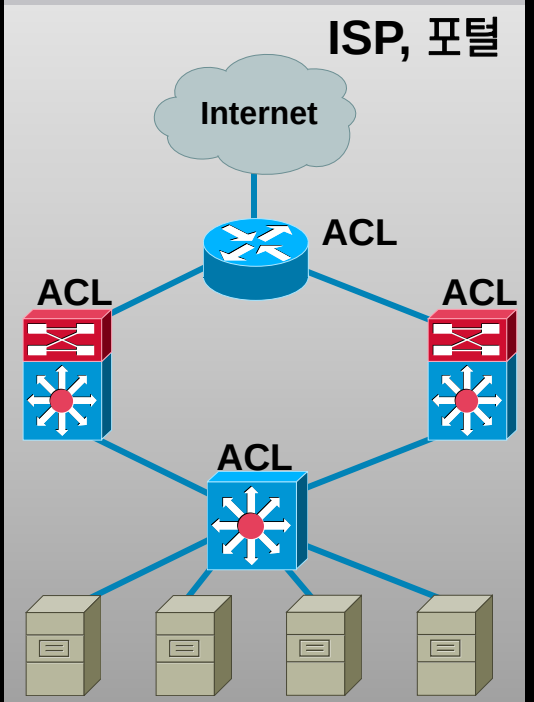
보안'>네트워크 보안 솔루션 업체들이 10기가급 초고속 대용량 트래픽 처리성능을 지원하는 방화벽, 침입방지시스템(IPS) 등 네트워크 보안 신제품 개발에 경쟁적으로 나서 올해 고성능 장비 시장 선점을 노린 접전이 예상된다.

특히, 올해 출시될 10기가급 고성능 보안 장비에는 방화벽, IPS와 같은 단일 보안 솔루션뿐만 아니라 다양한 보안기능을 한 장비에서 제공하는 통합보안(UTM) 제품도 포함돼 있어 주목된다.

기가비트급 시장 경쟁 가속화 예상
국내 방화벽/VPN 시장은 올해 멀티기가비트(4G 이상) 방화벽/VPN 경쟁이 가속화되고 다양한 부가 기능을 지원하는 장비 출시가 잇따를 것으로 예상된다. 또 방화벽/VPN의 교체가 UTM으로 이뤄지는 사이트가 급증할 것으로 보인다.
이에 방화벽/VPN 업체들은 기존 방화벽, VPN 시장을 지키고 성장성이 큰 UTM 시장에 진출하기 위해 올해 내 10G급 UTM 장비를 출시한다는 계획이다.

BW만 고려한 수평이동

But Now Still…



- 패킷 필터링 기반의 Access-list 의존
- 특정 서비스 Deny, All Permit
- 라우터, 스위치의 성능 이슈

Cisco ASA 5580 Series Overview

Highest Performance and Speed

- 업계 최고의 초당 Connection 성능 및 Throughput
- Data center 에 적합한 Ultra Low Latency

Highly Flexible Deployment

- 고급 네트워킹 기술의 적용

Highly Effective NetFlow Event

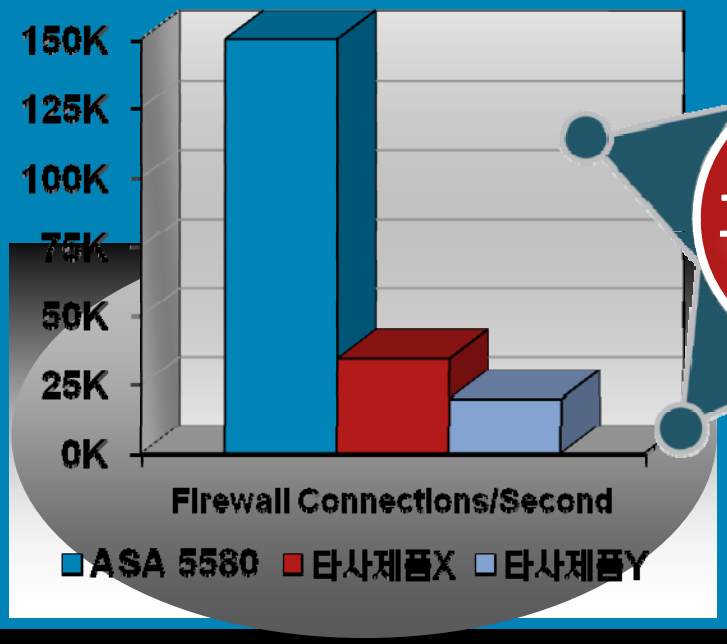
- NetFlow 기반의 Security Event Monitoring

현시대가 요구하는 고성능 Cisco 10G 방화벽 !!!

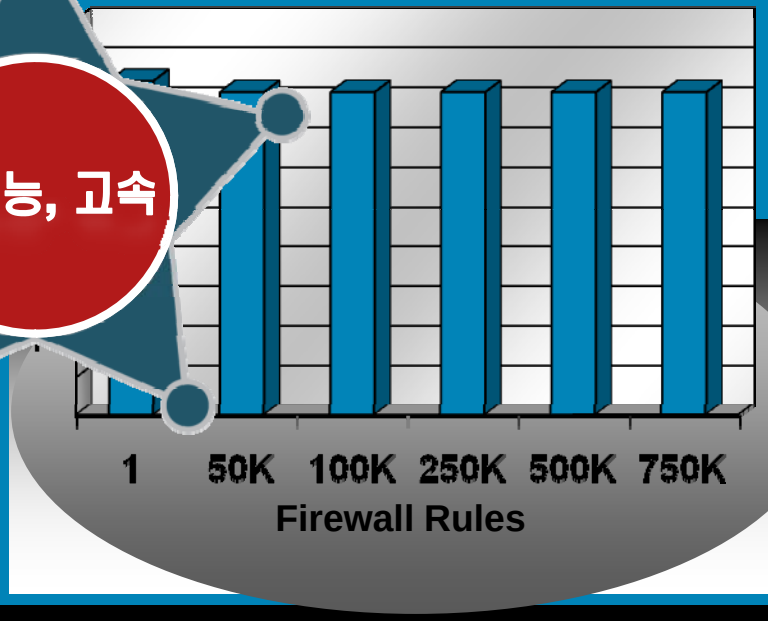
Highest Performance and Speed

현실화 된 동종업계 최고 성능 및 처리 속도

타사대비 **5~7배** 이상의 높은
Connection Rate 제공



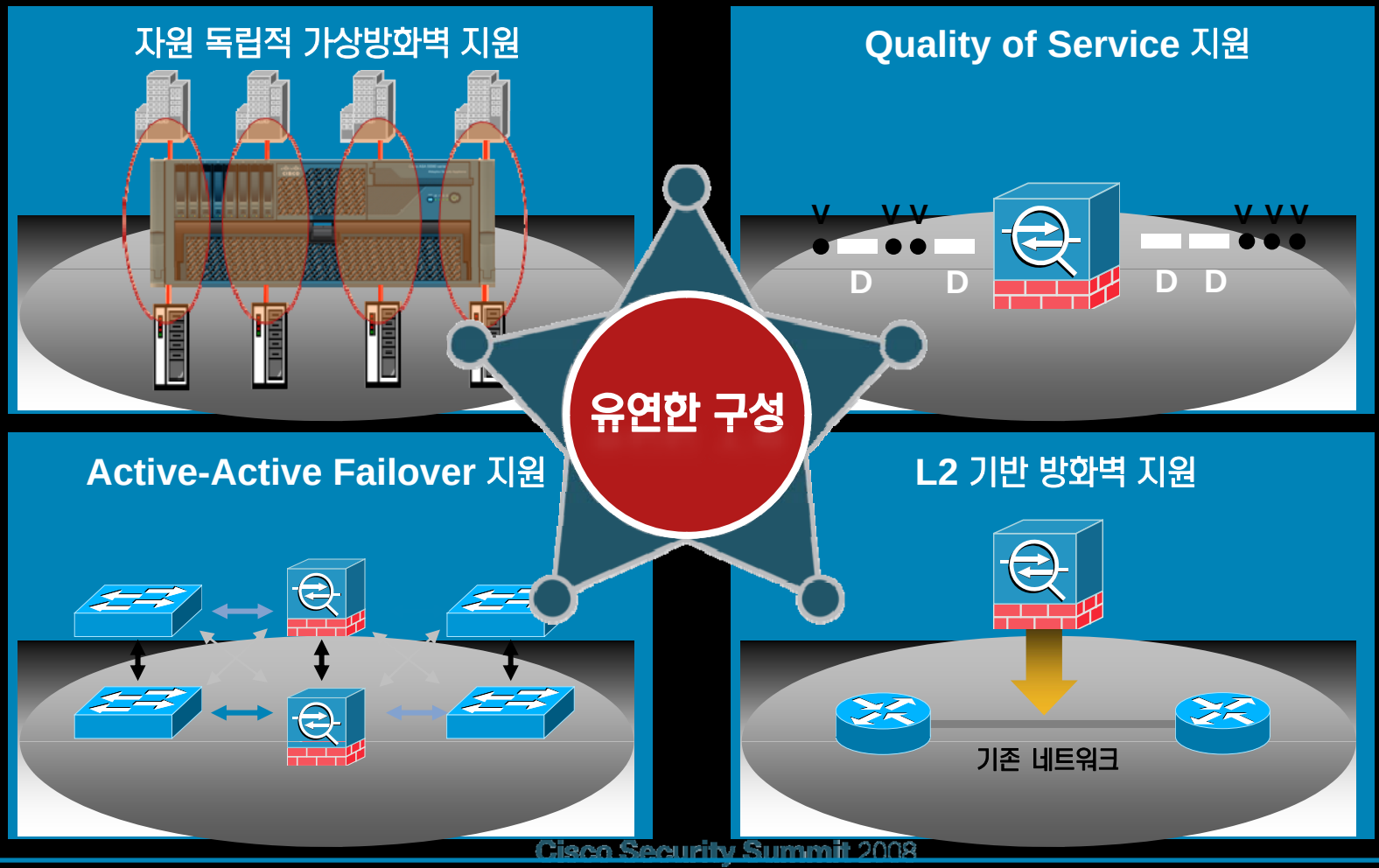
최대 75만개의 방화벽 정책 지원
➔ 성능에 전혀 영향이 없이 적용 가능



고성능, 고속

Highly Flexible Deployment

검증된 OS 기반의 고급 네트워킹 기능



Highly Effective NetFlow Event

Typical firewall syslog

syslog 302013 TCP connection creation

syslog 302015 UDP connection creation

syslog 302017 GRE connection creation

syslog 302020 ICMP connection creation

=

Cisco ASA5580 Netflow

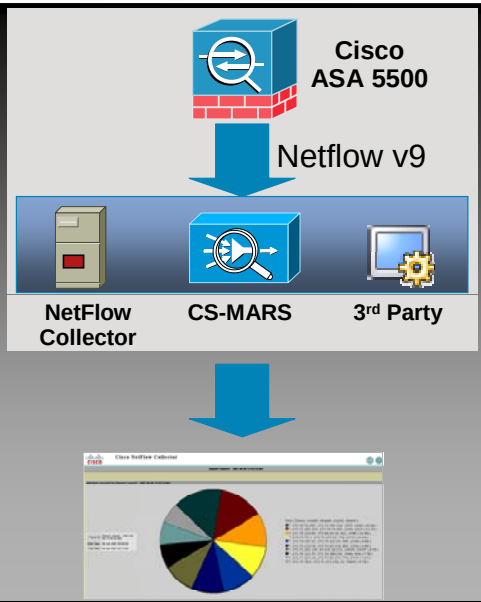
Flow creation event

Event Logging 의

Event 저장 스토리지

향상된 Event 분석 및 침해 판단

효율적인관리



대용량 Remote Access VPN 기능

Any Application

Any Endpoint

Any Policy

IPSec 및 SSL VPN 동시 지원

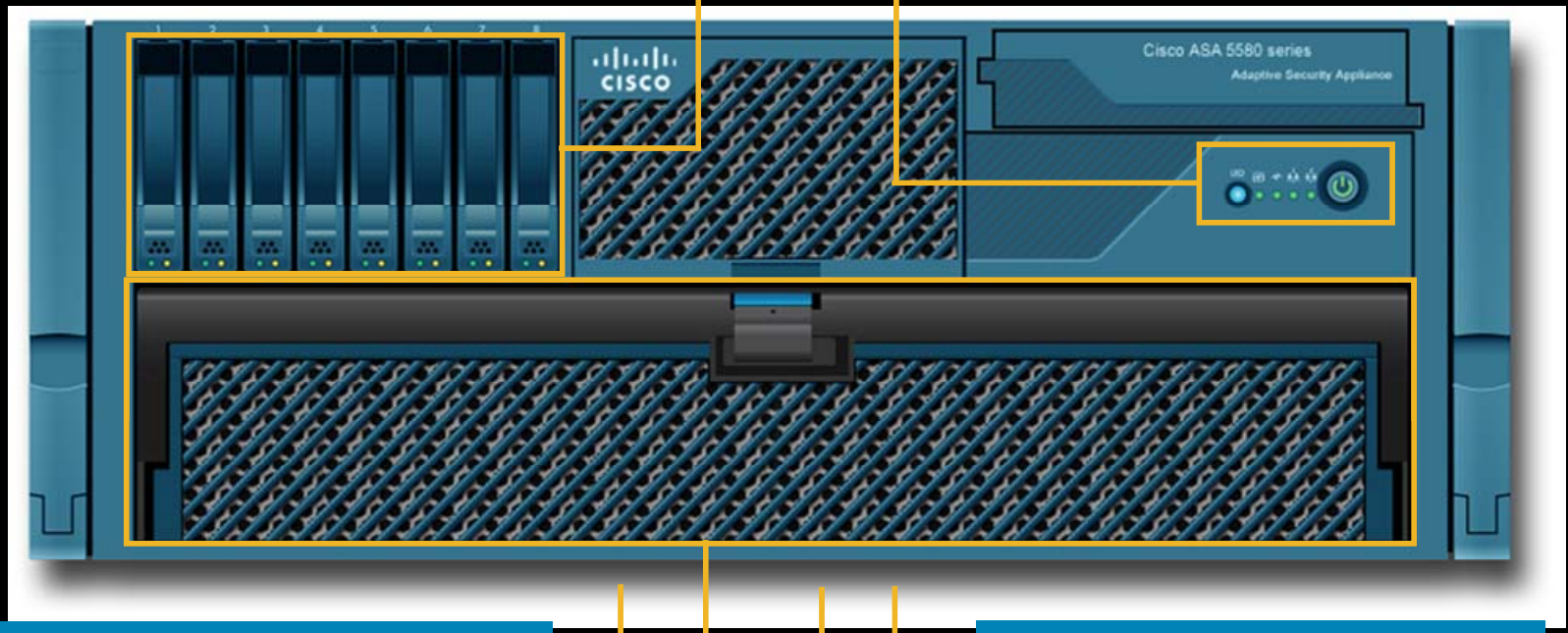
What's New?

- 시스템당 최대 **10,000** 동시 사용자 지원
- 클러스터링을 통한 최대 **100,000** 동시 사용자 확장 지원

Cisco ASA 5580 H/W 사양

총 8개의 Hard drive Bay

Power Button과 상태 LED



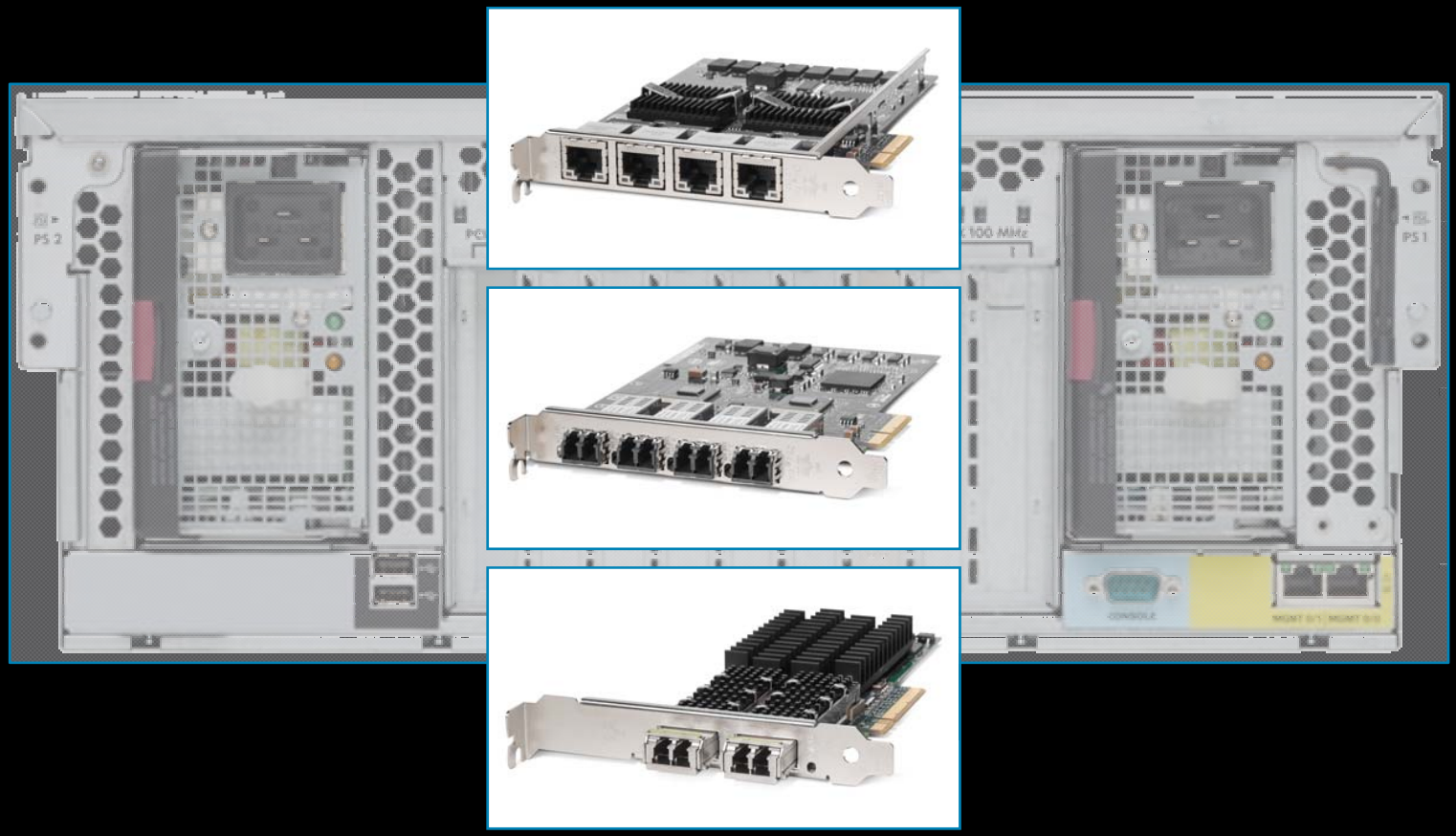
내부 Compact Flash
- 소프트웨어와 config 저장

Processing Engine
- 20~40개의 Upgrade Kit 계획

4RU Rack Mount Form Factor
26.5” Chassis Depth

Mounted on Rails for Easy
Access to Front and Back

인터페이스 확장성

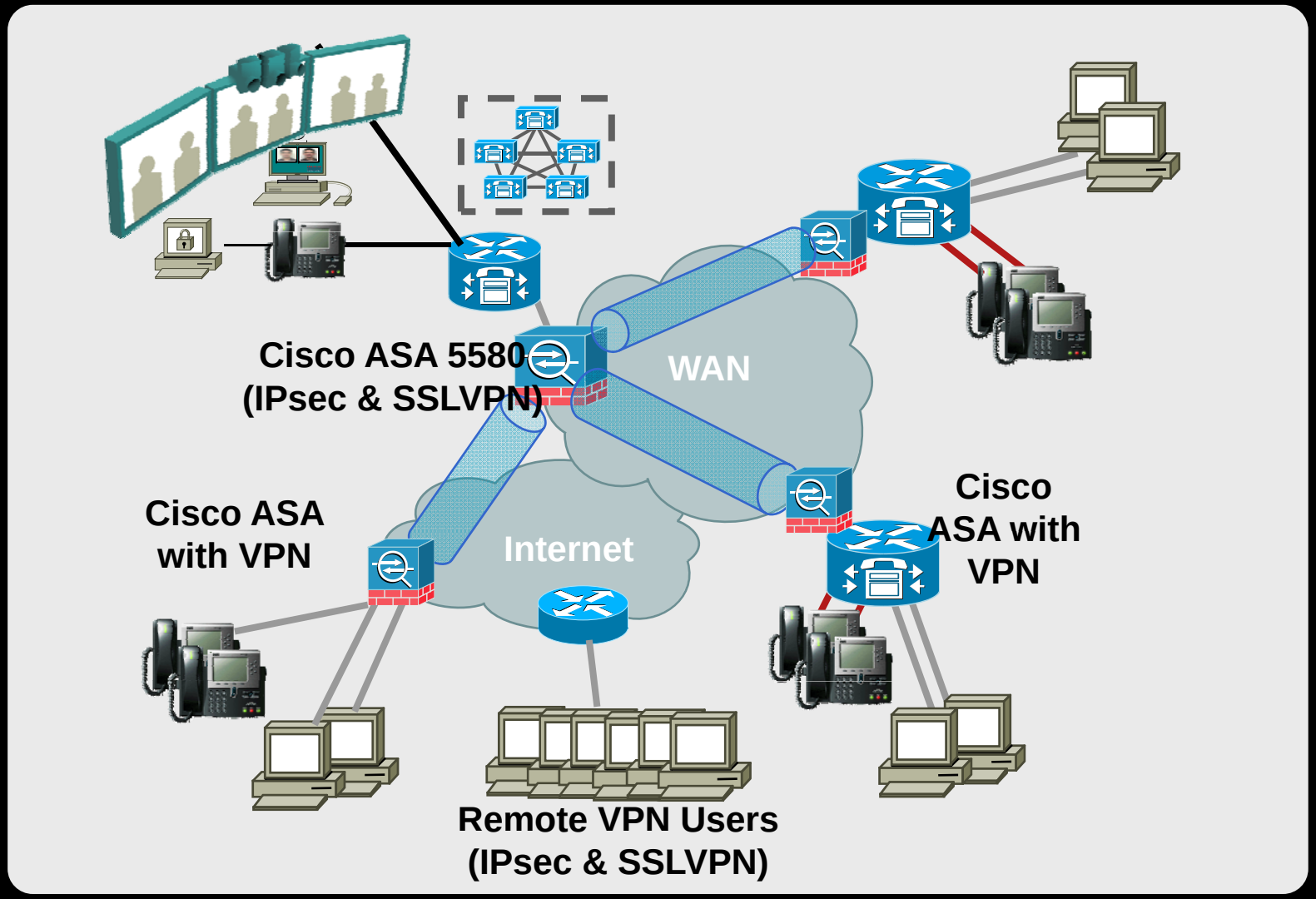


24개 Giga Port 또는 12개 10GE의 물리적인 확장성

기업 IDC 를 위한 Cisco 10G Firewall 구성

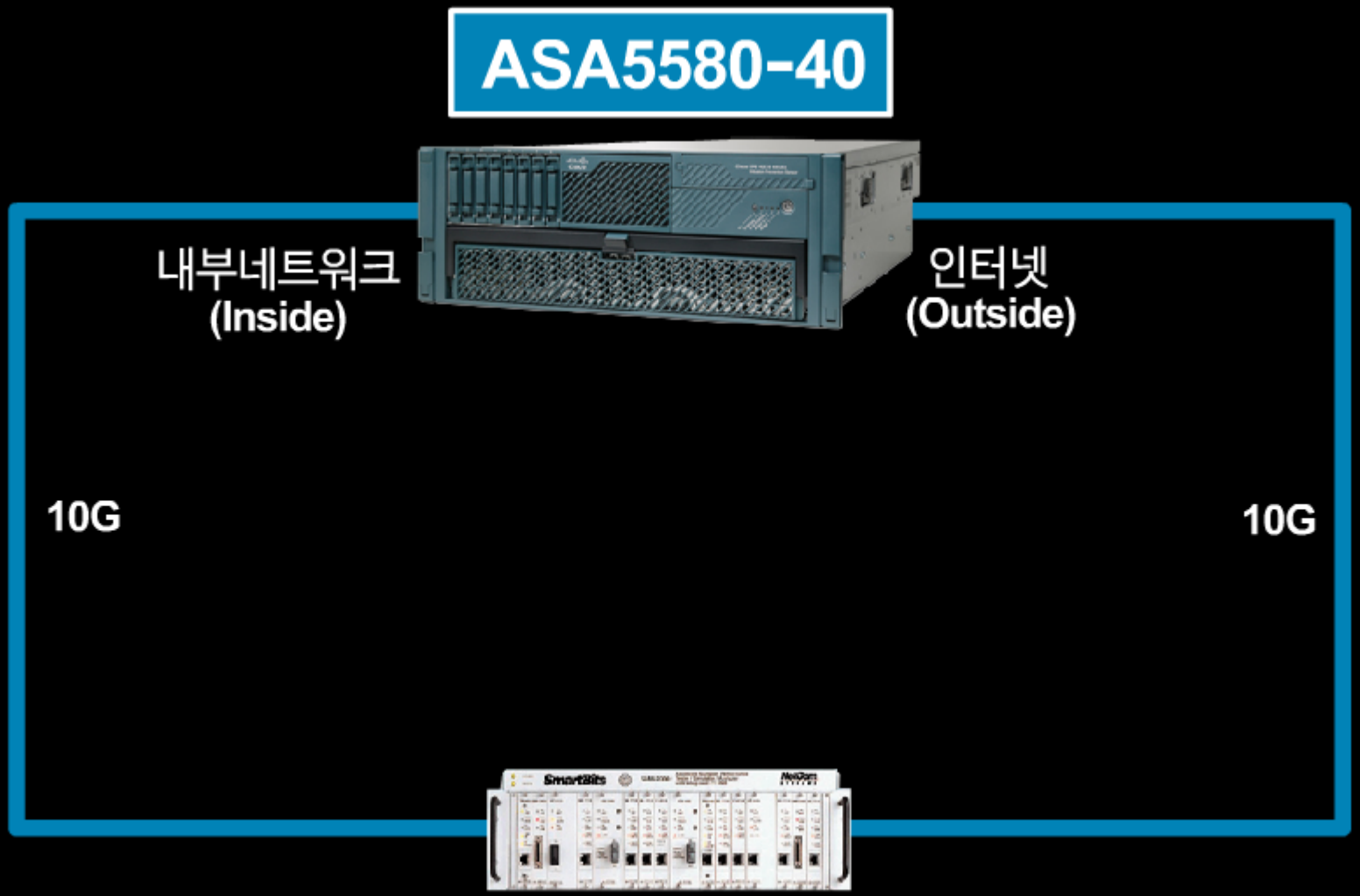
Layer	Typical Solution	Cisco Solution	Description
Front End Network •Security Net •Data Center Switch			•DC의 최종단 관문 방화벽 → Real 10G Firewall ASA5580-40 •하단 Layer 와 차별화된 1차 보안 관문화 •모든 서비스에 대한 통제
N-Tier App •SLB network •Web,App,DB, MainFrame			•Application 별 가상화 네트워크 구축 •C6K 기반의 FWSM, ACE를 통한 최후 방어선 •서비스 영역별 상세 보안 적용 •고효율의 완벽한 가상화
Storage network			

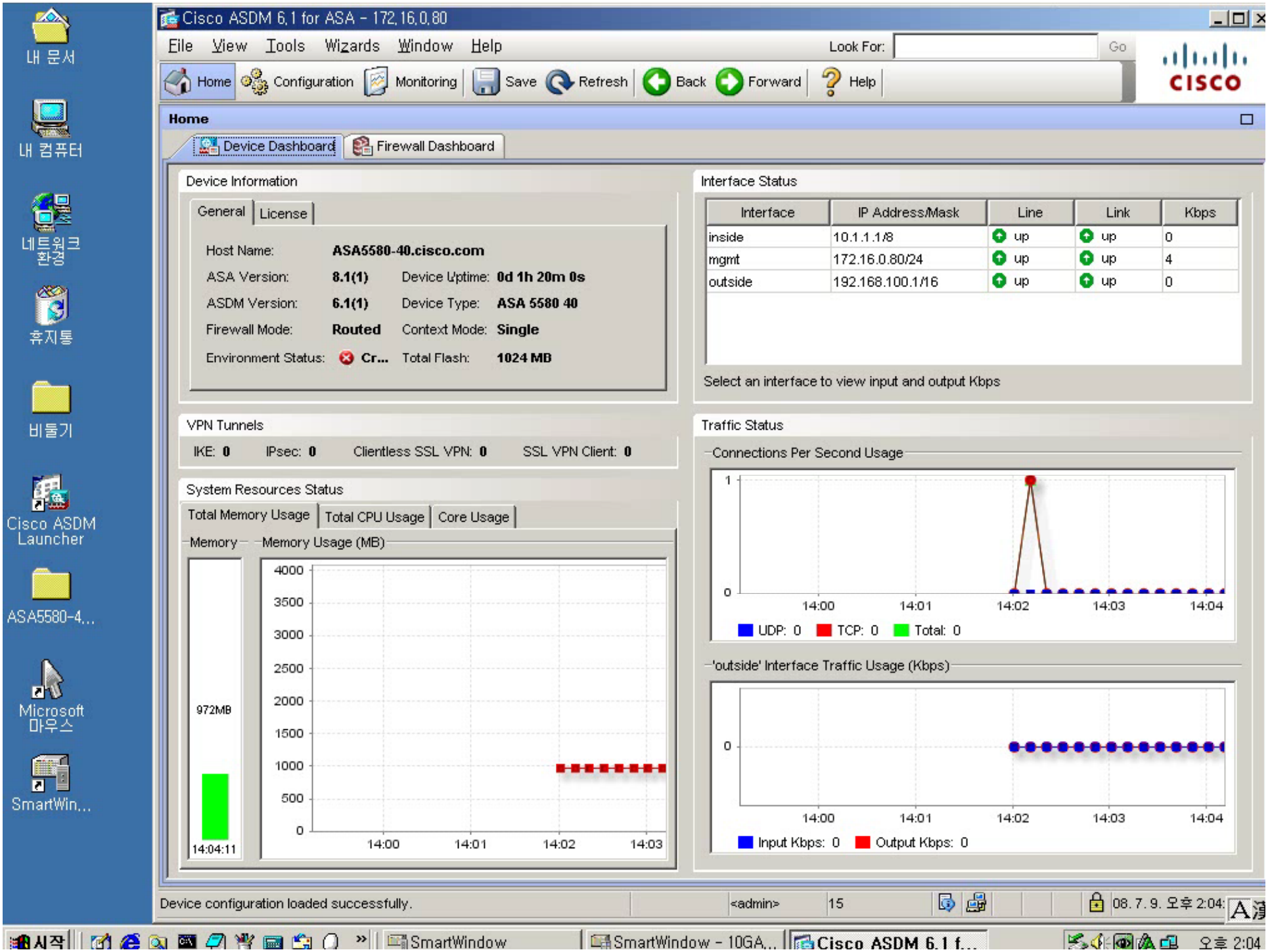
대용량 VPN Gateway Service



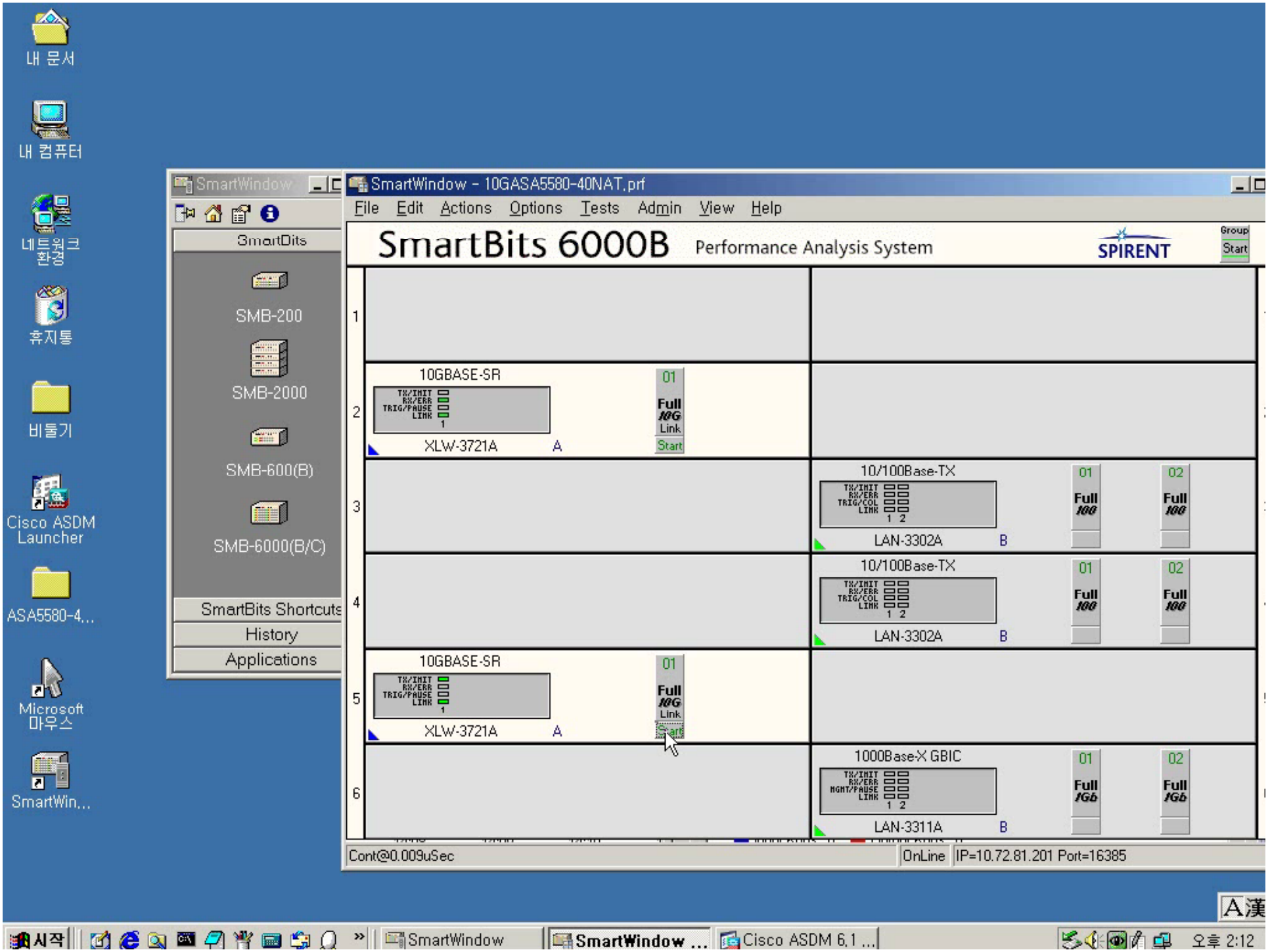
DEMO
10G Firewall 성능 시연

10Gbps 성능 시연




내 문서
내 컴퓨터
네트워크 환경
휴지통
비둘기
Cisco ASDM Launcher
ASA5580-4...
Microsoft 마우스
SmartWin...
Cisco ASDM 6.1 for ASA - 172.16.0.80
File View Tools Wizards Window Help
Look For:
Go
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Home
Device Dashboard
Firewall Dashboard
Device Information
General License
Host Name: ASA5580-40.cisco.com
ASA Version: 8.1(1) Device Uptime: 0d 1h 20m 0s
ASDM Version: 6.1(1) Device Type: ASA 5580 40
Firewall Mode: Routed Context Mode: Single
Environment Status: Cr... Total Flash: 1024 MB
Interface Status
Interface | IP Address/Mask | Line | Link | Kbps
inside | 10.1.1.1/8 | up | up | 0
mgmt | 172.16.0.80/24 | up | up | 4
outside | 192.168.100.1/16 | up | up | 0
Select an interface to view input and output Kbps
VPN Tunnels
IKE: 0 IPsec: 0 Clientless SSL VPN: 0 SSL VPN Client: 0
Traffic Status
Connections Per Second Usage
1
0
14:00 14:01 14:02 14:03 14:04
UDP: 0 TCP: 0 Total: 0
System Resources Status
Total Memory Usage Total CPU Usage Core Usage
Memory
Memory Usage (MB)
972MB
14:04:11
4000 3500 3000 2500 2000 1500 1000 500 0
14:00 14:01 14:02 14:03
'outside' Interface Traffic Usage (Kbps)
0
14:00 14:01 14:02 14:03 14:04
Input Kbps: 0 Output Kbps: 0
Device configuration loaded successfully.
<admin> 15
08. 7. 9. 오후 2:04:
시작
SmartWindow
SmartWindow - 10GA...
Cisco ASDM 6.1 f...
오후 2:04

200M 동시 연결 및 NAT 시연


내 문서
내 컴퓨터
네트워크 환경
휴지통
비둘기
Cisco ASDM Launcher
ASA5580-4...
Microsoft 마우스
SmartWin...
SmartWindow
SmartDits
SMB-200
SMB-2000
SMB-600(B)
SMB-6000(B/C)
SmartBits Shortcuts
History
Applications
SmartWindow - 10GASA5580-40NAT.prf
File Edit Actions Options Tests Admin View Help
SmartBits 6000B Performance Analysis System
SPIRENT
Group Start
10GBASE-SR
XLW-3721A A
10/100Base-TX
LAN-3302A B
10/100Base-TX
LAN-3302A B
10GBASE-SR
XLW-3721A A
1000Base-X GBIC
LAN-3311A B
Cont@0.009uSec
OnLine
IP=10.72.81.201 Port=16385
시작
SmartWindow
SmartWindow ...
Cisco ASDM 6.1 ...
오후 2:12

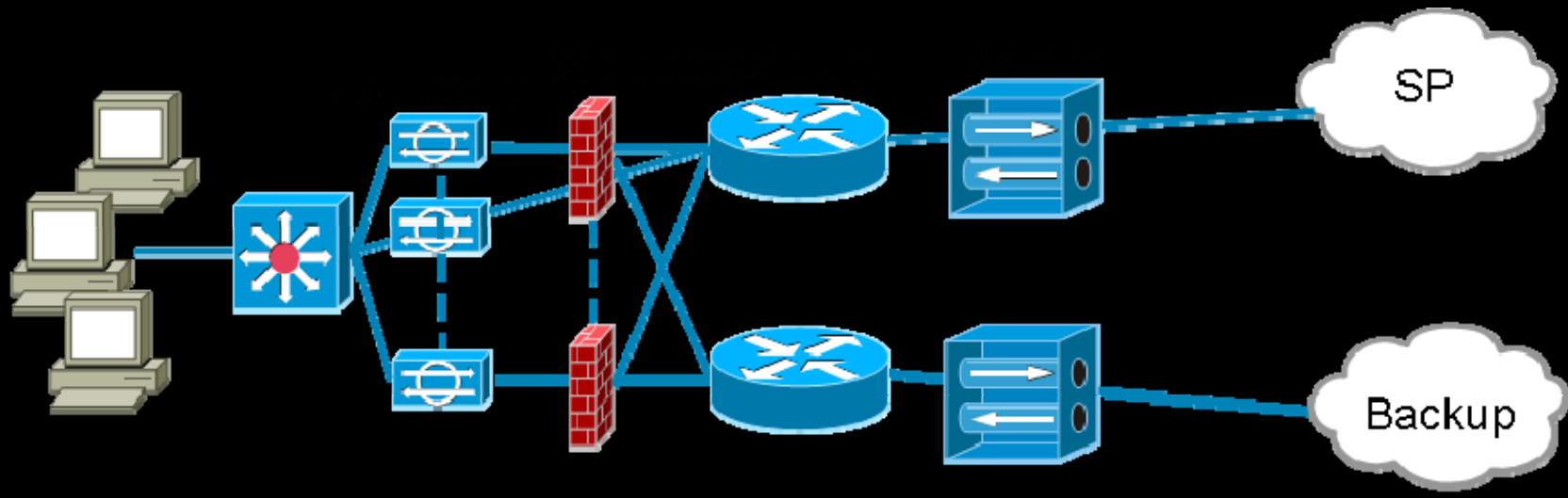
통합위협관리(UTM)솔루션

UTM 이란?

UTM = Unified Threat Management,
통합 위협 관리 솔루션

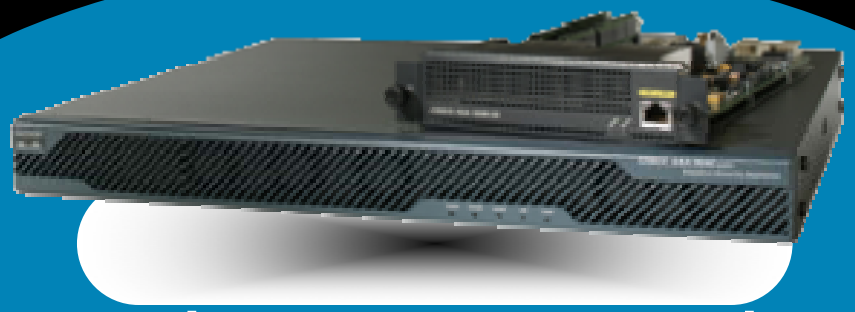
UTM의 필요성과 Cisco UTM 의 활용

- Cisco UTM의 활용

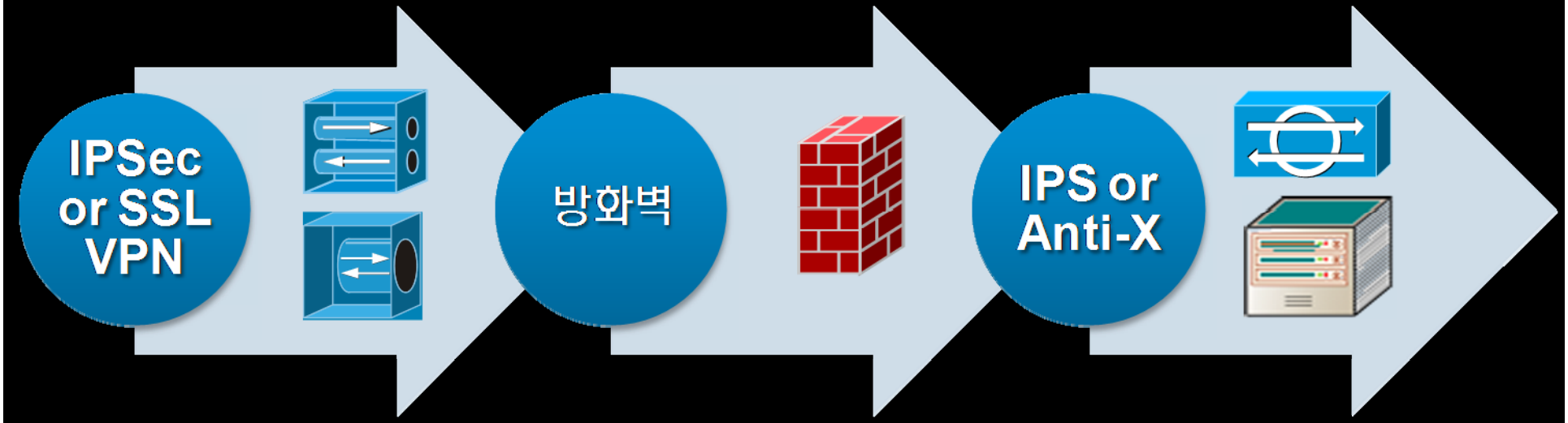


효과적인 지사 및 중소규모 기업의 보안방안은?

UTM 솔루션으로써의 Traffic Flow



Cisco ASA 5500 Series



서비스 모듈 옵션(선택적 사양)

IPS

Anti-X

Interface

Cisco ASA 5500 Series Advanced Inspection and Prevention Module (AIP SSM)

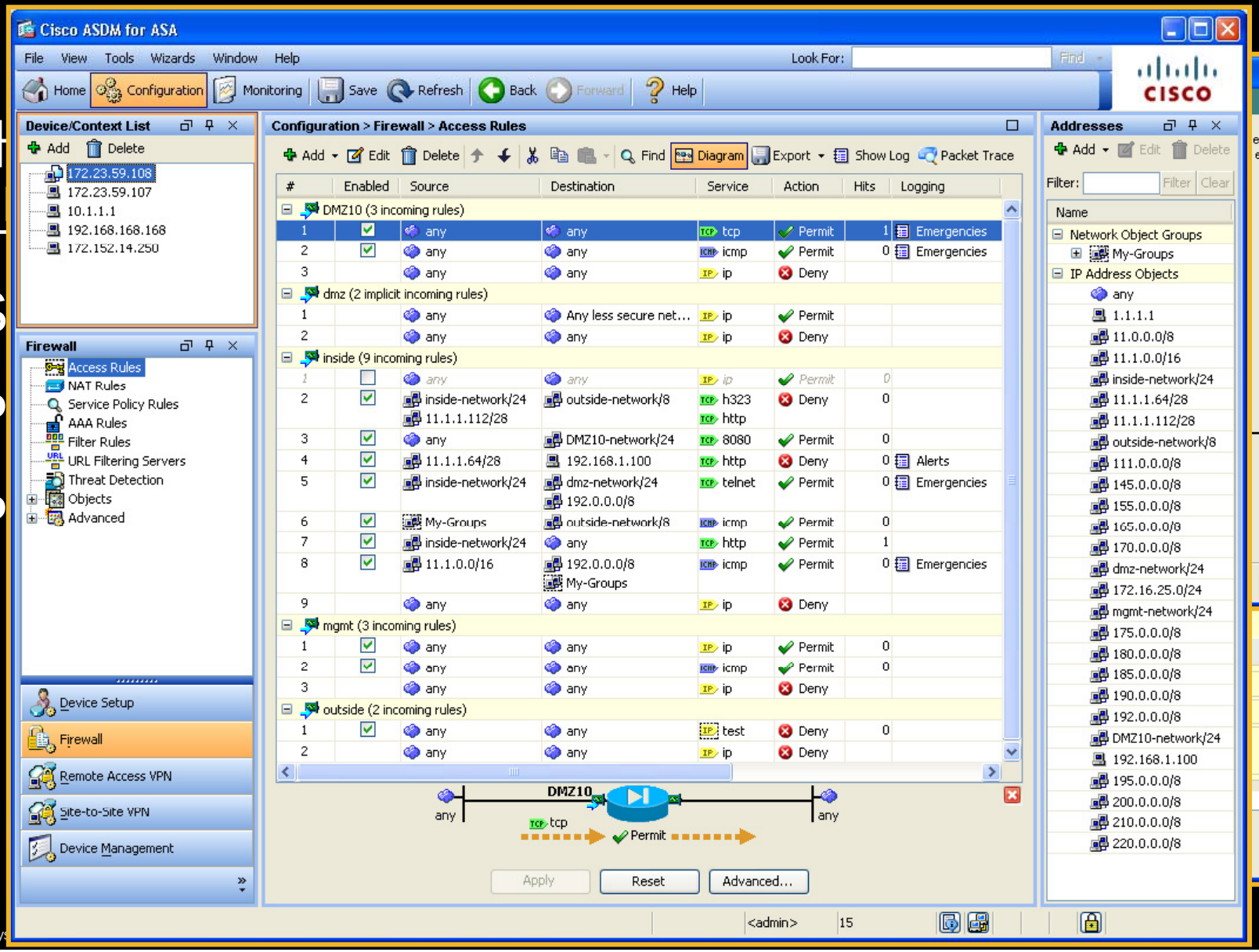
Cisco ASA 5500 Series Content Security and Control Module (CSC SSM)

Cisco ASA 5500 Series 4-Port GE Services Module (4GE SSM)

심층적인 보안 또는 네트워크 확장성 제공

Cisco ASDM v6.1 주요 관리 기능

- 사
  인
- S
- P
- P

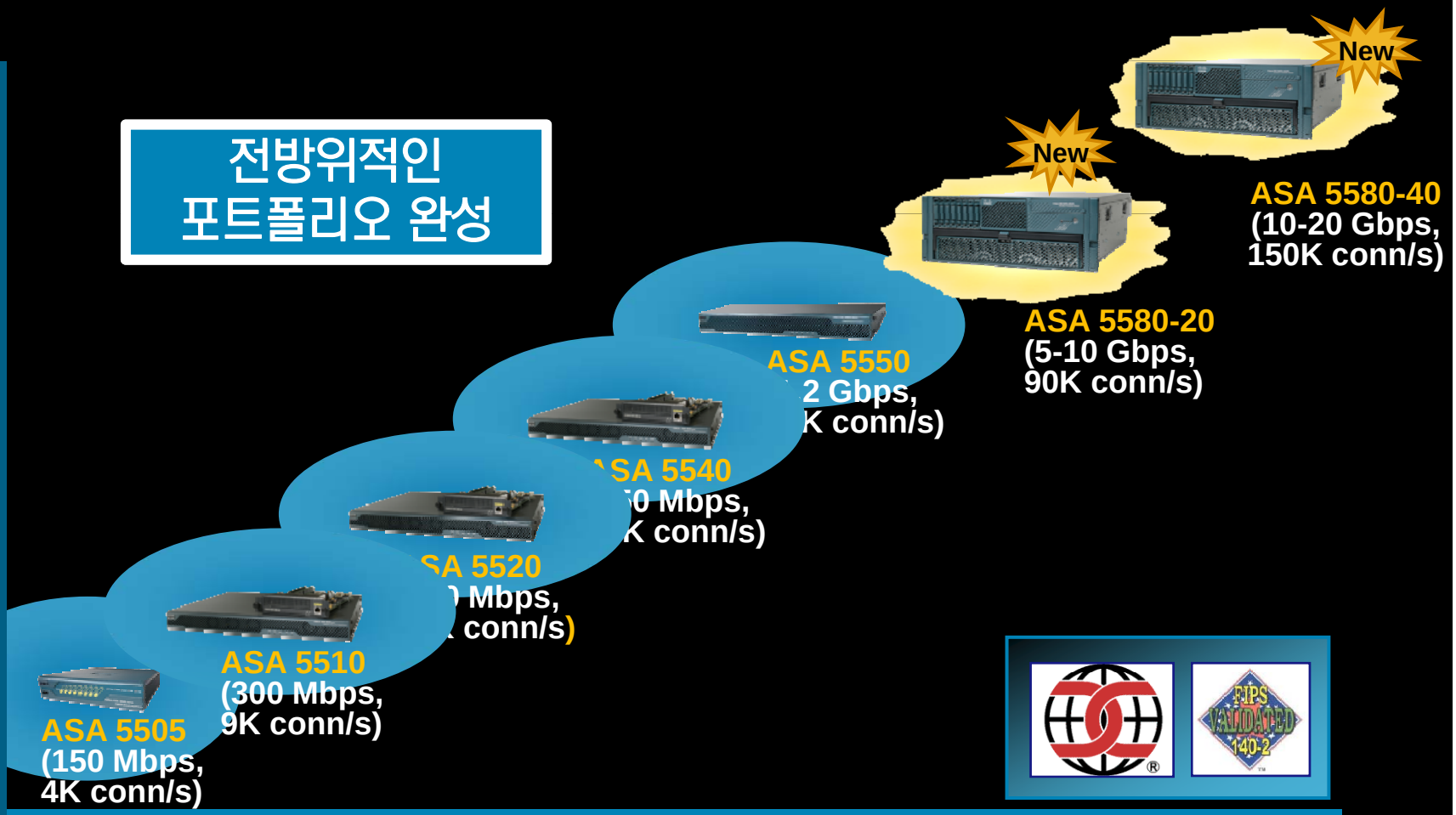


결 론

데스크탑 에서 10G 까지……

Cisco ASA 5500 Platforms

전방위적인
포트폴리오 완성

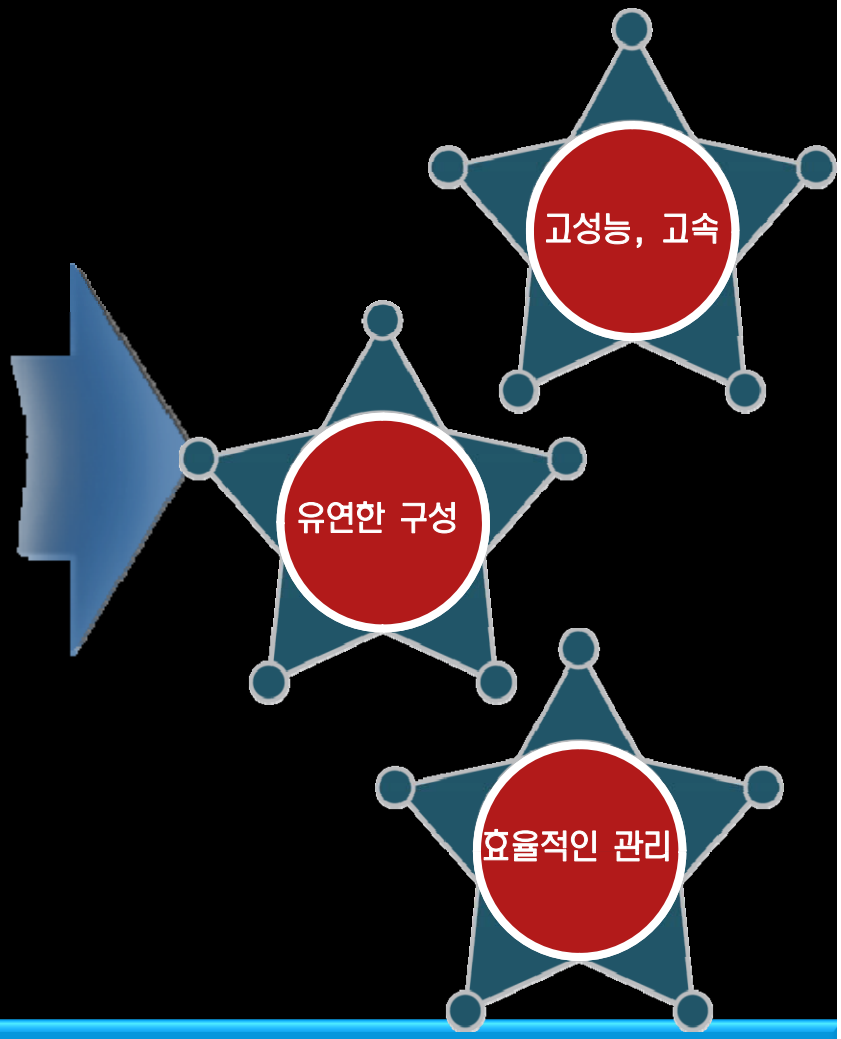


Teleworker | Branch Office | Internet Edge | Campus | Data Center

Why Cisco 10G Firewall?

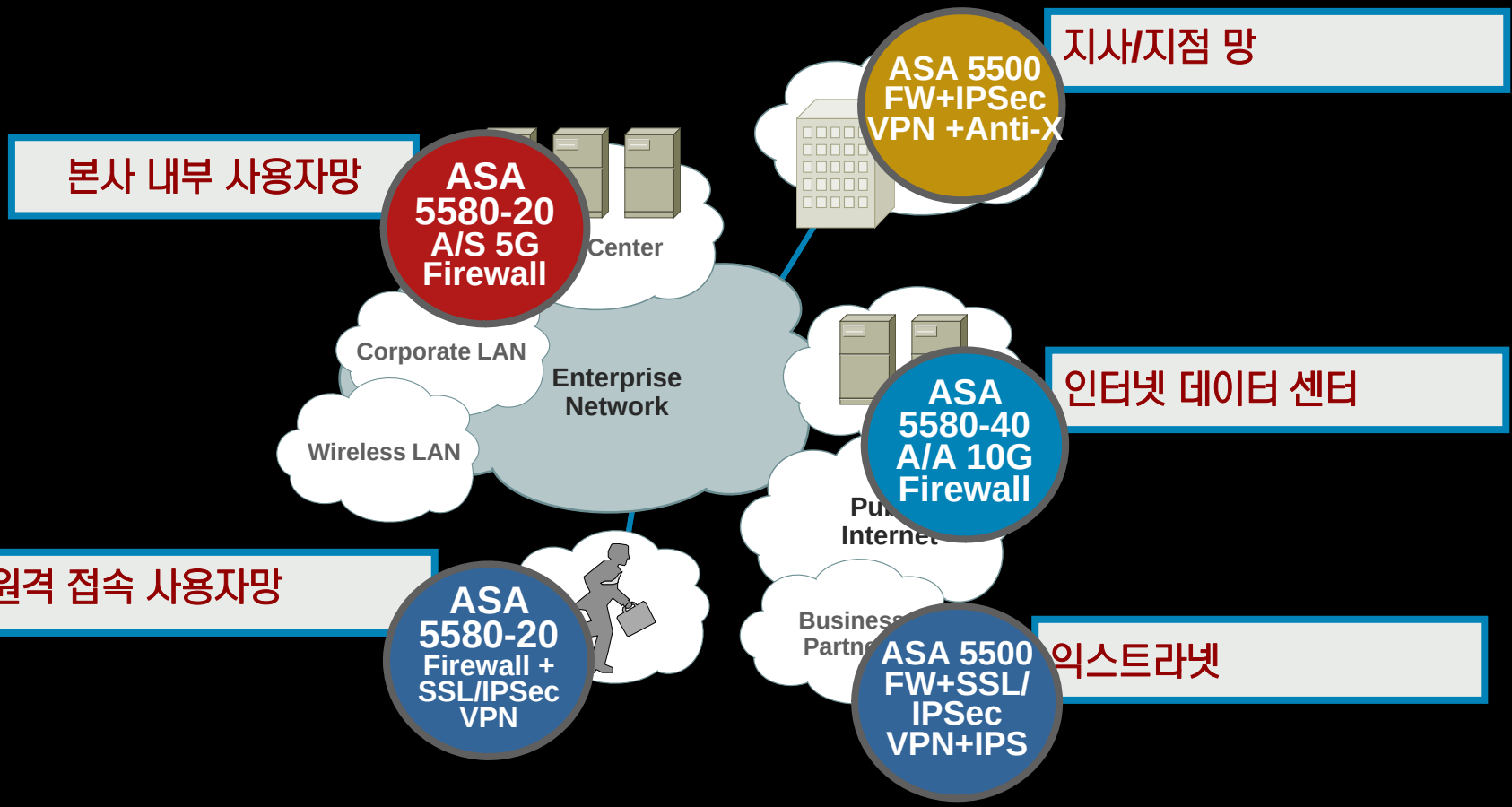
Cisco 10G 방화벽

- •동종업계 최고 **Connection Rate** 보장
- •**Real 10G** 성능 보장
- •안정성이 검증된 **OS** 기반의 고급네트워킹
- •**Netflow** 기반의 효과적인 보안이벤트 관리



현시대가 요구하는 고성능 **10G** 방화벽

Why Cisco UTM?



맞춤형 기업 보안 솔루션

CISCO