Borderless Network 4
Security and Video. Managed.

Unified Security

시스코 코리아, 김용호 차장

2011년 6월 14일

발표순서

- 시큐어 보더리스 네트워크 아키텍처의 진화
- 시큐어 보더리스 네트워크 솔루션 및 제품
- 시큐어 보더리스 네트워크의 적용
- 요약

시큐어 보더리스 네트워크의 진화

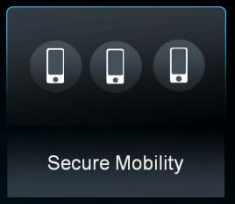
시큐어 보더리스 네트워크의 진화

아키텍처 기반의 새로운 프레임워크

프레임워크	 Secure Borderless Network	 Secure Mobility	 Secure Data Center	 Unified Security
솔루션		•ACSM •TurstSec v1.0	•Secure DC	•TrustSec v2.0
제품		•CSM 4.0	•ASA5585-X •AnyConnect 3.0 •VSG 1.0	•ISE 1.0 •ASA SM •ISR G2 ScanSafe
시기	2H’ 2009	1H’ 2010	2H’ 2010	NOW

Secure Borderless Network

Secure Moblity



내부 네트워크 환경

TrustSec 1.0

보안 및 정책

외부 네트워크 환경

AnyConnect Secure Mobility

로컬 데이터센터

본사

지사

ASA 5500

IronPort WSA

ScanSafe

NAC Appliance

ACS Appliance

Nexus

Catalyst Switch

고객

커피숍

재택근무

Software as a Service

Platform as a Service

Infrastructure as a Service

X as a Service

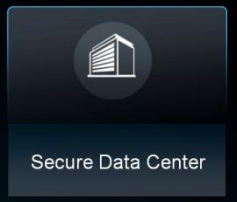
공항

모바일 사용자

해커

파트너

보안 플랫폼



Secure DataCenter

Cisco Secure Data Center

대용량	확장	단순화	보안성
ASA 5585-X	Virtual Security Gateway	AnyConnect TrustSec	Cisco SIO
NEW	NEW	ENHANCED	ENHANCED

Unified Security

신원 식별 엔진(Identity Service Engine) 기반 TurstSec 2.0

네트워크 정책 집행

트러스트섹 플래닝 및 서비스

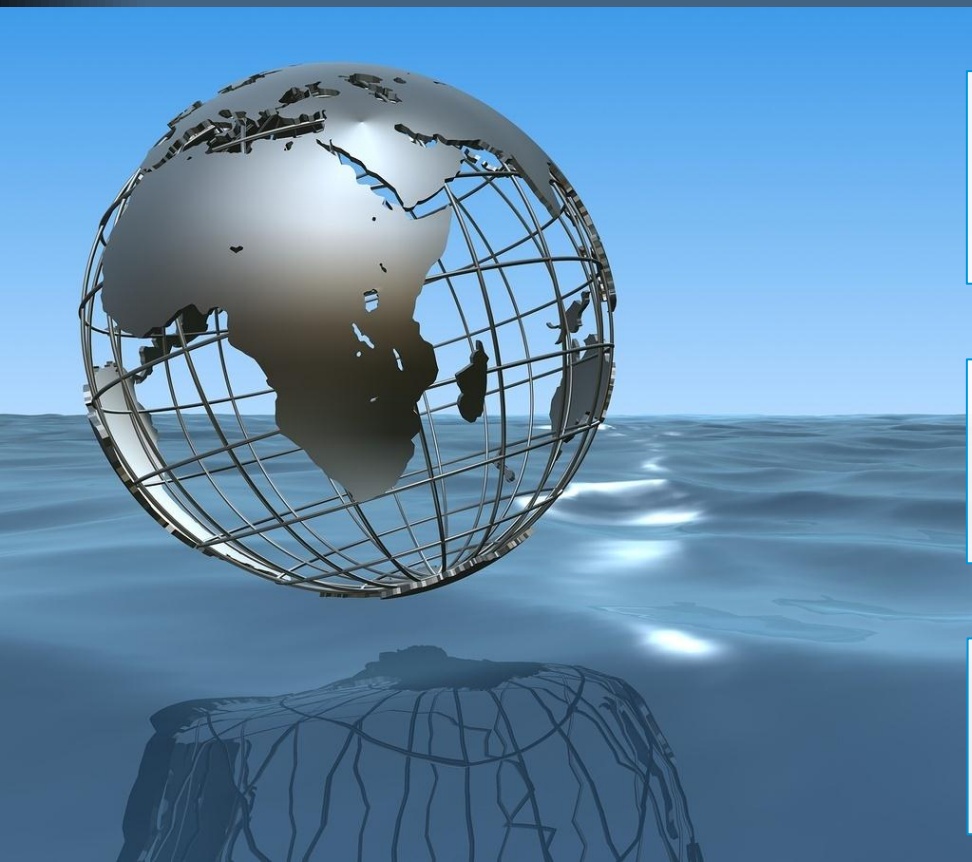
시큐어 보더리스 네트워크 솔루션 및 제품

TrustSec Solution

건강한 내부네트워크 유지를 위한 보안솔루션

Unified Security

Cisco TrustSec Solution 은 건강한 내부네트워크 유지를 위해 **신원기반의 네트워킹**및 **정책기반의 접근 통제**, **데이터 무결성 및 기밀성**을 제공하기 위한 솔루션



신원기반 네트워킹

- 속성별 접근 통제(802.1X, 시간, 위치, 단말기)
- 게스트 관리(NAC Guest Server)
- 디바이스 관리(NAC Profiler)

정책기반 접근통제

- 역할기반 그룹정책 적용(SGACL)
- Tagging 이용한 손쉬운 정책 관리 및 적용 (SGT,ACS 5.2)

데이터 무결성 및 기밀성

- NAC Server 을 통한 보완조치 및 접근통제
- MACSec 을 이용한 L2 기반의 암호화

TrustSec Solution
동작 방식

SecureX
Unified Security

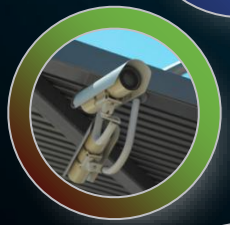
NAC Appliances

802.1x/Infrastructure

신원 정보	상황 정보	접근 통제

나 직원
내부직원, 마케팅부서
유선랜 연결
오후 3시

이 손님
방문객, iPad
무선랜 연결
오전 9시



보안카메라
Agentless 자산
MAC: F5 AB 8B 65 00 D4

오 컨설
외부 컨설턴트
본사,전략기획
무선랜 연결
오후 6 시

Group:
내부직원

Group:
계약직원

Group:
방문객

+

보안상태

접속위치

접속일시

기기 종류

접속 방식

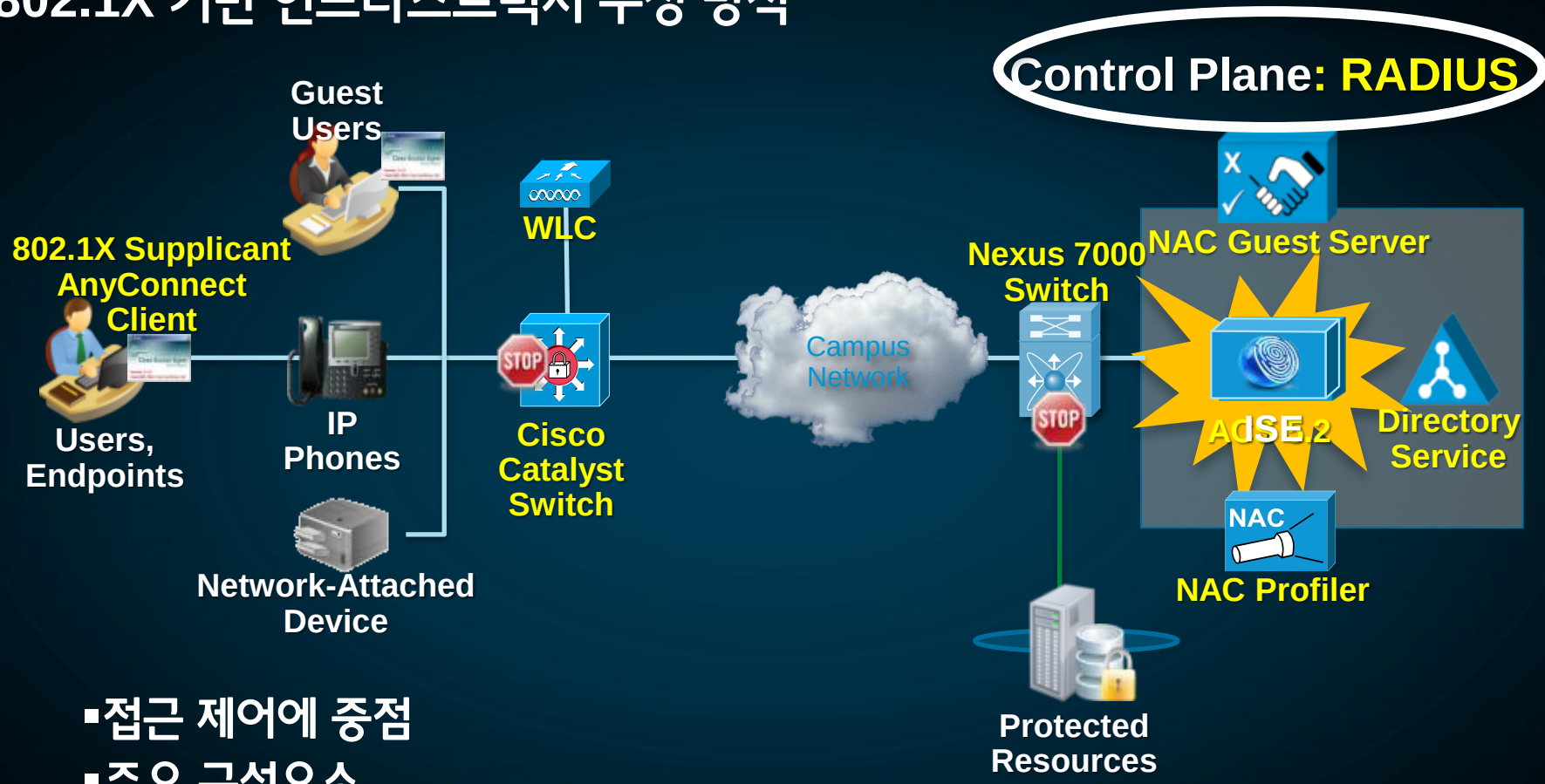
- 내외부 연결
- 제한된 연결
- 인터넷 연결
- 검역소
- 연결 차단

컴플라이언스
리포팅

ENHANCED

TrustSec 2.0

802.1X 기반 인프라스트럭처 구성 방식



- 접근 제어에 중점
- 주요 구성요소
  - ✓ACS 5.2
  - ✓AnyConnect Secure Mobility Client 3.0 or 802.1X Supplicant
  - ✓802.1X-enabled Cisco Catalyst and Nexus switches

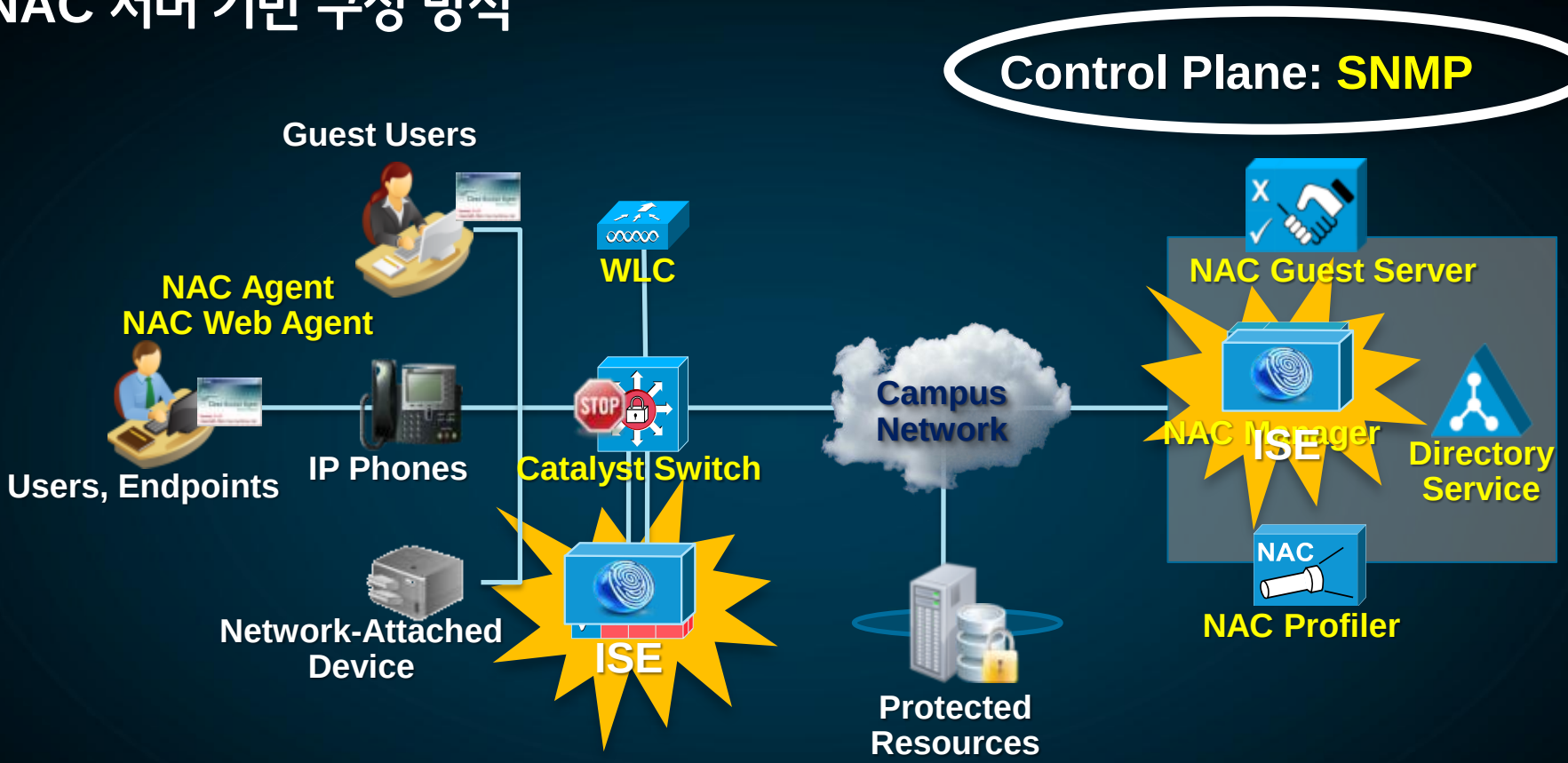
ENHANCED

TrustSec 2.0

NAC 서버 기반 구성 방식

SecureX

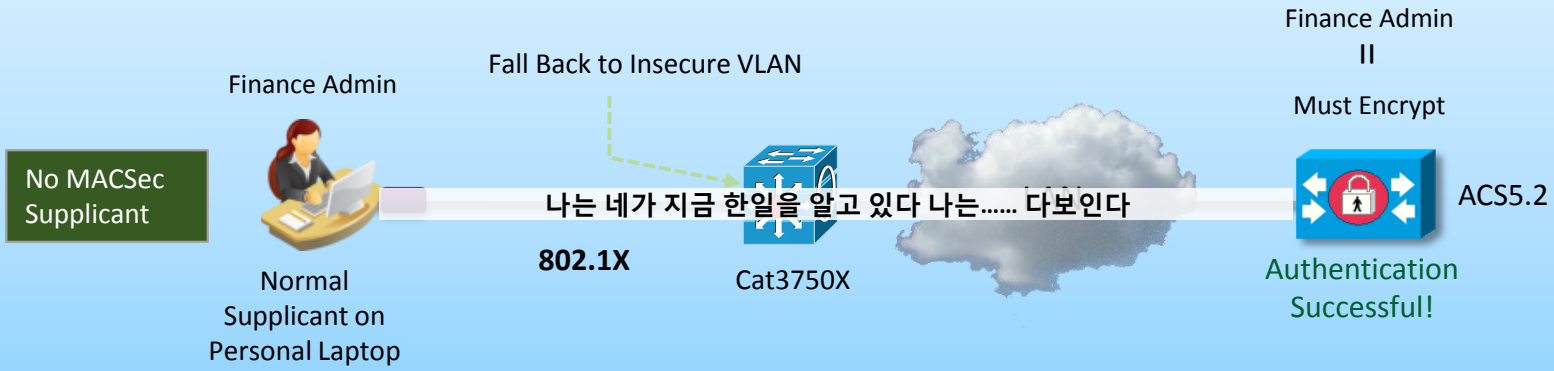
Unified Security



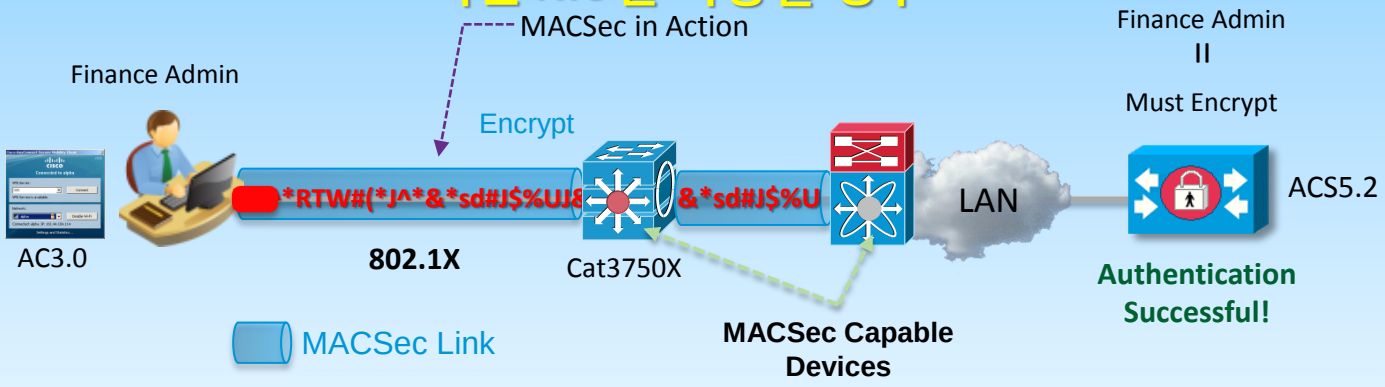
- 무결성 점검 및 치유에 중점
- 주요 구성요소
  - ✓NAC Manager
  - ✓NAC Appliance
  - ✓NAC/Web Agents

TrustSec 2.0
LAN 기반 데이터 기밀성 확장

타사 또는 OS 제공 기본 Client 사용시



AnyConnect 3.0 또는 MACSec 지원 NIC 을 사용할 경우



TurstSec 2.0
구성요소

Unified Security

인프라 구성요소

C6500/4500

C3560X/3750

Nexus 7K/5K

X

정책 및 보안 구성요소

NEW

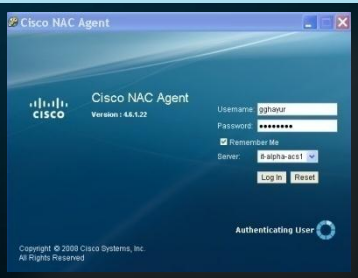
Identity Service Engine 1.0

Cisco 1121 Secure Access Control System 5.2

NAC Manager, NAC Server, NAC Profiler, NAC Guest Server

엔드포인트 구성요소

AnyConect 3.0 Client S/W



NAC Agent

업그레이드 및 마이그레이션

- 기존 NAC 및 ACS H/W 에 업그레이드 가능(1121/3315/3355/3395)
- 기존 H/W 장비에 대한 높은 할인율이 적용된 마이그레이션
- 모든 소프트웨어 라이센스에 대한 마이그레이션 라이센스 지원
- 기존 데이타 및 설정 마이그레이션 툴 제공 예정

Identity Services Engine

투자 보호

ASA Service Module NEW

대용량 고속 통합 보안 스위칭

Unified Security

- ASA v8.4.1 과 동일한 방화벽 기능
- 고성능 및 대용량 방화벽 서비스 모듈
- ASA 어플리안스와 동일한 설정 및 관리 인터페이스 제공
- 모든 ASA 제품군 OS 와 동일한 업그레이드 및 패치 시기 동기화

항목	성능 수치(FCS +6)
샤시 성능(BPS)	80Gbps+
모듈 성능(BPS)	20Gbps
최대 동시 커넥션수	1,000만 세션
최대 초당 신규 커넥션수(CPS)	35만 CPS
가상방화벽	250개
VLANs	1024

ASA Service Module

NEW

Catalyst 6500 Switches 지원 환경

Unified Security

CAT6k chassis

- WS-C6503-E: 3 slot chassis
- WS-C6504-E: 4 slot chassis
- WS-C6506-E: 6 slot chassis
- WS-C6509-E: 9 slot chassis
- WS-C6509-VE: 9 slot chassis

Supervisor cards

- VS-S720-3C-10GE
- VS-S720-3CXL-10GE
- • WS-SUP720-3B
- • WS-SUP720-3BXL

SUP2T Supervisor card post FCS

Cisco IOS Software Release

12.2(33)SXJ or later.

Cisco ScanSafe Cloud Services

Unified Security

웹 필터링 서비스

- 웹 사용 통제
- 웹 기반 어플리케이션 사용 가시화 및 통제
- In, Out-Bound 적용

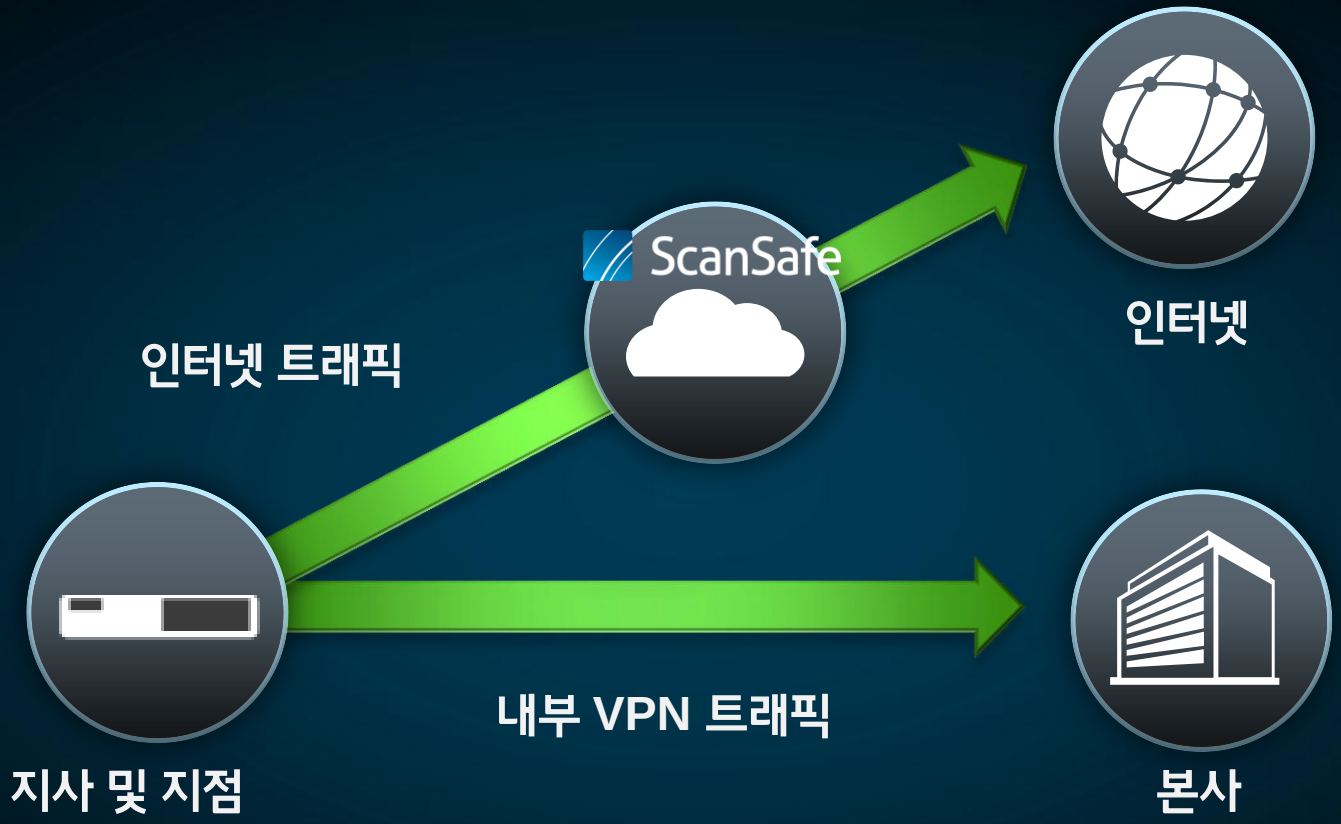
웹 보안 서비스

- 봇 등 악성 코드 차단
- 웹 컨텐츠 분석 및 통제
- 스크립트 에뮬레이션

중앙 리포팅

안전한 이동 업무 환경 지원

Cisco ScanSafe Integration with ISR G2



- 유연하고 간단한 구성 방식 → 지점 PC에 프록시 설정 및 Agent 설치 필요 없음
- 지사 및 지점의 인터넷 사용에 대한 통제 및 통계
- 인터넷 트래픽과 본사 업무용 트래픽 완벽 분리 →
- 트래픽 사용에 대한 효율적이면서도 안전한 관리

ISR G2 + ScanSafe 지원 기능

- IOS 보안 기능(SEC) 라이센스에서 지원
- ISR 880, 890, 19XX, 29XX and 39XX/E ISR G2 플랫폼에서 지원
- HTTP/HTTPS 트래픽 리다이렉션 지원
- 지점 및 지사 PC의 프록시 설정 및 별도의 Client 프로그램 설치 필요 없음

ISR G2 + ScanSafe 지원 기능

- LDAP 또는 AD sync를 통한 싱글사인온 기반 신원 식별 및 정책 적용
- ScanCenter 웹포탈 서비스를 통한 사용자 관리 및 설정, 다양한 통계 보고서 생성
- 기존 IOS 기반 방화벽 및 IPS 기능과 독립적이며, 동시 사용 가능

시큐어 보더리스 네트워크의 적용

국내 주요 보안 동향
2011년 9월 개인정보보호법 시행

현 행

29조 ~ 34조

- 기술적/관리적 및 물리적 보호 조치
- 처리방침 수립, 책임자 지정
- 개인정보 영향평가, 유출 통지

- 공공기관은 컴퓨터 등에 의해 처리되는 개인정보 파일만을 보호대상

- 분야별 개별 법에 따른 처리기준 존재

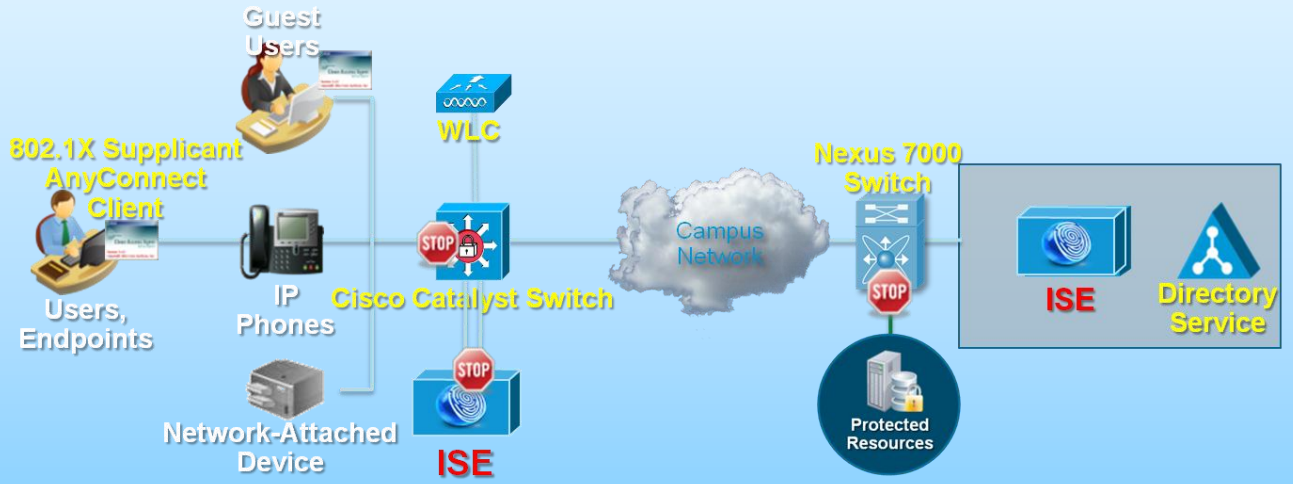
정보통신	정보통신망 이용 촉진 및 정보보호 등에 관한 법률
공공행정	공공기관의 개인정보 보호에 관한 법률
금융신용	신용정보의 이용 및 보호에 관한 법률
의료	의료법, 생명윤리및안전에관한법률 응급의료에관한법률

제 정

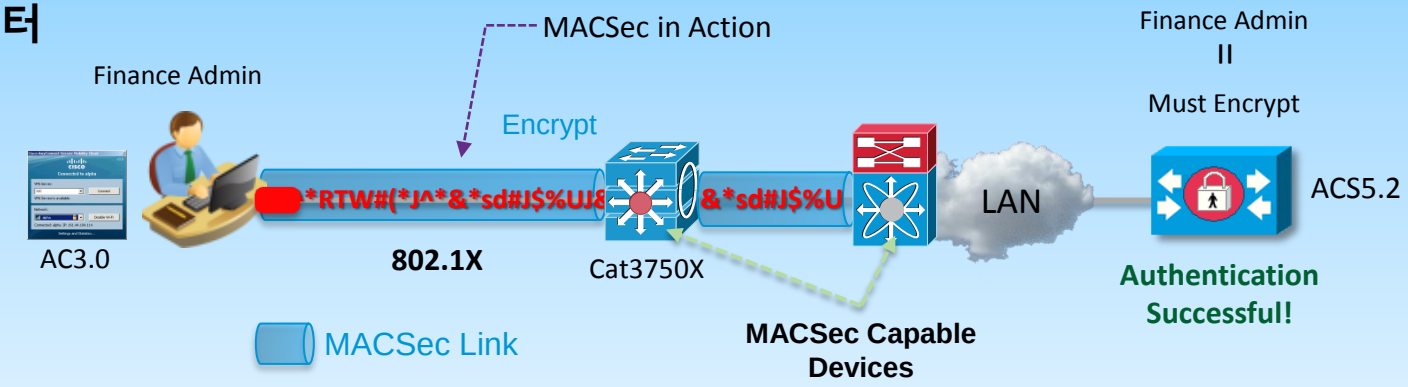
- 개인정보보호법 공포(2011. 3. 29) 및 시행(2011. 9. 30), 총 9장 75조
- 공공·민간 통합 규율로 법 적용대상 확대
- 현행법 적용을 받지 않던 오프라인 사업자, 의료기관, 협회·동창회 등 비영리단체, 국회·법원·헌법재판소·중앙선거관리위원회 등으로 확대
- 동사무소 민원신청서류 등 종이문서에 기록된 개인정보도 보호대상에 포함
- 공공·민간을 망라하는 개인정보처리 원칙과 기준 제시

개인정보보호법 대비 TrustSec 의 적용
내부 네트워크 접근 통제/감사 및 기밀성 확보

- 사용자 또는 디바이스 인증을 통한 신원식별
- 신원 및 접근 대상 자원별 접근 통제
- 인증 및 접근 기록/감사



- LAN상의 단말에서 부터 중요 자원 접근까지 암호화를 통한 기밀성보장
- 기존 VPN 과 동일한 수준의 암호화 제공



국내 주요 보안 동향

비디오 및 데이터 트래픽의 급증 및 중앙집중화

국내 주요 보안 동향

비디오 및 데이터 트래픽의 급증 및 중앙집중화

고속대용량 UTM ASA5585-X 및 ASA SM

데이터센터 트래픽 집중화에 안전한 고속 대용량 트래픽 처리

350,000 connections per second

10 million connections

20Gbps multi-protocol Firewall throughput

10Gbps IPS+FW

35Gbps large packet throughput

2Rack Units

350,000 connections per second

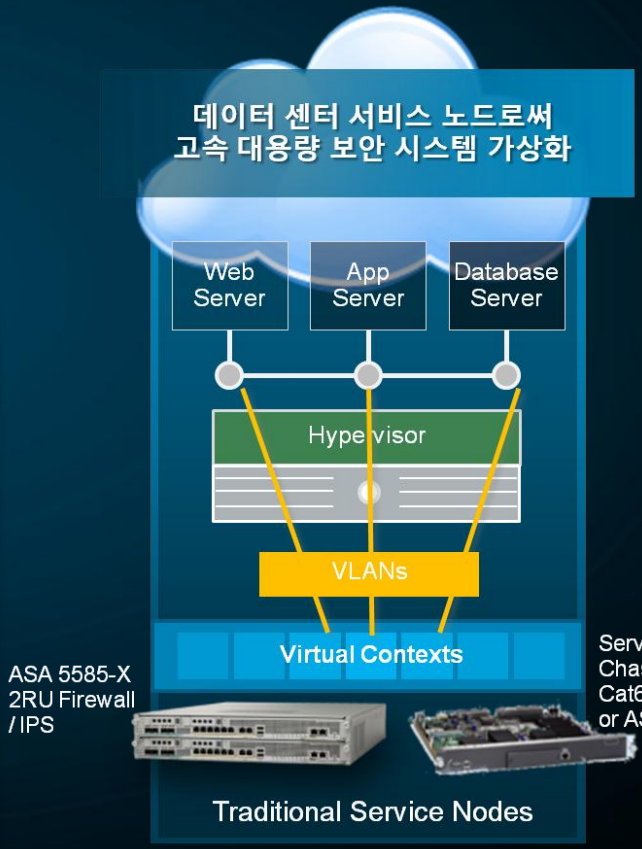
10 million connections

20Gbps multi-protocol Firewall throughput

Max 4 Module Per 1 C6K

Max 80Gbps Firewall Throughput

Max 1.2M CPS



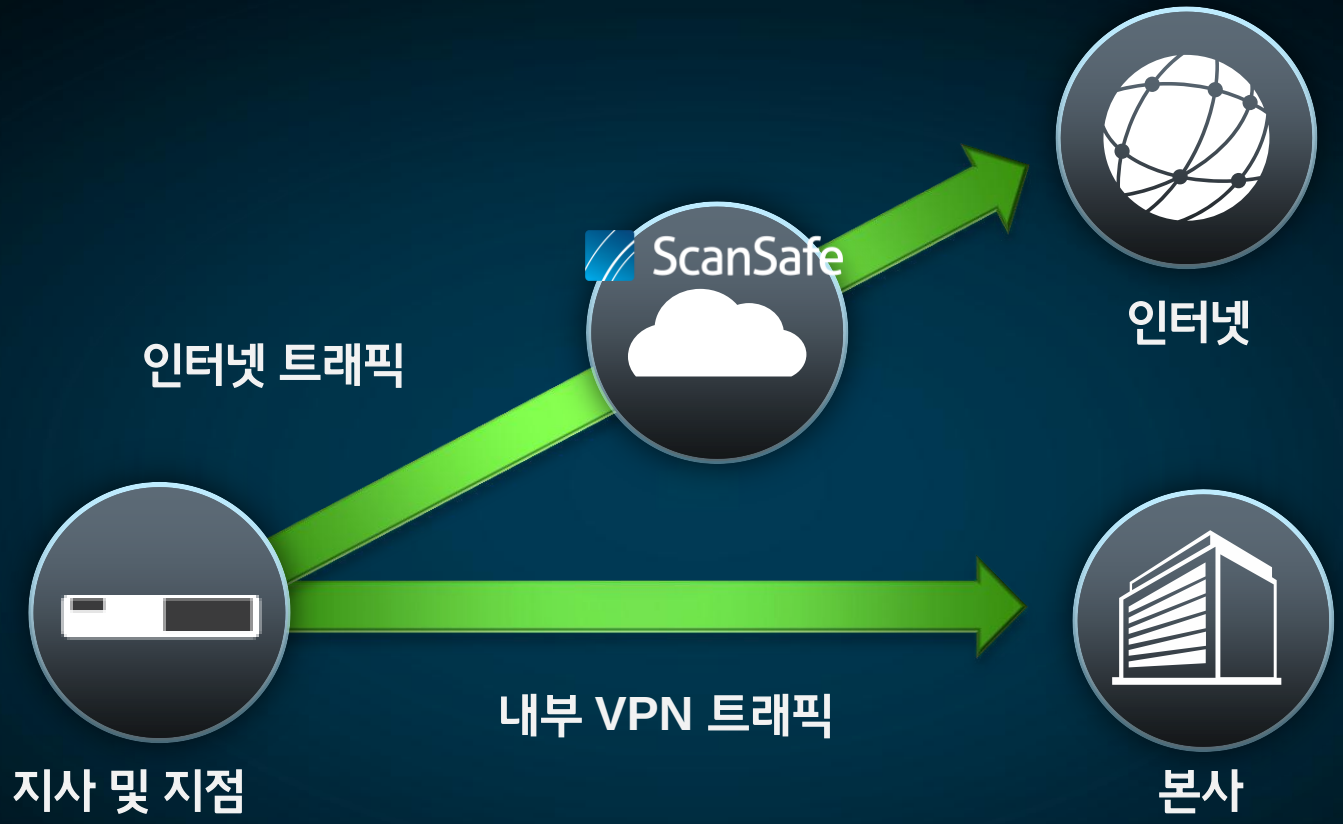
국내 주요 보안 동향

지점 및 지사 악성코드감염 및 정보 유출

- 본사와 연결된 망을 통한 정보 송수신
- 지사 및 지점의 보안 이슈
  - 내부자 고의 또는 실수로 인한 정보 유출
  - 인터넷상의 웹 서비스 및 어플리케이션을 통한 악성코드 감염

→ 지사 및 지점에서의 정보 유출

ISR G2 with ScanSafe 적용
지사 및 지점 정보 유출 및 악성코드 차단



- 본사 망에서 획득된 정보 또는 지사 내에 보관된 중요 정보의 유출 방지
- 지사 및 지점의 인터넷을 통한 웹서비스 및 어플리케이션 사용 통제
- 악성코드 감염으로 인한 2차 피해 차단

감사합니다.