# 2012 Cisco Plus Korea

Plus for your intelligent business and competitive advantage

# BYOD를 위한 시스코 시큐리티 솔루션

cisco

# BYOD 환경하의 보안 고려사항

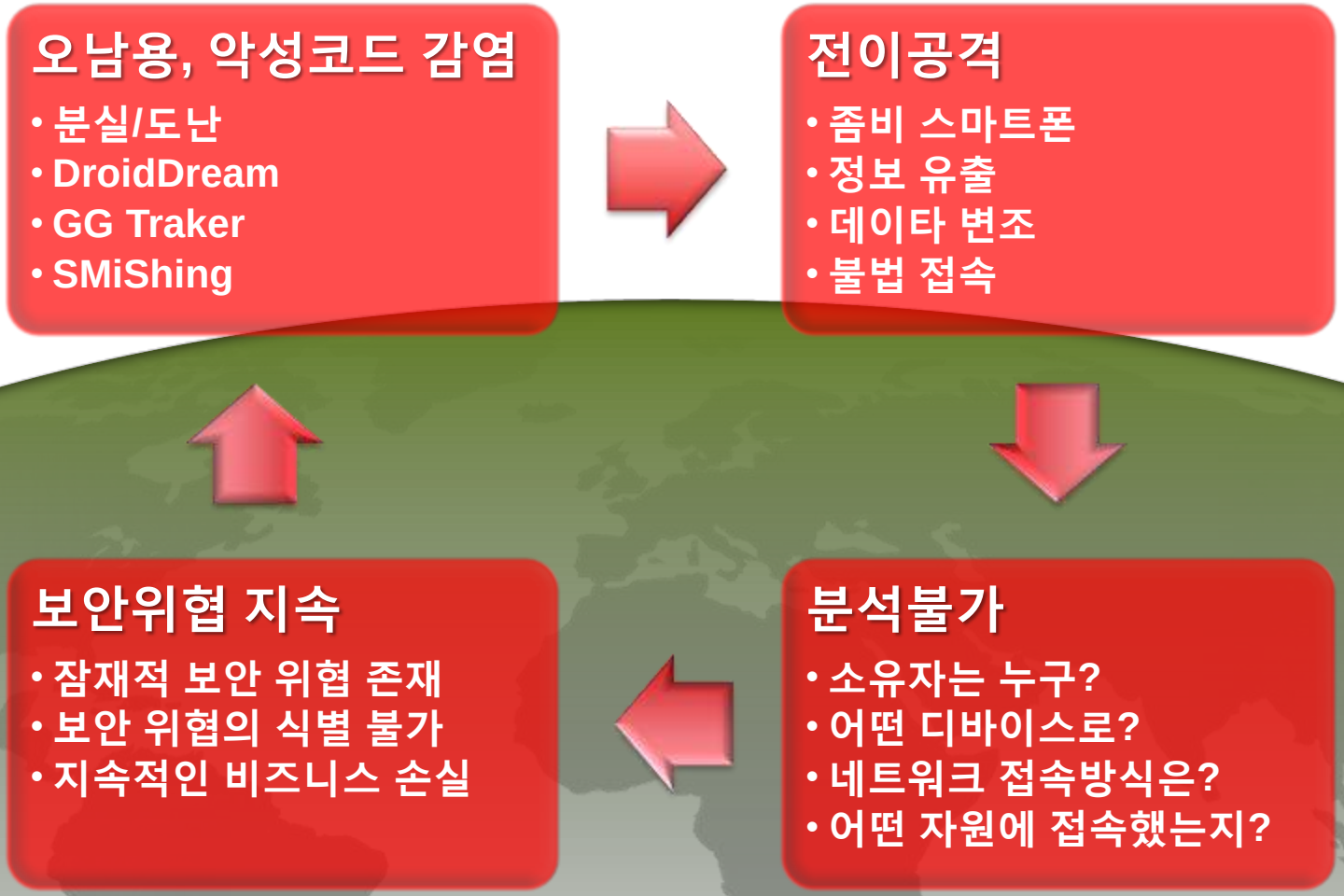
# Bring Your Own Device !!

커뮤니케이션 방식의 다양화

# 네트워크가 곧 새로운 업무환경

# 더욱 다양해지고 복잡해진 보안 위협

# 발생가능한 보안사고시나리오
# 악순환의 연속



# 누가, 무엇이 그리고 어떻게 네트워크 접속을 제어할 것인가?

# 시스코 BYOD 보안 솔루션 중점사항

**상황 인식 기반 통합인증**

"누가 그리고 무엇이 네트워크상에 있는가?"

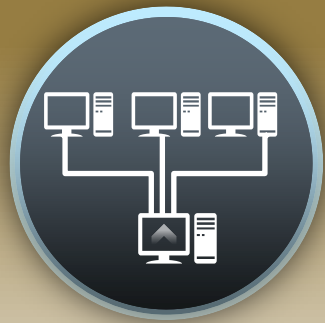
**상황 인식 기반 접근제어정책**

"어떤경우에 무엇을 접속할 수있게 할것인가?"

**확장성, 보안성**

"네트워크상 어디에서, 누구에게 어떤 보안을 적용할 것인가?"

**통합 운영 관리**

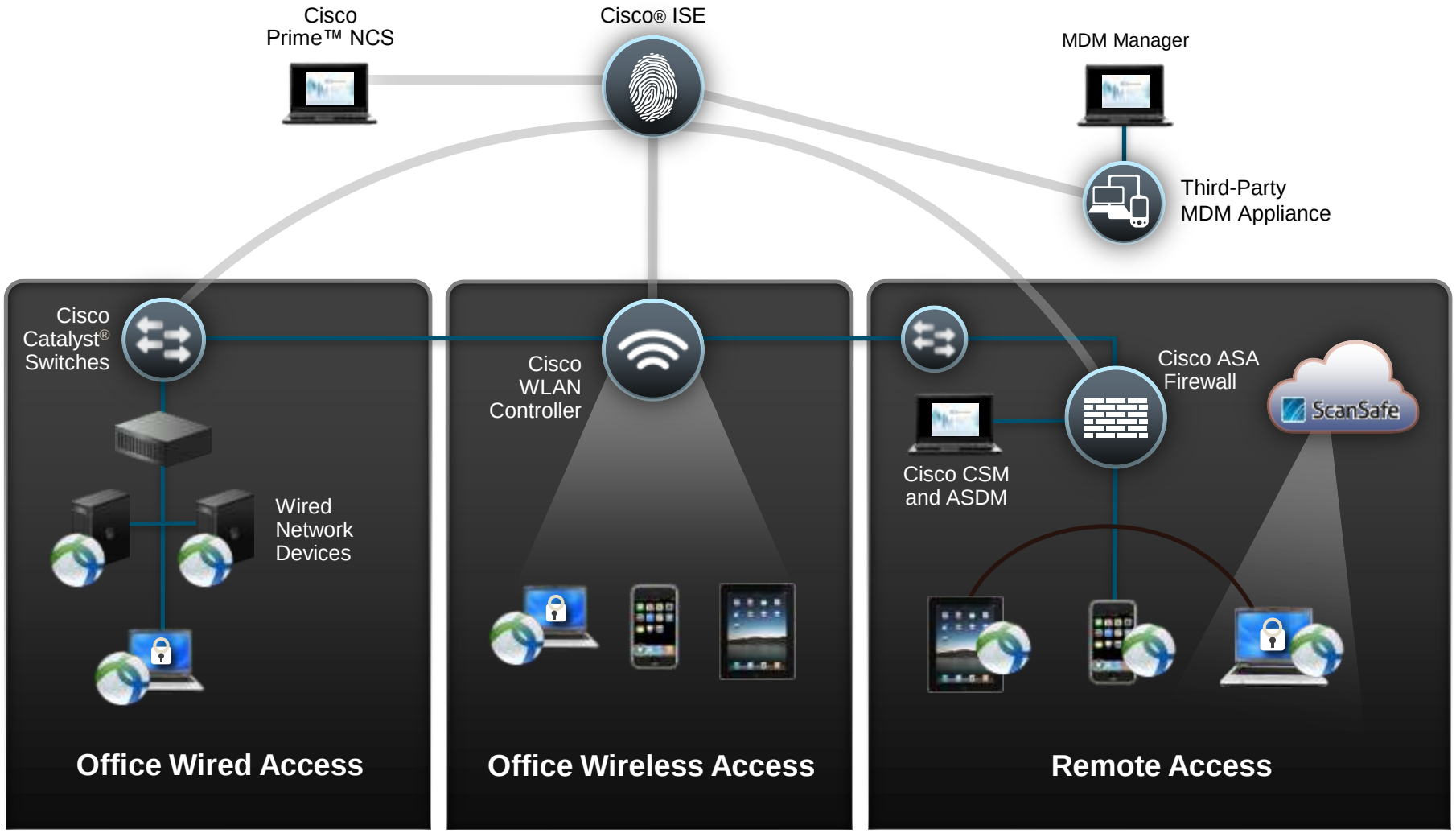


"운영 관리는 어떻게 할 것인가?"

상황인식 기반의 네트워크 통합 접근 제어

# 시스코 엔드투 엔드 BYOD 보안 솔루션

## 유선, 무선 및 원격접속까지 모든 접속환경에 대한 통합솔루션



# 시스코 BYOD 보안 솔루션

# 1.누가 그리고 무엇이 네트워크상에 있는가?

수작업 형태의 기기 식별 및 정책 적용

## 일반적인 기기 식별 및 인증 적용 시나리오

유,무선 및 원격 접속 등
각 네트워크별 기기식별
및 인증 방식 별도 운영

IP 단위의 접근 및 접속
제어 정책 적용

수작업 또는 IP 관리
솔루션에 의한 등록기기
MAC 관리

## 문제점

사용자별 기기수 증가
기기의 잦은 변경
기기별 접근 제어 난이

# 상황인식 기반 통합 인증

## 인프라스트럭처를 이용한 자동화된 기기 구분 및 식별

802.1X
MAB
WebAuth

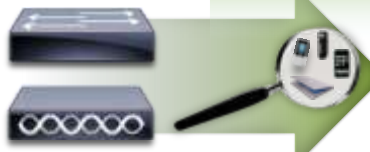
스위치, 라우터, 무선랜 억세스 포인트

### 속성별 인증방식 적용



### 자동 프로파일링

네트워크기반
디바이스센서




동적인
디바이스
스캐닝

## 해결방안

인프라스트럭처를
활용한 효과적인 기기
자동 식별 및 속성별
유연한 인증방식 적용

## 자동 프로파일링기술 적용 시나리오

**수집**

스위치에서 기기에 대한
정보 수집후 ISE로 리포팅

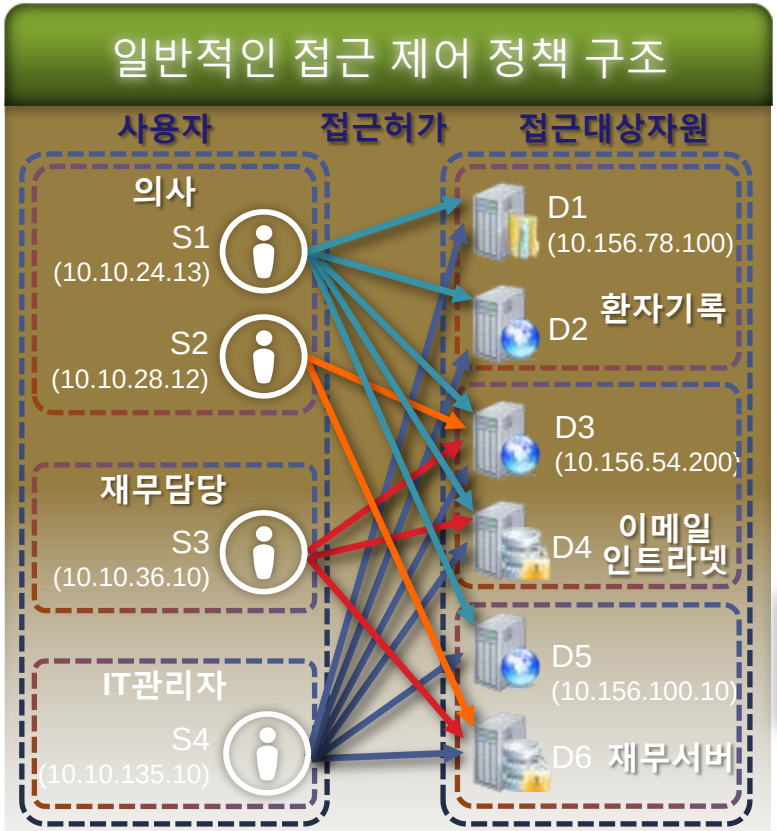
**식별**

ISE 디바이스 식별 및 플로우
정보 수집, 사용량에 대한
보고서 제공

**인증**

ISE 가 사용자 및 디바이스
정보 조합에 따른 차별화된
인증 방식 자동 적용

# 2. 어떤경우에 무엇을 접속할 수있게 할것인가?





## 일반적인 접근 제어 정책 적용 시나리오

사용자 IP 별 또는 기기 IP 대역별 단순 접근 제어 정책

보안 등급 없이 서비스 단위 접근대상 그룹화

사용되지 않는 정책에 대한 수작업 정리

## 문제점

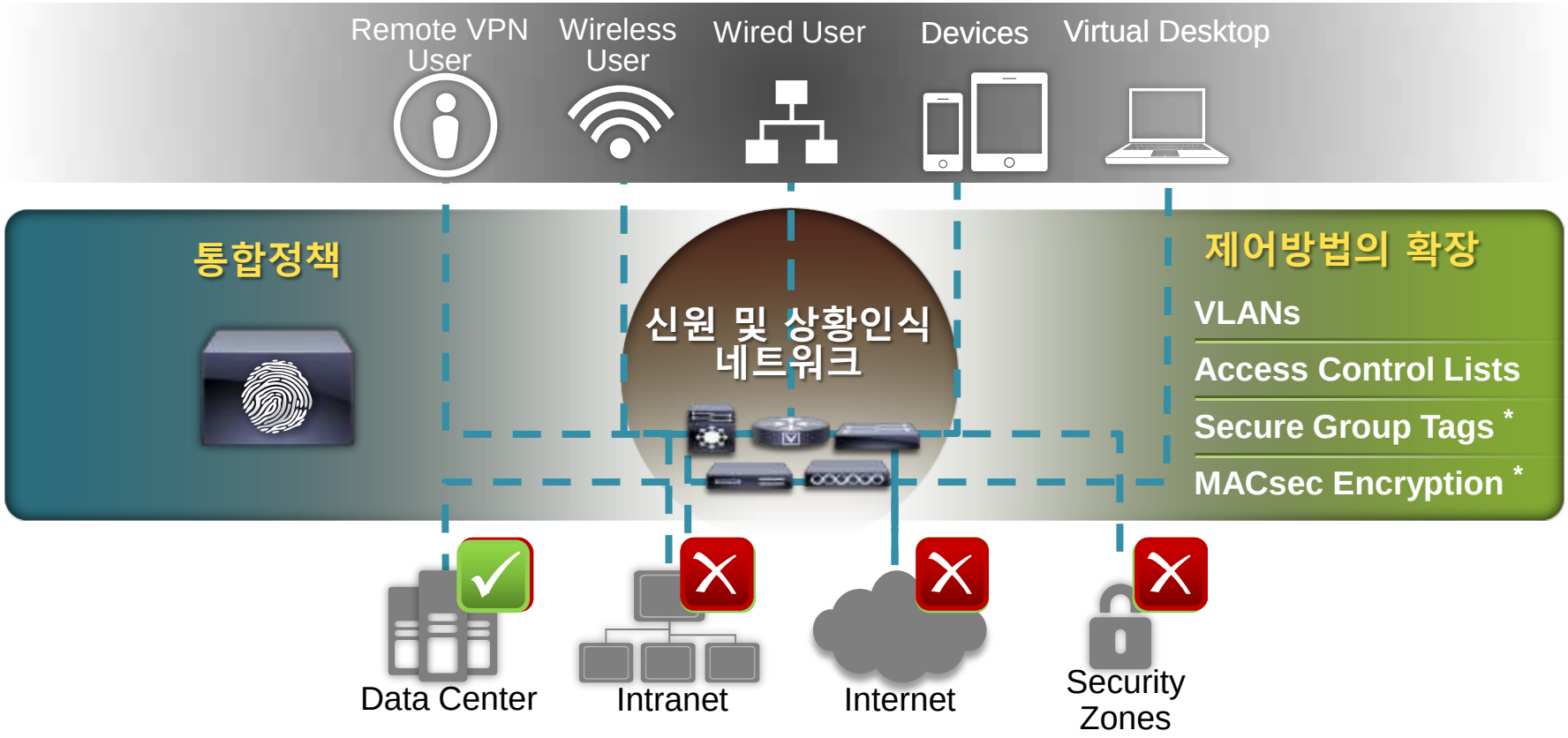
단순 IP기반 제어의 한계

정책의 복잡성 가중

잦은 변경에 따른 오류

# 상황인식기반 접근 제어 정책

## 다양한 속성의 상관관계 분석후 상황에 맞는 접근 제어 정책 자동 적용




### 해결방안

다양한 접근속성의 조합에 따라 인식된 상황별 접근자동제어

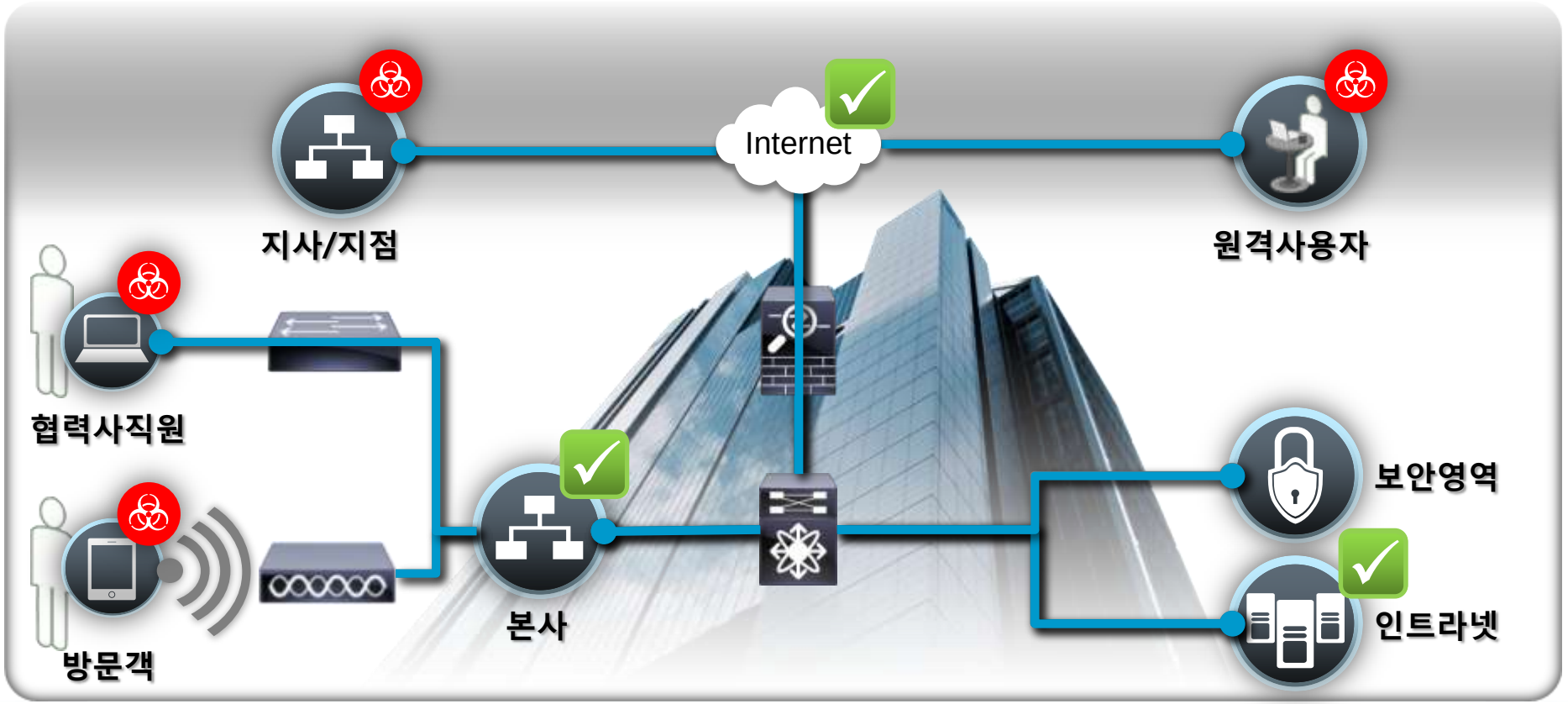
### 상황인식기반 접근 제어 정책 적용 시나리오

통합정책서버에서 상황별 접근 제어 정책 설정

다양한 접근 속성 조합별 상황에 따라 제어 방법 자동 선택

최종 접근 대상별 접근 제어 정책 적용

# 3. 네트워크상 어디에서, 누구에게 어떤 보안을 적용할 것인가?




## 일반적인 보안 적용 시나리오

방문객 모바일 기기
인증없이 인터넷 접근
허가 정책 상시 적용

협력사직원용 계정 생성
인터넷 및 제한된
인트라넷 접근 허가정책
추가

지사/지점 및 원격사용자
VPN 연결, 별도 접근제어
없음

## 문제점

사용자 식별불가
계정관리 안됨
접근위치에 따른 보안홀

# 확장성

## 임시계정 등록에서 폐기까지 시스템화된 라이프사이클 관리

**임시계정 라이프사이클**

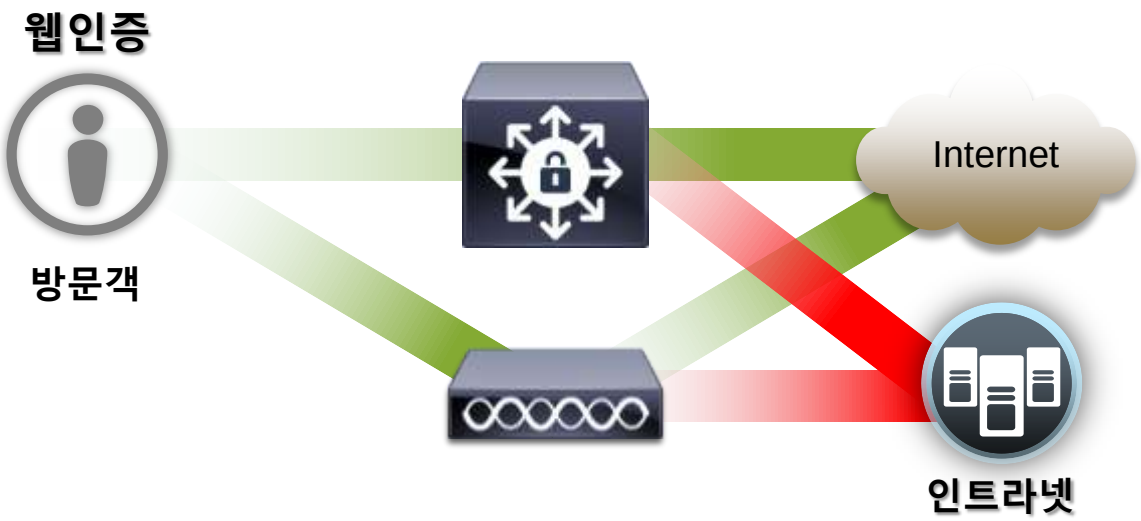
생성 | 알림 | 관리 | 보고

**임시계정 접근제어정책**

유무선 접속 인증

인터넷 접근허가

내부 접근제한




### 해결방안

임시계정 관리 포털을 통한 관리 및 자동 폐기, 내부 사용자 계정관리와 독립된 절차를 시스템화

### 임시계정 라이프사이클 관리 적용 시나리오

**생성**
임시계정 관리 포털 로그인후 계정 생성

**알림**
생성된 계정정보를 SMS, 이메일등으로 통보

**관리**
스폰서 및 계정 권한, 사용기간 설정 및 연장, 기한 전 폐기

**보고**
임시계정 사용 및 접속정보 로깅

# 보안성

## 언제 어디서나 안전한 접속 및 보안 정책 적용


### 해결방안

원격사용자, 지사 및 지점의 접근대상별 트래픽 암호화 및 컨텐츠보안적용

### Always On Security 적용 시나리오

**트래픽의 분리**

업무목적의 회사자원 접근용 트래픽과 인터넷 트래픽 분리

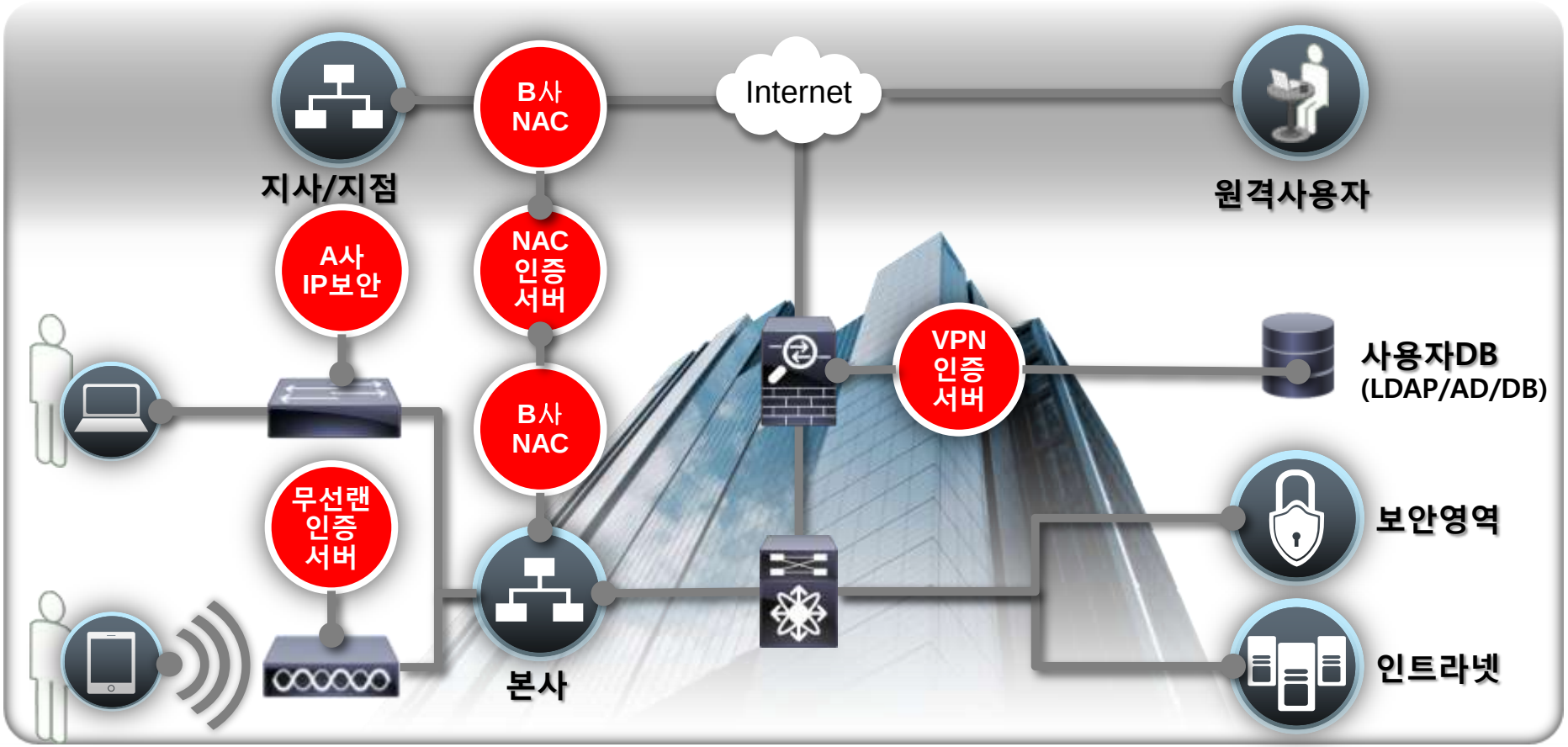
**암호화**

업무트래픽에 대해서 IPSec, SSL 및 L2TP 중 사용가능한 VPN 적용

**컨텐츠 보안**

클라우드 기반 보안 서비스를 통해 인터넷 사용시 악성코드 및 오남용 차단

# 4. 운영 관리는 어떻게 할 것인가?




## 일반적인 운영 관리 시나리오

고정 IP 기반 단순 IP관리 솔루션

접속 대상별 인증서버 혼재

NAC을 도입했으나 무선랜 인증 용도로만 사용

## 문제점

솔루션별 독자적 로깅

실시간 통합모니터링 불가

사고발생시 추적 난이

# 통합 운영 관리

## 인증 및 접근제어 정책 설정 및 적용 통합

A사 IP보안 + B사 NAC + NAC 인증 서버 + 무선랜 인증 서버 + VPN 인증 서버

통합

관리 정책 모니터링

## 해결방안

통합 접근제어 관리시스템으로 간소화, 모니터링 및 포렌식 수준의 리포팅 확보

## 자동 프로파일링기술 적용 시나리오

**관리**

인증 속성 및 방식, 접근제어 정책 설정

**정책**

인증 및 인가, 기기 자동 프로파일링, 보안 상태 점검

**모니터링**

시스템 상태 및 접속 현황 실시간 모니터링, 접속 로깅과 리포팅

# 사례별 적용방안

# 기업 BYOD 업무 환경의 발전 과정


| 차단 또는 제한 | 허용 | 확장화 | 혁신화 |
| --- | --- | --- | --- |
| 회사 소유 기기만 허용 | 사용자 소유 기기 인터넷 접근허용 무인증 | 소유자 및 기기 관리 특정 어플리케이션 접근 허용, 인증 (예시:모바일오피스) | 신서비스 및 협업 솔루션 접근 허용 디바이스 보안 (예시:VDI, SaaS, 비디오컨퍼런싱, MDM) |

# 시스코 BYOD 솔루션

## 전통적인 업무환경에서 혁신적인 업무환경까지 단계별 맞춤 솔루션화

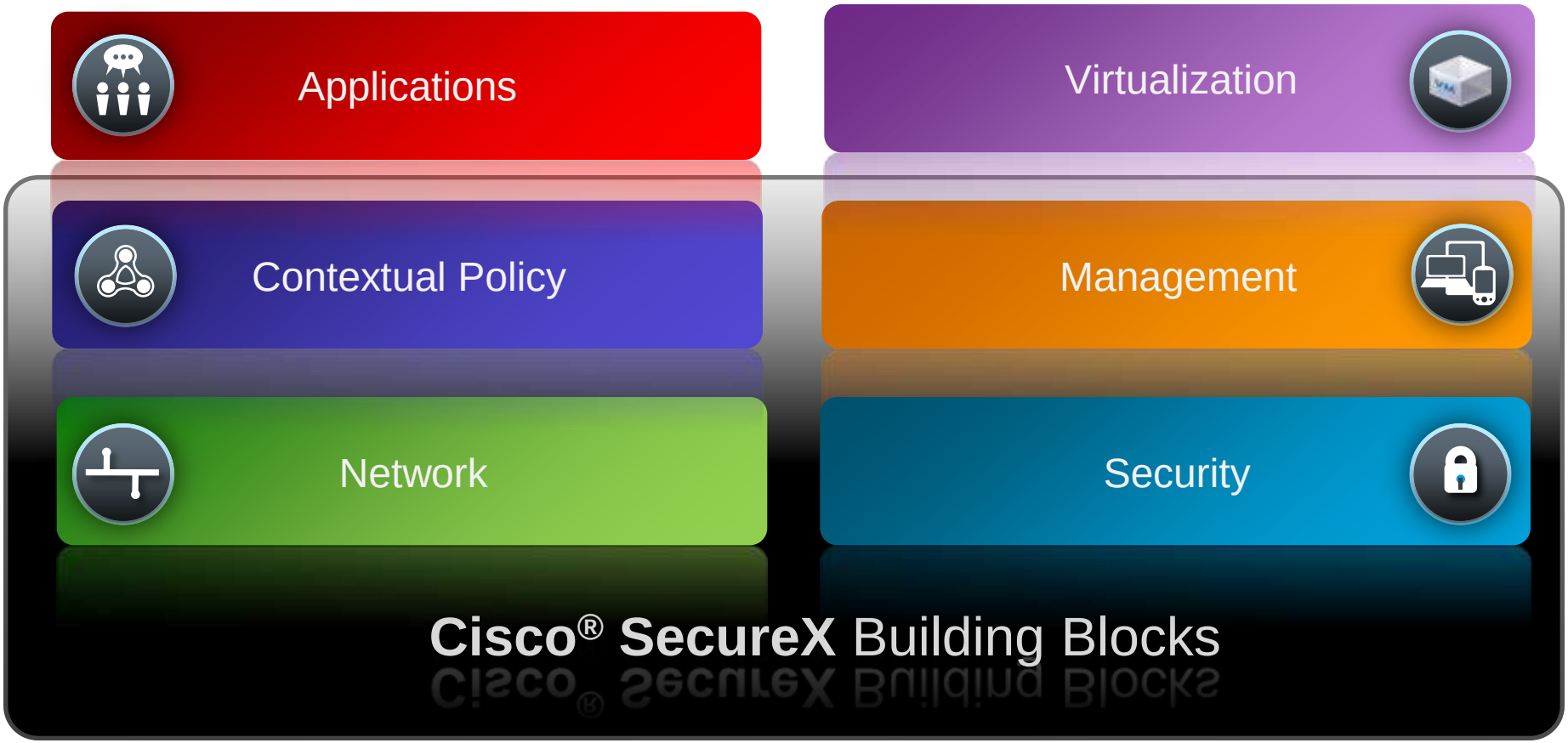

차단 또는 제한 | 허용 | 확장 | 혁신화

- Wired/Wireless/FW Infra
- ISE
- NCS

- Now Add
  - AnyConnect
  - IronPort
  - ScanSafe

- Now Add
  - MDM
  - Apps (Webex, Jabber, Quad)

# 시스코 BYOD 솔루션 블록



# 시스코 BYOD 보안솔루션 : 적용사례 #1

## 방문객에 대한 인터넷 접속 허용 및 회사 소유 디바이스의 접근만을 허용하기 위한 정책 적용

### 적용기술

- 802.1X, Profiling, Guest Access

### 솔루션 구성요소

- Cisco Switches + WLCs
- ISE
- NCS Prime

# 시스코 BYOD 보안솔루션 : 적용사례 #2

**회사 및 개인 소유의 디바이스에 대한 무선랜 및 회사외부 원격 접속 관리 및 활성화 정책적용, 개인 소유 디바이스는 이메일과 기본적인 웹서비스만 사용허용**

## 적용기술

- 802.1X, Profiling, Guest Access, BYOD on-boarding

## 솔루션 구성요소

- Cisco WLCs
- ASA & AnyConnect
- ISE
- NCS Prime

# 요약

# BYOD 환경에서의 네트워크 보안 고려사항

1. 누가 그리고 무엇이 네트워크상에 있는가?
2. 어떤경우에 무엇을 접속할 수있게 할것인가?
3. 네트워크상 어디에서, 누구에게 어떤 보안을 적용할 것인가?
4. 운영 관리는 어떻게 할 것인가?

**상황인식 기반의 네트워크 통합 접근 제어 정책 고려 필수!!**

# BYOD 환경에서의 네트워크 보안 솔루션

## 상황인식 기반의 네트워크 통합 접근 제어

1. 상황인식 기반의 통합인증

2. 상황인식 기반의 접근제어 정책

3. 확장성, 보안성

4. 통합관리

## 시스코 BYOD 보안 솔루션!!!