Cisco START!
Strategic Transformation
Revolutionary Technology
2008

“ 데이터센터 보안 및 애플리케이션 네트워크 서비스”

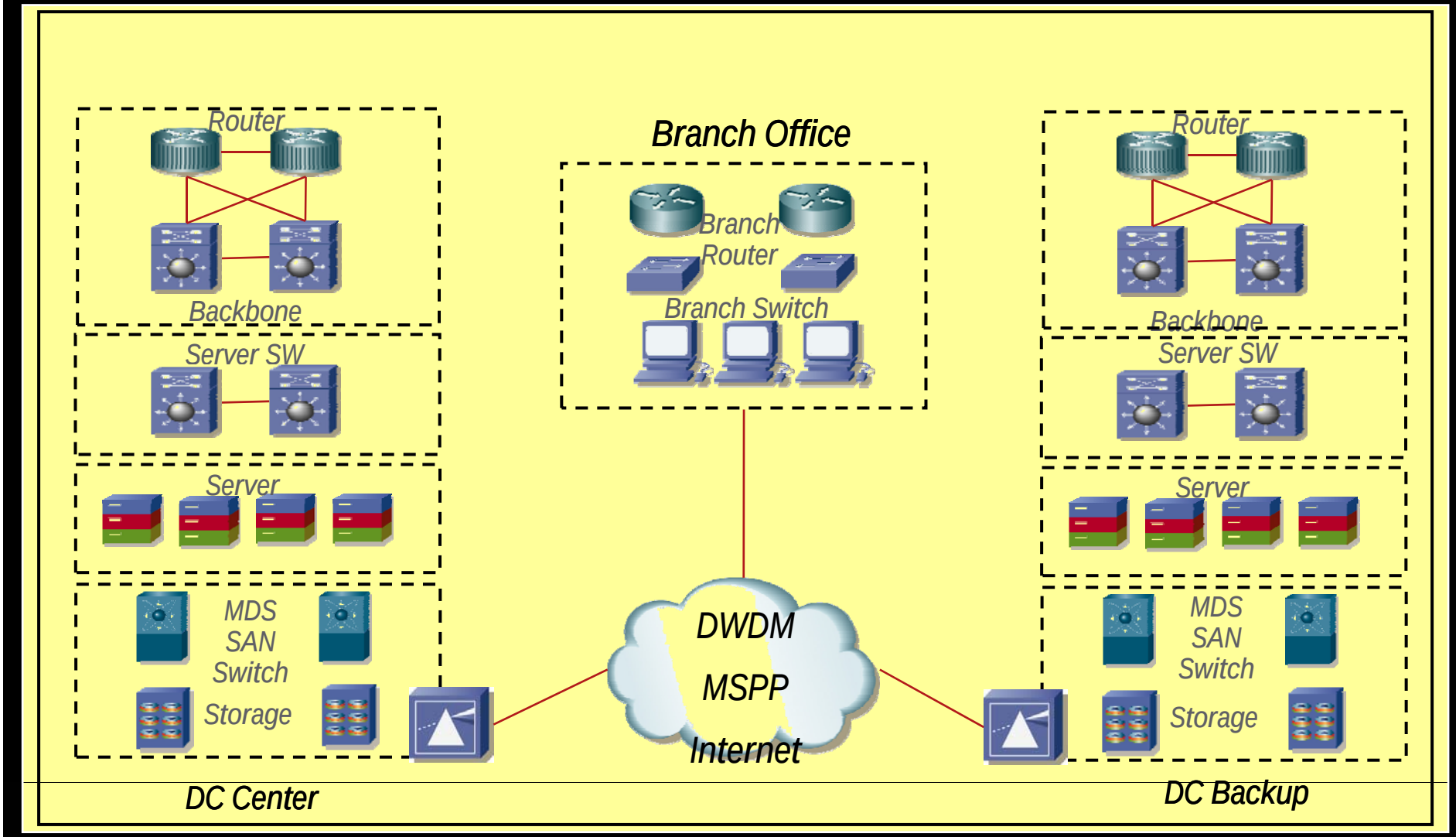
2008.03.11

최 우 형 (whchoi@cisco.com)
Cisco Korea

Cisco START!
Strategic Transformation Revolutionary Technology 2008

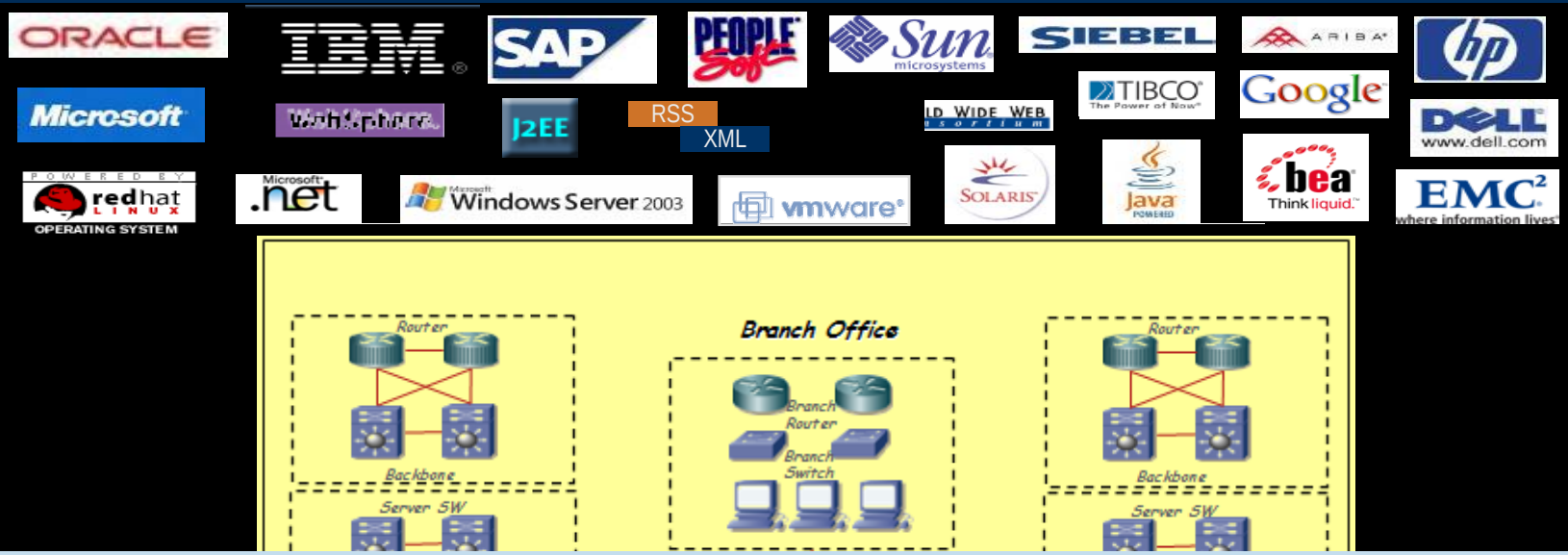
DataCenter 3.0
그 새로운 변화와 요구

오늘날 DataCenter Architecture.



변화하는 DataCenter Architecture.

- Web 2.0 시대의 도래 – 유기적 연동과 다양한 Application
- 새로운 Application Architecture 의 구성 요구



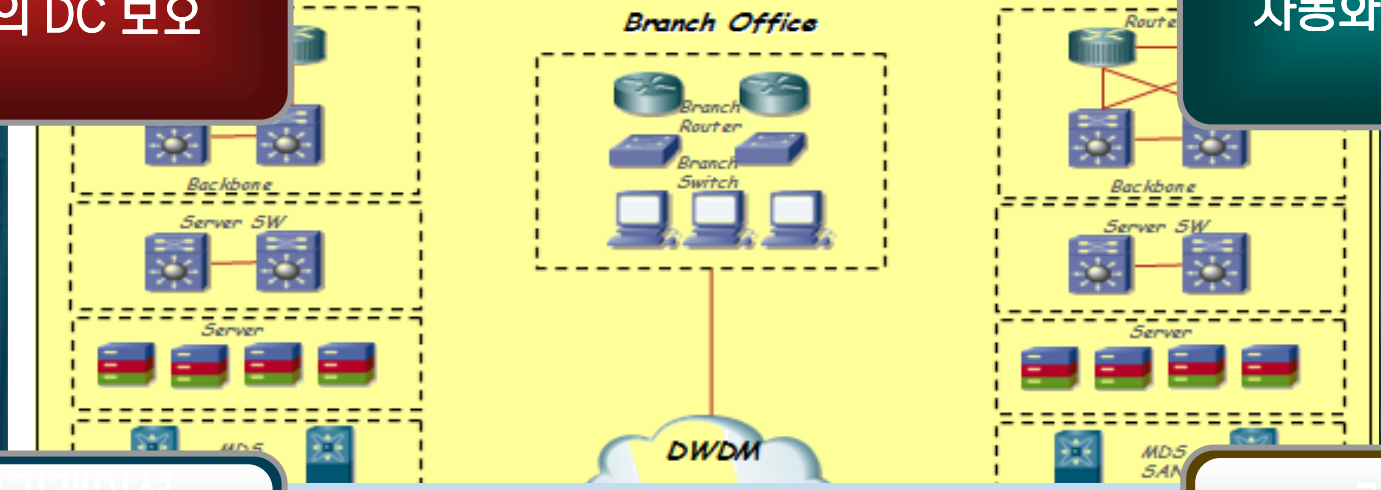
DataCenter 3.0 을 위한 요구 사항
보안 & Application 최적화

보안

내,외부 위협으로
부터의 DC 보호

자동화

DC Mgmt 의
자동화 관리/구성



**어플리케이션
최적화**

빠른 응답속도
대역폭 최적화

가상화

가상화를 통한
투자보호

Cisco START!
Strategic Transformation Revolutionary Technology 2008

DataCenter 3.0
- DC 보안 서비스 -

DataCenter를 위협하는 요소들
전방위로 늘어나는 DC 위협

2007년 국내/외 보안 동향

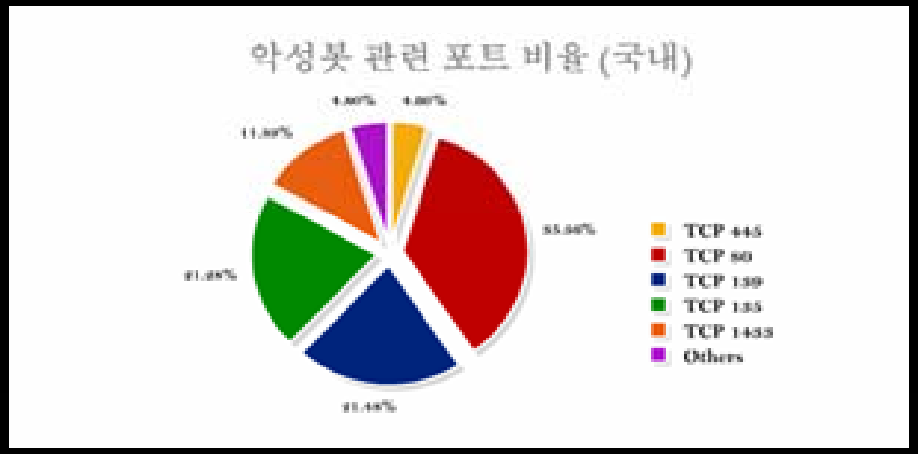
- SPAM Volume 100 % 증가
  - 전세계적으로 연간 Spam 160조 발생
  - 인당 하루 스팸메일 수신 20 통
- SPAM Mail의 위험성 증가
  - Spam 메일의 83%가 URL 포함
  - URL 기반 Virus 256% 증가
- Self Defending Bot Net
  - Bot Net의 빠른 진화
- Virus가 더 이상 주인공이 아니다.
  - Virus의 DDoS 성격으로의 진화

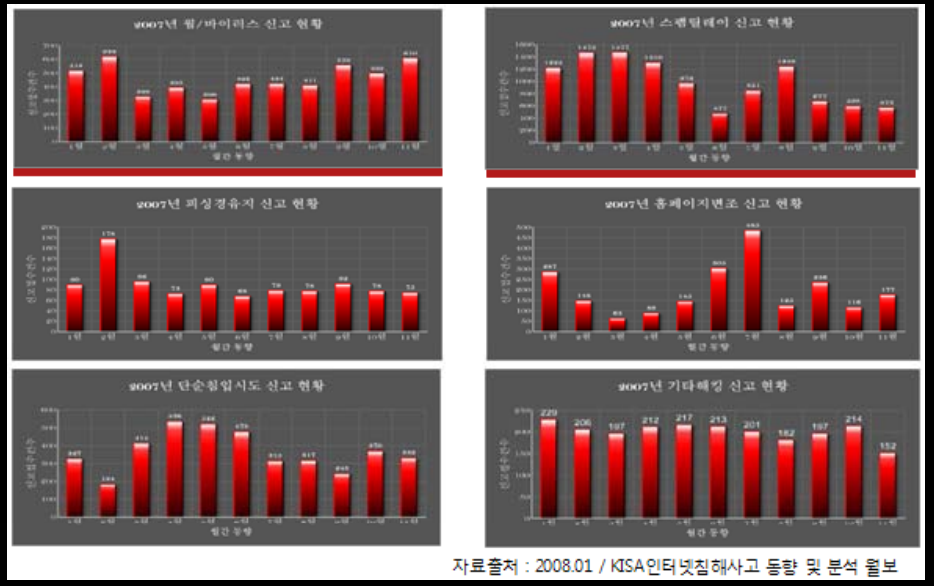
자료출처 :
Cisco/IronPort 2008 Security Trend Report

- 공격의 국지성 심화
- 대가성 범죄 급증
- 웹 사이트 해킹 심화
- 허위 안티스파이웨어 급증
- Bot Net 기승
- 이동저장장치 노린 악성코드 기승
- 스파이웨어 전파방법 지능화
- 악성코드 은폐 방법의 고도화
- ARP 스프핑과 악성코드의 결합
- 애플리케이션 취약점 공격다양화

자료출처 : 안철수연구소 2007 10대 보안위협

자료출처 : 2008.01 / KISA인터넷침해사고 동향 및 분석 월보



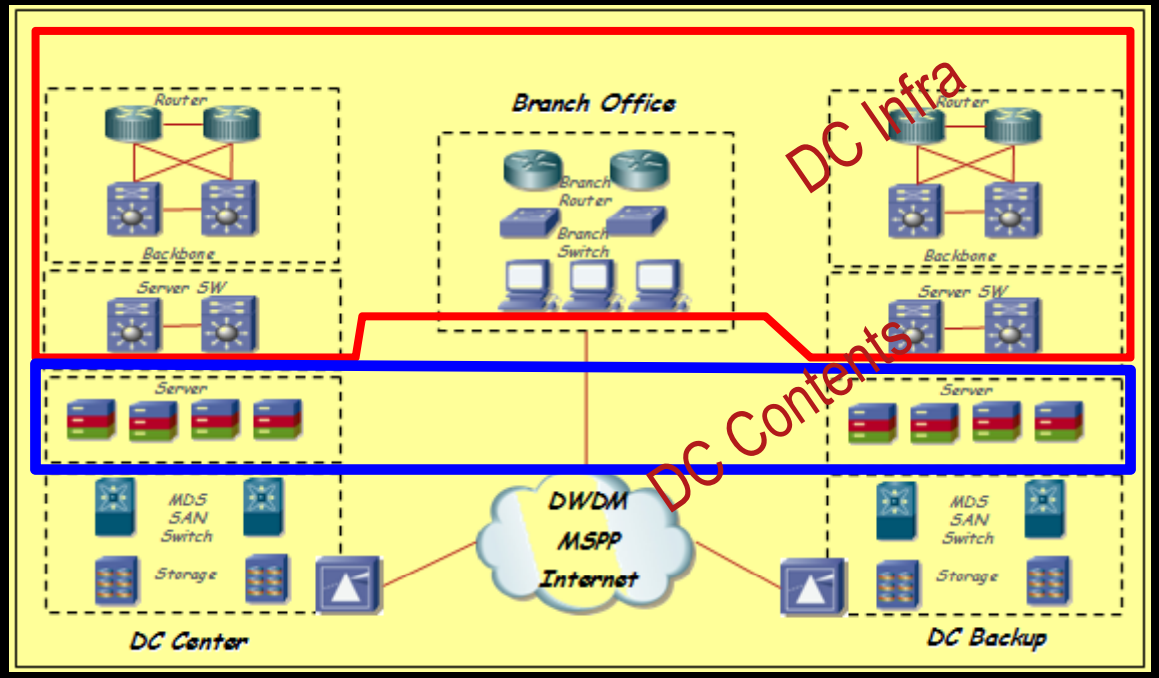


자료출처 : 2008.01 / KISA인터넷침해사고 동향 및 분석 월보

Cisco START! 2008

DataCenter를 위협하는 요소들
DC Infra와 Contents 위협

- DC Infra 및 Contents 등 모든 요소들이 위협의 대상
- 점점 더 지능화되는 공격과 위협들



Tear Drop, Session Hijacking, Jolt, Bloop, Targa,Bonk, Boink, Fraggle, Xmas scan, Ping of Death,Smurf, Fraggle,TCP SYN flood, DNS attacks,DDOS, Mail ttacks Fragmentation attacks, UDP attacks, TCP stream obfuscation, Worms,Trojans, dSniff, Man-in-the-Middle,Route poisoning, etc

SQL Injection, Cross-Site Scripting, Command Injection , Cookie/Session Poisoning, Application Reconnaissance, LDAP Injection, Buffer Overflows, Directory Traversals, Attack Obfuscation, Application Platform Exploits, Parameter Tampering, Spyware, Root Kits, Firepass, HTun, Httptunnel, Hopster, etc

DC 3.0 보안 서비스 요구 사항

어플리케이션 보안 — Value-Added 컴포넌트

IP 기반 비즈니스 환경을 위한 안전한 Application 제공

Protect the CRM, ERP, PLM, HCM.

어플리케이션 커뮤니케이션 채널 — 데이터 인터페이스

DataCenter의 안전한 어플리케이션 서비스 접속을 위한 환경 제공

Protect the XML, SOAP, SQL, DHTML

서비스 레이어 — 가상화 서비스

효율적인 보안 서비스 운용을 위한 가상화 서비스

Secure Infrastructure and Protocols

데이터 센터 인프라 보안 — 패킷 전송 서비스

패킷 전송의 기반인 인프라에 대한 강력한 보호 기술 서비스

안전한 컨텐츠 제공을 위한 데이터 센터 보안 서비스 제공

DC Infra & Edge 의 보호를 위한 기술 청사진

Core Infra 보안

기본 보안 - RACL , uRPF

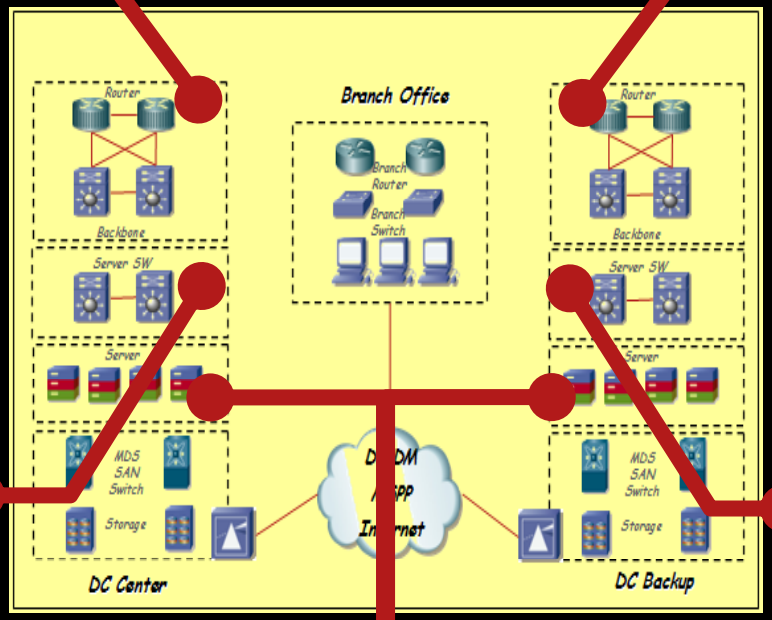
장비 보호 – CPP

장비 인증/감사 – TACACS+ , Netflow, Syslog

DDoS Protection Svc

장비 기반 DDoS 방어 – RTBH , ACL

Enhanced DDoS 전문 방어 솔루션 도입 필요



Server/Access Switch Edge

기본 보안 - ACL, Port Security, DAI, PVLAN, QoS

장비 보호 – CPP, Root Guard, BPDU Guard

장비 인증/감사 – TACACS+, Netflow

Firewall Svc

10G 이상의 고성능 방화벽 서비스

가상화 기반의 효율적인 사용

L7 Deep Inspection 서비스

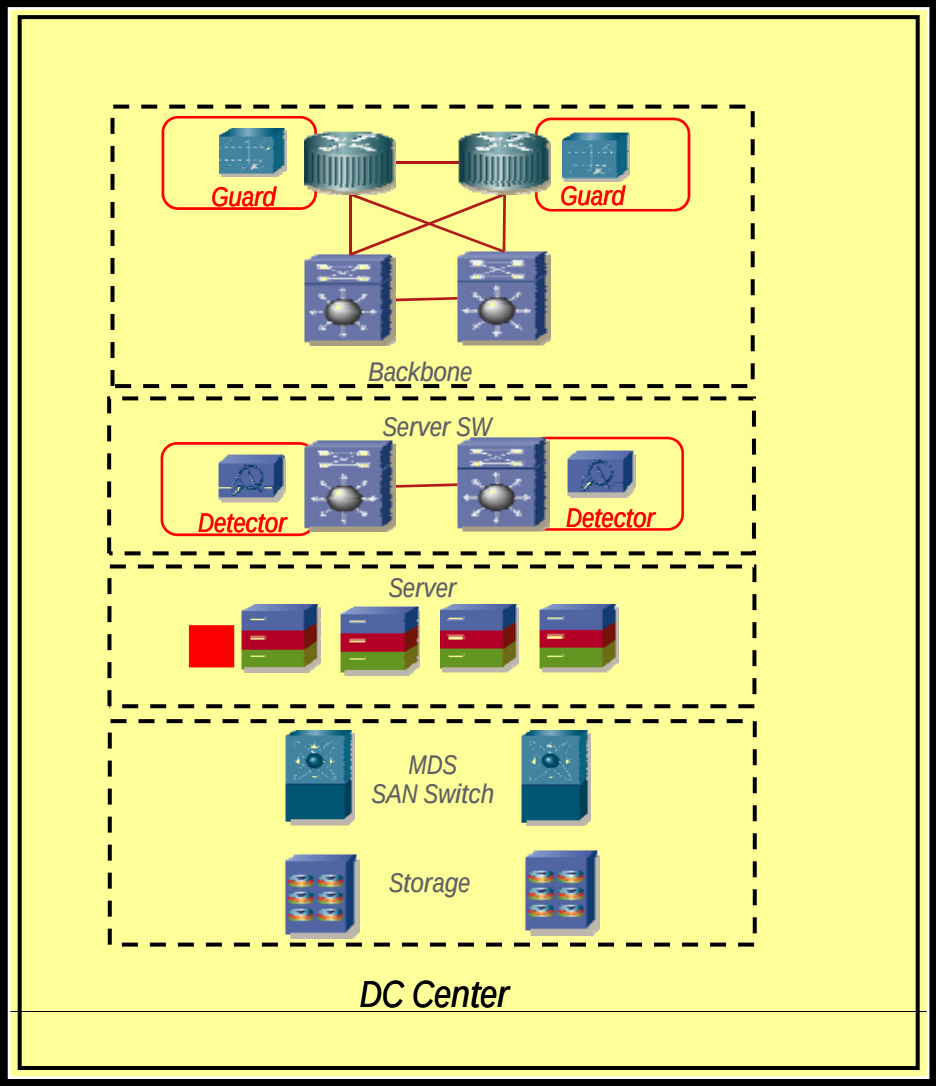
Application 보안

HTTP Inspection , Web 2.0 서비스를 위한 XML 보안 서비스

서버 보안을 위한 Host IPS

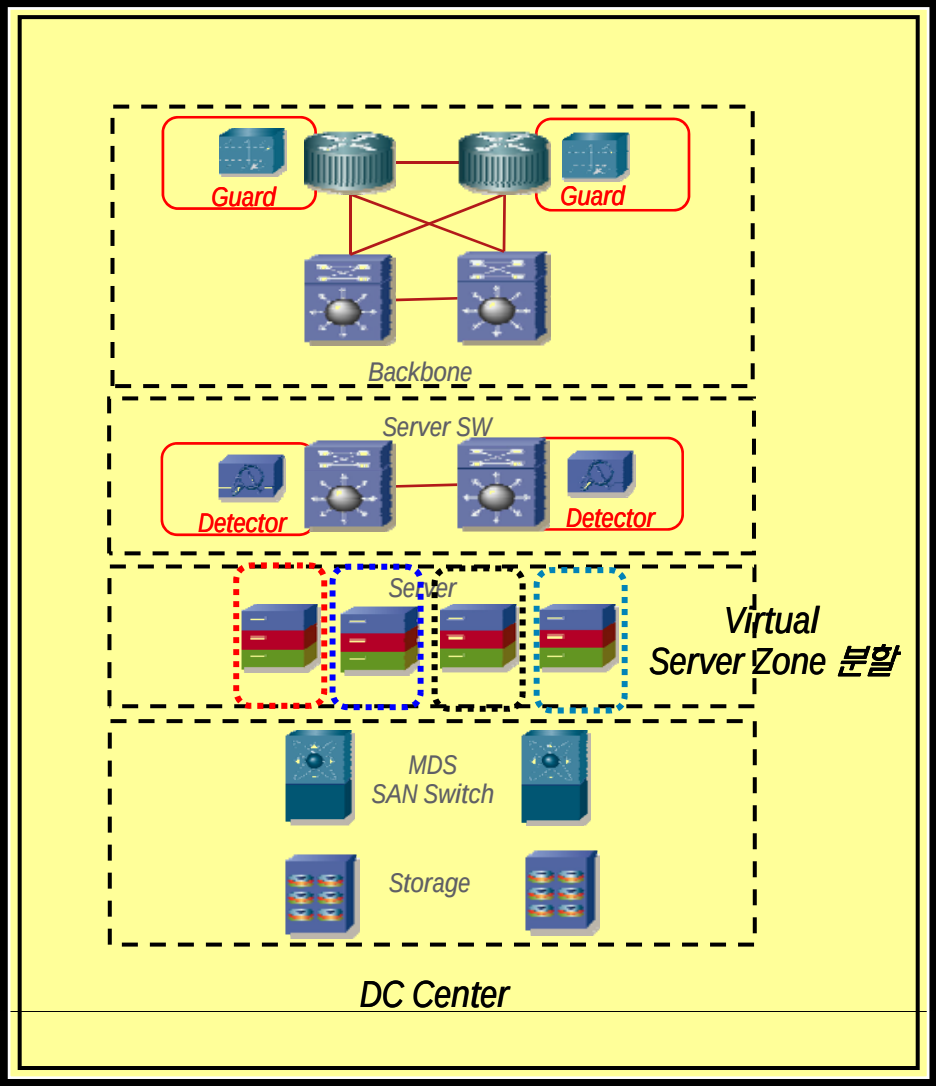
- 보안 서비스의 자동화 & 가상화 구현 -

DC Infra & Edge 의 보호
DDoS 공격으로 부터의 보호



- ❑ DDoS 공격 위협
  - ❖DC Contents Server를 향한 대규모 DDoS 공격
  - ❖웹 기반의 좀비 공격
- ❑ DDoS 공격으로 인한 피해
- ❑공격시 중요 Contents 서비스 중지
  - ❖ High CPU Load / 대역폭 잠식…
  - ❖ Internet 기반의 서비스 장애
  - ❖ 대외 신뢰도 및 금전적 손실 발생
- ❑ 장시간 장애 발생 가능성
  - ❖ 변조된 IP 공격이 발생하거나, 대규모 Traffic 공격일 경우 지속적인 장애가 발생할 가능성 높음…

DC Infra & Edge 의 보호
DDoS 공격으로 부터의 보호



- 각 Virtual Zone 별 Passive Monitoring
  - Contents 별 동작 방식 자동 학습
- 이상 Traffic 발생 시 AGM(Guard)에 통보
- Guard는 이상 Traffic으로 향하는 목적지에 대해, BGP Advertise
- 목적지로 향하는 Traffic에 대한 Guard의 MVP Filtering 동작
- 정상적인 Traffic은 원래의 목적지로 향하도록, Injection 구성

데이터 센터의 최대적 DDoS 공격 방어 및

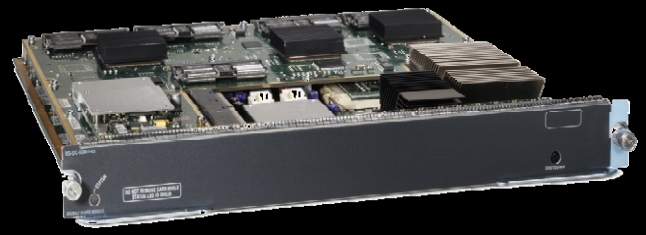
비즈니스의 연속성을 지속적으로 확보 !!!

DC Infra & Edge 의 보호
ADM Module 소개

Learning Based

Flexibility

High Availability



ADM (Anomaly Detection Module)

❑ 성능

- ❖ 2Gbps / 300만 동시 접속 처리
- ❖ 500개 Zone 구성 및 Policy 적용 가능
- ❖ 동시 150개 Zone에 대한 실시간 방어
- ❖ 1msec 이하의 Latency / jitter
- ❖ 7GB DDRAM, 1GB Compact Flash 제공

❑주요 기능

- ❖ Spoofed, Non-Spoofed Packet 탐지
- ❖ TCP Attack 탐지 – Flag 기반 공격 탐지(Syns, Syn-acks, acks, fins, fragments)
- ❖ UDP Attack 탐지 – Random port Flood, Fragment
- ❖ ICMP Attack 탐지 – Unreachable , echo, Fragment
- ❖ DNS Attack 탐지 / SIP Attack 탐지
- ❖ HTTP Get Flood Attack 탐지
- ❖ IP Attack /Fragment Attack /BGP Attack 탐지

DC Infra & Edge 의 보호
AGM Module 소개

Multistage Verification

Flexibility

High Availability

AGM (Anomaly Guard Module)

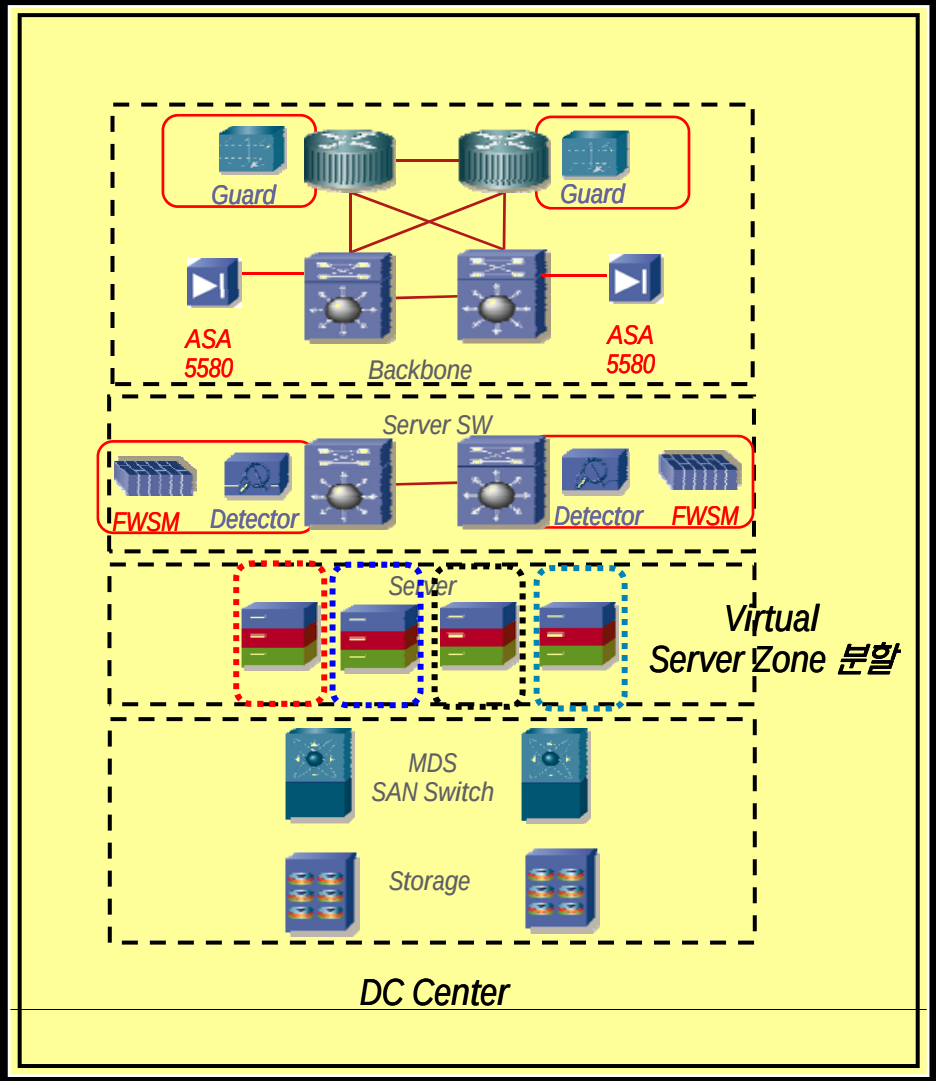
❑ 성능

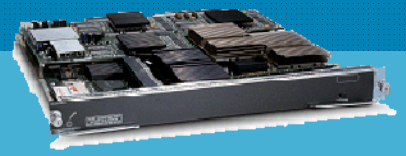
- ❖ 3Gbps / 450만 동시 접속 처리
- ❖ 15만개 다이나믹 필터 적용
- ❖ 500 개 서로 다른 Zone 정의 가능
- ❖ 실시간 50개 Zone 방어 가능
- ❖ 7GB DDRAM, 1GB Compact Flash 제공

❑ 주요 기능

- ❖ Spoofed, Non-Spoofed Packet 방어
- ❖ TCP Attack 방어 – Flag 기반 공격 방어(Syns, Syn-acks, acks, fins, fragments)
- ❖ UDP Attack 방어 – Random port Flood, Fragment
- ❖ ICMP Attack 방어 – Unreachable , echo, Fragment
- ❖ DNS Attack 방어 / SIP Attack 방어
- ❖ HTTP Get Flood Attack 방어
- ❖ IP Attack /Fragment Attack /BGP Attack 방어

DC Infra & Edge 의 보호
고성능 방화벽 기반의 보안 서비스 구현





- ❑ 강력한 성능 기반의 방화벽 서비스
- 5.5 Gbps ~ 16Gbps / 2.8Mpps ~ 5.5Mpps
- 100만 동시 접속 ~ 150만 동시 접속
- 10만 CPS ~ 15만 CPS
- ❑ 강력한 보안 정책 지원
- 7만 개 ~ 75만개 방화벽 정책 지원
- ❑ 가상화 방화벽 지원을 통한 투자 보호 및 운영 효율성
- 50 개 가상화 방화벽 ~ 250개 가상화 방화벽 제공
- ❑ 다양한 프로토콜의 심도 깊은 분석 기법 제공
- ❑ L2/L3 방화벽 모드 지원
- ❑ ASDM 기반의 차별화된 GUI Interface 제공

DC Firewall 구성
Cisco DC 보안 솔루션 디자인 – FWSM 소개

High Performance

Intelligent Service

Service Virtualization

FWSM (Fire Wall Service Module)

❑ 성능

- ❖ 5.5Gbps (단일 샤시 최대 4장 20Gbps)
- ❖ 2.8Mpps / 1M 동시접속 / 100K CPS
- ❖ 1000개 Vlan/ Context 당 Routed Mode 256개,TP Mode 8개 Vlan Pair 지원
- ❖ ACL 80K / NAT 256K
- ❖ Virtual Context 250개(기본 3개 포함)

❑ 주요 기능

- ❖ L2/L3(Transparent,Routed Mode) 방화벽 지원
- ❖ Dynamic/ Multicast Routing 지원 – OSPF,RIPv1/2, PIM Sparse Mode v2, IGMPv2
- ❖ PVLAN 지원
- ❖ Deep Inspection 지원 – Core Internet Protocol, DB/OS Service, Multimedia/VoIP
- ❖ Active/Standby, Active/Active 지원
- ❖ DDoS Attack 방어 기능 제공

DC Firewall 구성
Cisco DC 보안 솔루션 디자인 – ASA 5580

High Performance

Intelligent Service

Service Virtualization

ASA 5580 Series

❑ 성능

- ❖ 10Gbps (Real Traffic) / 16Gbps (1400Byte 기준)
- ❖ 5.5Mpps / 1.5M 동시접속 / 150K CPS
- ❖ 100개 Vlan 지원 / 24개 Gigabit Interface & 12개 10G Interface 지원
- ❖ 보안 정책 최대 75만개 지원
- ❖ Virtual Context 50개(기본 3개 포함)

❑ 주요 기능

- ❖ L2/L3(Transparent,Routed Mode) 방화벽 지원
- ❖ Dynamic/ Multicast Routing 지원 – OSPF,RIPv1/2, PIM Sparse Mode v2, IGMPv2
- ❖ 802.1Q 지원을 통한 유연한 가상화
- ❖ Deep Inspection 지원 – Core Internet Protocol, DB/OS Service, Multimedia/VoIP
- ❖ Active/Standby, Active/Active 지원
- ❖ Netflow v9 지원

DC Firewall 구성
Cisco DC 보안 솔루션 디자인 – ASA 5580

16Gbps 방화벽 처리

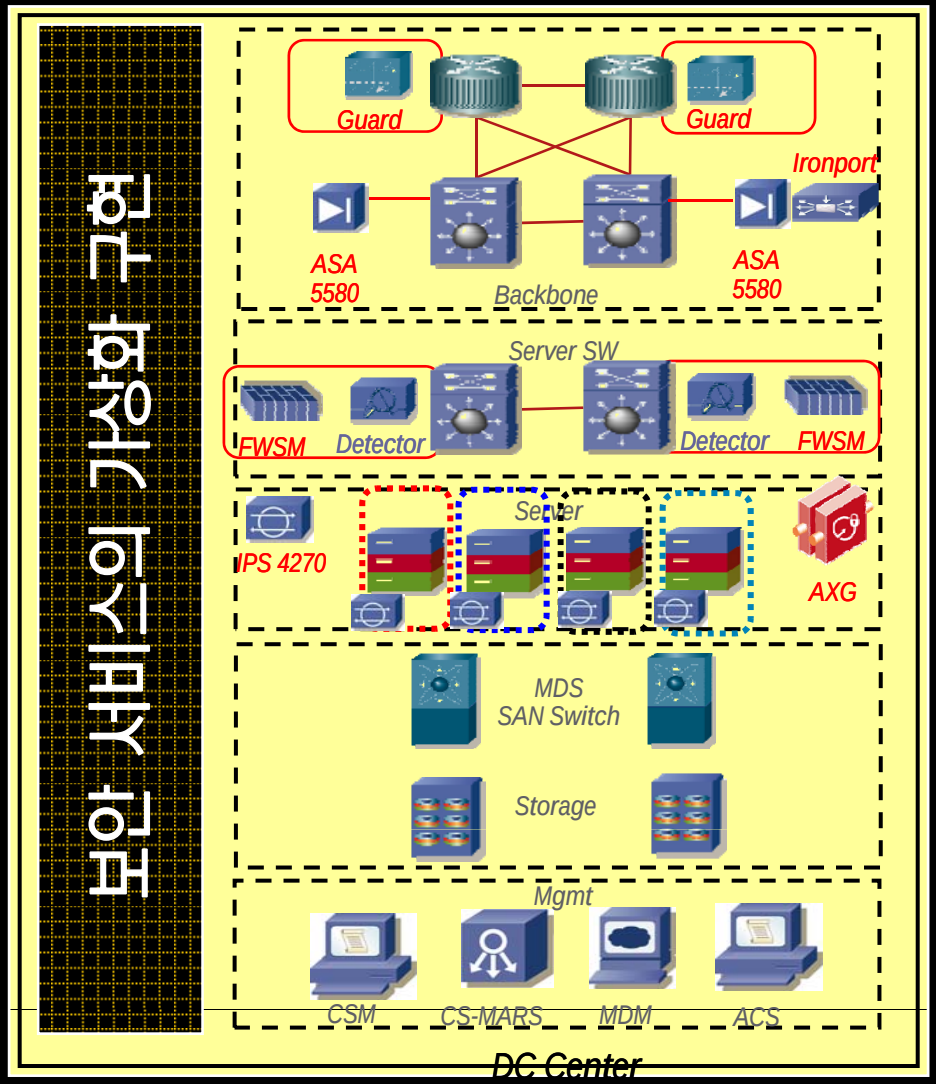
초당 150,000 CPS

동시 접속 150만 처리

DC를 위한 방화벽 솔루션

ASA 5580 Series

Cisco DataCenter 보안 청사진



DataCenter Infra/Edge 보안

Cisco IOS 보안 기술
ACL, CoPP, uRPF, RTBH,DAI, Port Security, PVLAN, Netflow ...

DataCenter 보안 기반 서비스

ASA 5580 , FWSM – 고성능 가상화 방화벽
Guard/Detector – 완벽한 DDoS 방어 구축
IPS 4270 – 중요 자산을 위한 침입탐지 서비스

DataCenter Application/서버 보안

ACE/AXG – Web/SOAP(XML) 기반의 공격 방어 및 제어
IronPort – Web/Mail 보안의 지능화 구현

DataCenter 관리통합/자동화

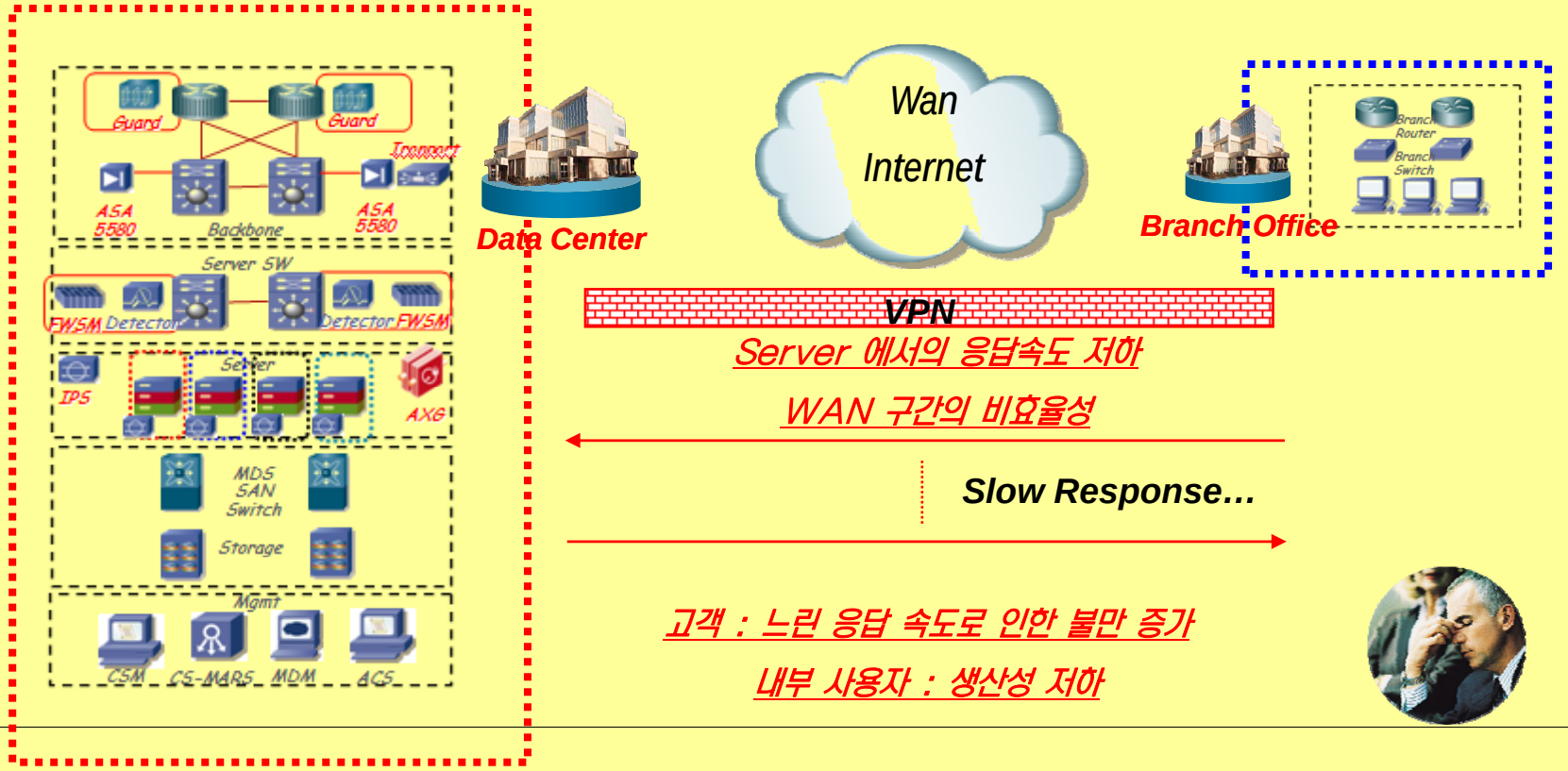
CSM 3.1 – 통합 보안솔루션 Provisioning
CS-MARS – 지능형 위협 관리 솔루션
MDM – 통합 DDoS 방어 체계 관리 솔루션

Cisco START! Strategic Transformation Revolutionary Technology 2008

DataCenter 3.0
- Application 최적화 서비스 -

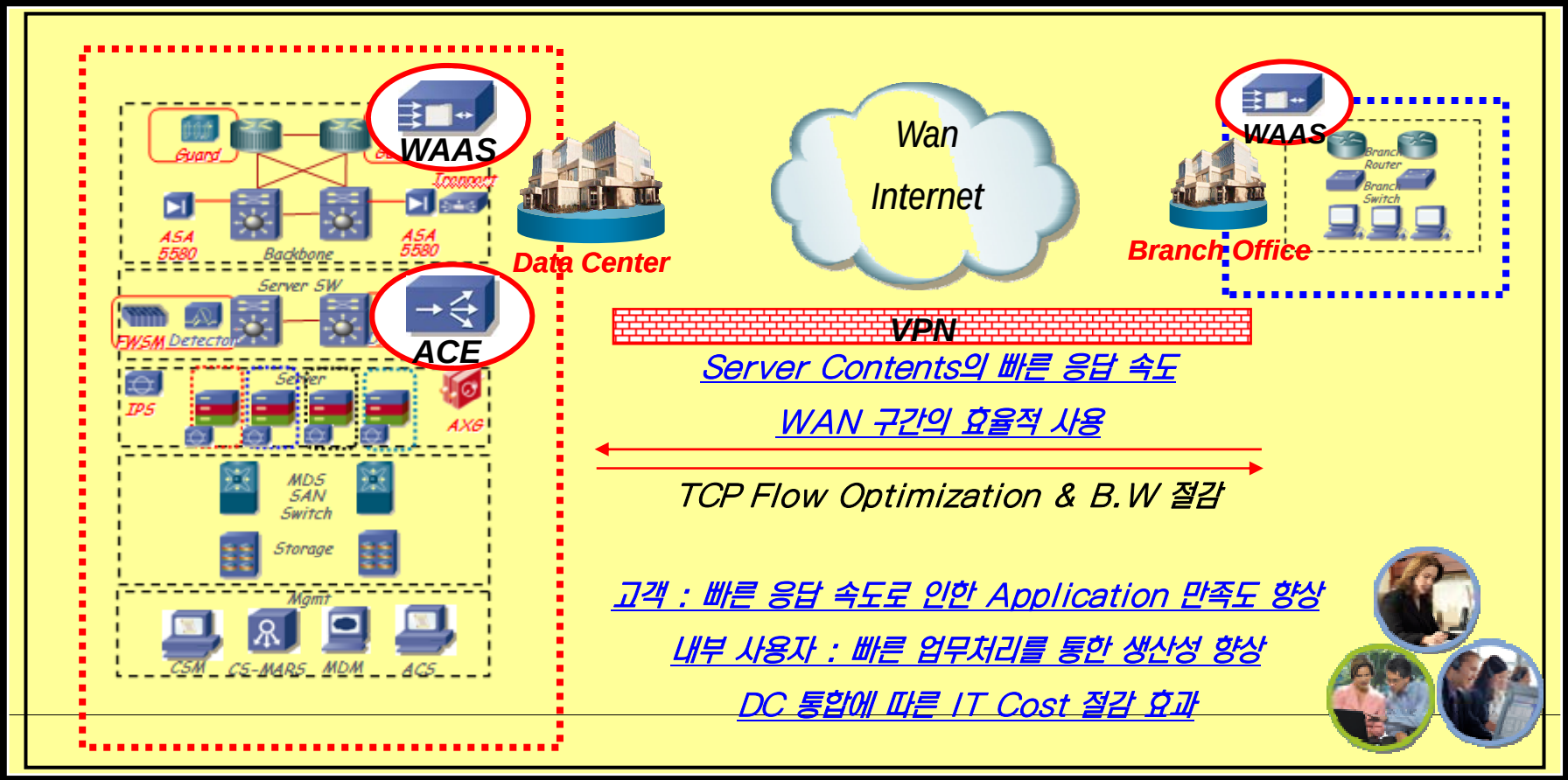
오늘날 DataCenter Challenge...
Application 응답속도와 WAN 효율성

- Web 2.0 Application 기반 서비스 확장으로 인한 응답 속도 중요성
- DataCenter 3.0 시대 흐름에 따른 통합화로 인한 WAN 사용 효율성 이슈

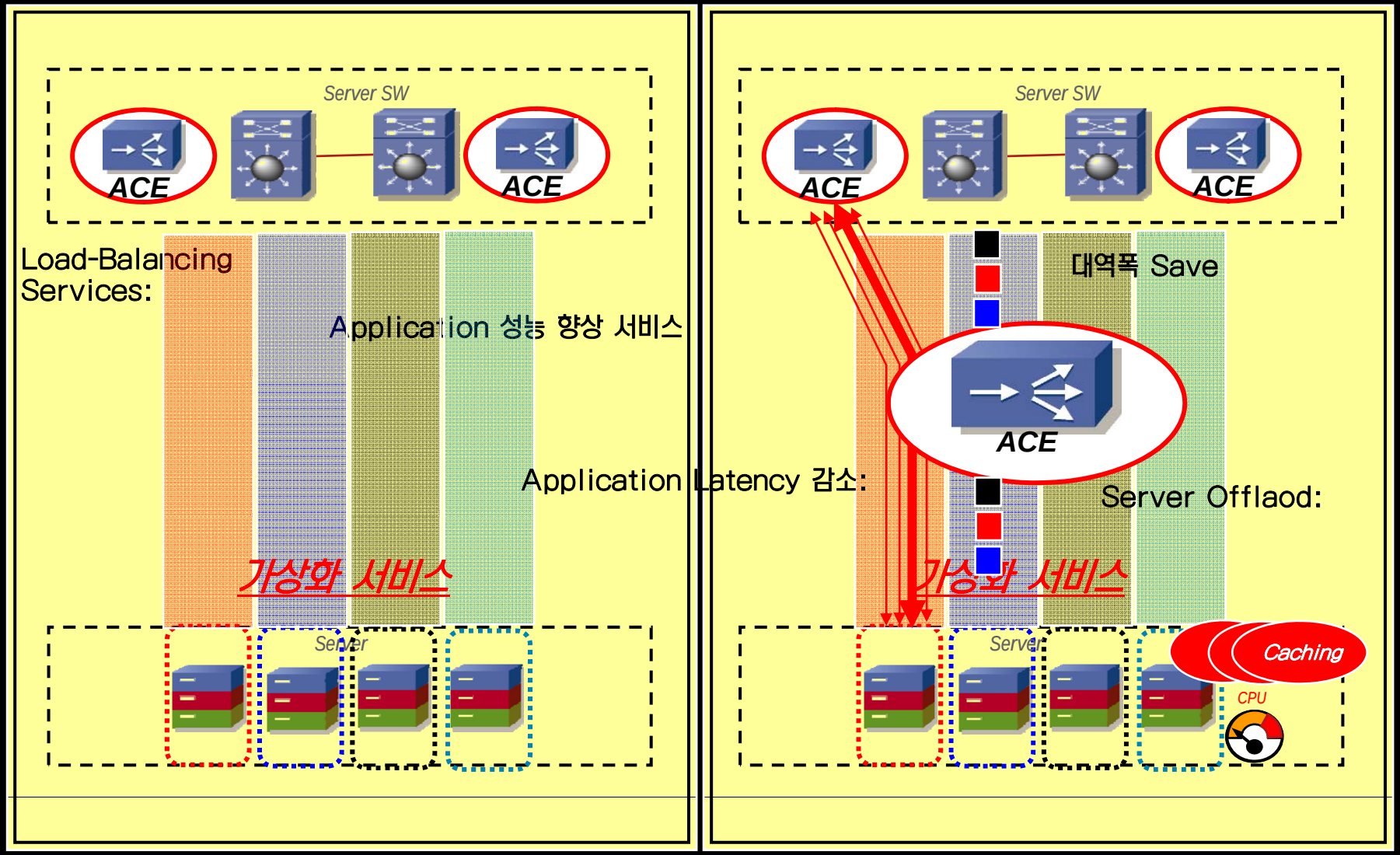


DC를 위한 Cisco Application 최적화 솔루션 ACE / WAAS

- ACE 솔루션 기반의 향상된 Application 처리 제어 서비스 제공
- WAAS 솔루션 기반의 WAN 구간의 최적화 서비스 제공



DC를 위한 Cisco Application 최적화 솔루션
ACE 기반의 Application 가속 서비스



DC를 위한 Cisco Application 최적화 솔루션
ACE 모듈

Content Switching

Security

SSL Offload

ACE (Application Control Engine)

❑ 성능

- ❖ 16Gbps/8Gbps/4Gbps (Fabric Enabled)
- ❖ 6.5Mpps / 4M 동시접속 / 348K CPS
- ❖ 4000개 Vlan/Probe 지원
- ❖ ACL 256K / NAT 1M
- ❖ Virtual Context 250개(기본 5개 포함)

❑ 주요 기능

- ❖ Role Based Access Control 지원
- ❖ Reflexive ACL, TCP/IP normalization, protocol fixup
- ❖ HTTP Deep Inspection
- ❖ TCP/SSL Offload
- ❖ Modular Policy CLI
- ❖ TCP Connection State Tracking
- ❖ uRPF Check

DC를 위한 Cisco Application 최적화 솔루션
ACE 4710

Content Switching

Security

SSL Offload

ACE 4710

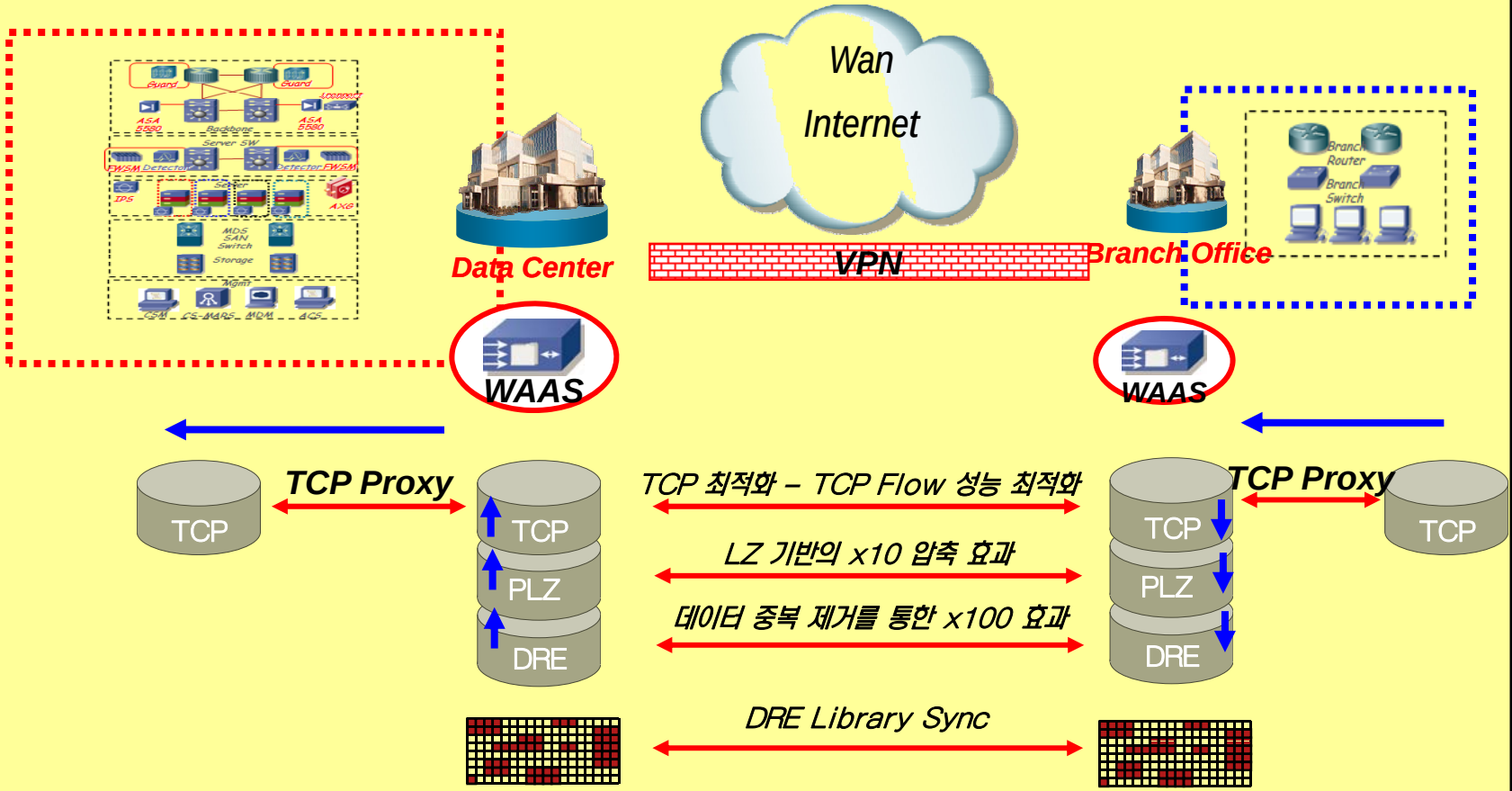
❑ 성능

- ❖ 1Gbps/2Gbps
- ❖ 1M 동시접속 / 120K CPS
- ❖ 4000개 Vlan/Probe 지원
- ❖ ACL 40K / NAT 64K
- ❖ Virtual Context 20개(기본 5개 포함)

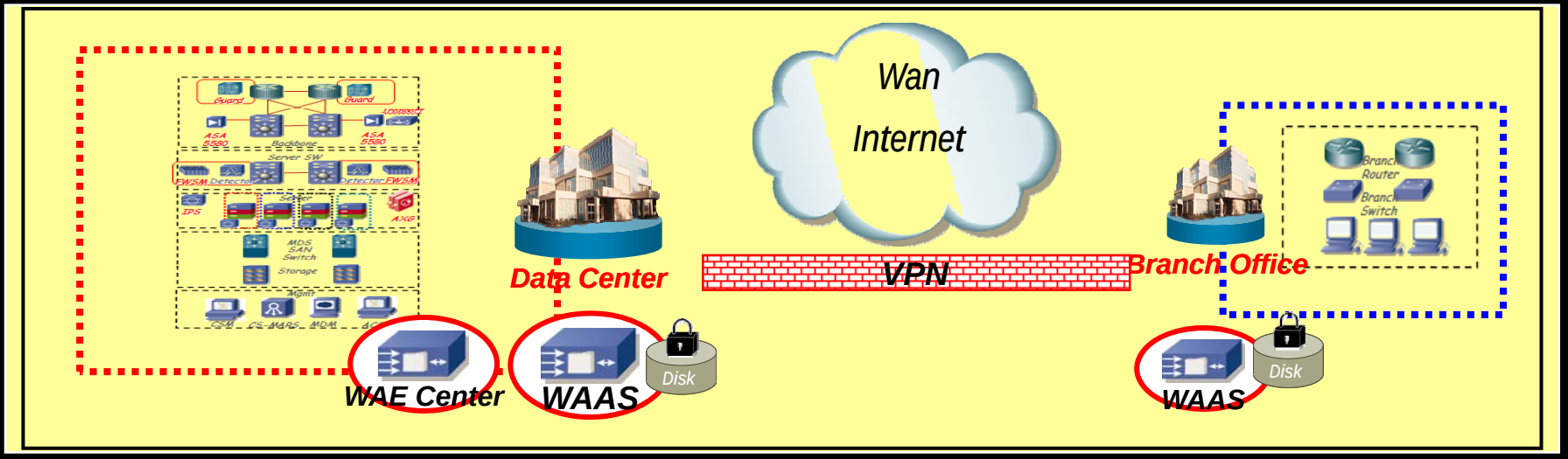
❑ 주요 기능

- ❖ Role Based Access Control 지원
- ❖ Reflexive ACL, TCP/IP normalization, protocol fixup
- ❖ 다양한 어플리케이션 Deep Inspection
- ❖ TCP/SSL Offload
- ❖ 대역폭 최적화 기능 - Delta Encoding / Smart Image Optimization, HTTP Compression
- ❖ 응답속도 최적화 기능 - Flash Forward, Smart Redirect, Browser Connection Multiplexing

DC를 위한 Cisco Application 최적화 솔루션
Cisco WAAS 기반의 WAN 최적화



DC를 위한 Cisco Application 최적화 솔루션
Cisco WAAS 구성의 유연성



다양한 구성 방법

In Line
Out of Path–물리적구성 변경없는 간단한 적용

뛰어난 성능 및 확장성

Cisco ACE & WCCP 기반의 대규모 확장성
업계 최대성능의 WAN 가속 솔루션 보유

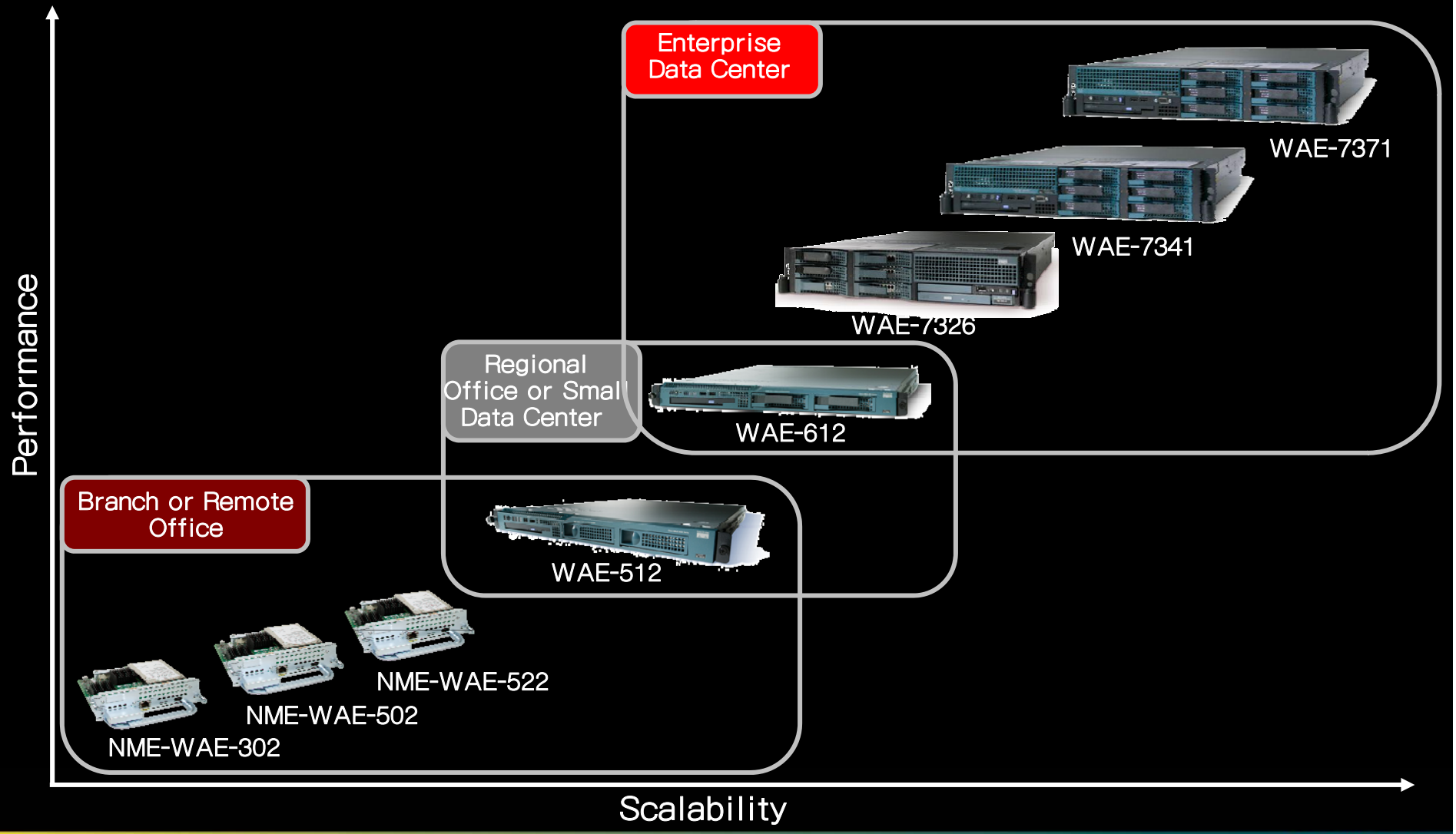
손쉬운 구성 설치

Auto Discovery – 자동 장비 인식 구성 기능
Center 통합 관리 – GUI 기반 센터 통합 구성 관리

DC 를 위한 맞춤형 솔루션

기존 기업의 보안과 QoS 변경 없는 구성
Disk 분실 시 안전한 데이터 보호를 위한 암호화

DC를 위한 Cisco Application 최적화 솔루션
Cisco WAAS 제품군 시리즈



DC를 위한 Cisco Application 최적화 솔루션
Cisco WAAS 주요 제품군

TCP Flow Optimization

LZ,DRE Compression

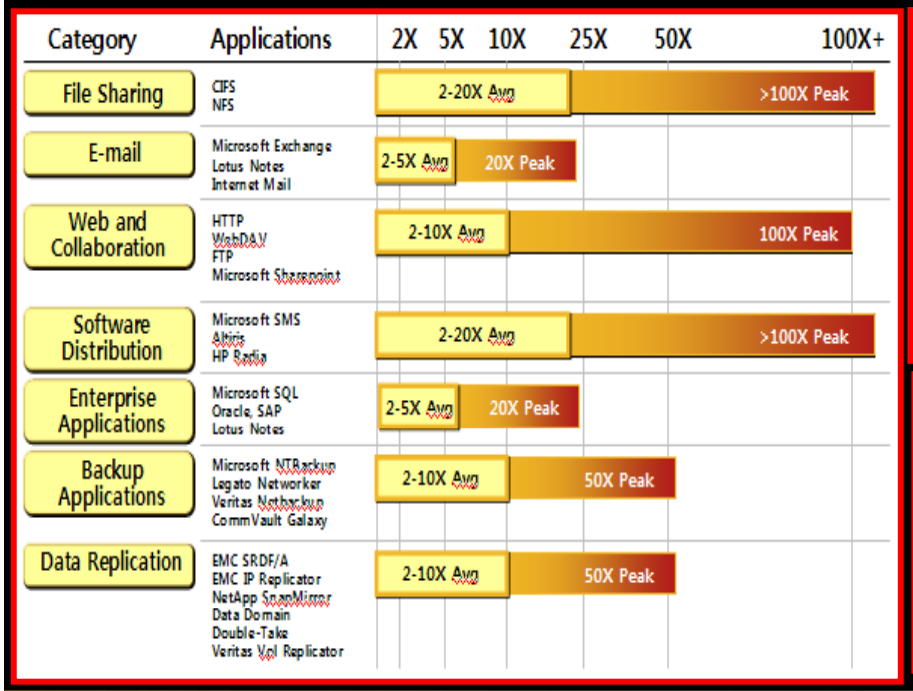
High Performance

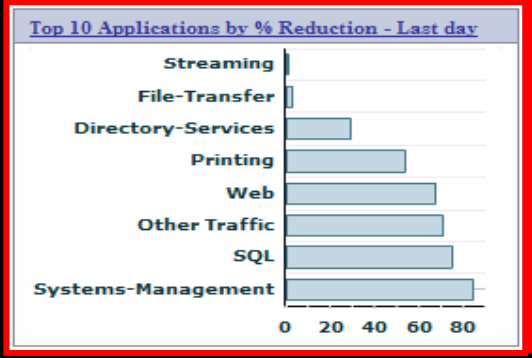
WAE 7341 / 7371

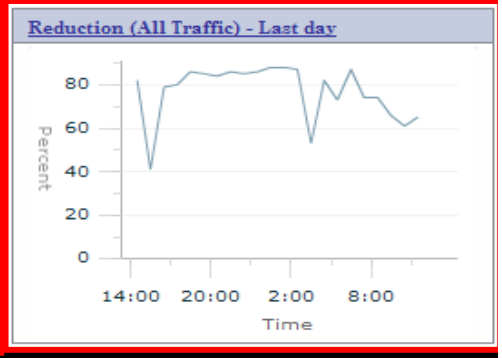
- WAE 7341
  - Dual Core Processor / 12G RAM **제공**
  - 310Mbps WAN Connection / 12K Optimized TCP Flow
  - 900GB RAID-5 / Hot Swap SAS Disk
  - TFO,DRE,LZ **기법** , Disk **암호화 등 제공**
  - In Path, WCCP/PBR **등과 연계한** Out of Path **구성 제공**
- WAE 7371
  - Dual quad-Core Processor / 24G RAM **제공**
  - 1Gbps WAN Connection / 50K Optimized TCP Flow
  - 1.5TB RAID-5 / Hot Swap SAS Disk
  - TFO,DRE,LZ **기법** , Disk **암호화 등 제공**
  - In Path, WCCP/PBR **등과 연계한** Out of Path **구성 제공**

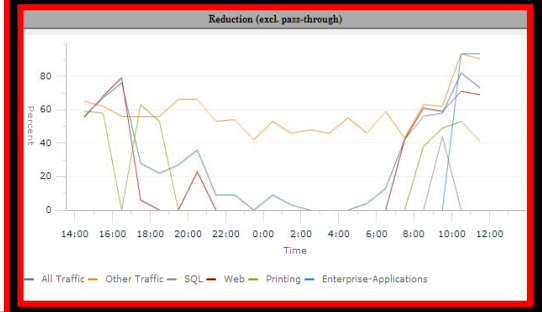
DC를 위한 Cisco Application 최적화 솔루션
Cisco WAAS를 통한 가시적 효과

- Web 2.0 기반 Application 응답 속도의 획기적 개선
- 고비용 WAN Infra의 대역폭 Save 을 통한 비용 절감 효과
- Intelligent Server Offload – Caching & Optimization
- Green DataCenter 구축 – Server Consolidation , 상면, Power, Cooling 감소 효과





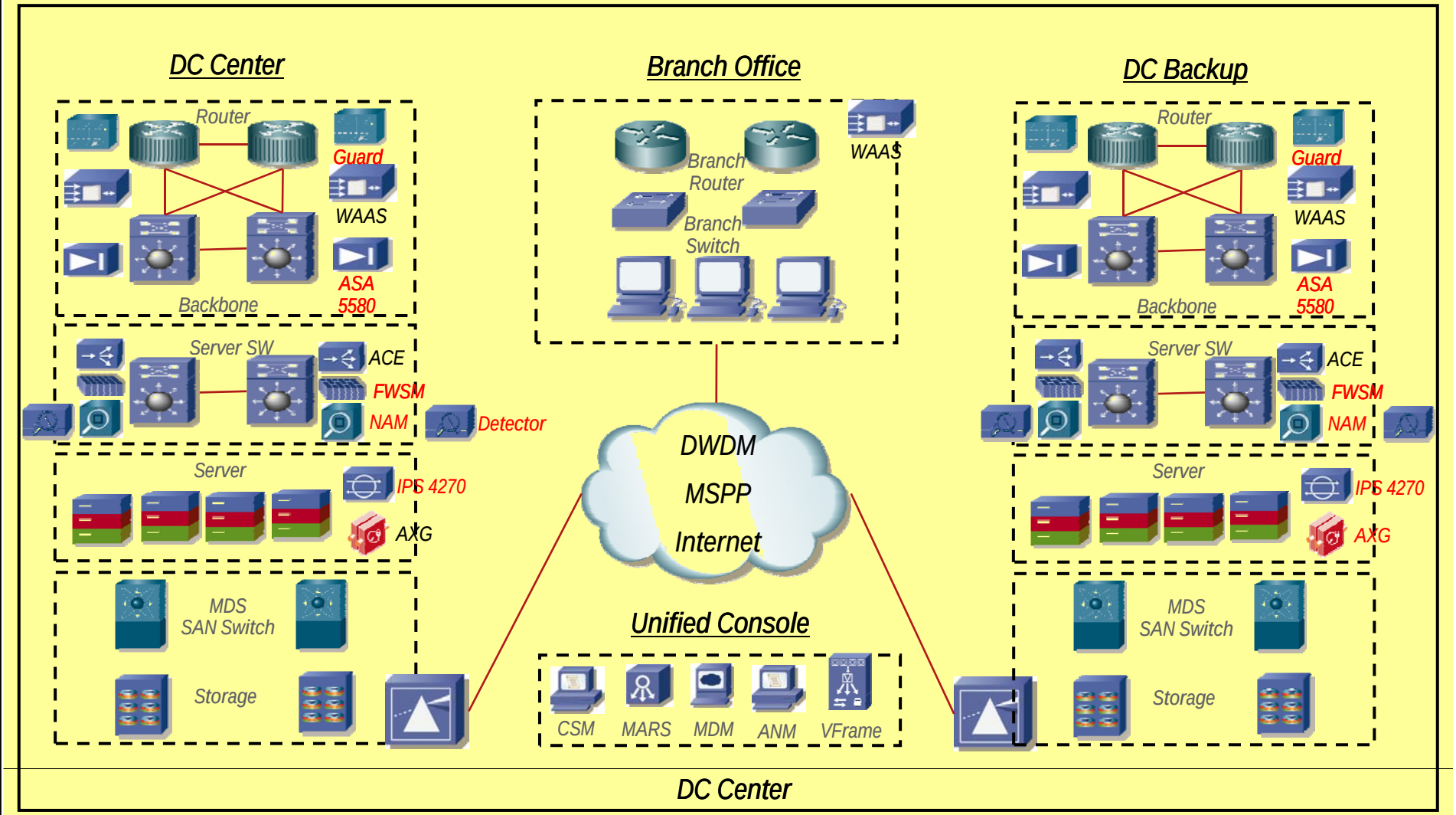


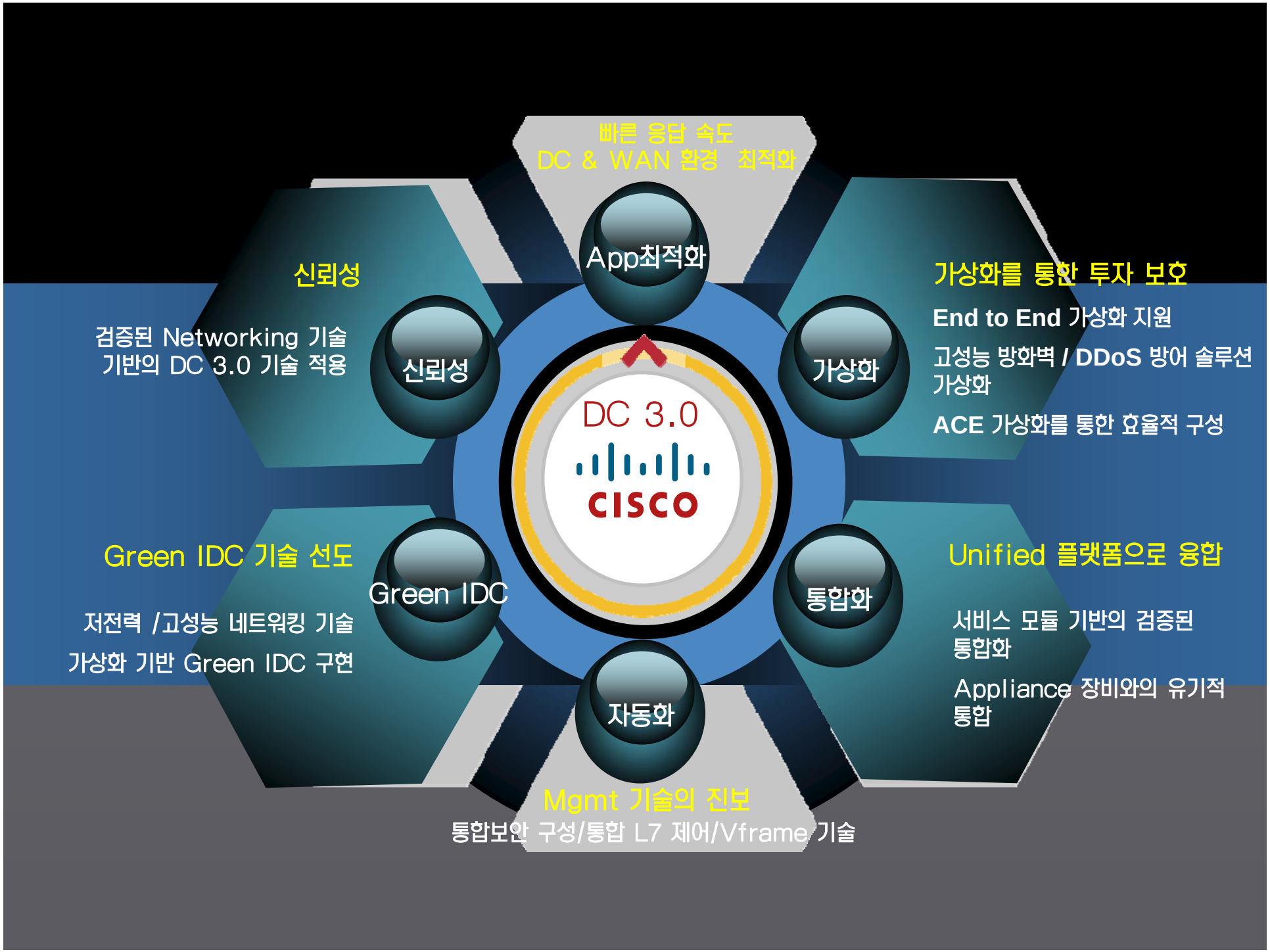


Cisco START!
Strategic Transformation Revolutionary Technology 2008

Cisco DataCenter 3.0
보안 / Application 최적화 서비스

데이터 센터 보안 및 어플리케이션 서비스 청사진
Cisco DC 3.0




빠른 응답 속도
DC & WAN 환경 최적화
App최적화
신뢰성
검증된 Networking 기술
기반의 DC 3.0 기술 적용
신뢰성
가상화를 통한 투자 보호
End to End 가상화 지원
고성능 방화벽 / DDoS 방어 솔루션 가상화
ACE 가상화를 통한 효율적 구성
가상화
DC 3.0
CISCO
Green IDC 기술 선도
저전력 /고성능 네트워킹 기술
가상화 기반 Green IDC 구현
Green IDC
통합화
Unified 플랫폼으로 융합
서비스 모듈 기반의 검증된 통합화
Appliance 장비와의 유기적 통합
자동화
Mgmt 기술의 진보
통합보안 구성/통합 L7 제어/Vframe 기술


CISCO