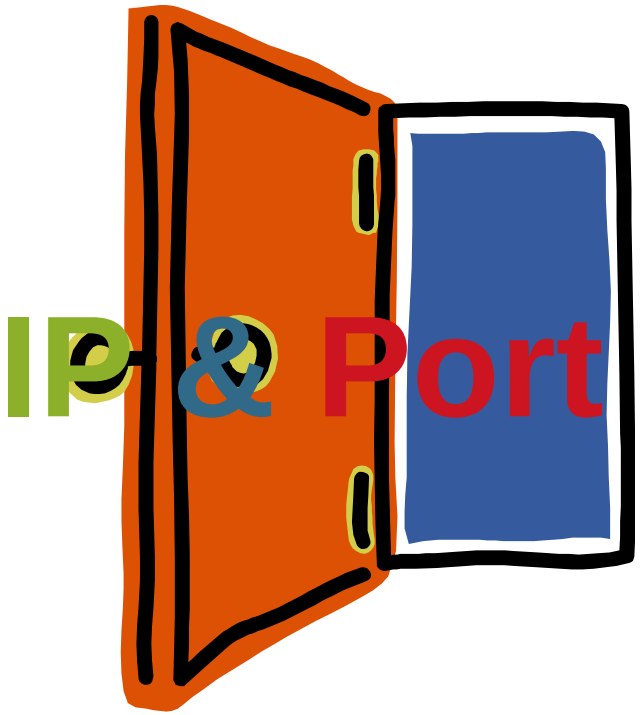
금융권 망분리 및 가상화 환경에서의 차세대 보안 적용 방안

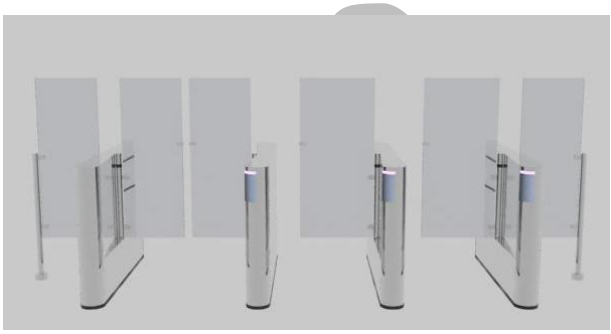
paloalto networks.

차세대 보안 이란 무엇인가?

paloalto networks.

차세대 보안의 필요성





paloalto networks.

차세대 보안의 필요성 변화하는 환경 vs 변하지 않는 보안

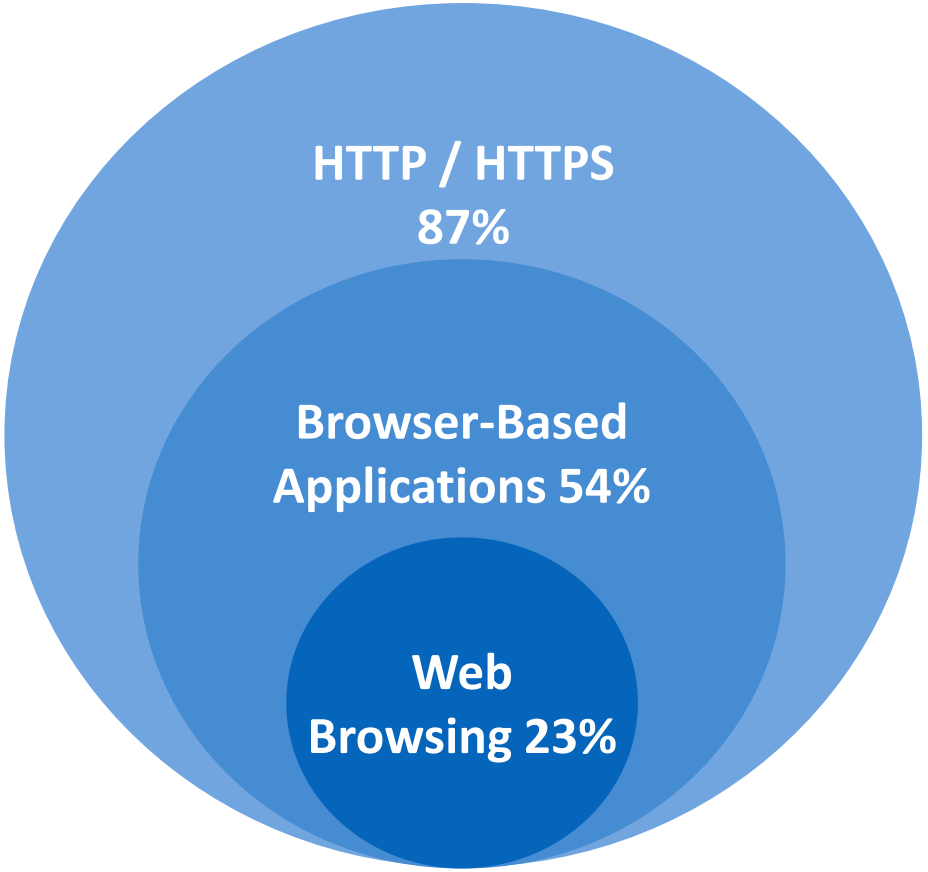
애플리케이션의 시대,

그리고 Advanced Threats 시대의 보안

- 새로운 애플리케이션이 매일 새롭게 생겨남
- 애플리케이션은 더 이상 포트와 프로토콜의 규칙을 따르지 않음
- 애플리케이션은 레거시 네트워크 보안을 우회할 수 있게 디자인되고 있음
- 공격자의 전문성이 유래없이 높음

paloalto networks.

차세대 보안의 필요성 변화하는 환경 vs 변하지 않는 보안



paloalto networks.

차세대 보안의 필요성 변화하는 환경 vs 변하지 않는 보안

paloalto networks.

차세대 보안의 요건

1. 포트, 프로토콜, SSL, 우회 기술에 관계없이 애플리케이션 분석
2. IP 주소가 아닌 사용자 인식
3. 애플리케이션을 통해서 유입되는 위협을 실시간으로 방어
4. 애플리케이션에 대한 세밀한 Visibility(가시성) 및 Control(제어)
5. 성능저하를 최소화하면서 멀티 기가 비트 성능 제공

Next Generation Security

paloalto networks.

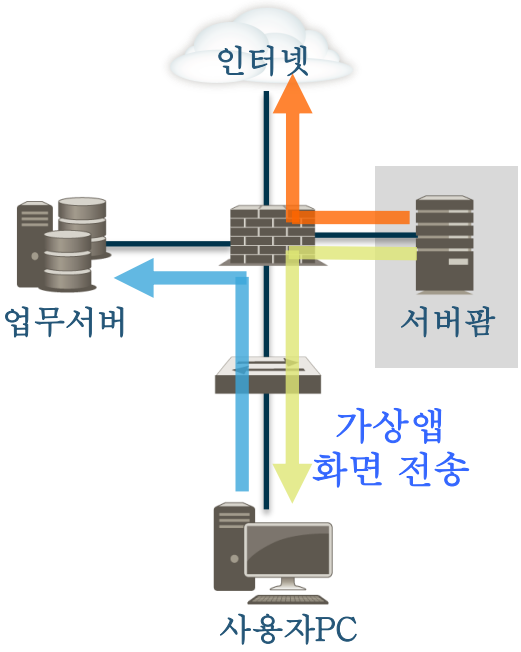
망분리 환경에서 차세대 보안이 왜 필요한가?

paloalto networks.

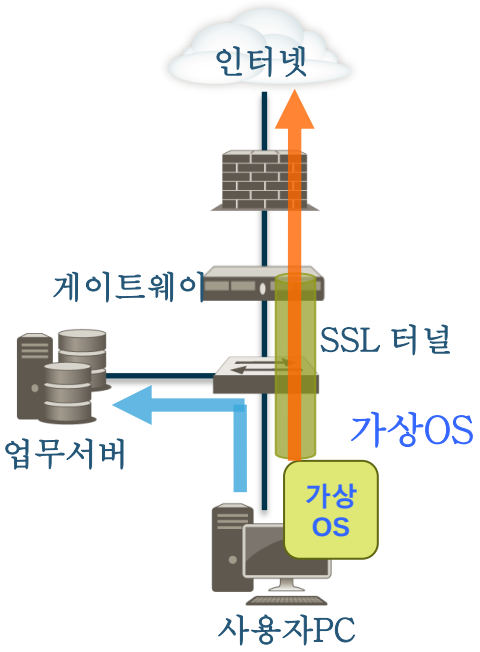
망분리 후의 고민……

다양한 방법으로 독립적인 환경을 구축 했지만……

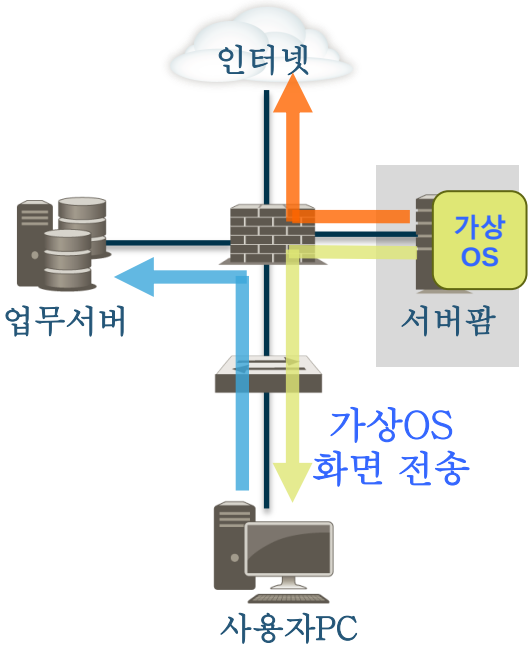
물리적 망분리



논리적 망분리
CBC(Client Based Computing)

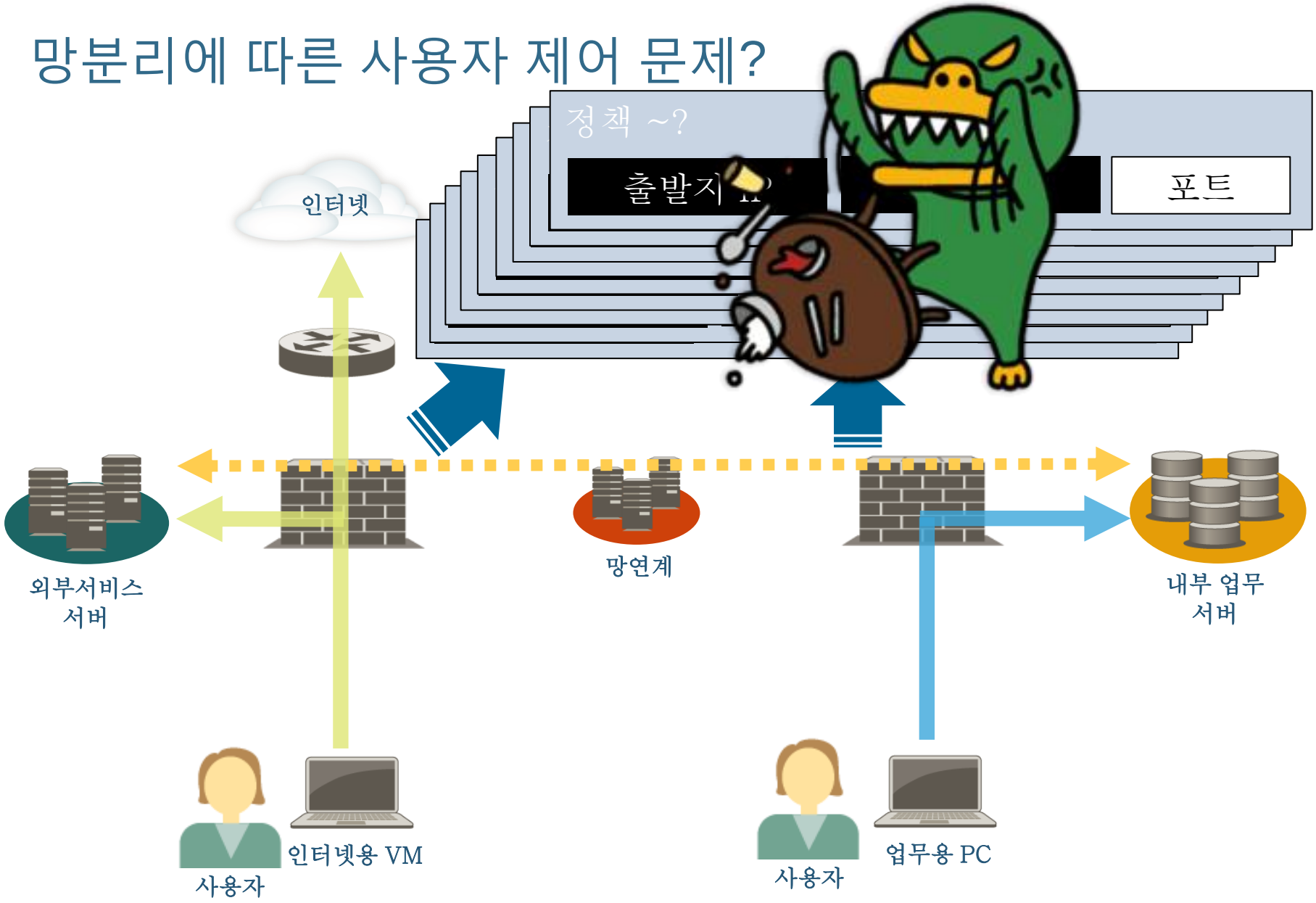


논리적 망분리
VDI(Virtual Desktop Infrastructure)



paloalto networks.

망분리에 따른 사용자 제어 문제?



paloalto networks.

망분리 환경에서 차세대 보안이 왜 필요한가?

1. 다양한 인증 시스템과의 연동을 통해 사용자 기반 보안으로의 전환
2. *영역별 분리에 따른 가상 보안 시스템 구성*

paloalto networks.

차세대 보안의 사용자 기반 적용 사례

AD 연동을 통한 사용자 제어

Mina

내부 업무서버

User별 방화벽 정책 적용

Source Interface	Destination Interface	Source IP	Destination IP	Service	Application	User/ Group	Action
Any	Internet	Any	Any	Any	Web Browsing	Mina	Allow
Any	DMZ	Any	Any	Any	Any	Mina	Deny

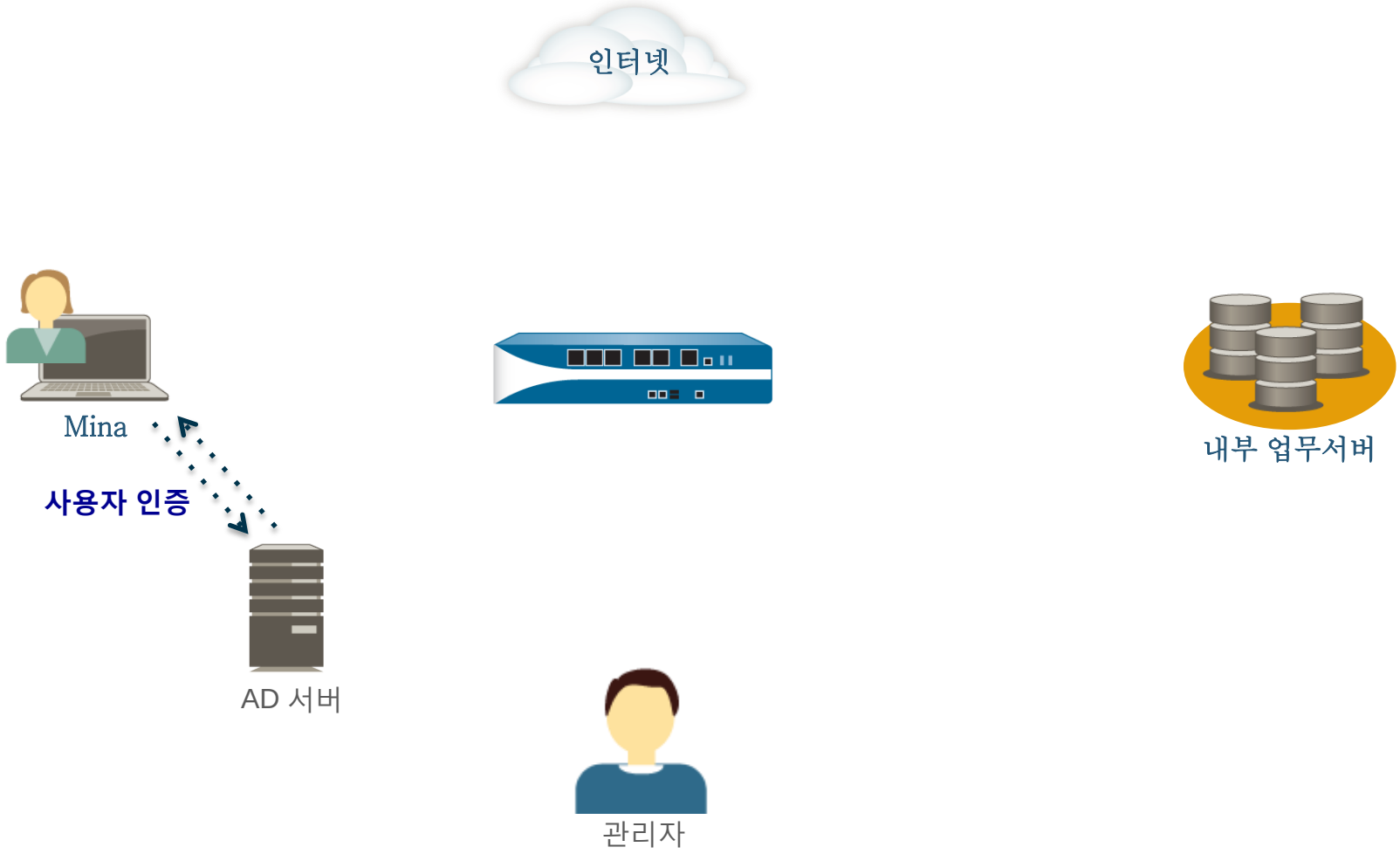
AD 서버

관리자

paloalto networks.

차세대 보안의 사용자 기반 적용 사례

AD 연동을 통한 사용자 제어



차세대 보안의 사용자 기반 적용 사례

AD 연동을 통한 사용자 제어

Mina

내부 업무서버

AD 서버

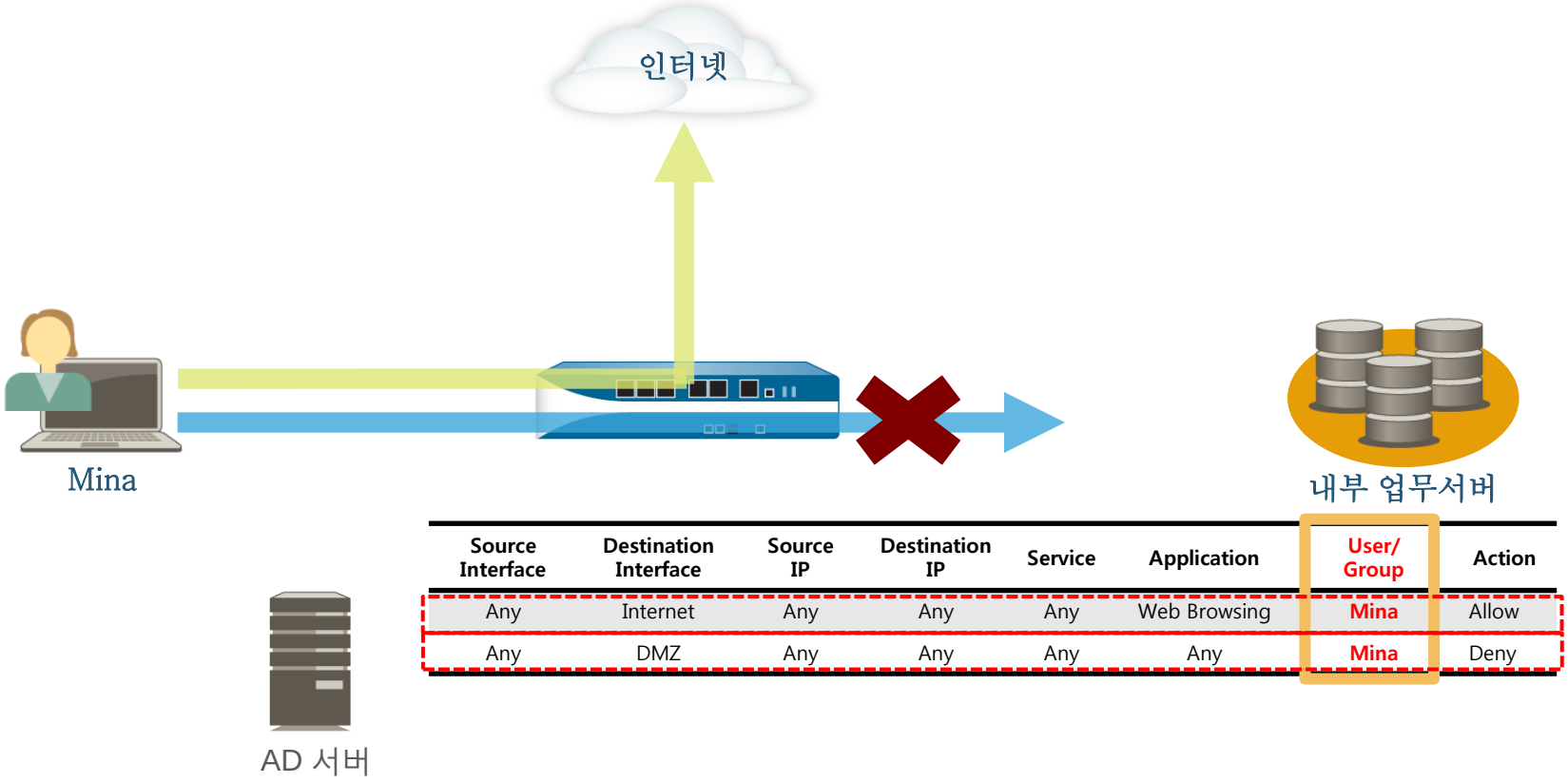
사용자 로그인 정보 수집

Username	IP Address
Mina	10.1.1.7
billyjo	10.1.1.4
kschoi	10.1.1.92
...	...

paloalto networks.

차세대 보안의 사용자 기반 적용 사례

AD 연동을 통한 사용자 제어

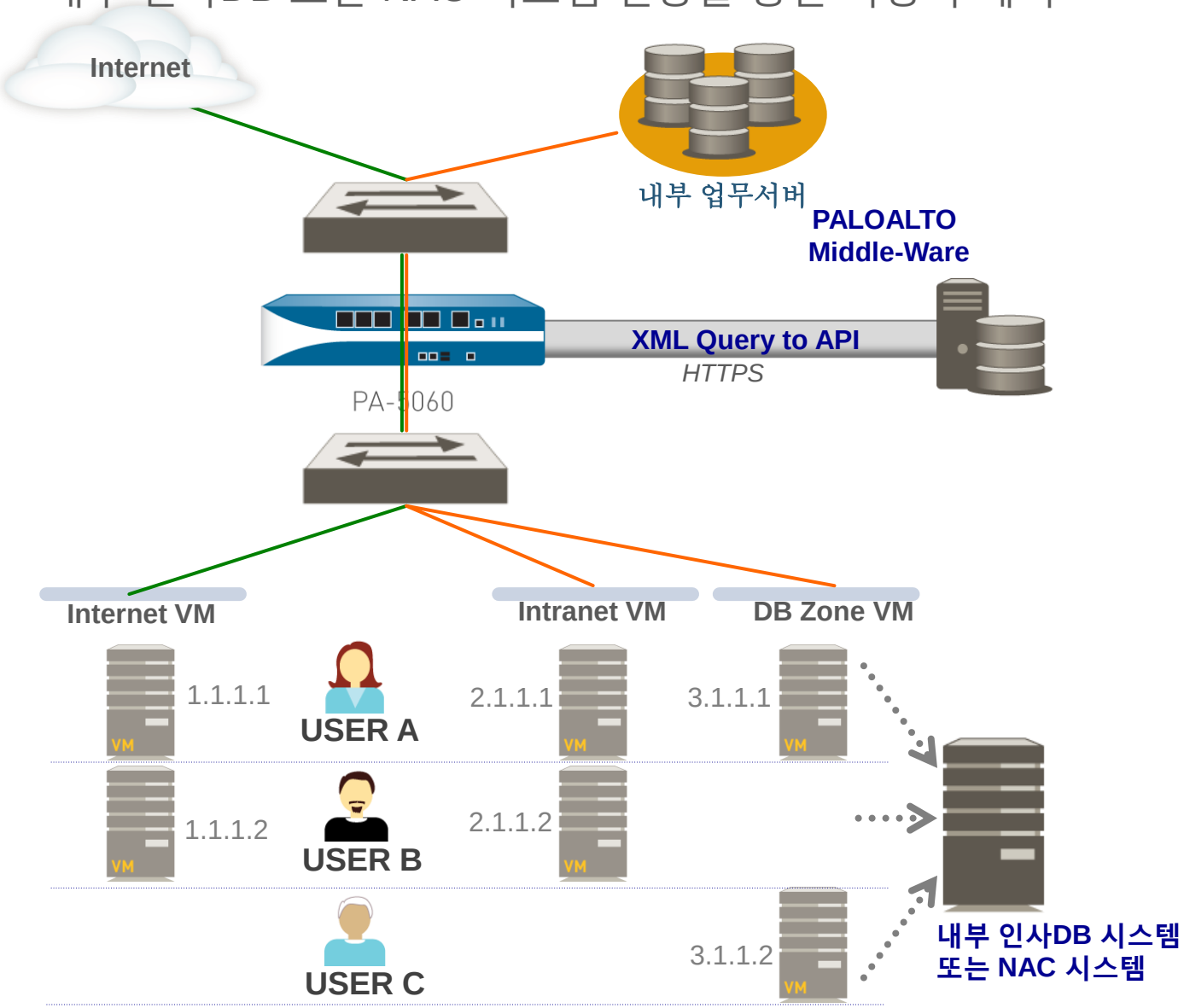


Source Interface	Destination Interface	Source IP	Destination IP	Service	Application	User/ Group	Action
Any	Internet	Any	Any	Any	Web Browsing	Mina	Allow
Any	DMZ	Any	Any	Any	Any	Mina	Deny

paloalto networks.

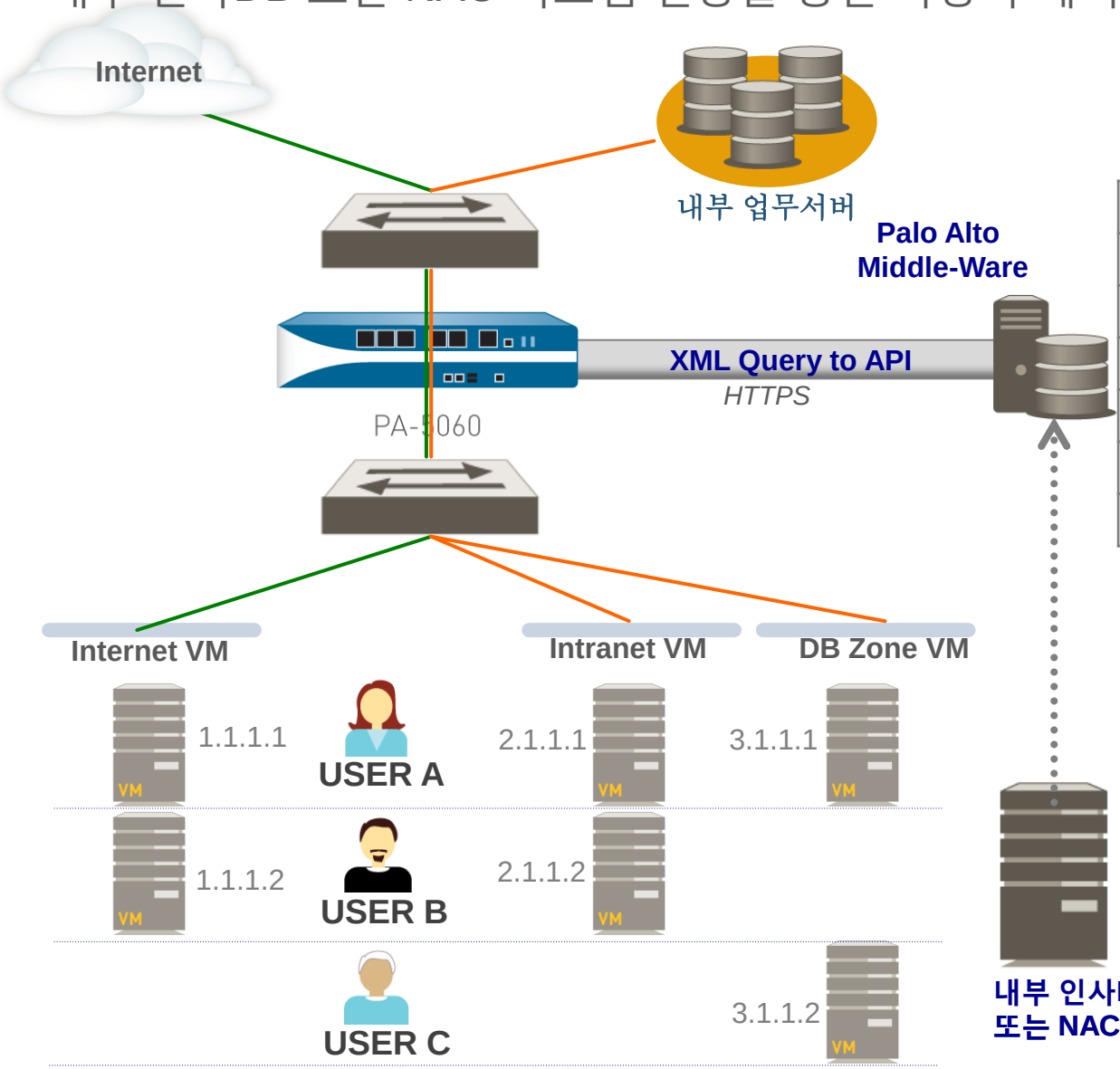
차세대 보안의 사용자 기반 적용 사례

내부 인사DB 또는 NAC 시스템 연동을 통한 사용자 제어



차세대 보안의 사용자 기반 적용 사례

내부 인사DB 또는 NAC 시스템 연동을 통한 사용자 제어



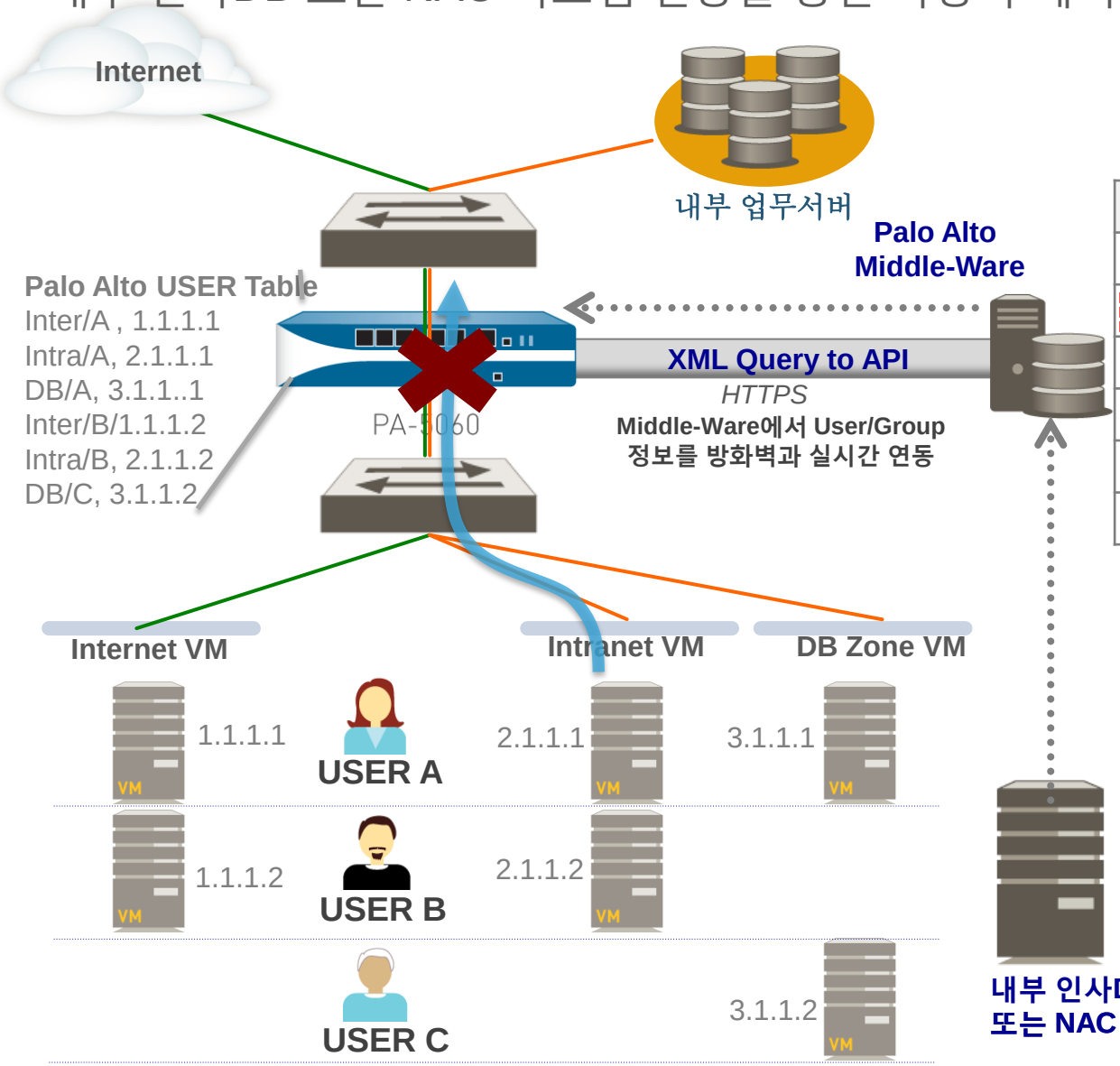
USER-ID	IP	H-name	Action
A	1.1.1.1	Inter-A	ADD
A	2.1.1.1	Intra-A	DELETE
A	3.1.1.1	DB-A	ADD
B	1.1.1.2	Inter-B	ADD
B	2.1.1.2	Intra-B	ADD
C	3.1.1.2	DB-C	ADD

Middle-Ware로 주기적으로 사용자 정보 업데이트

paloalto networks.

차세대 보안의 사용자 기반 적용 사례

내부 인사DB 또는 NAC 시스템 연동을 통한 사용자 제어



USER-ID	IP	H-name	Action
A	1.1.1.1	Inter-A	ADD
A	2.1.1.1	Intra-A	DELETE
A	3.1.1.1	DB-A	ADD
B	1.1.1.2	Inter-B	ADD
B	2.1.1.2	Intra-B	ADD
C	3.1.1.2	DB-C	ADD

Middle-Ware로 주기적으로 사용자 정보 업데이트

paloalto networks.

차세대 보안의 사용자 기반 적용 사례

계정관리 시스템 또는 NAC 시스템과 Syslog를 통한 사용자 제어

Mina

내부 업무서버

Syslog 연동

계정관리 시스템
또는 NAC 시스템

User별 보안 정책 적용

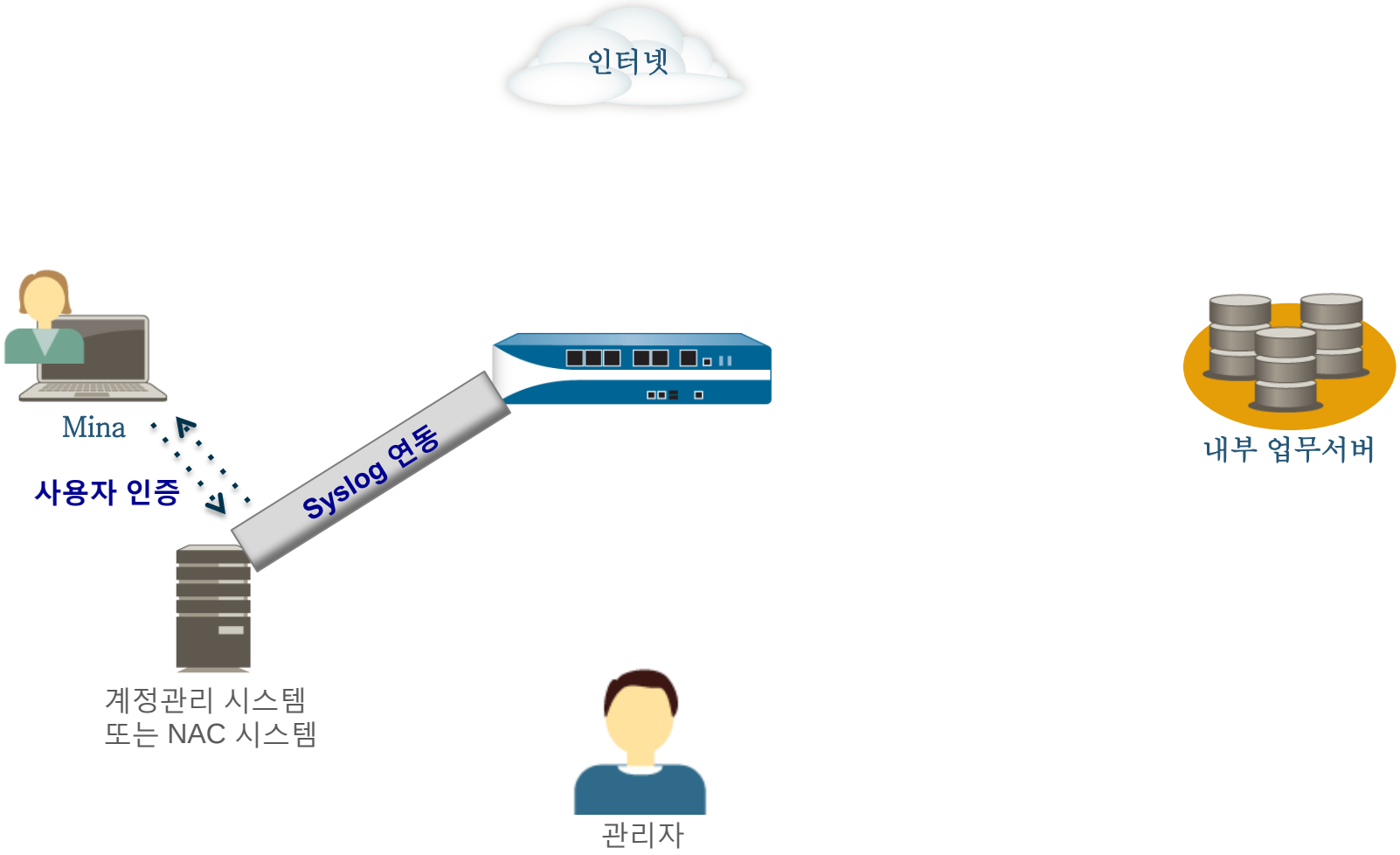
Source Interface	Destination Interface	Source IP	Destination IP	Service	Application	User/ Group	Action
Any	Internet	Any	Any	Any	Web Browsing	Mina	Allow
Any	DMZ	Any	Any	Any	Any	Mina	Deny

관리자

paloalto networks.

차세대 보안의 사용자 기반 적용 사례

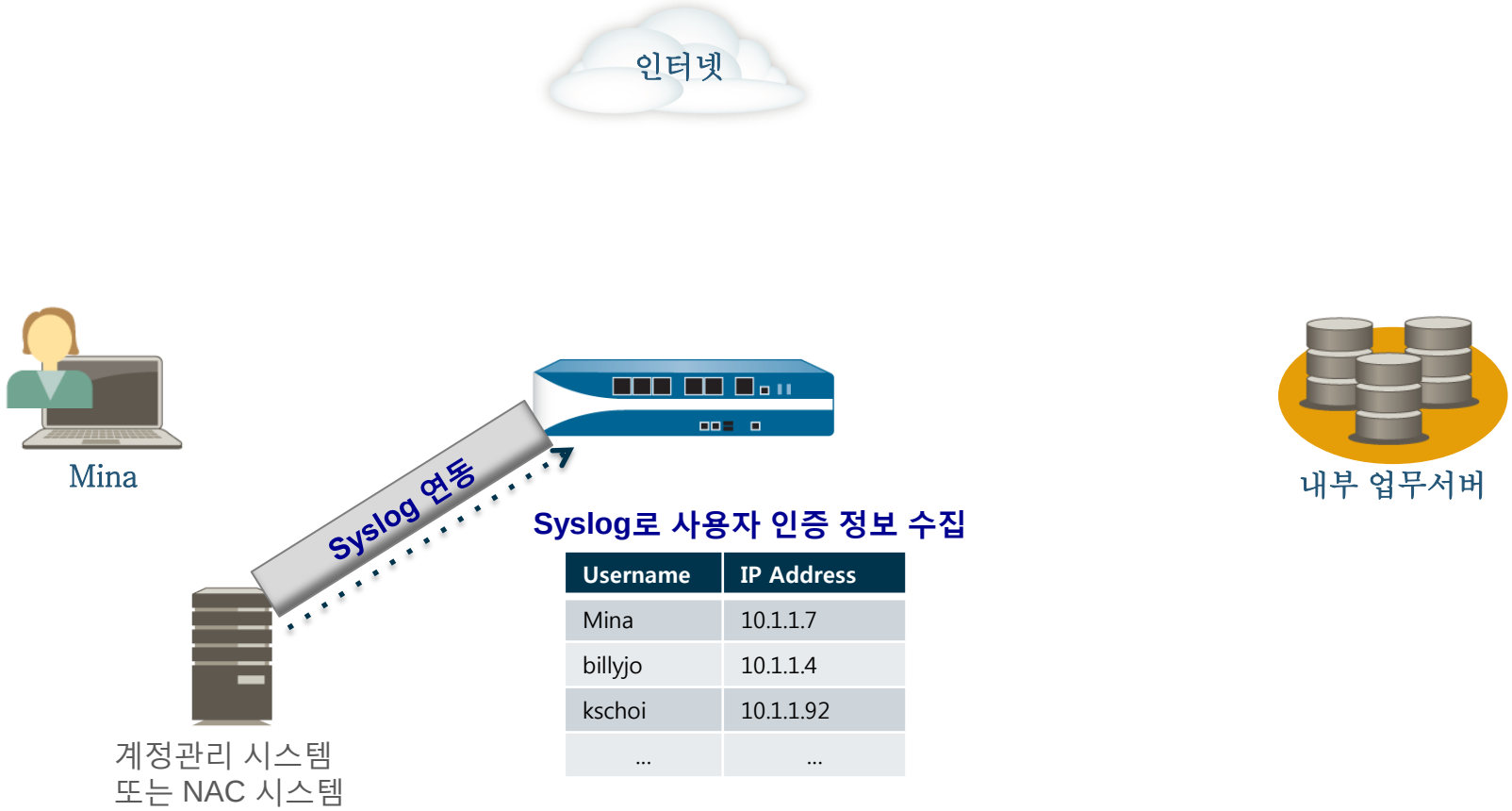
계정관리 시스템 또는 NAC 시스템과 Syslog를 통한 사용자 제어



paloalto networks.

차세대 보안의 사용자 기반 적용 사례

계정관리 시스템 또는 NAC 시스템과 Syslog를 통한 사용자 제어



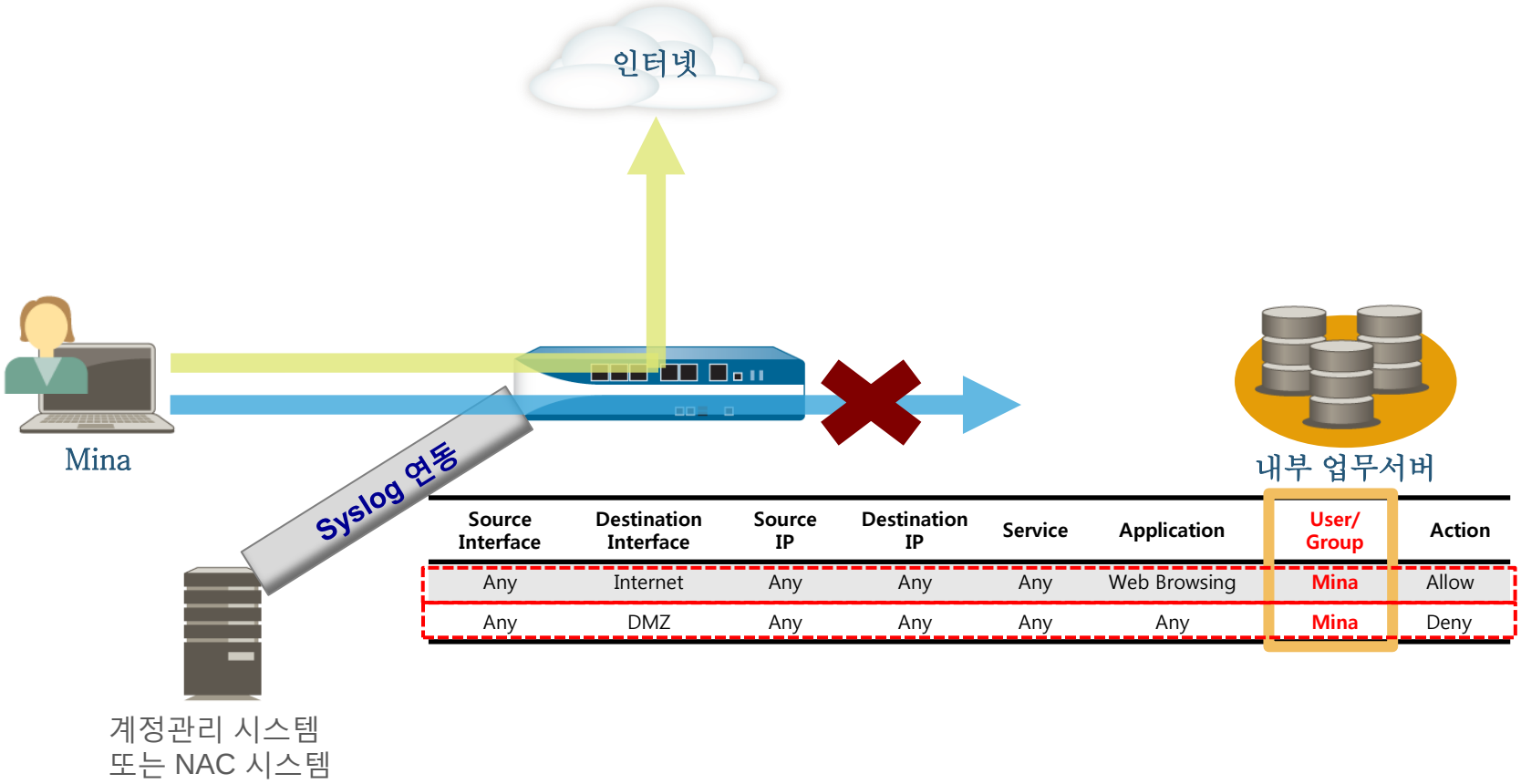
Syslog로 사용자 인증 정보 수집

Username	IP Address
Mina	10.1.1.7
billyjo	10.1.1.4
kschoi	10.1.1.92
...	...

paloalto networks.

차세대 보안의 사용자 기반 적용 사례

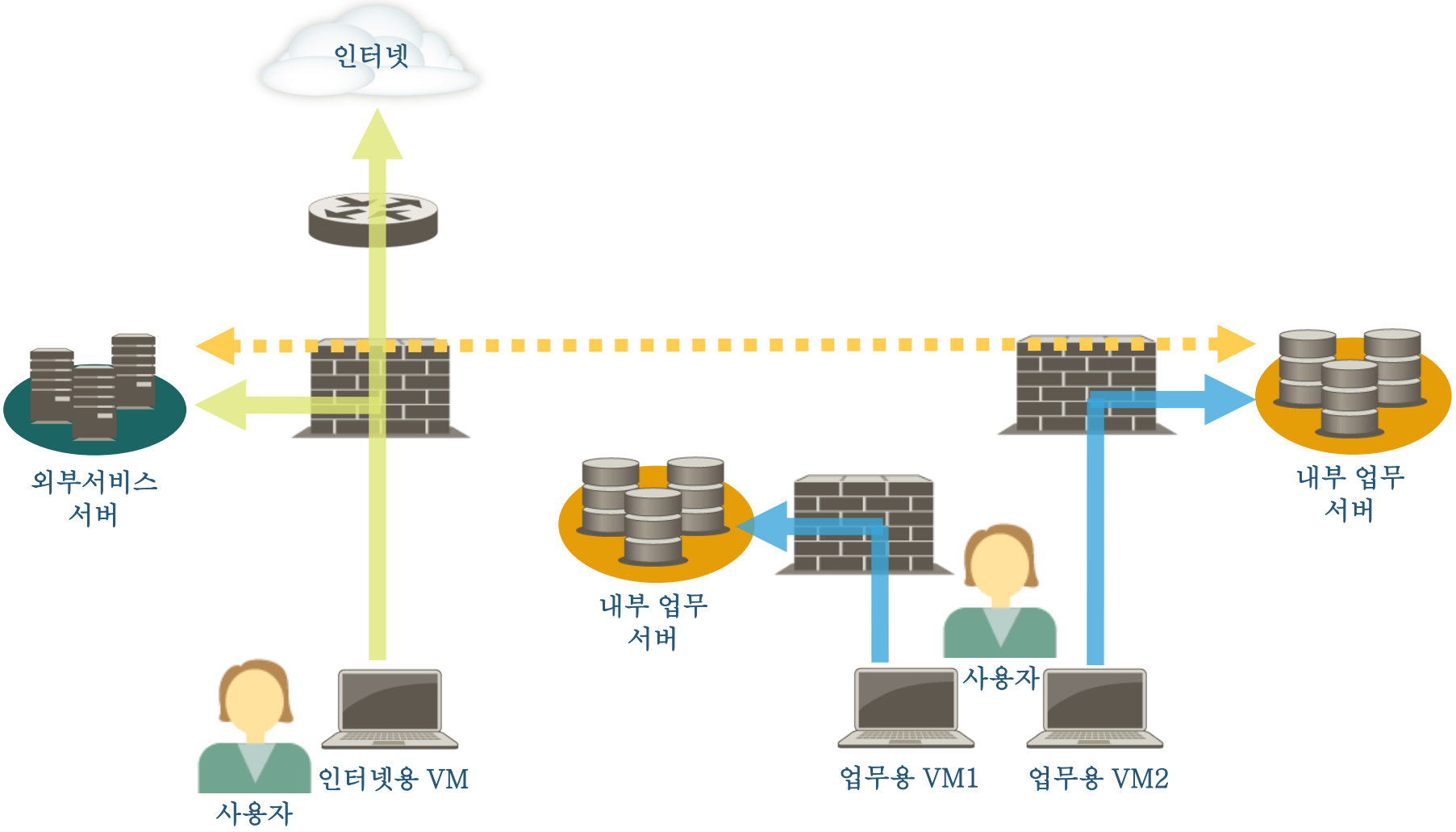
계정관리 시스템 또는 NAC 시스템과 Syslog를 통한 사용자 제어



Source Interface	Destination Interface	Source IP	Destination IP	Service	Application	User/ Group	Action
Any	Internet	Any	Any	Any	Web Browsing	Mina	Allow
Any	DMZ	Any	Any	Any	Any	Mina	Deny

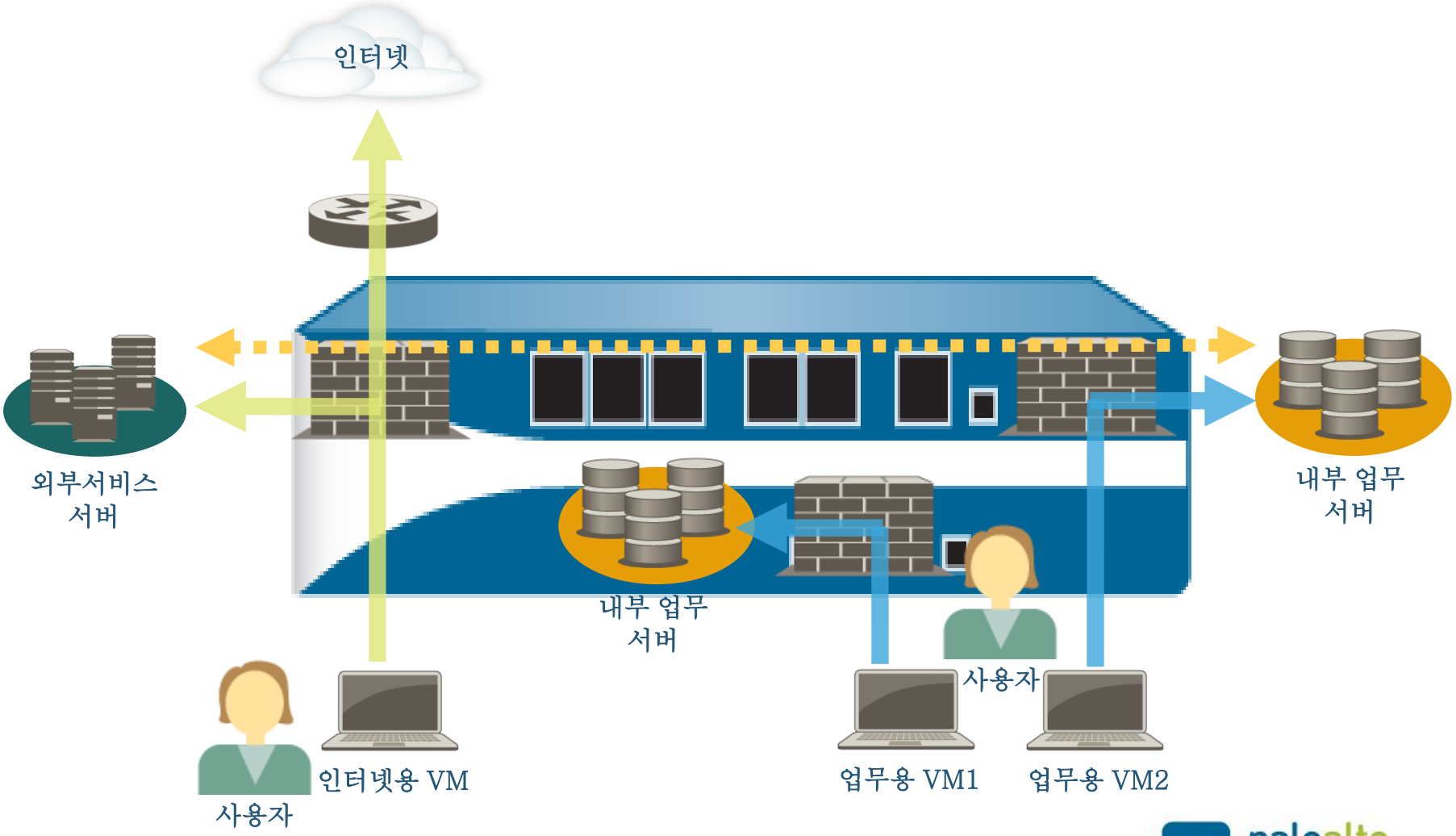
paloalto networks.

영역별 방화벽 분리가 필요한 경우?



2. 영역별 가상화 시스템 적용 사례

가상화 시스템을 이용하여 인터넷 망과 여러 업무 영역별로 완벽하게 분리하여 통합 구성



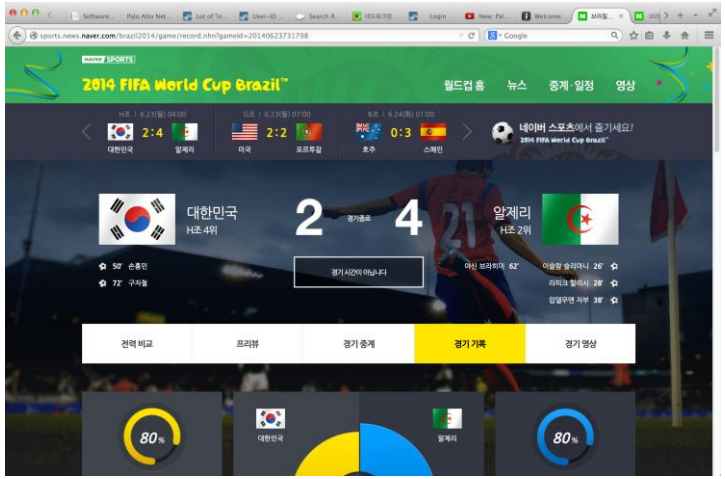
paloalto networks.

사용자 기반에서의 차세대 보안 적용 방안

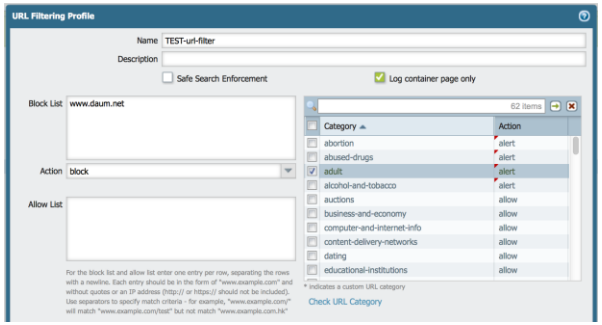
1. *사용자의 웹필터 보안 적용*
2. *사용자별 애플리케이션 기반의 트래픽 제어*
3. *사용자별 애플리케이션 기반의 파일 제어*

paloalto networks.

1. 사용자별 URL 필터를 통한 WEB 필터 사례



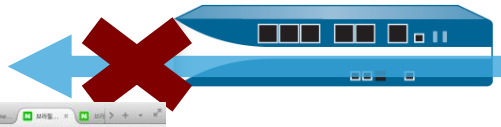
URL 필터 적용



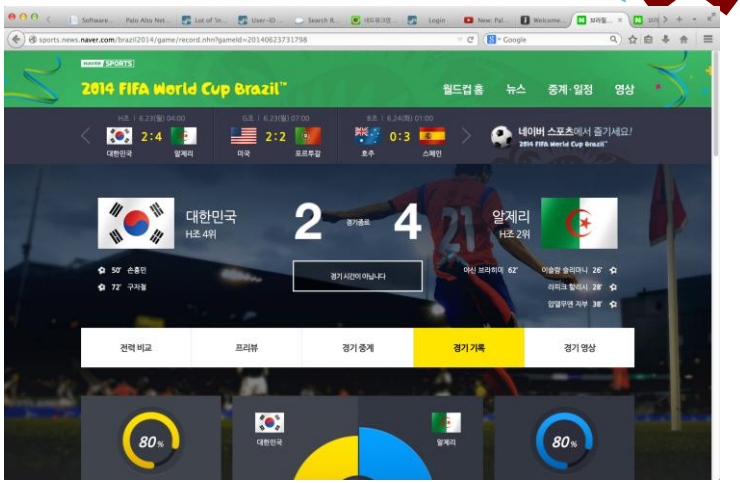
관리자

paloalto networks.

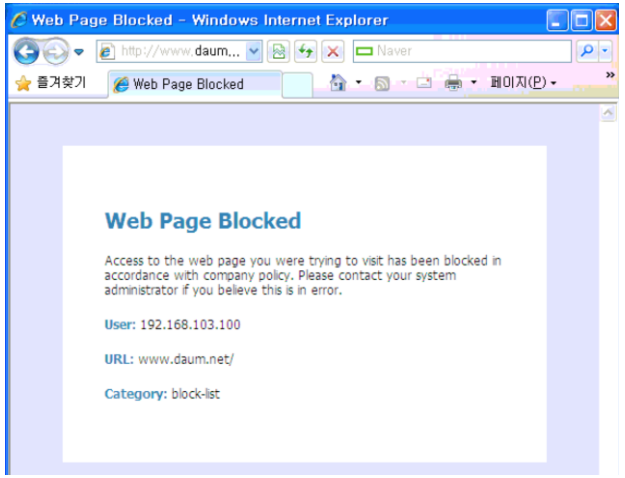
1. 사용자별 URL 필터를 통한 WEB 필터 사례



Mina

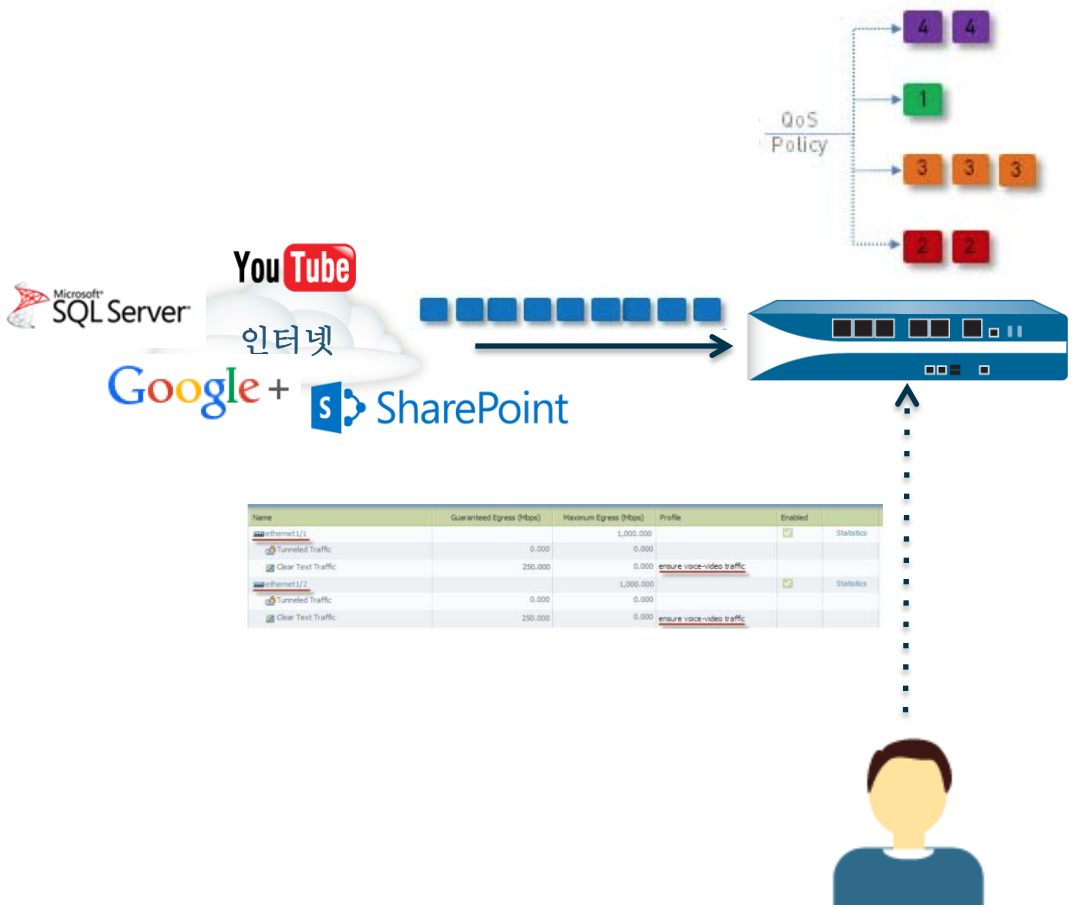


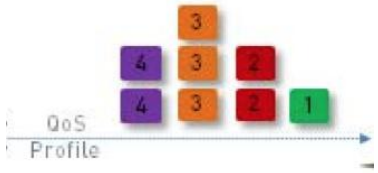
관리자



paloalto networks.

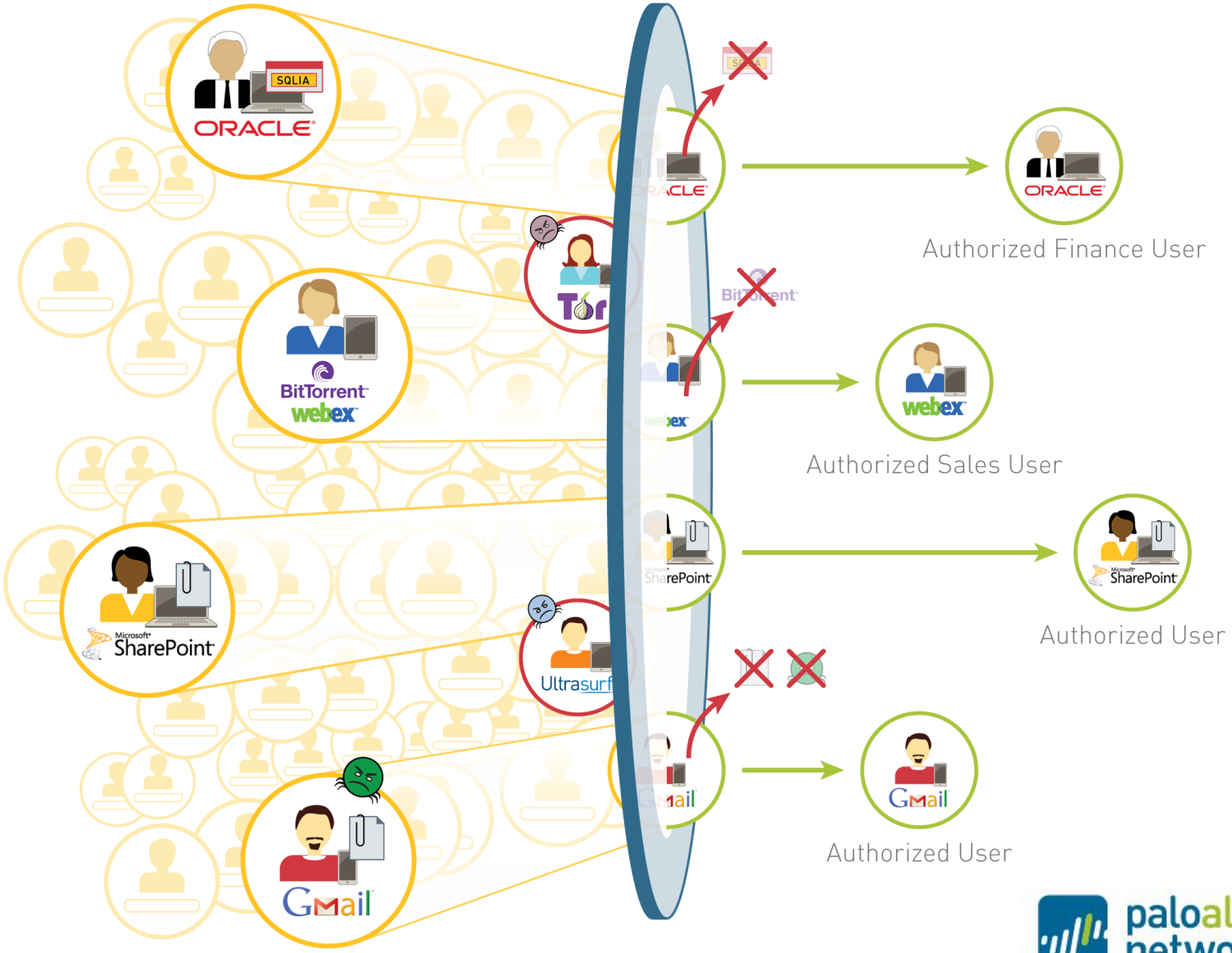
2. 사용자별 애플리케이션 기반의 트래픽 제어 사례(QoS)





paloalto networks.

3. 사용자별 애플리케이션 기반의 파일 제어 사례



paloalto networks.

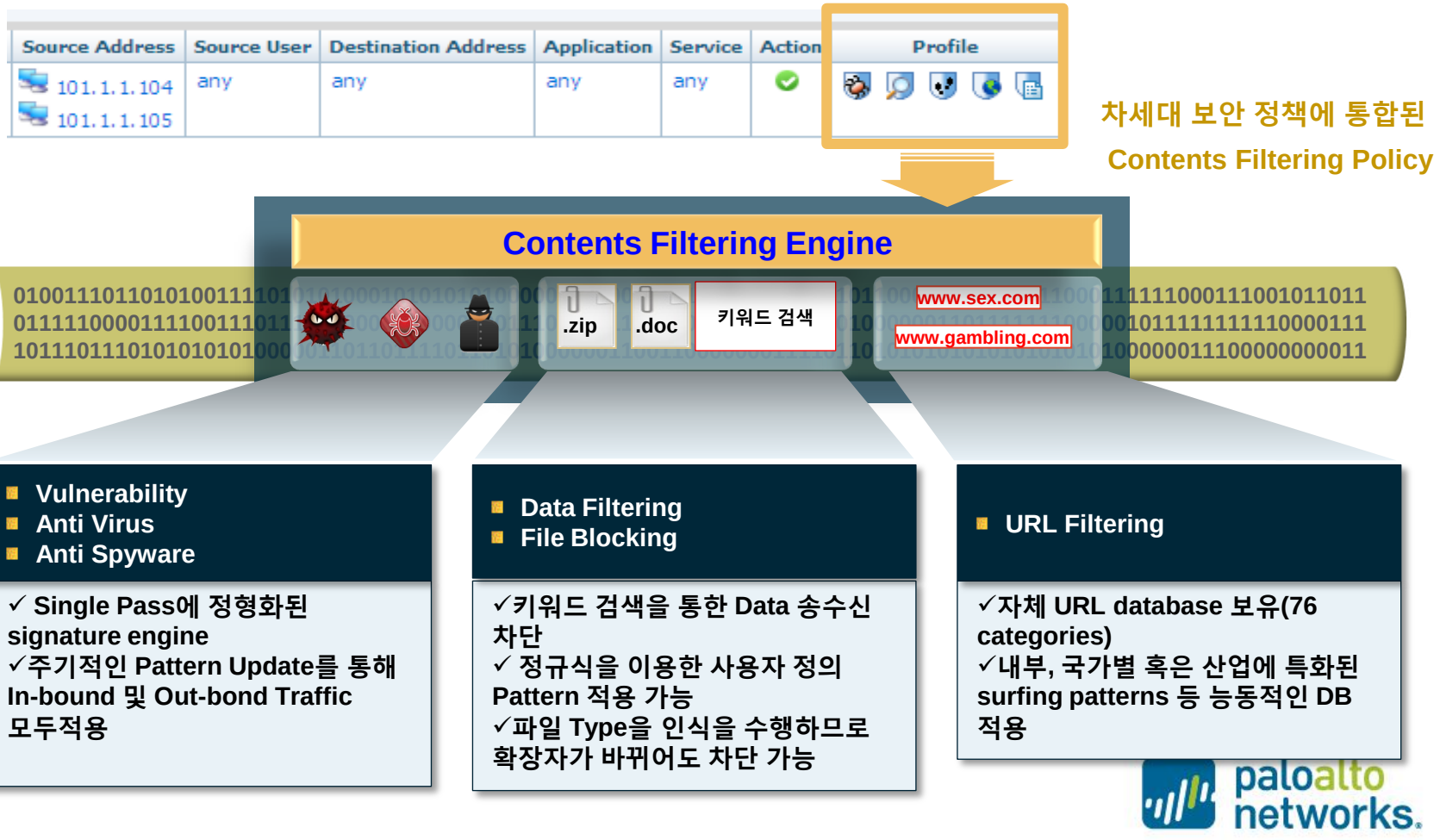
차세대 보안의 통합된 보호와 가시성

1. *통합된 공격 및 위협 차단*
2. *통합된 모니터링 가능*

paloalto networks.

1. 통합된 공격 및 위협 차단 사례

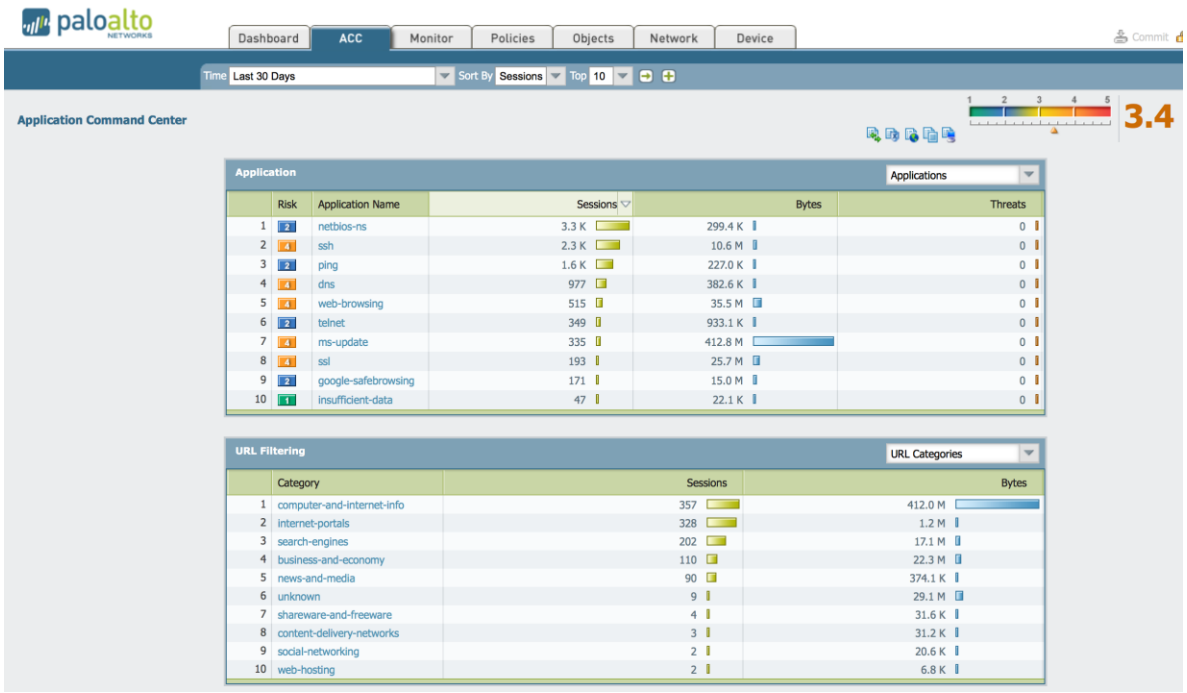
- **송수신 Data의 Contents (Application Data) 부분을 분석하고 제어할 수 있는 기능**
- **Contents Filtering Engine은 공격 및 위협 차단(Vulnerability, Virus, Spyware), 내부정보 유출 차단(File Blocking, Data Filtering) 및 URL Filtering 등의 기능을 수행**



2. 사용자, 애플리케이션, 위협요소 등에 대한 가시성 제공

사용자 및 애플리케이션의 사용 상태 정보를 실시간으로 확인하므로써 정책 정의에 유연성 제공

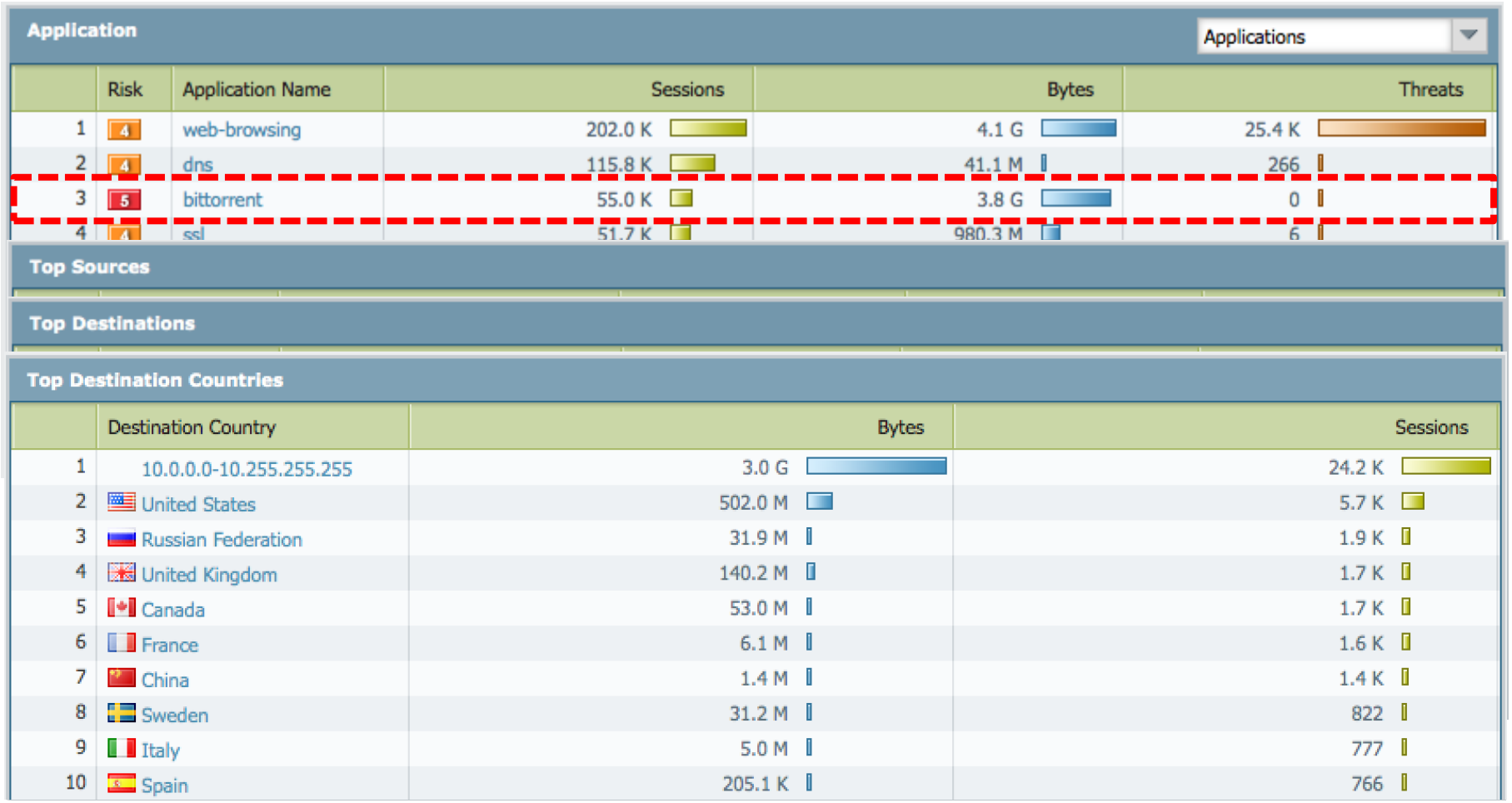
WHO	WHERE	WHAT	HOW
		webex Microsoft SharePoint 2010 MySQL SAP	 Exploits, malware, spyware
User/Group/Device	Server/Hardware	Application	Content



Application Command Center(ACC)

paloalto networks.

2. 사용자, 애플리케이션, 위협요소 등에 대한 가시성 제공



Application — Applications

	Risk	Application Name	Sessions	Bytes	Threats
1	4	web-browsing	202.0 K	4.1 G	25.4 K
2	4	dns	115.8 K	41.1 M	266
3	5	bittorrent	55.0 K	3.8 G	0
4	4	ssl	51.7 K	980.3 M	6

Top Sources

Top Destinations

Top Destination Countries

	Destination Country	Bytes	Sessions
1	10.0.0.0-10.255.255.255	3.0 G	24.2 K
2	United States	502.0 M	5.7 K
3	Russian Federation	31.9 M	1.9 K
4	United Kingdom	140.2 M	1.7 K
5	Canada	53.0 M	1.7 K
6	France	6.1 M	1.6 K
7	China	1.4 M	1.4 K
8	Sweden	31.2 M	822
9	Italy	5.0 M	777
10	Spain	205.1 K	766

paloalto networks.

확장된 차세대 보안 적용

APT 보안을 통한 보안성 강화

paloalto networks.

APT 대응은 Point Product이 아닌 **Solution**이 필요

1 공격의 유입 경로를 줄임

- 허용 **애플리케이션** 분류
- 고 위협 애플리케이션 차단
- 알려진 바이러스, 익스플로잇 차단
- 쉽게 악용되는 **파일 타입차단**

2 Unknown 위협 차단

- 모든 애플리케이션 분석
- SSL 디크립션을 통한 HTTPS 트래픽 분석
- **WildFire 샌드박스를 통한 행위기반 분석**

3 프로텍션 생성

- C&C 트래픽 탐지/차단:
- DNS 트래픽 내의 악성 도메인 접근 시도
- URL 필터링(PAN-DB)
- C&C 시그니처 (anti-spyware)

외부로부터 의심스러운 파일 (실행파일/문서파일) 유입

와일드파이어 Cloud센터 또는 샌드박스로 전송

1시간 내에 새로운 시그니처(AV, DNS, C&C), 멀웨어 URL 필터가 완성되어 각 방화벽으로 배포됨

paloalto networks.

감사합니다!

paloalto networks.