Security Solution for Service Provider

박 찬광

Cisco Systems Korea

KEY Message

1. SP 고객에 대한 보안 서비스가 SP의 새로운 사업 영역으로 부각되고 있다.
2. SP보안의 단편적인 것이 아닌 전체적이고 구조적인 접근이 필요하다.
3. Cisco의 Clean Pipes Architecture 와 Network기반 보안 서비스를 통해 End-to-End 보안 솔루션으로 구현 가능 하다.

목 차

- Industry 동향
- SP security is Really Business Control
- Cisco 솔루션
  - Clean Pipes
  - Network Based 보안 서비스
- Summary

Industry 보안 동향

Industry 에는 어떤 일이 ? – 보안

SP의 보안 ?

- 더 이상 특정한 “기술적인 요소” 가 아닌 “비즈니스 요구사항”
- **Infrastructure**의 보안은 “ 서비스 전달” 의 가장 기본적인 요소

최근 DDoS 공격의 성격 변화

- 단순하고 기본적인 공격의 형태에서 탈피, 복합적이고 지능적인 악성 공격 형태로 변화 (예, **not just SYN floods and ICMP** 공격)

고객 요구사항의 변화

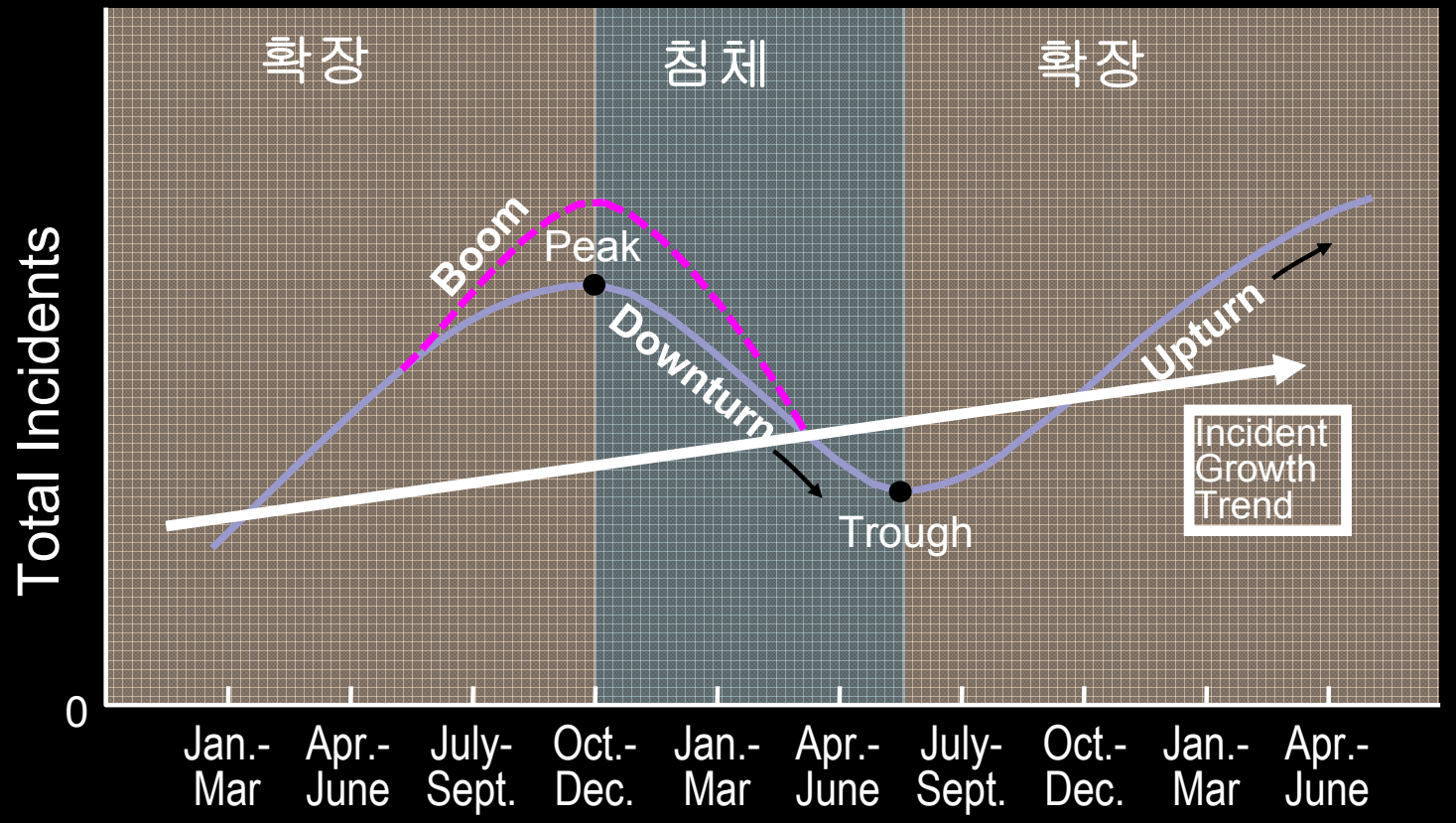
- **Inbound** 뿐만 아니라, **Outbound**에 대한 보호도 아울러 요구됨
- 위협노출 요소에 대한 적극적인 방어 기술 요구

위협에 대한 적극적인 방어 필요

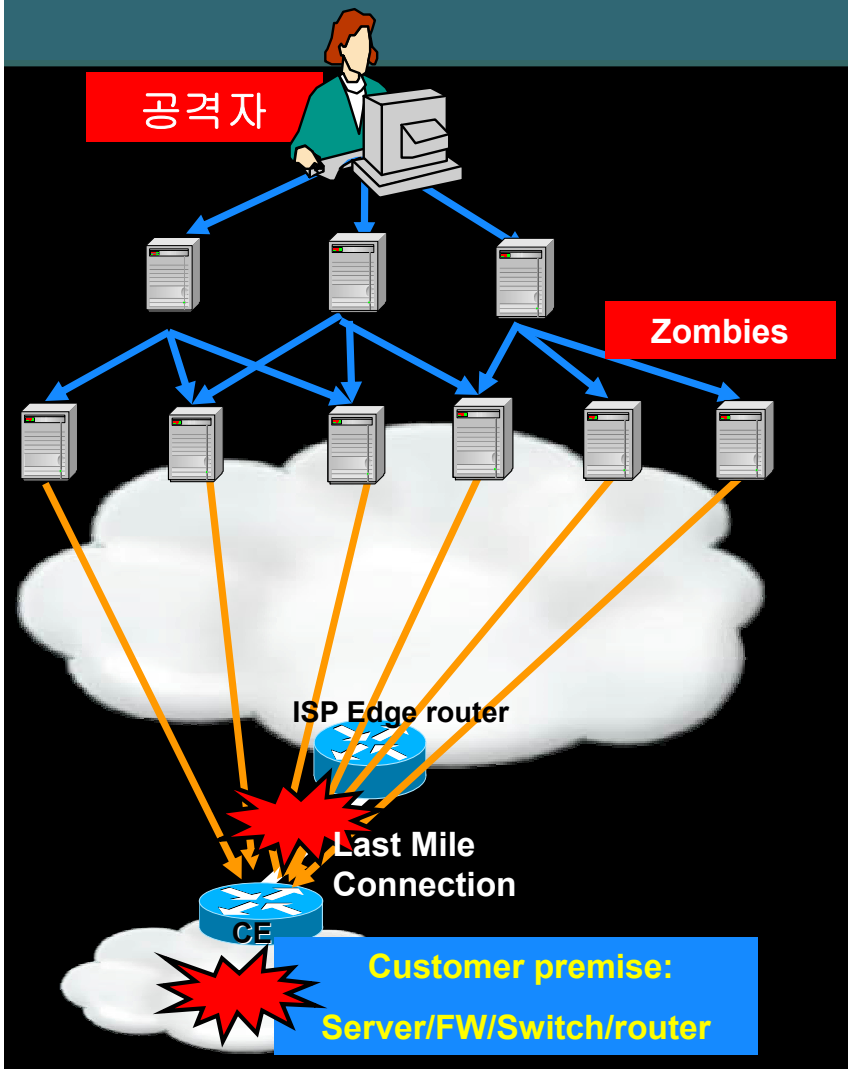
- **DDoS**공격 , **Worm** 전파의 지속적인 증가와 더불어 비즈니스에 영향 증가
- 보안 위협에 대한 수동적인 방어 에서 적극적인 방어로 전환 필요
- 적극적인 탐지 및 완화 기술의 필요성 부각

위협적인 범죄 행위는 계속 됩니다..쭈~~~~욱

위협적인 범죄 행위의 **Cycles**



BOTNETS – DDoS 공격을 쉽게 할 수 있다.



- **BOTNETs for Rent!**
- **BOTNET :**

  - zombie 프로그램이 설치되어 침입한 컴퓨터들로 구성되며, 중앙 통제 컴퓨터에 대해 직접적으로 공격 가능.

  - ICMP공격, **TCP** 공격과 **UDP** 공격, **http overload** 등의 다양한 종류의 **DDoS** 공격을 가능 하게 함.

  - 불과 **1000**여개의 **zombie**들로 구성된 작은 수의 **BOTNET** 은 전체 망 및 고객사의 **Network**에 도 치명적인 손상을 가져올 수 있음.

- **DoS** 공격에 의한 영향 요소

  - Application , HOST/Server 대역폭 , **Infrastructure** 등.

DDoS Attacks per DAY

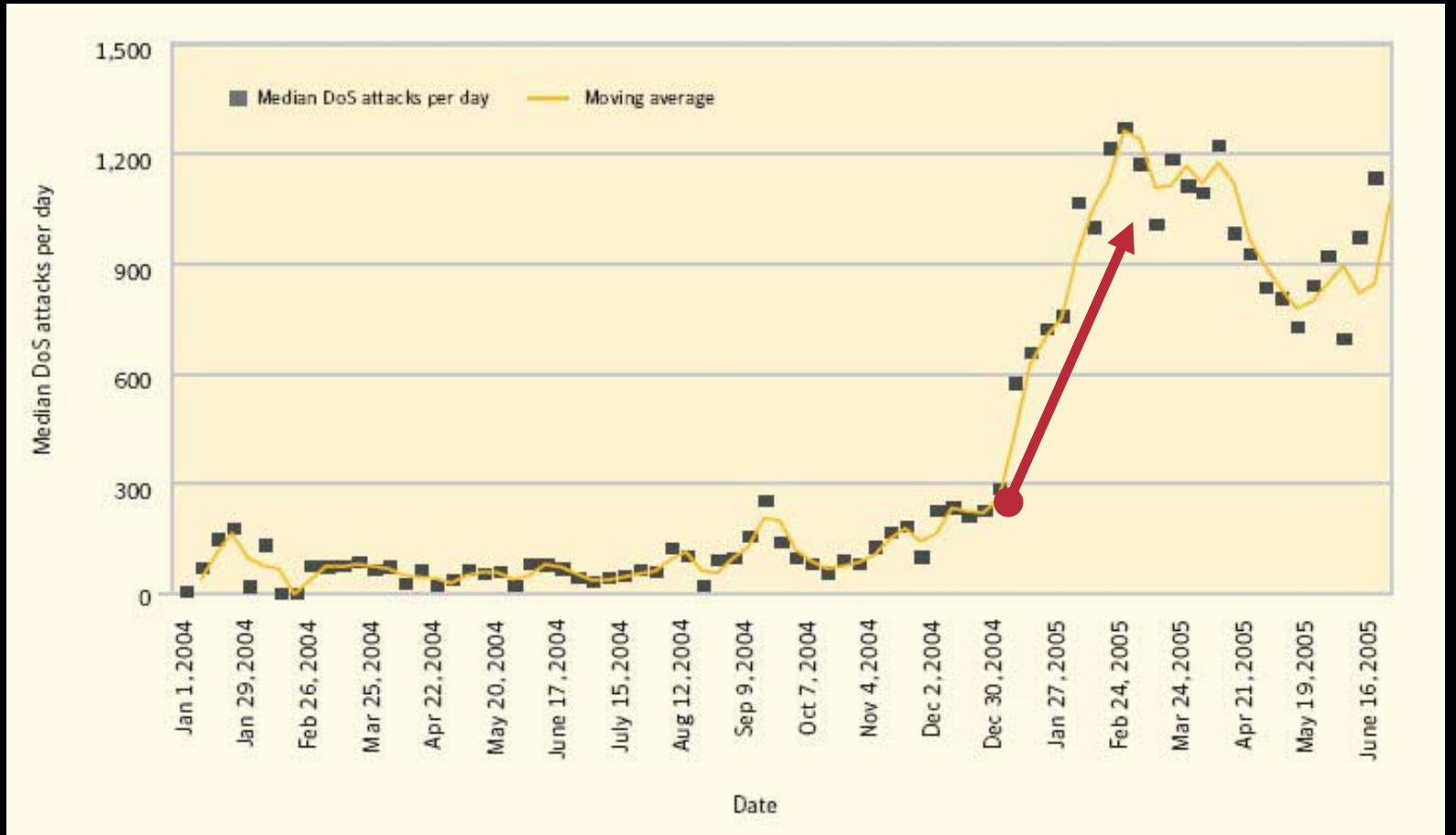


Figure 2. DoS attacks per day

Source: Symantec Corporation

SP Security is Really Business Control

Service Provider IP 보안 이슈

Service Provider 보안의 실체

- 보안은 **Internetworking** 의 미래

  - 인터넷 추세의 변화 : 기존의 “절대적인 신뢰의 인터넷” 에서 “지속적인 의심의 인터넷”으로 변화

- 위협의 경제효과 :

  - 위협의 요소가 곧 비즈니스의 기회로 변화

- 지속적인 서비스 전달을 위한 가장 기초적인 형태의 보안 **infrastructure** 필요 : 우선적 선행 과제

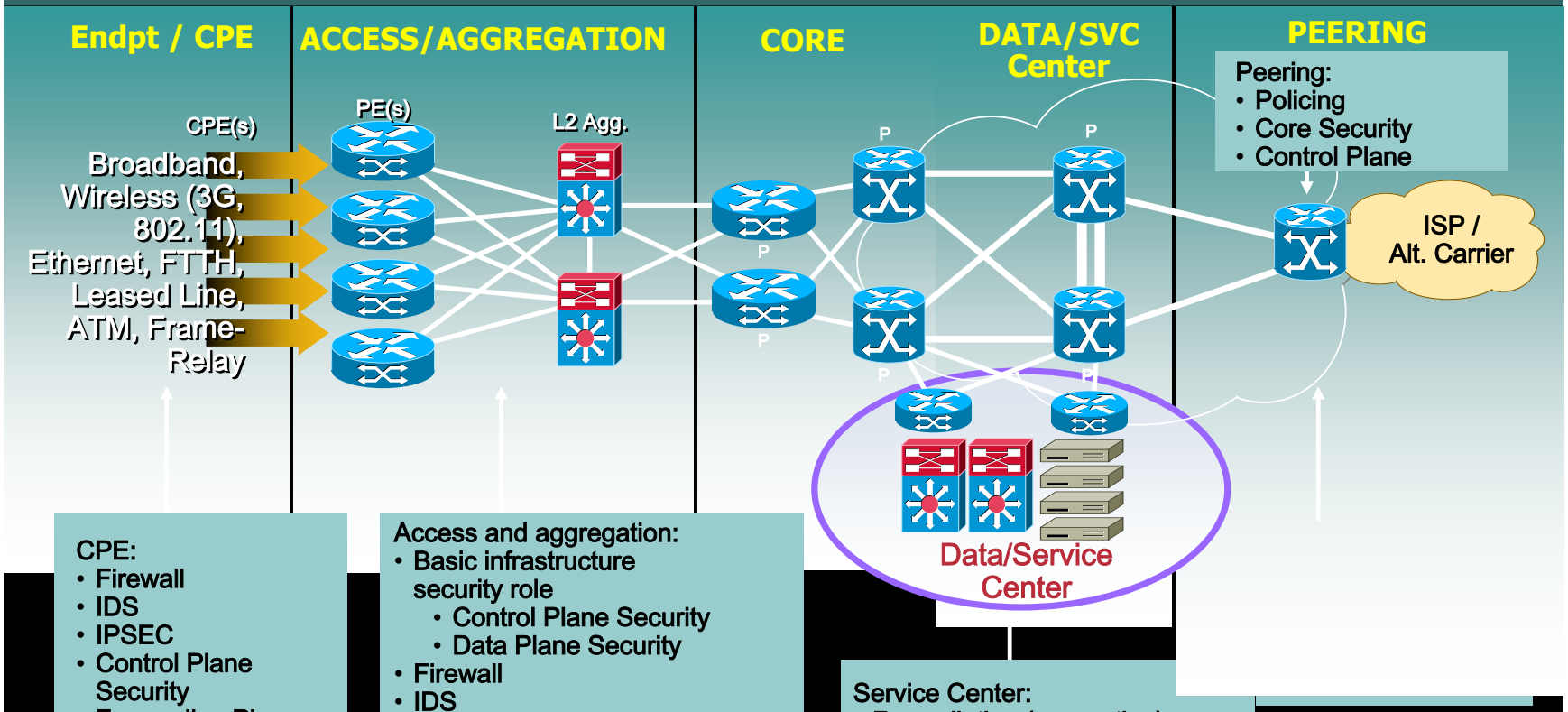
- **Network** 장비의 기본적인 보안 기능 들이, 지속적인 정책 시행 모델 안으로 합쳐짐.

  - **QOS = Security**
  - **HA = Security**
  - **Edge Policy = Security**

- 위협에 대한 반응시간을 개선 하고, 취약요인을 감소시키고, **revenue** 창출의 기회로 바꿔야 함.

차세대 Network – SP Security as part of Business Control Framework

전체 **Network**에서의 보안의 역할



Current Analysis
Technologies mapped within the Framework

Trust/Identity	Visibility	Correlation	Instrumentation/ Management	Isolation (Virtual)	Policy Enforcement
AAA	Netflow v5/8/9 Cache	SIMS	SNMP/ RMON/MIBs	Service Modules	Remote-Triggered BGP + uRPF v2
Routing Authentication (MD5)	NBAR	CIC-Security	Embedded Device Managers	VRF/VRF-Lite	Control Plane Policing
ISAKMP	IP Source Tracker	Protego	Syslog	GuardXT/DetectorXT Zones	BTSH
PKI	DetectorXT	Arbor + NF	Netflow MIB	CLI-Views (Role Based)	Firewalls
GuardXT – Active Verification	IDS/IPS (IOS, CSA, NIDS)	CSA-MC	CPU/memory Thresholding	Tunnels; LSP, IP, L2TPv3, 6to4	ACLs, Filters
Image Verification	Service Control Engine/Application (P-Cube)	Cisco Works SECMon	SAA	CEF, dCEF	MQC, QPPB
802.1x	RIPE (Raw IP Traffic Export)		IOX- XML Interface		IPSec (encryption policy)
uRPF v1 (strict)	Topologies (CDP, Routing protocols, MPLS LDP)		Config Rollback Config Logger		Policy Based Routing
RSA Certificates	SPAN/ERSPAN/ VACL Capture		Resilient Config		GuardXT-Multi Verification process
SSH	NAM		Login Enhancements (password re-try delay)		SSG/I-Edge
DHCP Snooping, IP Source Guard NAC (CSA)					

Clean Pipes Technologies Map

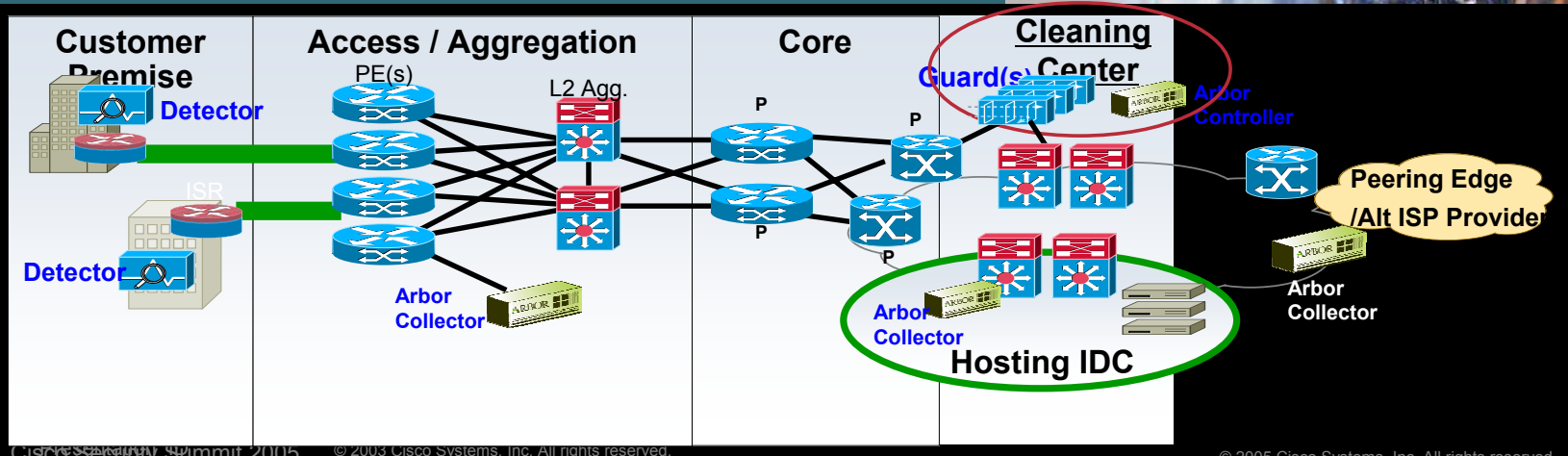
Trust/Identity	Visibility	Correlation	Instrumentation/ Management	Isolation (Virtual)	Policy Enforcement
AAA	Netflow v5/8/9 Cache	SIMS	SNMP/ RMON/MIBs	Service Modules	Remote-Triggered BGP + uRPF v2
Routing Authentication (MD5)	NBAR	CIC-Security	Embedded Device Managers	VRF/VRF-Lite	Control Plane Policing
ISAKMP	IP Source Tracker	Protego	Syslog	GuardXT/DetectorXT Zones	BTSH
PKI	DetectorXT	Arbor + NF	Netflow MIB	CLI-Views (Role Based)	Firewalls
GuardXT – Active Verification	IDS/IPS (IOS, CSA, NIDS)	CSA-MC	CPU/memory Thresholding	Tunnels; LSP, IP, L2TPv3, 6to4	ACLs, Filters
Image Verification	Service Control Engine/Application (P-Cube)	Cisco Works SECMon	SAA	CEF, dCEF	MQC, QPPB
802.1x	RIPE (Raw IP Traffic Export)		IOX- XML Interface	Diversion / Injection	IPSec
uRPF v1	Topologies (CDP, Routing protocols, MPLS LDP)		Config Rollback Config Logger		Policy Based Routing
RSA Certificates	SPAN/ERSPAN/ VACL Capture		Resilient Config		GuardXT-Multi Verification process
SSH	NAM		Login Enhancements (password re-try delay)		SSG/I-Edge
DHCP Snooping, IP Source Guard NAC (CSA)	BGP Policy Accounting		SDEE		

Clean Pipes

Cisco 솔루션

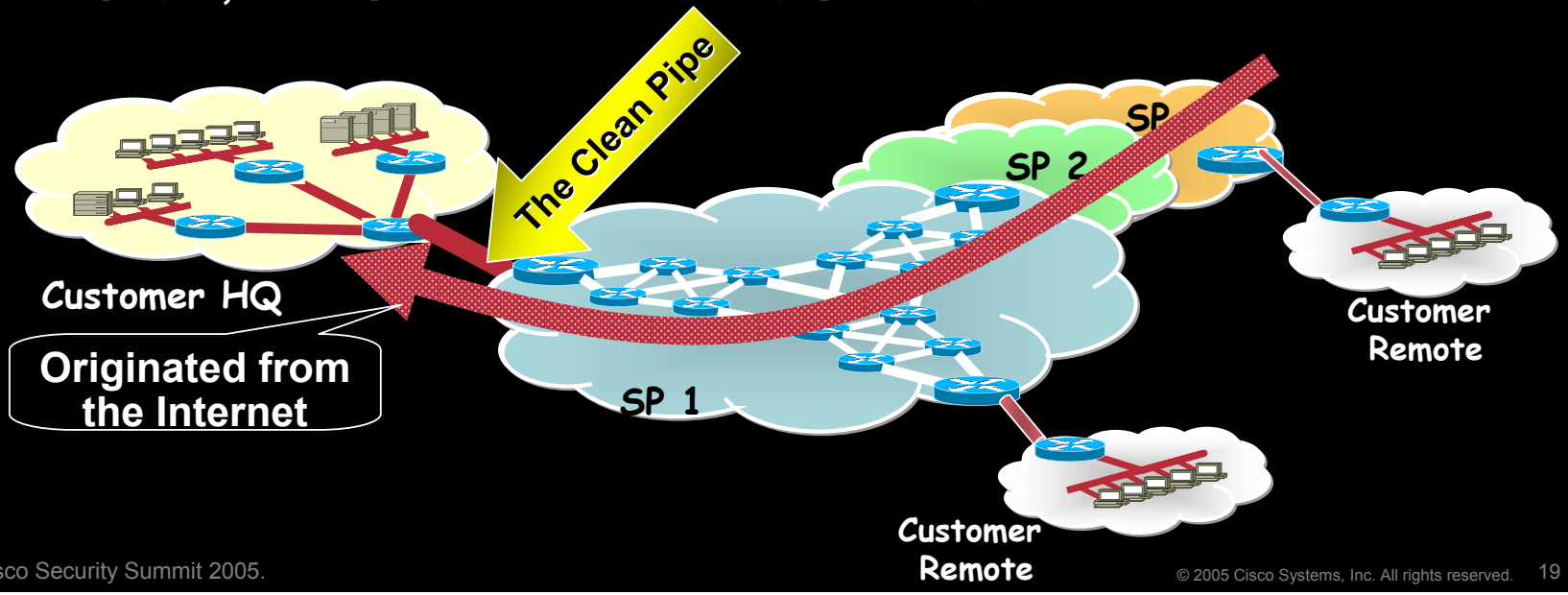
- Clean Pipes
- Network 기반 보안 서비스

Clean Pipes ?

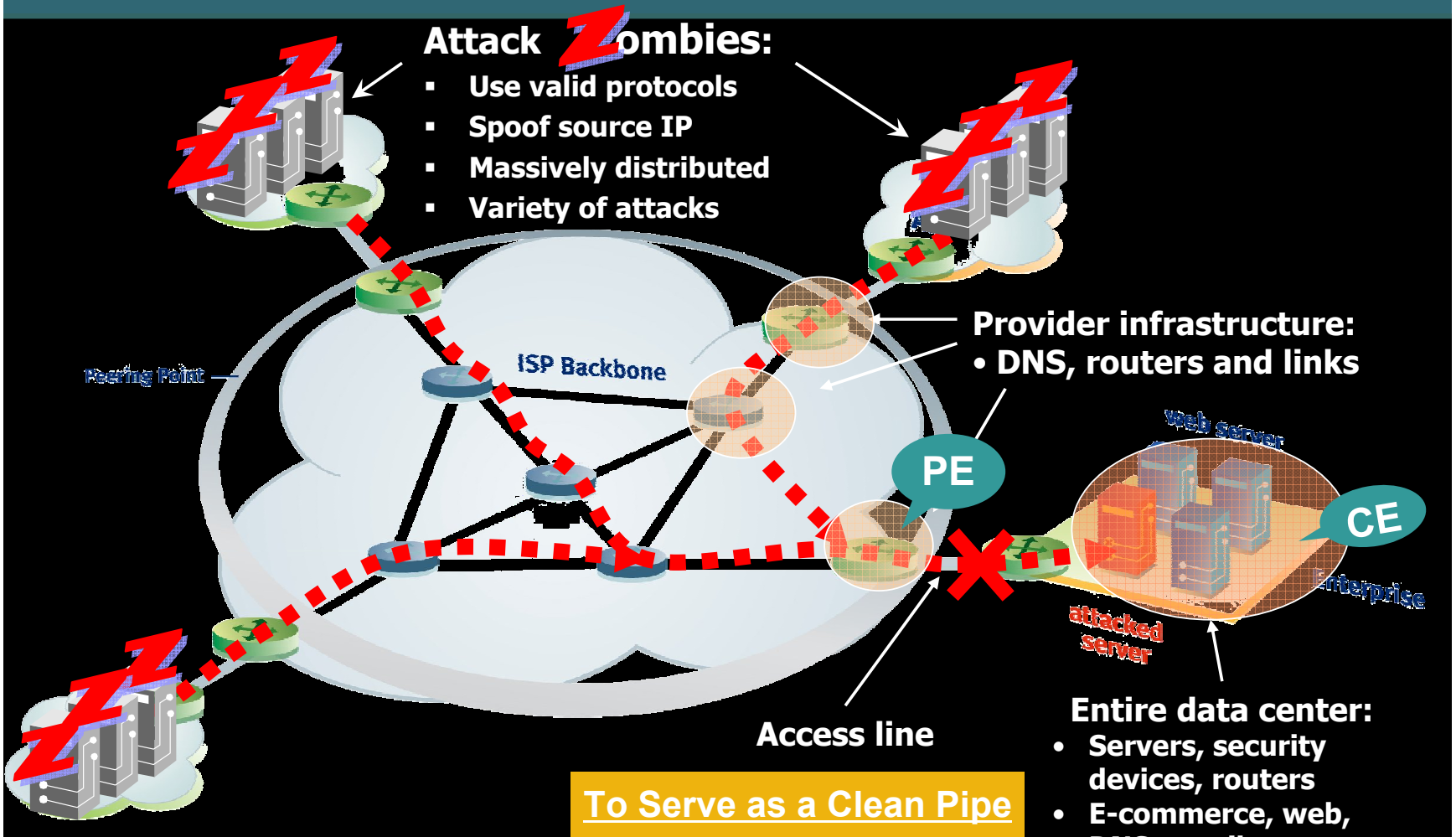


Clean Pipes is

- **Clean Pipes** 란 보안 위협요소로 부터 모든 서비스와 그 서비스를 전달하는 **connectivity** , 즉 **data pipe** 를 보호하기 위해 구축하는 입증되고, 진보된 **Architecture** 이다.
- **DoS** 공격 및 원치 않는 위해 트래픽으로 부터 **SP** 및 고객 **Network** 내의 중요 요소 와 자원 을 보호하고 , 나아가 이익 창출이 가능할 수 있도록 검증되고, 잘 구성된 **Network** 기반의 통합 솔루션이다.



DDoS 취약성
Multiple Threats and Targets



Clean Pipes 란 ?
Clean Pipes Solution의 적용 모델

III

Peering Edge | Cleaning Center | IDC (Hosting Centers)

II

Clean Pipes Solution의 기본이 되는 Tools

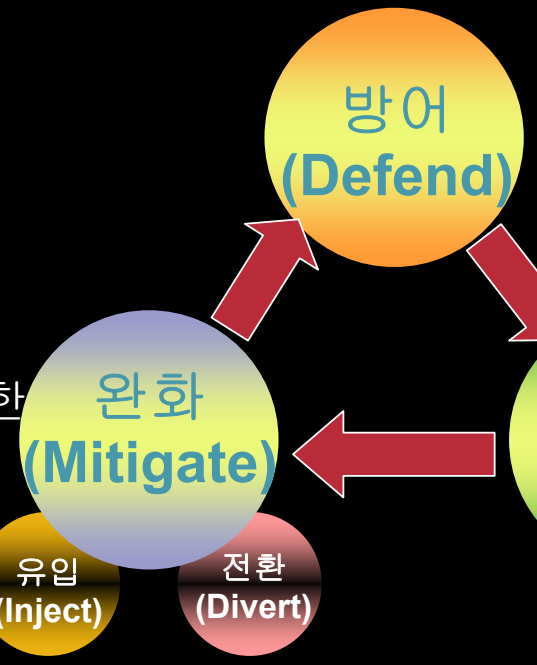
- iACL, rACL, AnyCast, uRPF, RTBH, QPPB (Rate Limiting), NetFlow Telemetry, Cisco Guard, Cisco Detector, Arbor Peakflow SP.
- A well tested and clearly defined set of toolkits.

I

Securing Data Plane | Securing Control Plane | Securing Management Plane | Securing the Services

SP "인프라"에 대한 보안 구축을 기반으로 최상의 설계 구현

Clean Pipes 솔루션



Network 인프라에 대한
기본적인 보호(NFP),
Data plane and Control Plane 보호

NetFlow data
수집을 통한
위협 탐지

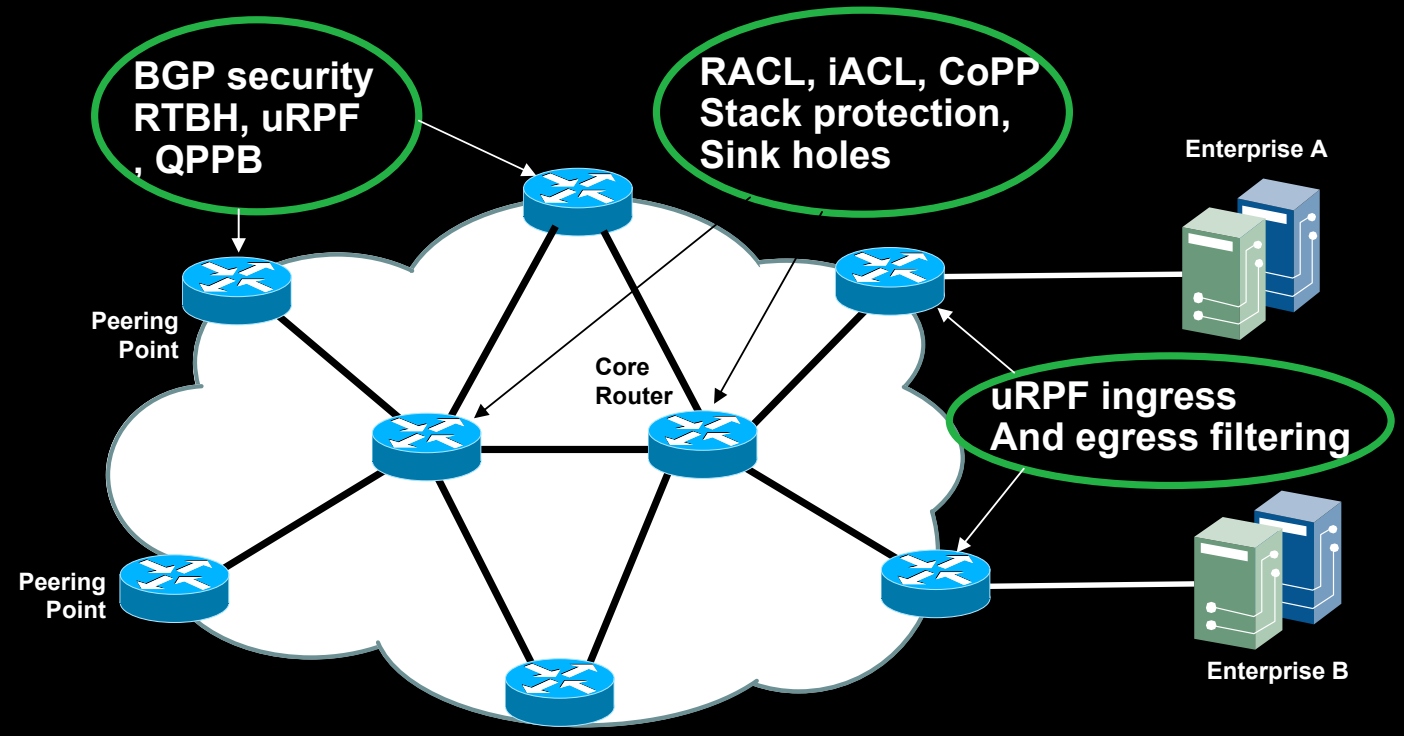
Cisco guard를
이용하여 clean 한
traffic 으로 전환

Clean 한 트래픽을
다시 유입

공격 트래픽을
cleaning 센터 쪽으로 돌림

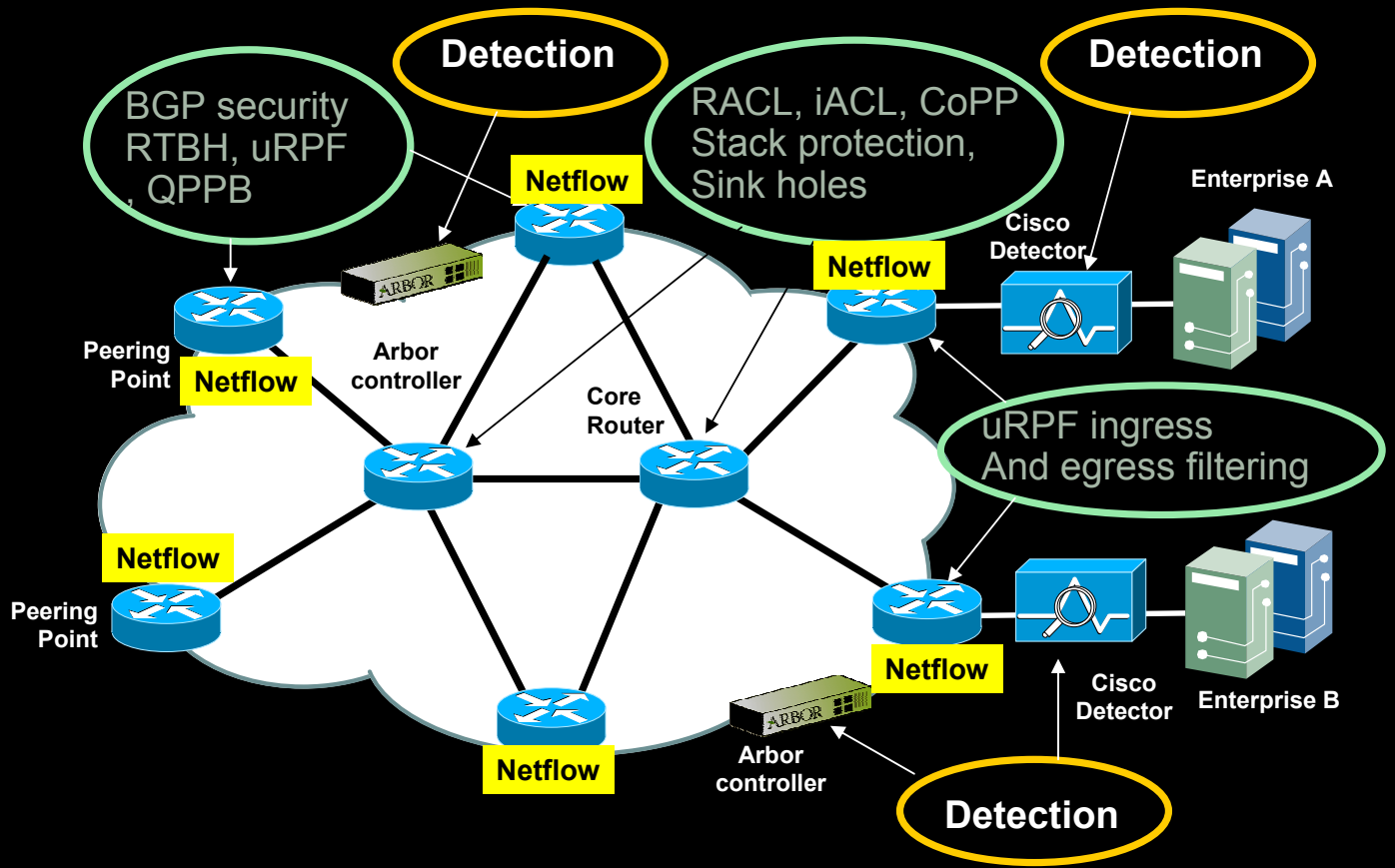
Clean Pipes – 방어(Defense)

방어
(Defend)



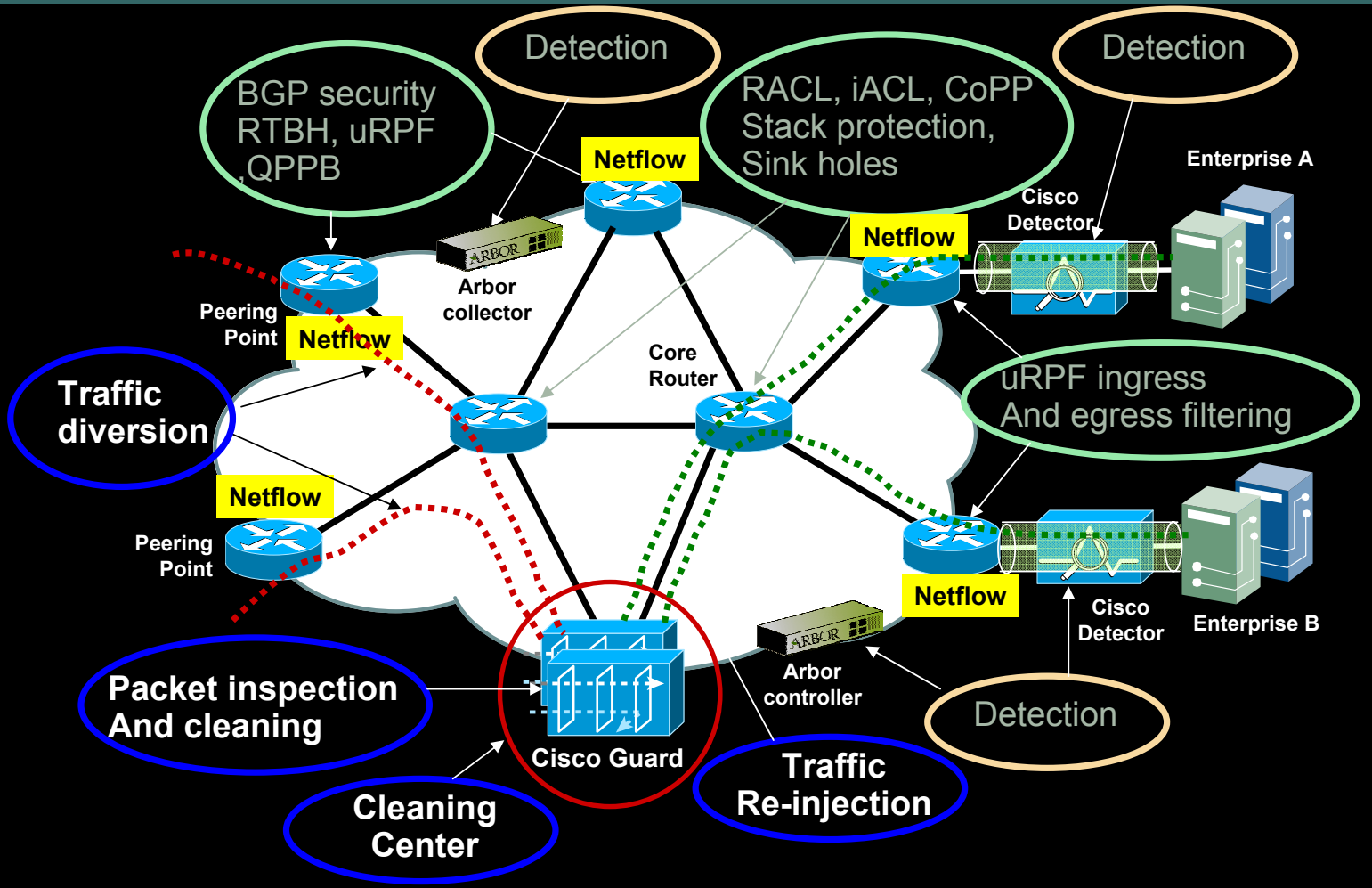
Clean Pipes – 탐지(Detection)

탐지
(Detect)



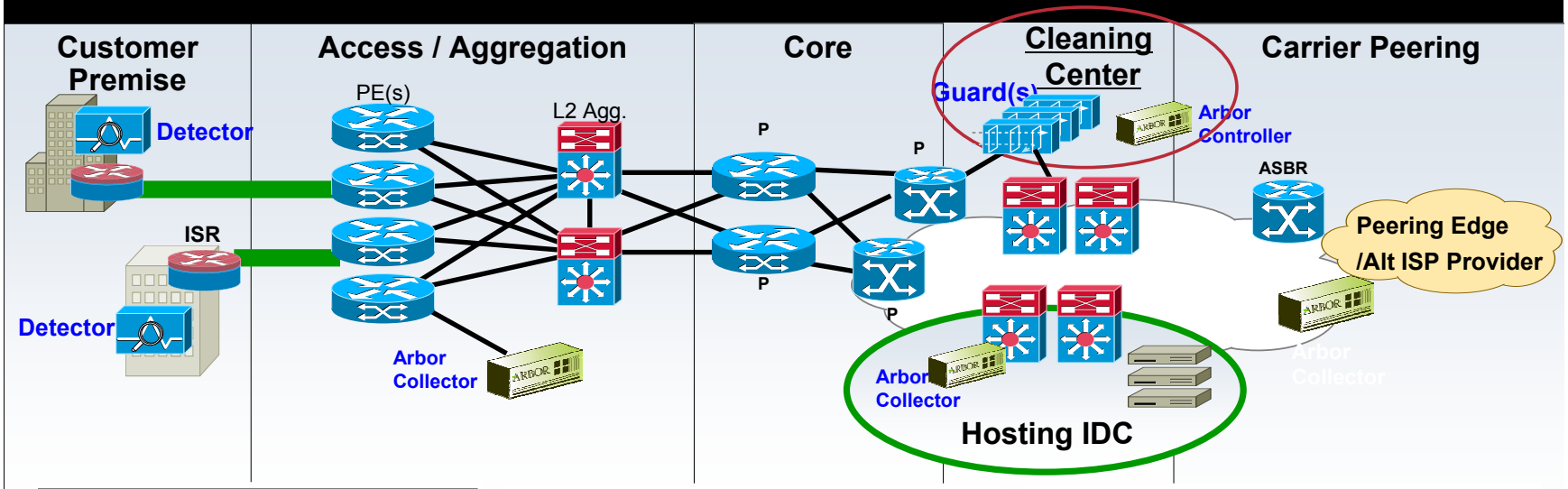
Clean Pipes – 완화(Mitigation)

완화
(Mitigate)



Clean Pipes

Network Based On-Net Anomaly Detection + Threat Mitigation



Customer Service
Protect SP last Mile

Protect Customer's Internet Producing Assets

Hosting Center
Protect Customer's Online Assets
Maximize Customer's Availability
- Content
- E-Commerce

Protect Data Center Resources

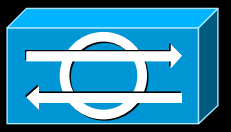
Peering
Identify attacks as they Ingress SP network
Mitigate Attacks at the point of Entry
Protect Overall Network:
- Performance
- Quality
- Availability

Network Based Solution – Solve Complex problem

Scale to Mulit-Gigabit, Works within a sustainable Operational Model, Not an Inline Solution

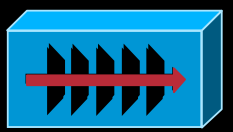
Clean Pipes – 기능적인 구성요소

탐지(Detection)

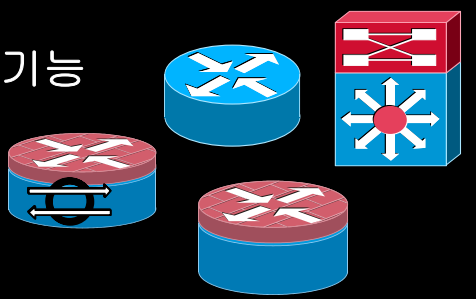


- **Cisco Anomaly Detector Service Module**
- **Arbor PeakFlow SP: Netflow를 이용한 DDoS 탐지**

완화(Mitigation)



- **Cisco Guard Service Module:** 위해 트래픽에 대한 **Cleaning** 및 재유입 기능 수행
- **Cisco Routers/Switches**에서 제공하는 기본적인 보안 기능
- **Prerequisite Security Best Common Practices :**
  RTBH, uRPF, Anycast, iACL, RACL, CoPP, BCP38



관리(Management)

- **WBM (Web Based Management)**
  Tools used for effective detection, monitoring and administration of the overall solution.

Guard Service and Anomaly Detector Service Module Catalyst 6500 / Cisco 7600

Guard Service Module

- DDos 완화 – Business 연속성 보장
  Anti-Spoofing
  Anti-Zombie (Bot)
  Mitigate TCP, Mis-Use attacks, DNS attacks, HTTP ½ open attacks, etc…
- Statistical Analysis combined with Anomaly Recognition
- Dynamic Filters – Filter BAD, Allow Good

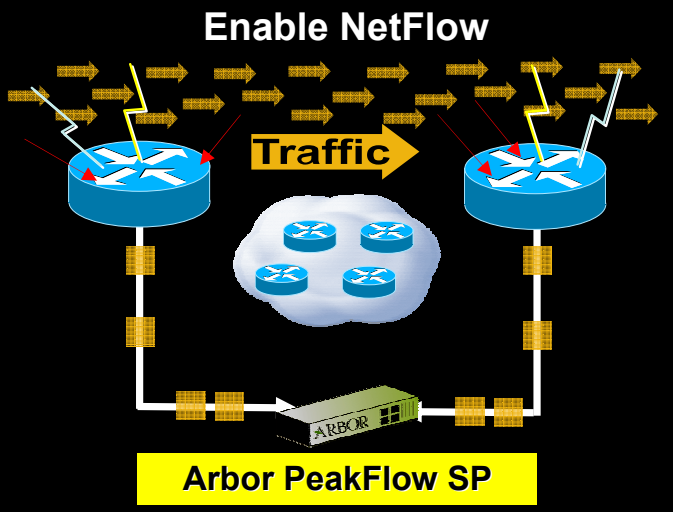
Anomaly Detector Service Module

- 행위 인지
- Profiles built via Network Learning
- Ready-to-Use Profiles available
- Trigger GuardXT Appliance and Service Module for Protection

Common Feature Set with Standalone Appliance

Arbor Peakflow SP and Cisco IOS NetFlow

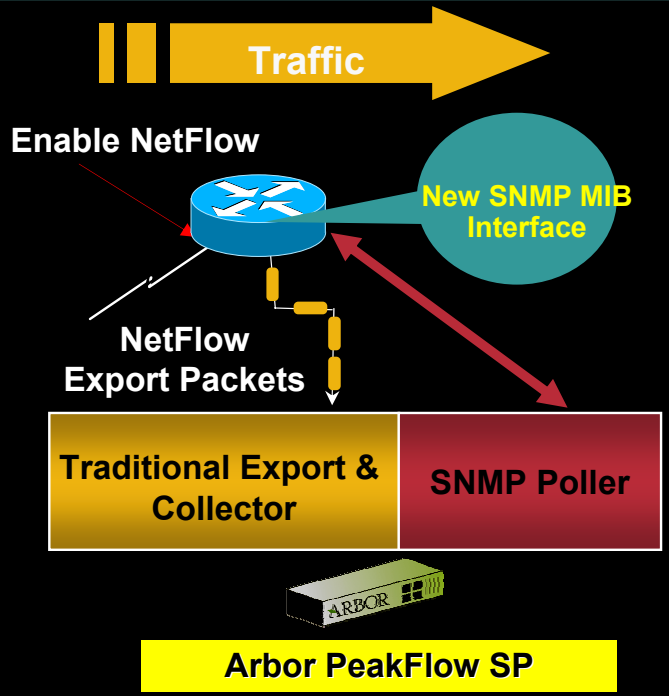
- NetFlow is a standard for acquiring IP network and operational data
- 트래픽 분석을 위해 Arbor Peakflow SP 로 data export
- Security Incident 의 탐지 및 분류
- It is a form of telemetry pushed from the routers and turns each NetFlow enabled router into a sensor



- Characterize Flows & understand traffic behaviour
- Export Flow information
- What is being attacked and origination of attack
- How long the attack is taking place
- Size of packets used in the attack

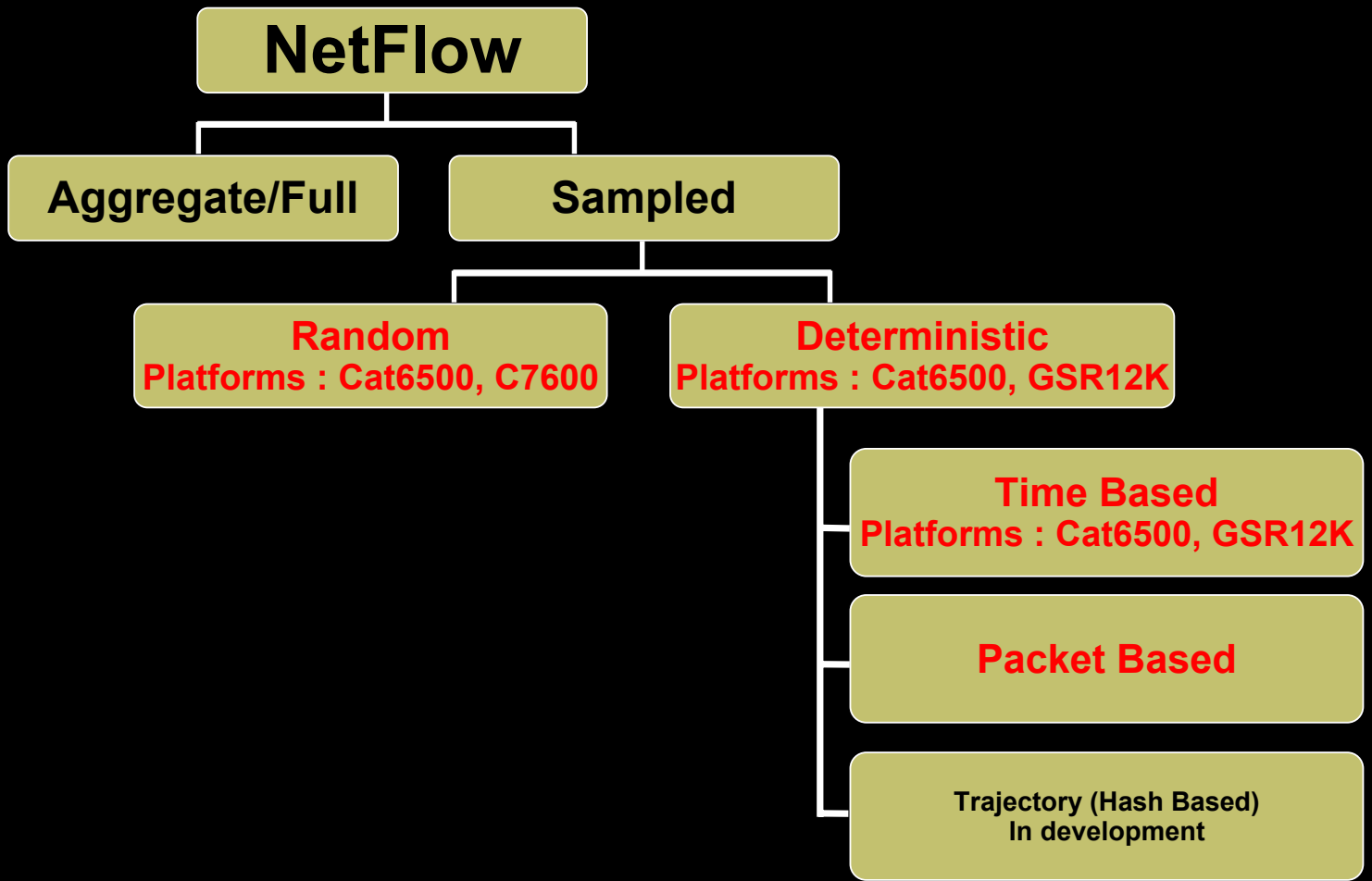
7 Unique Key 에 의한 Flow 정의

- Source IP address
- Destination IP address
- Source port
- Destination port
- Layer 3 protocol type
- Type of Service (ToS) byte (Differentiated Services Code Point (DSCP))
- Input logical interface (ifIndex)

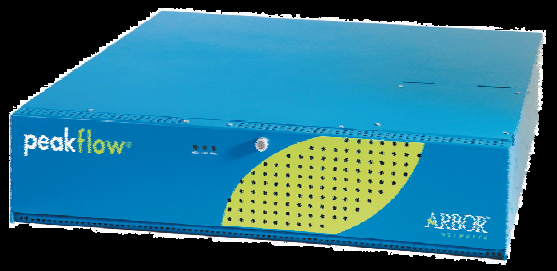


Export Packets
- Approximately 1500 bytes
- Typically contain 20-50 flow records
- Sent more frequently if traffic increases on NetFlow-enabled interfaces

NetFlow Types



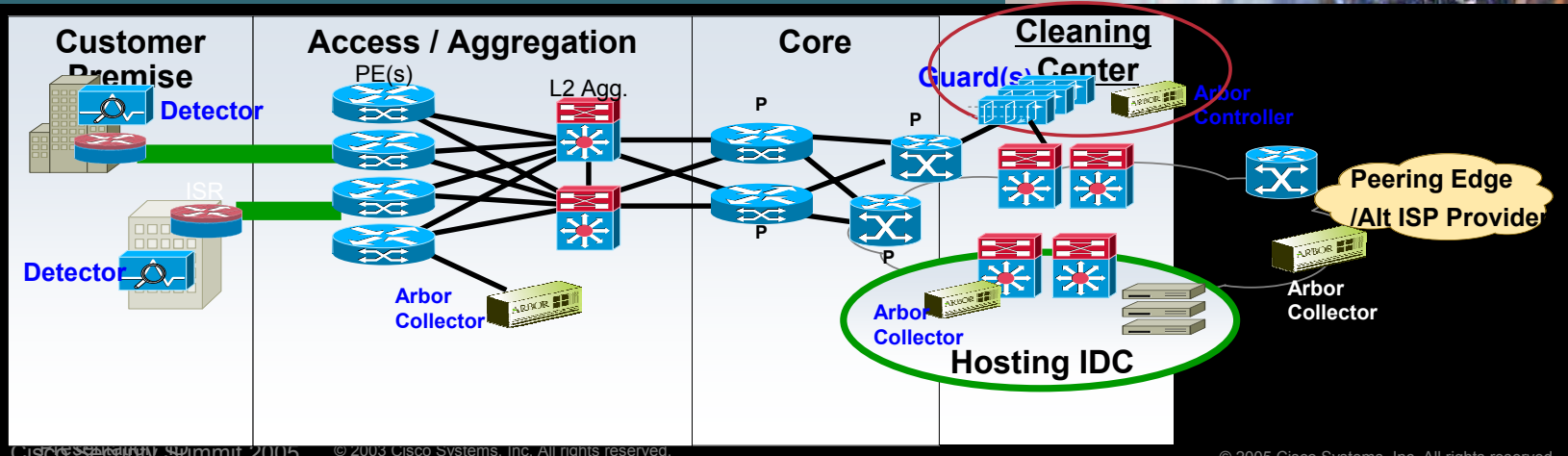
Arbor PeakFlow SP



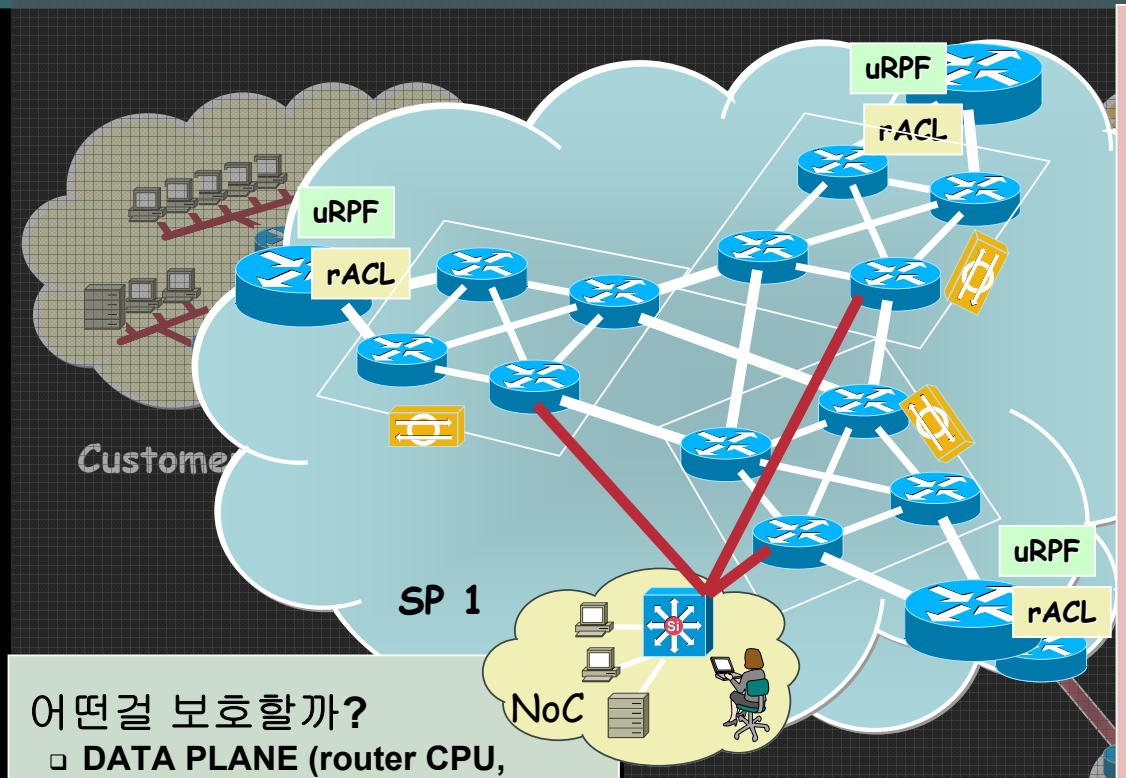
- 소형 **(2RU) , 전원 이중화 제공**
- **Port : 2 GigE, 1 Serial console , 6 Optional PCI slots(Copper or Fiber)**
- 고 성능 제공 **: Configured for Netflow (OC48+) and Packets (GigE)**
- **SP** 규격 만족 **: NEBS Level3 certified (AC or DC) , ETSI**

Network Anomaly Detection	**Peakflow SP** 는 최소한의 **network configuration**만으로 **signature update** 없이도 **network**의 특정 행위에 대해 탐지 기능 제공
Intelligent Mitigation Management	**Peakflow SP**는 특정 **access** 규칙의 발생, **blackhole** 통합, **sinkholing** 등을 통해 새로운 위협에 직면했을 때 신속하게 대응할 수 있는 통합 솔루션이며 , 통합 관리 **console** 제공

Clean Pipes 의 적용 예



Security -- SP Core 관점



보안 기능 적용 —

- Data Plane Configurations
  - Unicast RPF
  - rACLs, CoPP, CAR, etc.
  - Other (e.g. ICMP rate limits)
- Control Plane Configurations
  - rACLs, CoPP
  - Routing Plane protection (BGP peer authentication, route filtering via prefix filters, route maps, SPD)
  - Management Plane protection (SNMP v3, TACACS+, vty ACLs, NTP authentication)
- Network “visibility” tools
  - Netflow for traffic and DDoS analysis

Arbor

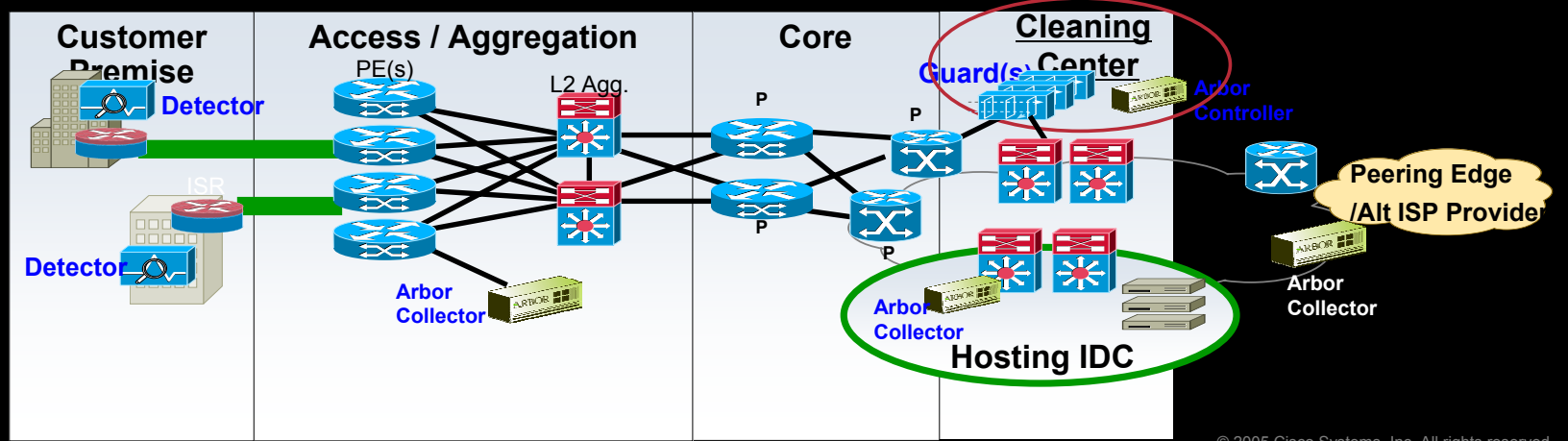
어떤걸 보호할까?

- DATA PLANE (router CPU, bandwidth)
- CONTROL PLANE (routing integrity, management, Back Office)

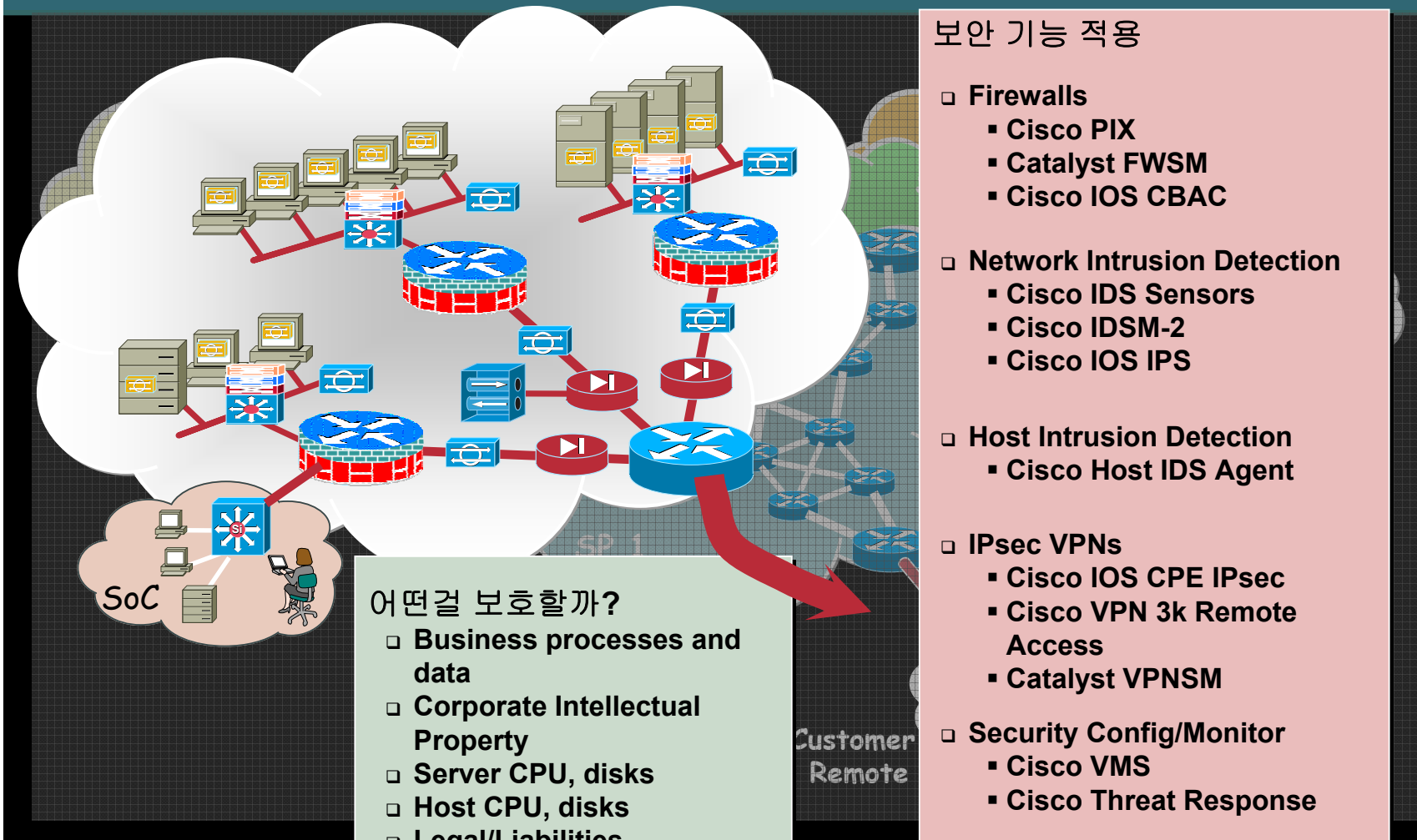
‘Clean Pipes’ Solution의 이점
- Service Providers

- 차별화된, 고 부가가치의 보안 서비스 제공
- 더욱 더 효과적인 완화

  - 기업 **network** 의 **egress point** 에서부터 위협요소를 제거함으로써, **network**의 **redirect** 와 공격 완화가 쉬워지고, 결과적으로 **Network- level**까지의 **DoS** 공격 방어를 가져온다.
- **Trust model**을 구축 함으로써 기업고객의 불안정하고 위협적인 요소를 감소 시키며, 잠재적인 이익 증가 가능성



Security -- Enterprise 관점



어떤걸 보호할까?

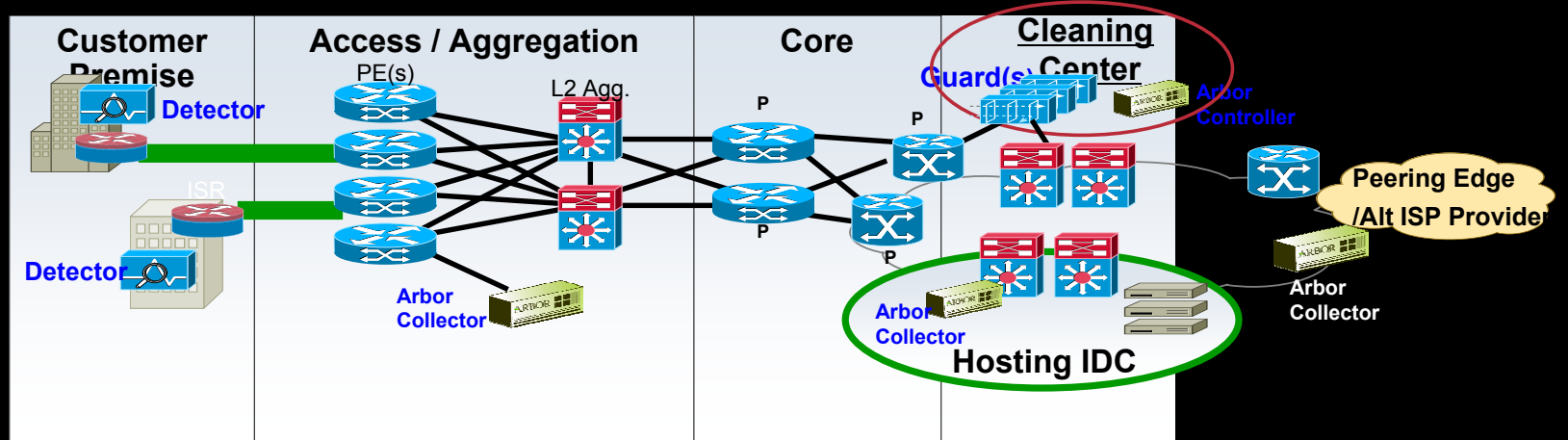
- Business processes and data
- Corporate Intellectual Property
- Server CPU, disks
- Host CPU, disks
- Legal/Liabilities

보안 기능 적용

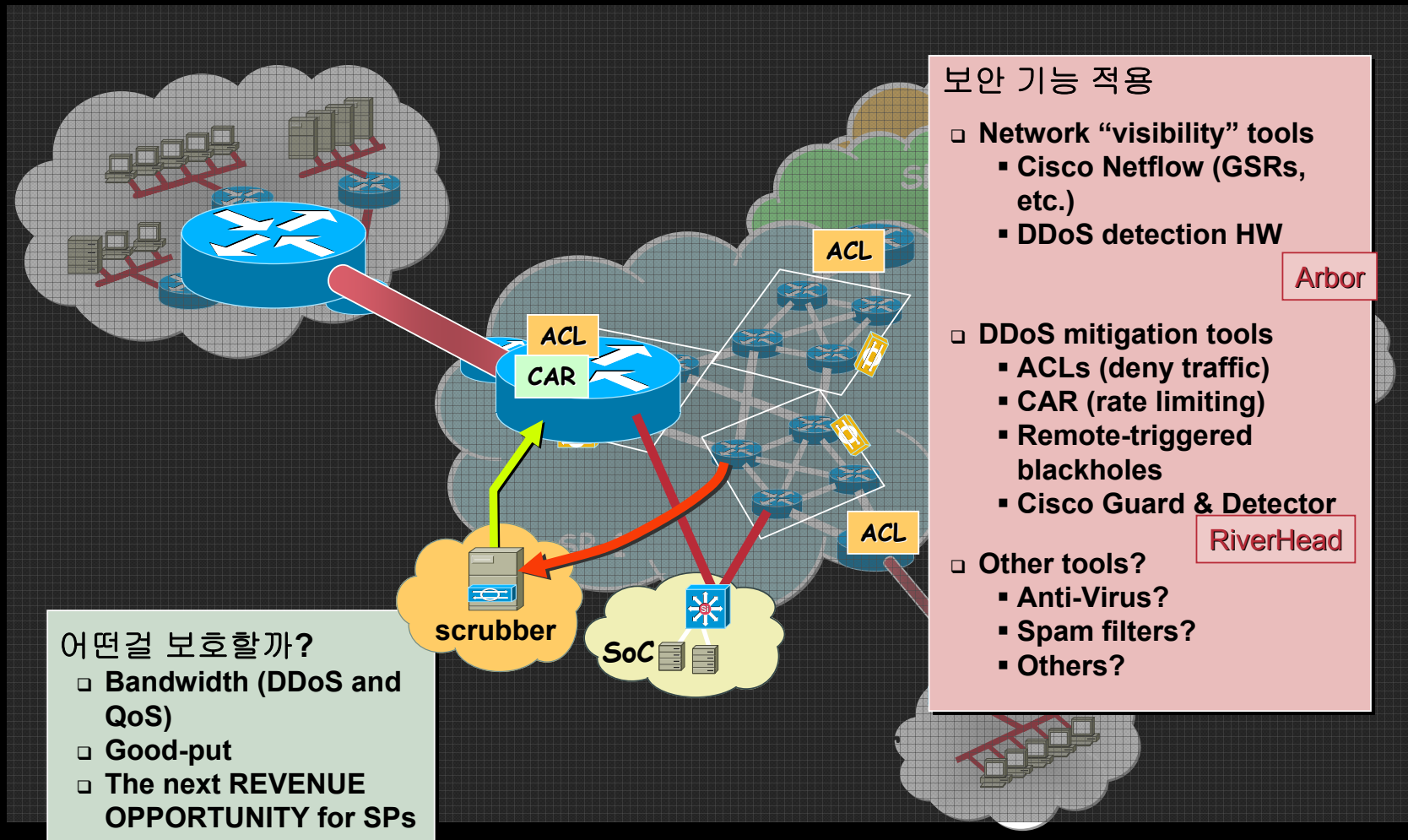
- Firewalls
  - Cisco PIX
  - Catalyst FWSM
  - Cisco IOS CBAC
- Network Intrusion Detection
  - Cisco IDS Sensors
  - Cisco IDSM-2
  - Cisco IOS IPS
- Host Intrusion Detection
  - Cisco Host IDS Agent
- IPsec VPNs
  - Cisco IOS CPE IPsec
  - Cisco VPN 3k Remote Access
  - Catalyst VPNSM
- Security Config/Monitor
  - Cisco VMS
  - Cisco Threat Response

‘Clean Pipes’ Solution의 이점 - Enterprises

- 적극적이며, 실시간 적인 완화
  - **SP mitigates without customer’s notification or involvement and alerts customer in real-time.**
- 적은 투자대비 최대 보호 효과
  - **no additional hardware at customer site.**
- **Addresses the problem at the “right” place**
- **Improved servers’ uptime ➔** 생산성 증대



Security -- SP Customer Link…



보안 기능 적용

- Network “visibility” tools
  - Cisco Netflow (GSRs, etc.)
  - DDoS detection HW

Arbor

- DDoS mitigation tools
  - ACLs (deny traffic)
  - CAR (rate limiting)
  - Remote-triggered blackholes
  - Cisco Guard & Detector

RiverHead

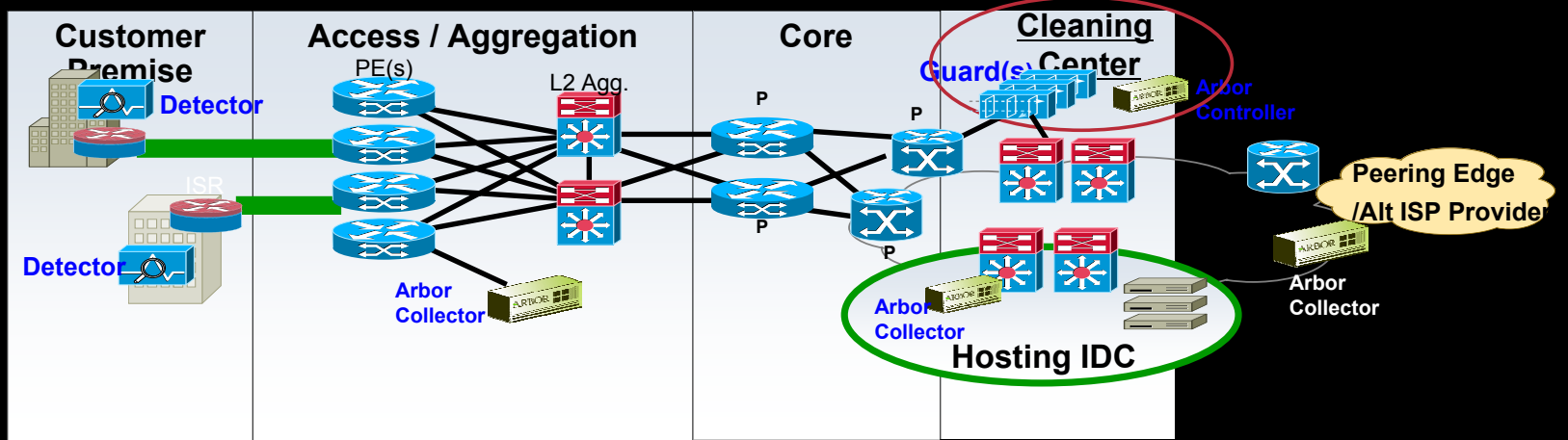
- Other tools?
  - Anti-Virus?
  - Spam filters?
  - Others?

어떤걸 보호할까?

- Bandwidth (DDoS and QoS)
- Good-put
- The next REVENUE OPPORTUNITY for SPs

‘Clean Pipes’ 적용 시 고려 사항

- 현재의 **Network**이 얼마나 안정적인지 , 보안성은 어떻게 되는지 여부**?**
- 보안팀이 구성 되어 있는지 , 어떤 **Tool**을 가지고 있는지 여부 **?**
- 어떤 형태의 공격에 대해 완화 솔루션을 제공할 것인가 **?**
- 장비의 위치선정 **:** 강력한 효과를 내기 위해 어느 위치에 놓아야 하나**?**
- 라우팅 **– clean Zone**으로 유해 트래픽 흐름 전환 및 재 유입
- 성능 및 확장성
- 고 가용성
- 관리 및 **SLA**

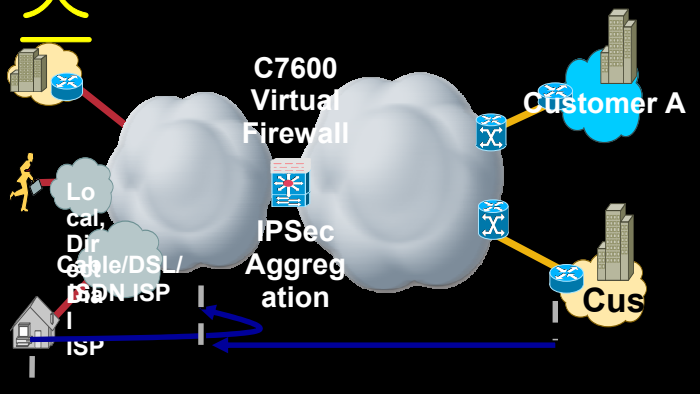


Network 기반 보안서비스

-VRF-Aware IPSec VPN

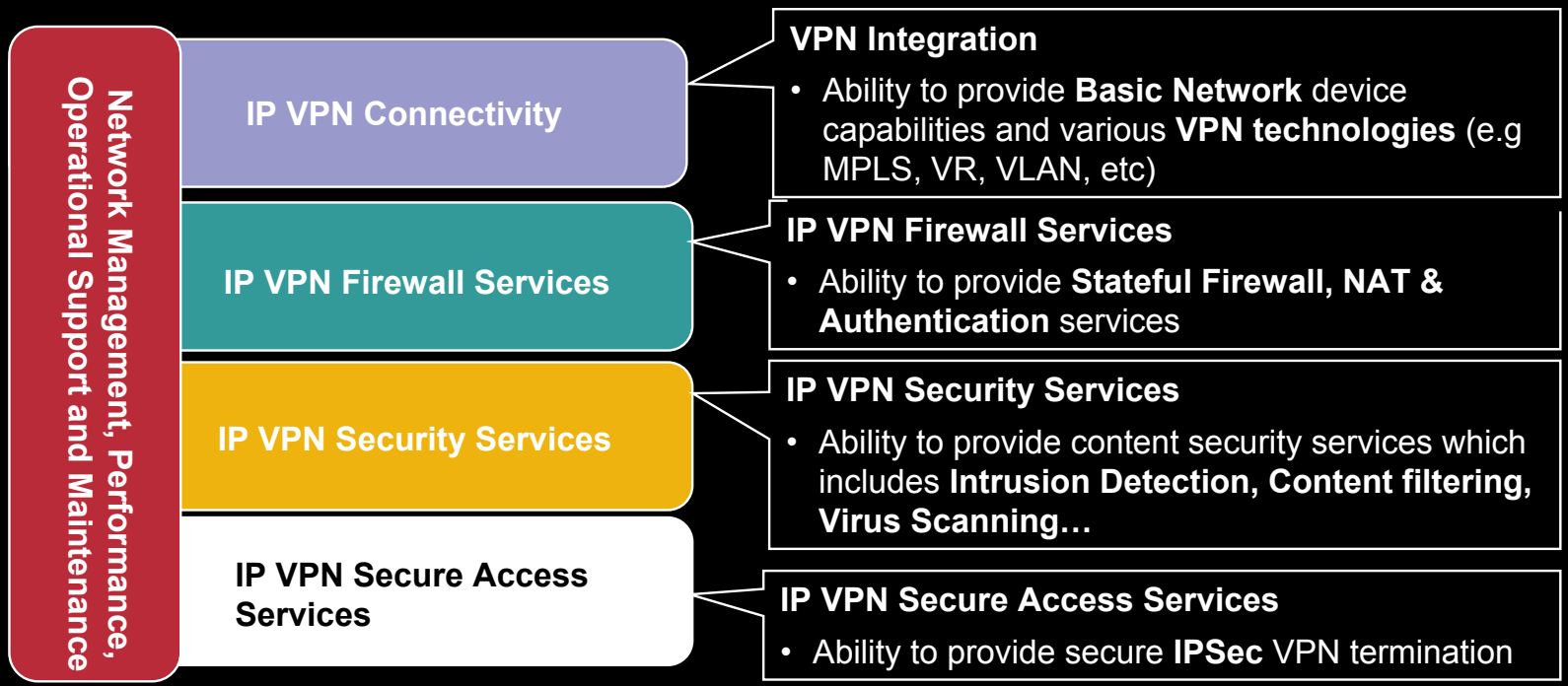
-Virtual Firewall

-Virtual Web VPN



Cisco Network 기반 보안 서비스 정의

Network based Security VPN solution is to incrementally deliver "virtualized" security services in an "integrated" fashion on network edge platforms to enable our Service Provider to generate incremental revenue



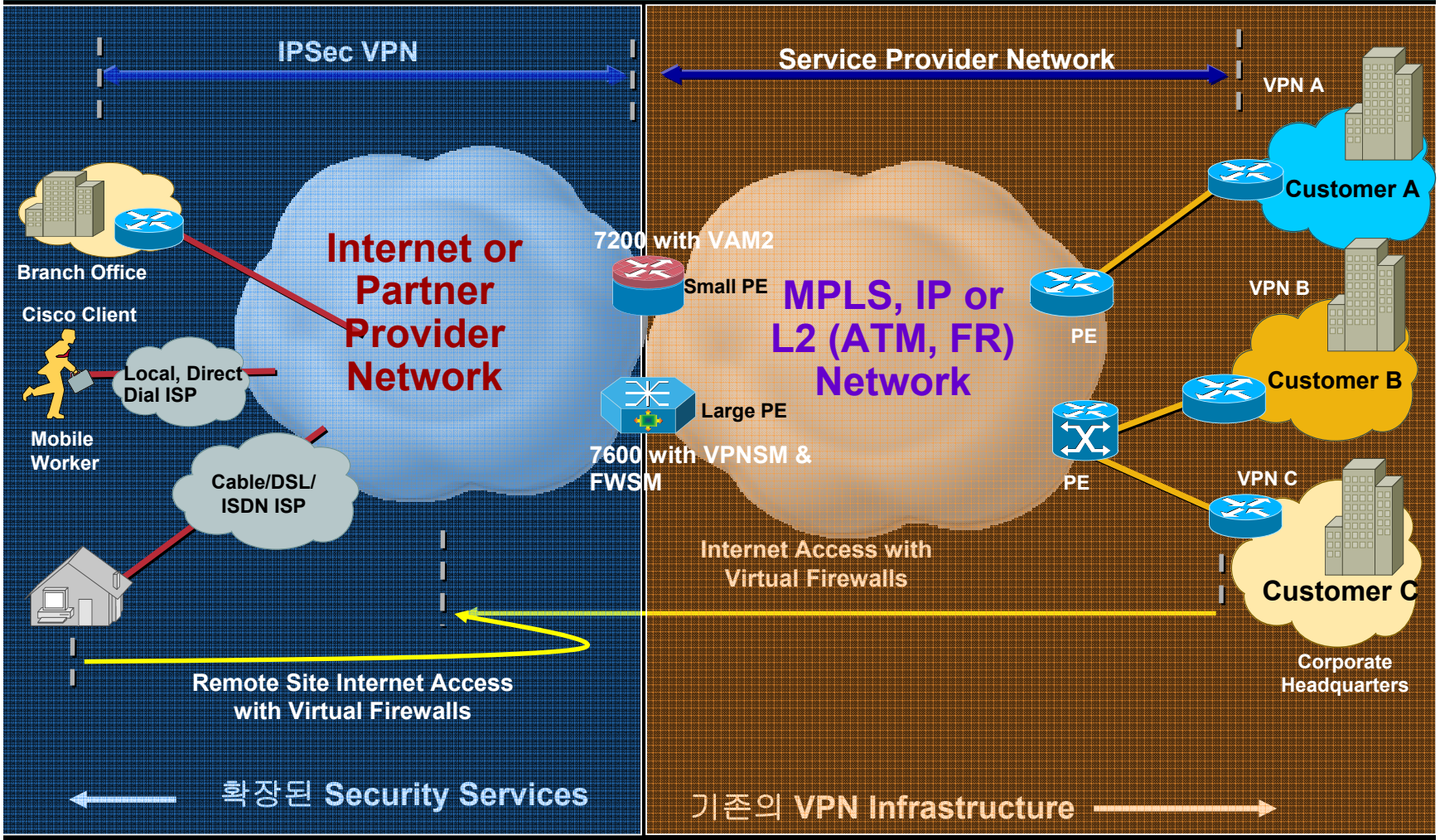
Network 기반 보안 서비스 기대 효과

- **Secure VPN(**원격 및 **Site-site**접속**) / Firewall** 등 보안 서비스를 통한 차별화된 고객 유치로 매출 증대
- 고객에게 솔루션 제공함으로써 **Biz partner**로 영업 형태 전환가능 , 기존고객의 타 사업자로 이탈 최소화
- **Broadband**와 기존 인프라**(MPLS, L2 infra)**를 적절히 연동,
  다양한 연결성 구현 **(Virtual IPSec + MPLS)**
- 다수의 **VPN**가입자에게 제공되는 다양한 보안 기능을 단일 장비에 구현함으로써 **CAPEX** 절감, 중앙집중 관리 용이

  (Cat6500/C7600 with Service Module)

Network 기반 보안 서비스 : Aswan 2.0

Available Now on 7200/7301 and 7600/6500



Aswan 2.0: Network 기반 보안 서비스

- **Cisco 7200 / 7301**

  VRF-Aware IPSec: Max 1K Site-Site, 2K RA tunnels, 250 VRFs
  VAM2 for DES/3DES and AES-128 via Hardware

- **Cisco 7600 / 6500 with Sup720-3B or Sup720-3BXL**

  FWSM 2.3
  - **L2 or L3 Virtual Firewalls, up to 4 blades per chassis**
  - **Up to 250 vFW per blade / Up to 1,000 per platform**
  - **80K ACLs per blade**
  - **1M concurrent connections per blade**
  - **Up to 100K connections/sec for HTTP, DNS and SMTP**

  VRF-aware IPSec
  - **1 VPNSM**
  - **1K IPSec+GRE Site-Site tunnels**
  - **4K Site-Site tunnels**
  - **6K Remote Access tunnels**
  - **512 VRFs**

Aswan 2.5: Network-Based Security Services

- **Cisco 7200 / 7301 IOS 12.3(14)T March 2005**

  VRF-aware IOS Stateful Virtual Firewalls
  VRF-aware IPSec Box-Box Active/Standby Stateful HA
  - Adds support for Remote Access and PKI
  IPSec Static Virtual Tunnel Interfaces
  - For replacement of IPSec+GRE Site-Site
  New VAM2+
  - Adds AES-192 and AES-256 in Hardware
  - Designed for future: GDOI, IPSec for IPv6, IKEv2, SSL VPN

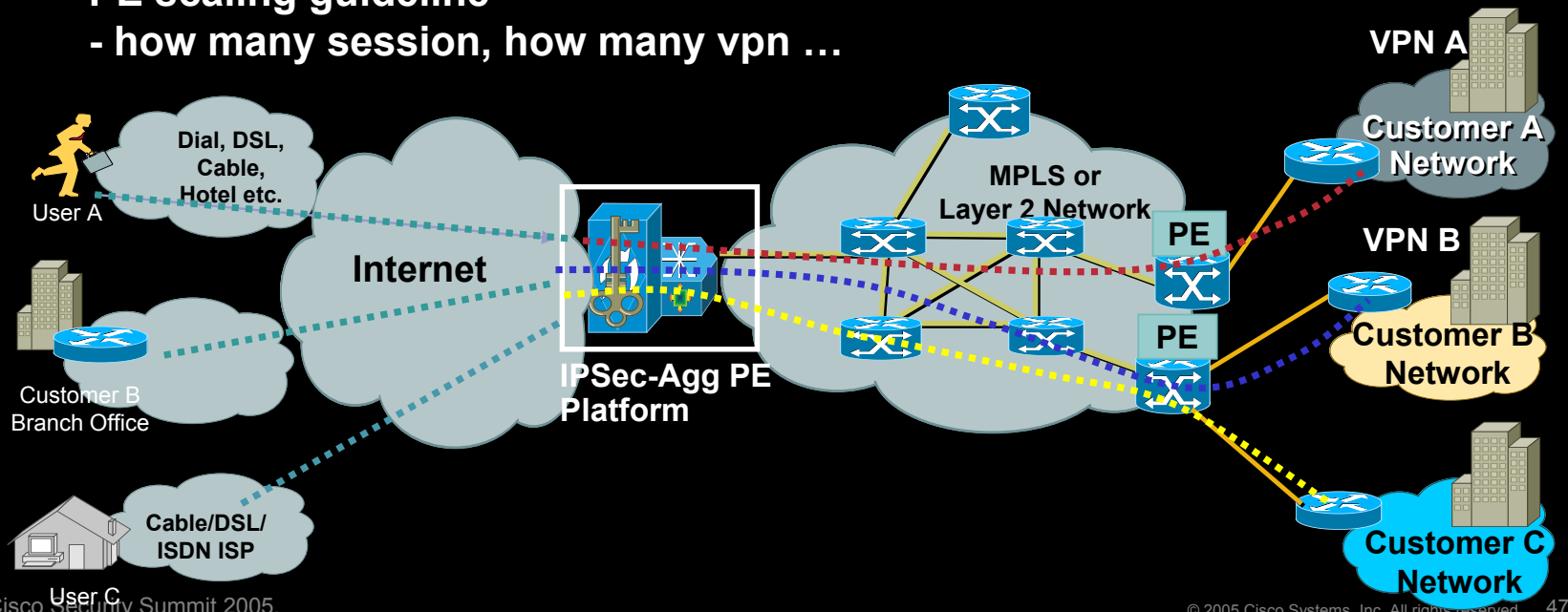
- **Cisco7600 / 6500 with Sup720-3B or Sup720-3BXL**

  DMVPN (phase 1 and 2) per VRF
  VRF-aware IPSec stateful HA
  Multi-blade (up to 6) with VRF-Aware IPSec
  1K VRF-LIte per platform
  New IPSec VPN SPA with AES and Jumbo Frame support
  New SSL VPN Module with Virtualized SSL VPNs

Network 기반 Virtual IPSec VPN 서비스

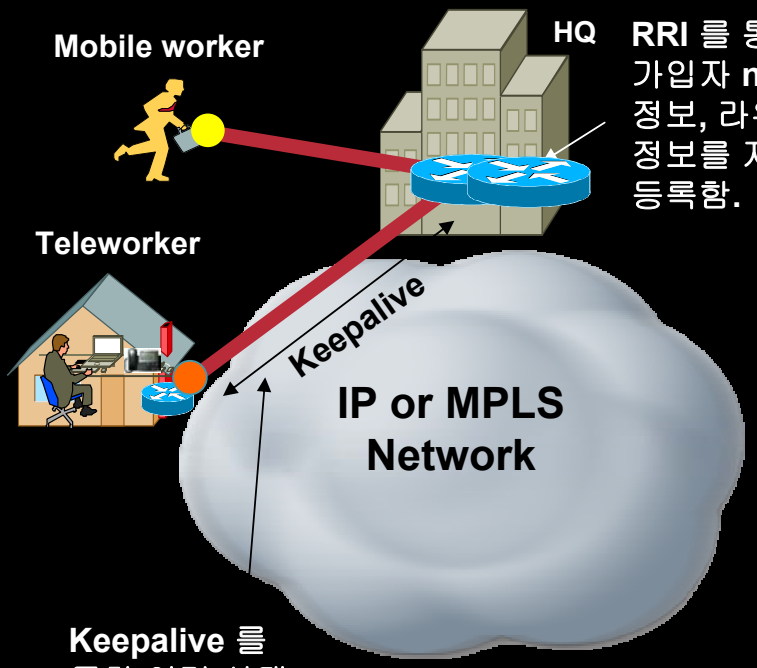
Network 기반 IPSec 네트워크 요구 사항

- Virtual IPsec and mapping to Service Provider Network (MPLS-VPN , L2)
- IPsec over MPLS
- 원격 VPN 접속의 Radius 인증 제공
- Dynamic Routing 가입자를 위한 GRE 지원
- Redundancy with Multiple Peers, HSRP, Anycast
- PE scaling guideline
  - how many session, how many vpn …



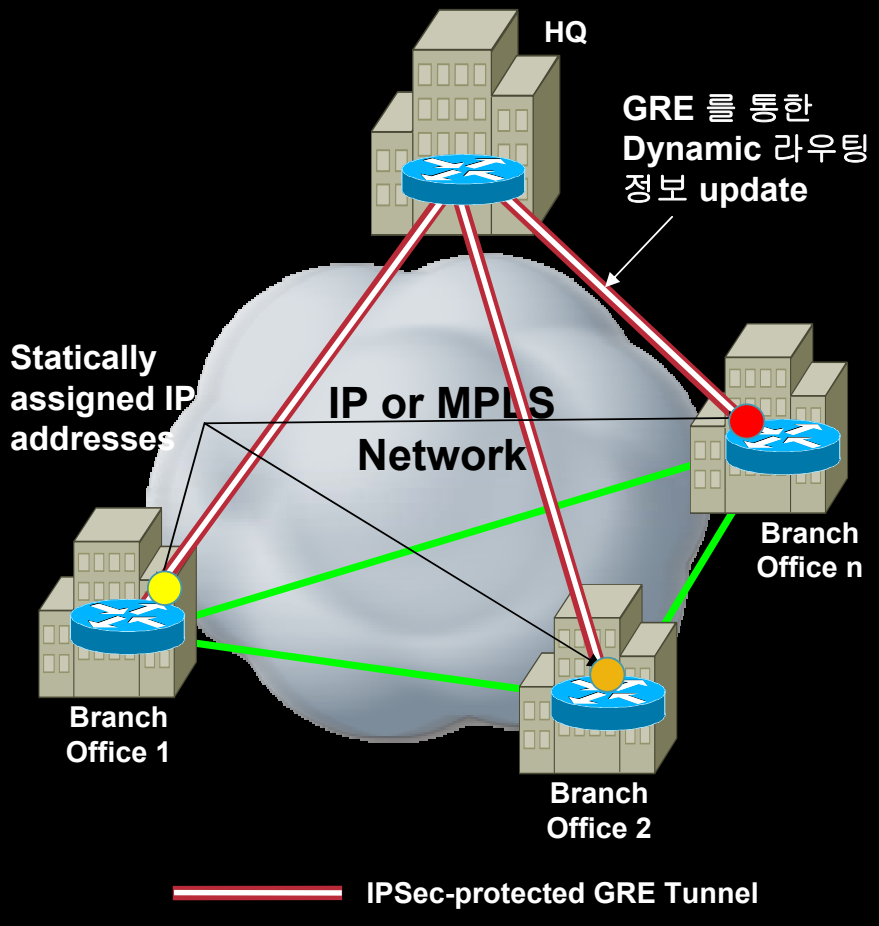
IPsec VPN 연결 유형
Remote Access

- 고객의 요구에 의해 필요 시 **Temporary IPSec VPN** 제공
- **oversubscription of the headend** 지원
- **Hub-and-Spoke topology**의 전형적인 구조 지원 **(Remote device**에서 터널 요청**)**
- **software** 또는 **hardware VPN clients**를 이용하여 유동 **IP address**를 할당 하여 **IPSec VPN** 제공.
- **RADIUS** 를 이용한 **username** 과 **passwords** 제공 또는 **Digital Certificates** 를 이용하여 사용자 인증
- 직접적인 인터넷 접근을 위한 **split tunneling** 지원
- 연결 가용성 확인을 위한 **DPD (Dead Peer Detection)**지원 및 **dual Headends** 를 이용한 이중화 지원

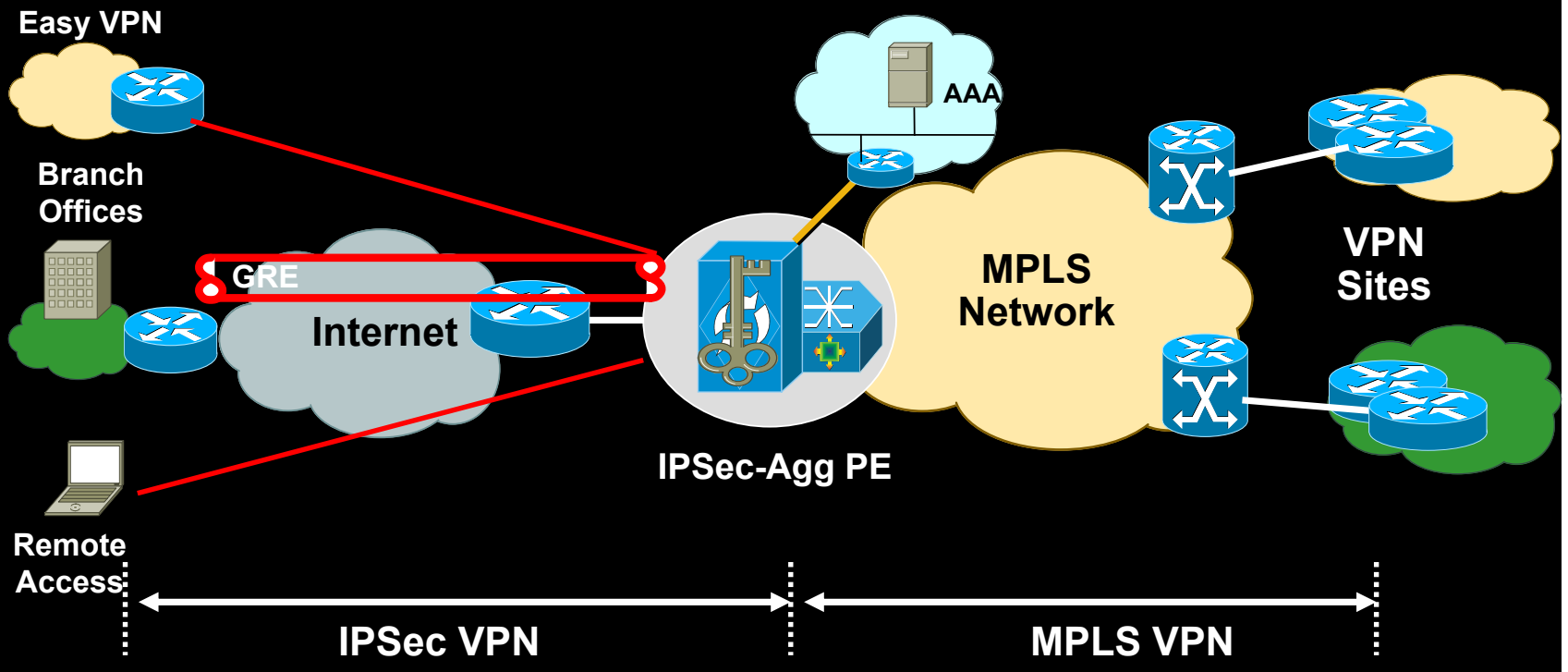


IPsec VPN 연결 유형
Site-to-Site VPN

- 기업 고객간 영구적인 **IPSec VPN** 연결 제공
- **Hub-and-Spoke** 의 전형적인 구조의 토폴로지 제공(필요 시 **mesh** 형태의 구조도 제공가능)
- **IPSec** 을 지원하는 라우터 에서 고정된 할당 **IP address** 지원
- 상호 인증을 위해 **Pre-shared keys** 또는 **Digital Certificates** 이용 하여 인증 후 터널 생성
- 기업고객간 **Dynamic** 라우팅 프로토콜 지원을 위해 **GRE tunnels** 지원
- 직접적인 인터넷 접근을 위한 **split tunneling** 지원
- **GRE** 를 이용하여 **Multicast Traffic** 지원



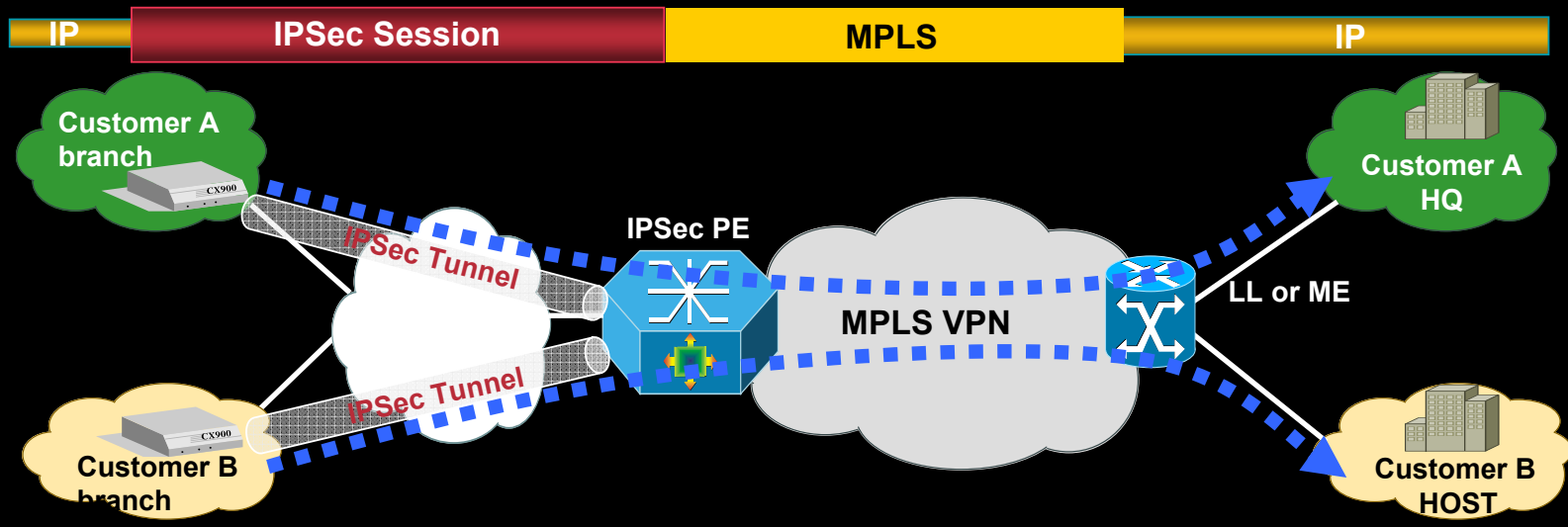
IPSec VPN과 MPLS VPN 망과의 연동



- **IPSec session** 연결/종료 관리 : **IPSec-Agg PE**
- 각 기업 고객별 **IPSec** 세션과 **MPLS VPN** 과의 맵핑
- **Radius** 를 이용한 **IPSec Client** 의 인증 관리
- **VPN** 고객별 분리된 **Crypto** 정책 **(crypto policy)** 정의 가능

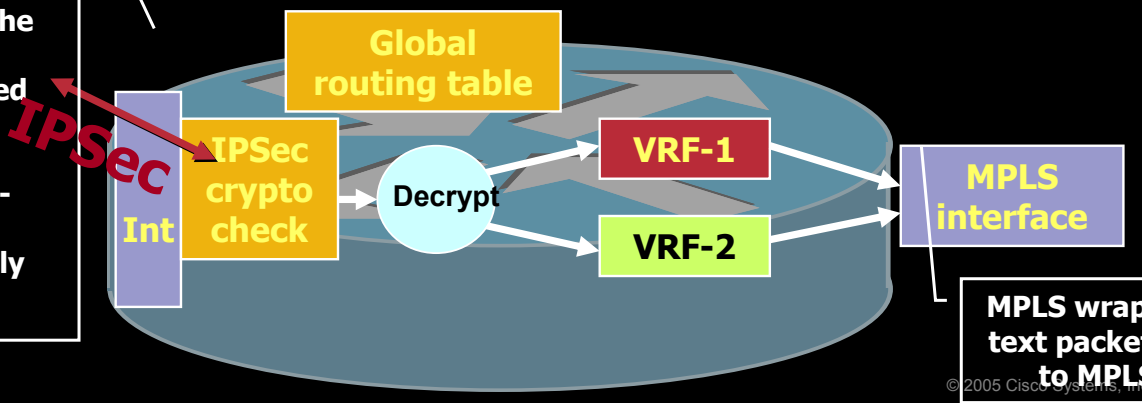
IPSec to MPLS with Virtualization 구성

Virtual IPsec using Multiple interface for all VPNs



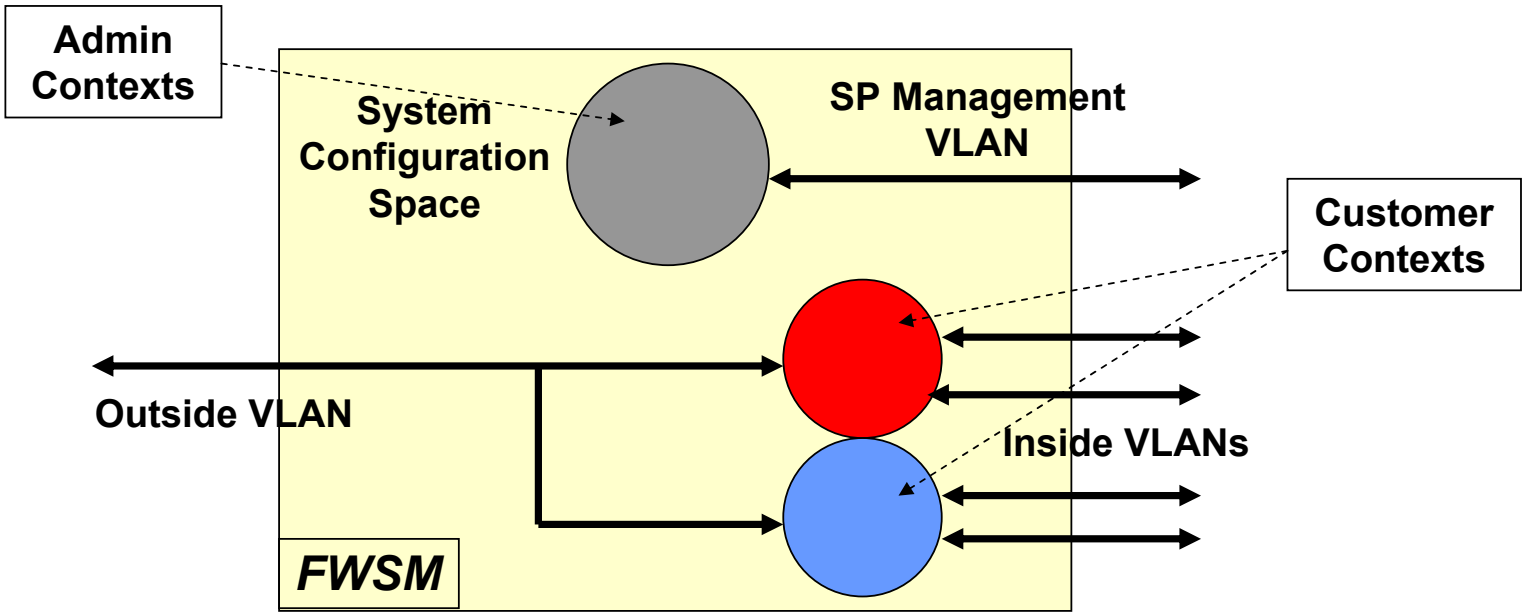
- Based on the IKE authentication, the IPSec tunnel is directly associated with the VRF.
- Decrypted clear-text packets forwarded directly to the right VRF.

Single or multiple Interface/Public IP address for all the VPNs



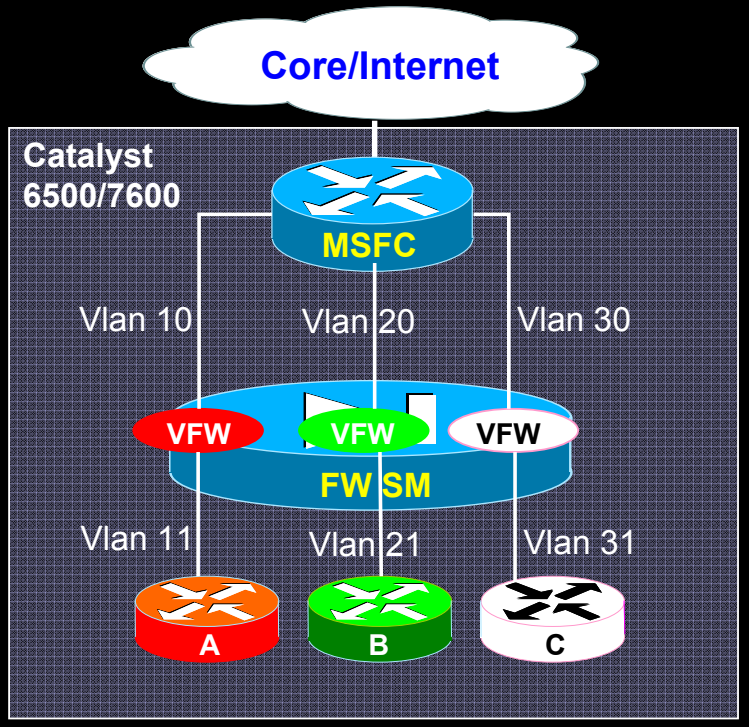
Network 기반 Virtual Firewall 서비스

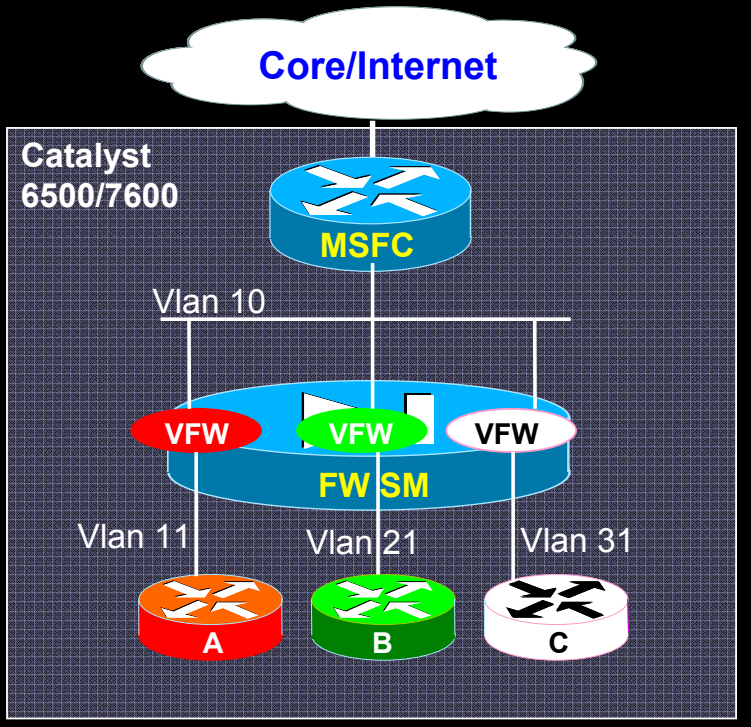
Virtual Firewall 이란?
Multiple Security Contexts



- 고객별 논리적인 방화벽 구성/지원
- 단일 모듈 안에 **100**가지의 가상 방화벽 구성
- 보안 정책의 다양성/유연성 제공
- 각 **Contexts**는 고객 고유의 방화벽 및 **VPN** 제공(**ACL, NAT**등)
- 시스템 관리자에 의한 방화벽 생성 및 관리

Virtual Firewall 이란?

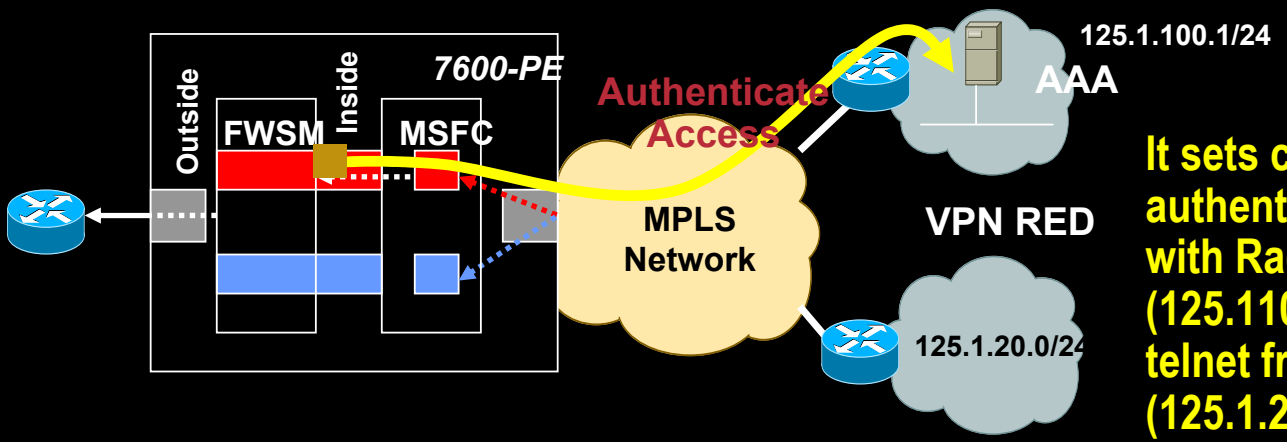




- 예, 3개의 고객 ⇨3개의 보안 **contexts –** 단일 모듈내에 최대 **100** 고객 수용
- **VLANs can be shared if needed (VLAN 10 on the right-hand side example**
- 각각의 **context** 는 기업고객 자체의 단일화된 정책 수용 **(NAT, access-lists, fixups, etc.)**

각 고객별 Context 관리
Context Access Control

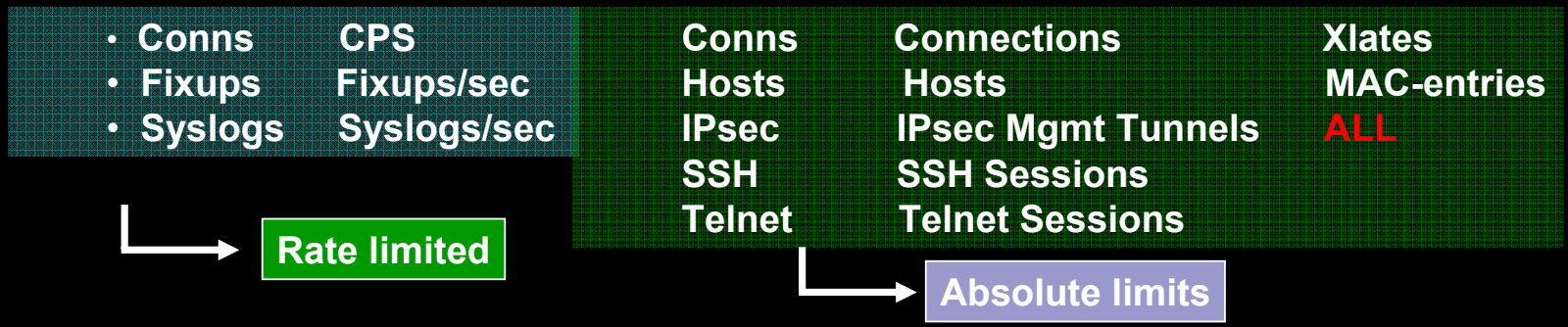
- 기업 고객이 가질 수 있는 권한 :
  - telnet/ssh 를 이용하여 고객 자신의 정보 접근 및 제어
  - 고객 자신의 정책 제어
- 기업 고객이 가질 수 없는 권한 :
  - 자신의 context 를 제외한 다른 고객 정보
  - 고객 자신에게 설정 되어 있는 지원관리(resource limiter)
- SP는 system space/admin context 를 이용하여 전체 모든 context 를 관리할 수 있다.



It sets context red to authenticate telnet users with Radius server (125.1100.1) and permits telnet from only one subnet (125.1.20.0/24)

자원 제한/관리
Resource Limiter

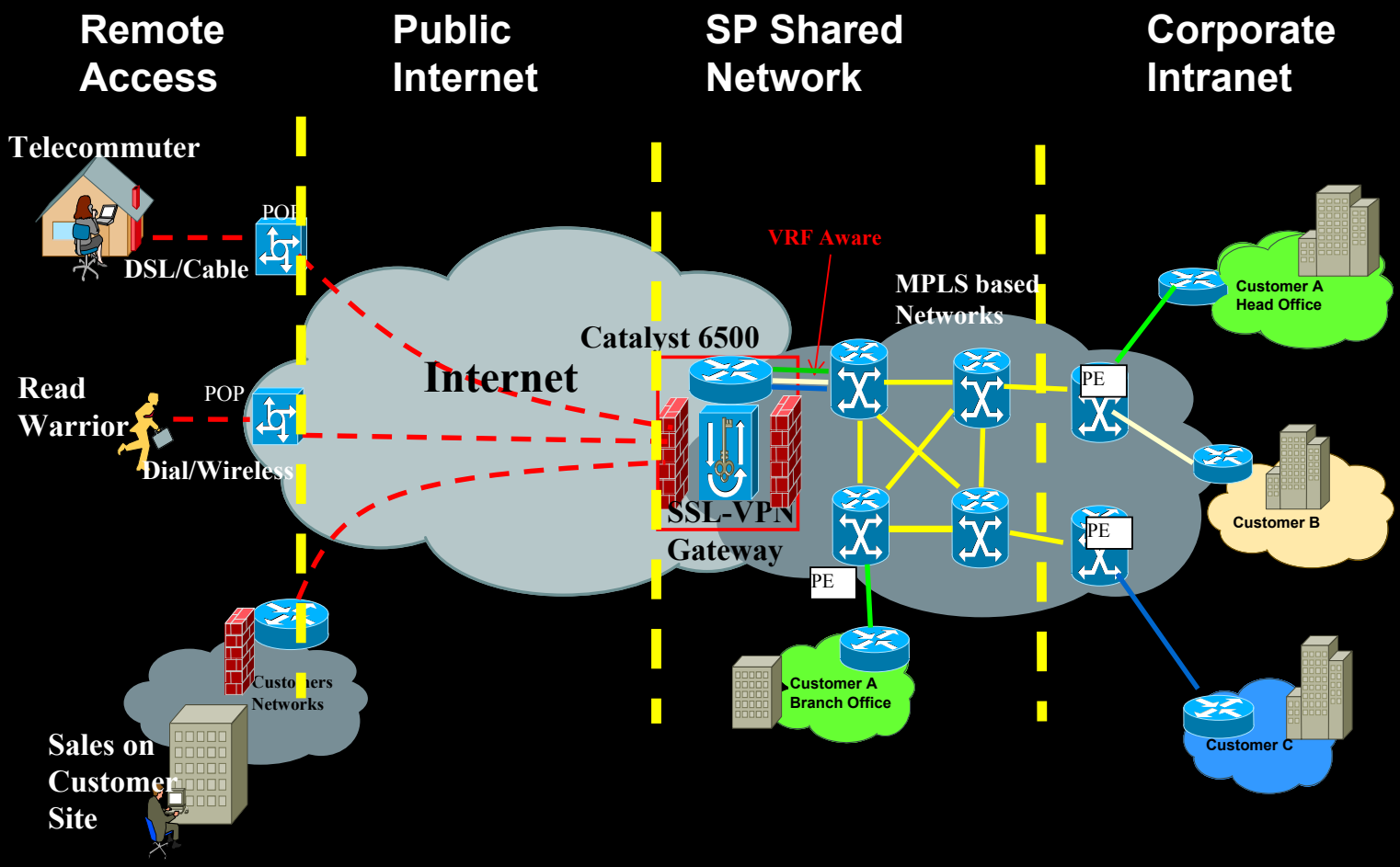
- **system mode**에서 ***classes***를 정의
- 개별 **contexts**에 각각의 클래스를 맵핑
- **Class**내에 특정한 자원제한을 적용하여 제한 가능



- **Limits specified as integer or %; 0 means no limit**
- **Resources *can* be oversubscribed: e.g. class assigns max 10% of resources, but 50 contexts are mapped to it**

Network 기반 Virtual Web VPN 서비스

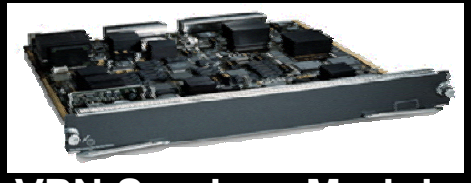
Network-Based SSL VPN Service



Network 기반 보안 서비스 제품 및 솔루션

Catalyst 6500 / Cisco 7600 Service Modules

Integrated 5Gbps Firewall



VPN Services Module (VPNSM)

SSL Module (SSL)

Integrated Multi-Gbps VPN

Secure Content(SSL) Accelerator

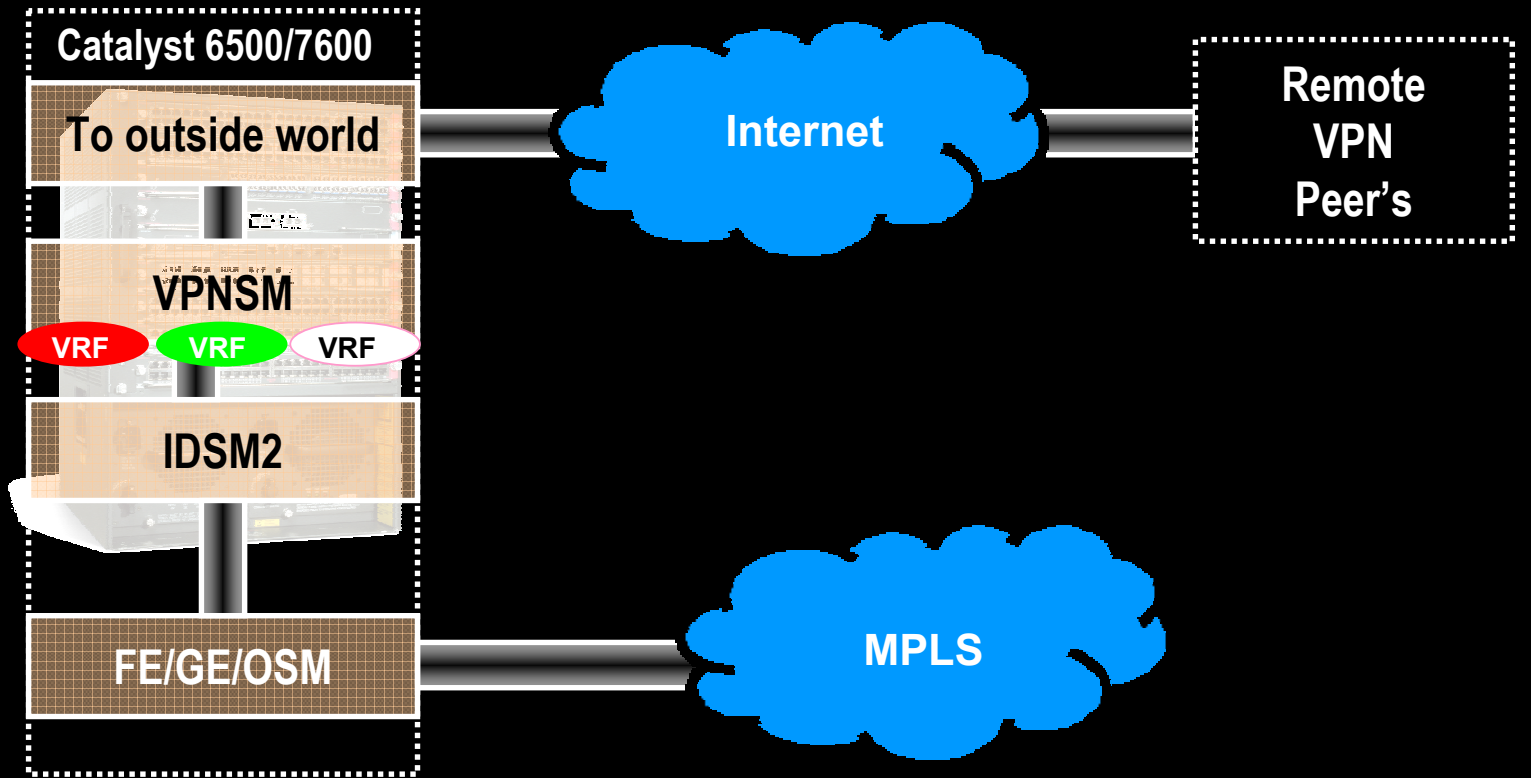
NEW

VPN SPA Services Module (VPN-SPA SM)

Integrated Multi-Gbps VPN

Service Module 의 조합 1

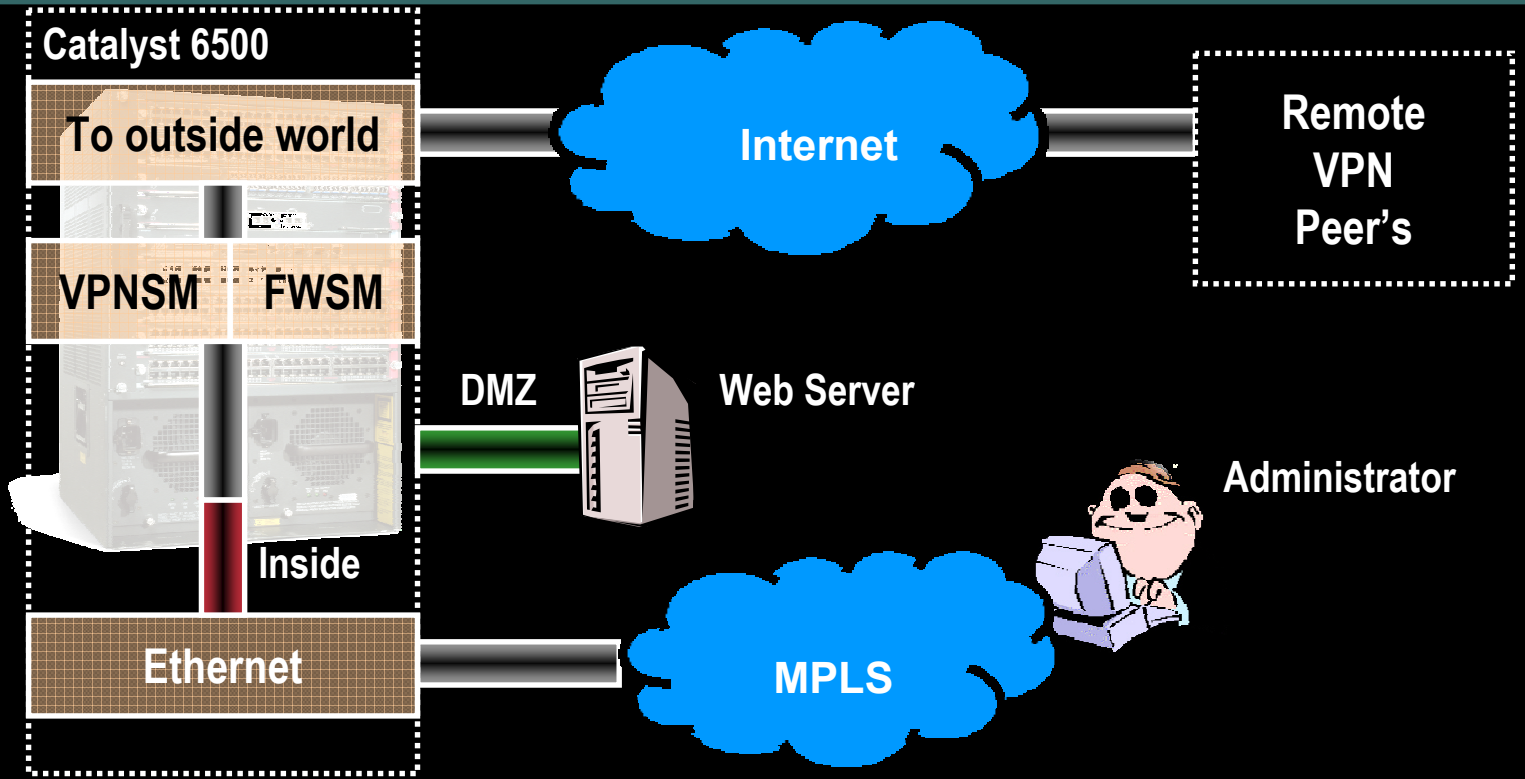
Scenario 1 - IDSM2 + VPNSM …



In this scenario, the VPNSM provides secure remote-access to MPLS-VPNS. The decrypted packet for each of the VPNs/VRFs goes thru the IDS for intrusion Detection.

Service Module 의 조합 2

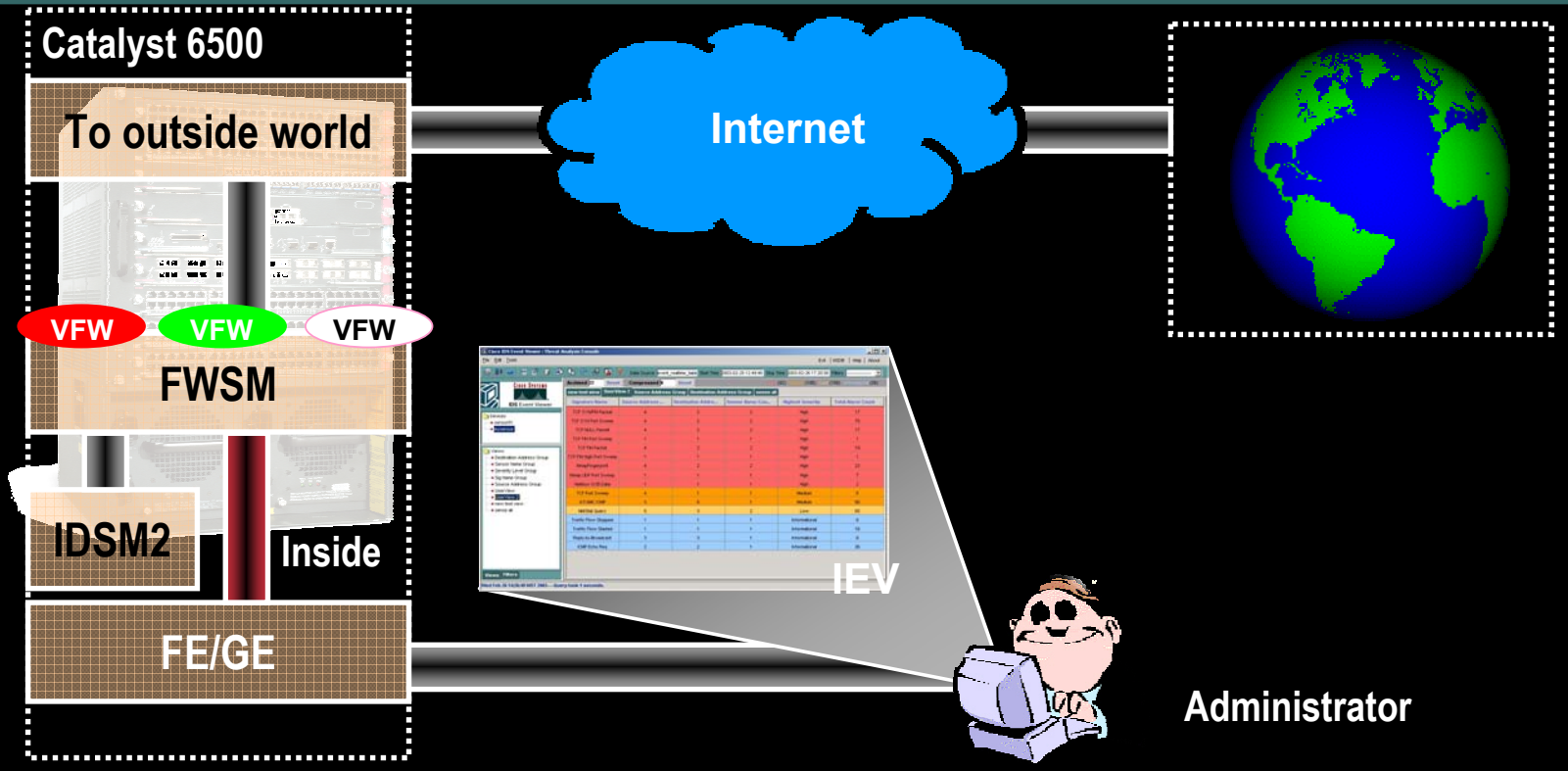
Scenario 2 – FWSM + VPNSM …



FWSM is used to provide Internet service to MPLS-VPN customers
Permits traffic from certain VPN Peer's to only access Server Farm in DMZ
Other VPN Peer's can access Inside/MPLS network

Service Module 의 조합 3

Scenario 3 – FWSM + IDSM2 …

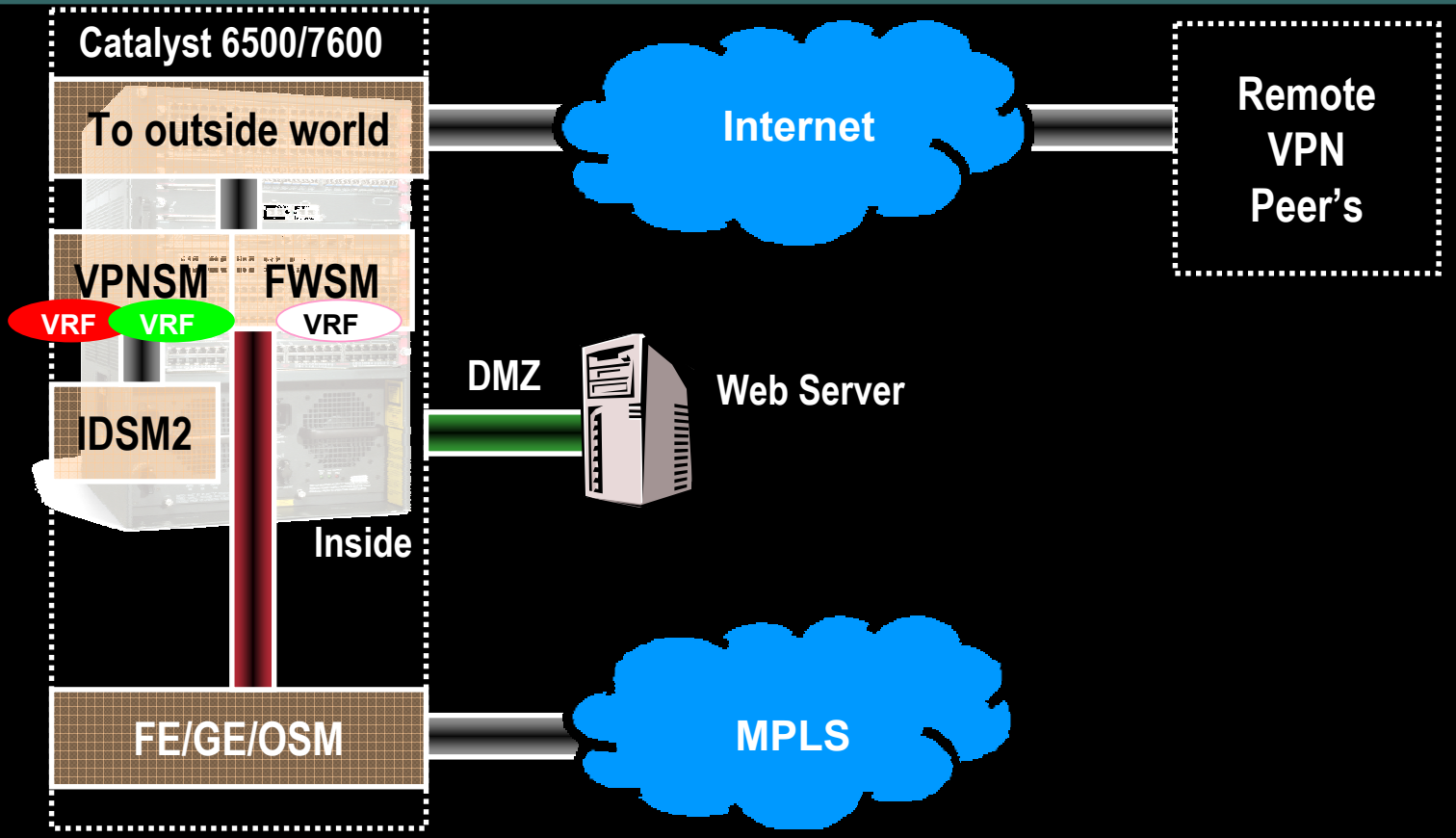


In this scenario, the IDSM will monitor traffic on different inside VLANS of the FWSM. Each VLAN representing a VPN Customer

The IDSM2 uses standard signatures to monitor the network for intrusion attempts…

Service Module 의 조합 4

Scenario 4 – FWSM + VPNSM + IDSM2 …



In this scenario, the VPNSM provides secure remote-access, FWSM provides Internet Offload And the IDSM provides intrusion detection service for decrypted packets coming out of the VPNSM

Summary

SP 보안 : 2 가지 중요 요소

Infrastructure 보안 (Core)

- 보장된 서비스를 제공 하기 위해 “기본적인 보안”에 충실한 네트웍 구축 **(SLA 및 service delivery)**
- 인프라에 위협이 되는 요소를 탐지, 완화 시킬 수 있으면서 고 가용성의 서비스를 제공 가능

보안 서비스
(Core, Head-End, CPE, End-Host)

- 이익 창출에 충실한 서비스 : **Virtual Firewall , Virtual IPSec VPN** 등을 통하여 기업 고객의 요구사항을 모두 만족 시킬 수 있는, 지능화된 인프라

Intelligent , Control

- 위협요소를 관리 하기 위해, 인프라를 자유스럽게 제어 할 수 있어야 하며,
  새로운 비즈니스 형태의 서비스를 자연스럽게 추가 할 수 있는 지능화되고, 자동화된 인프라 구축

Service Provider에 대한 기업 고객의 요구사항?

- **DoS and worm** 공격에 대한 최소한의 영향

  - 기업고객은 중단 없는 비즈니스에 집중 요구

- 자동화된 보호 시스템

  - 요구하는 보안 솔루션은, 서비스 **Network** 및 **Infrastructure**에 대해 최소한의 변경 만이 필요

- 고객의 요구사항은 **Inbound** 뿐 아니라 **Outbound** 에 대한 보호도 요구함

  - **Outbound**의 **DoS** 공격과 **worm** 트래픽은, **inbound traffic**에 의해 영향을 받을 수 있는 중요자원의 위협 만큼이나, 위협에 노출 되기 쉽다

SP는 과연 이러한 문제를 해결할 수 있나?

YES !

- **"Help, the Internet is down!"** → 분명히 해결 될 수 있습니다.
  - **Reverse the process - "The Internet was down, but we fixed it for you."**
- **Cisco**와 **Cisco-**파트너의 기술과 제품이 가능하게 해줍니다.
  - **Cisco NetFlow, Cisco Guard and Detector, BGP-triggered blackhole routing, and partners like Arbor allow SPs to provide proactive services**
  - **Cisco**는 많은 보안 **tool**을 제공하며, 이 모든 것들을 **SP**는 사용할 수 있으며, 고객들에게 제공 할 수 있습니다.
- 기업 고객들은 기꺼이 이러한 서비스에 대해 비용을 지불할 수 있습니다.
  - 만약 , 인터넷 장애 발생으로 인하여 비즈니스의 중단 **(customer service, on-line order** 등) 이 초래 될 수 있다면 ,
  - 기업 고객은 기꺼이 이러한 보안 위협으로부터 보장된 네트웍을 이용하며, 비용을 지불할 것입니다.

Cisco : Service Provider의 보안 파트너

- 진보된 기술과 어플리케이션, 입증된 솔루션 과 제품군으로 서비스 지원
  - **Clean Pipes, Network** 기반의 보안 서비스
- 성공적인 인프라 구축을 위해 검증된 솔루션 의 가이드
  - **NFP** , 네트웍의 기초적인 보안 기능 적용
  - **Router/Switch, Cisco IOS**
- 시장주도적인 서비스의 제공
  - 업계 최고의 성능 제공 및 호환성, 확장성 제공
  - 단일 플랫폼 에서의 **multiple** 솔루션 제공
  - 고객의 요구사항에 대한 다양한 선택 및 적응성 제공