Advanced Network Security with Virtual IPS in a Public Cloud

퍼블릭클라우드에서 가상IPS를 이용한 고급 네트워크 보안

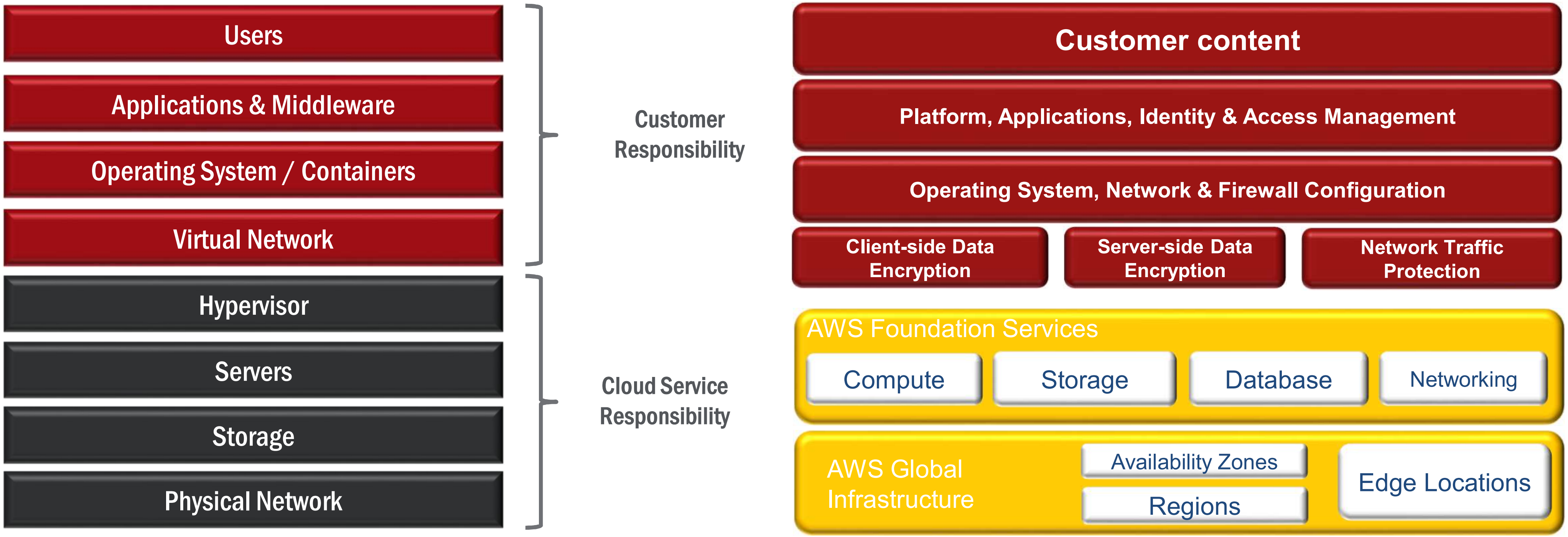
이 재영 CTO | (주) 초록에스티

Overview

- Security in the Public Cloud
- McAfee Virtual Network Security Platform
- McAfee vNSP Components
- McAfee vNSP Functions to Protect Public Cloud
- McAfee vNSP Solution
- McAfee vNSP Deployment
- McAfee vNSP Case Scenarios

Security in the Public Cloud

Top Challenges for Protecting Workloads in AWS


Users
Applications & Middleware
Operating System / Containers
Virtual Network
Hypervisor
Servers
Storage
Physical Network
Customer Responsibility
Cloud Service Responsibility
Customer content
Platform, Applications, Identity & Access Management
Operating System, Network & Firewall Configuration
Client-side Data Encryption
Server-side Data Encryption
Network Traffic Protection
AWS Foundation Services
Compute
Storage
Database
Networking
AWS Global Infrastructure
Availability Zones
Regions
Edge Locations

McAfee Virtual Network Security Platform

Key Benefits

Scalability

Advantages

Scale based upon changing dynamics of virtualized workloads in Web Services

- McAfee vNSP는 가상화된 Workloads의 동적인 변화에 기반하여 확장됩니다.
    - **증가된 트래픽에 기인한 네트워크 버스트 발생 인지**
    - **필요한 처리량 성능을 충족하는 데 필요한 추가 센서를 배치**
    - **작업 부하 요구 사항을 충족하도록 자동으로 확장**
- 관리자가 신규, 현재 및 변화된 Workload에 네트워크 보호를 신속하게 제공

McAfee Virtual Network Security Platform

Key Benefits

Protection and Detection

Advantages

True protection from lateral threats, in addition to North-South attacks

- North-South Traffic 검사 뿐만 아니라 East-West Traffic 보호와 고급 위협을 보호하기 위해 가상 데이터 센터에 적용
  - **고급 위협에 대한 보호**
  - **알려지지 않은 새로운 위협에 대한 보호**

McAfee Virtual Network Security Platform

Key Benefits

Manageability and Automation

Advantages

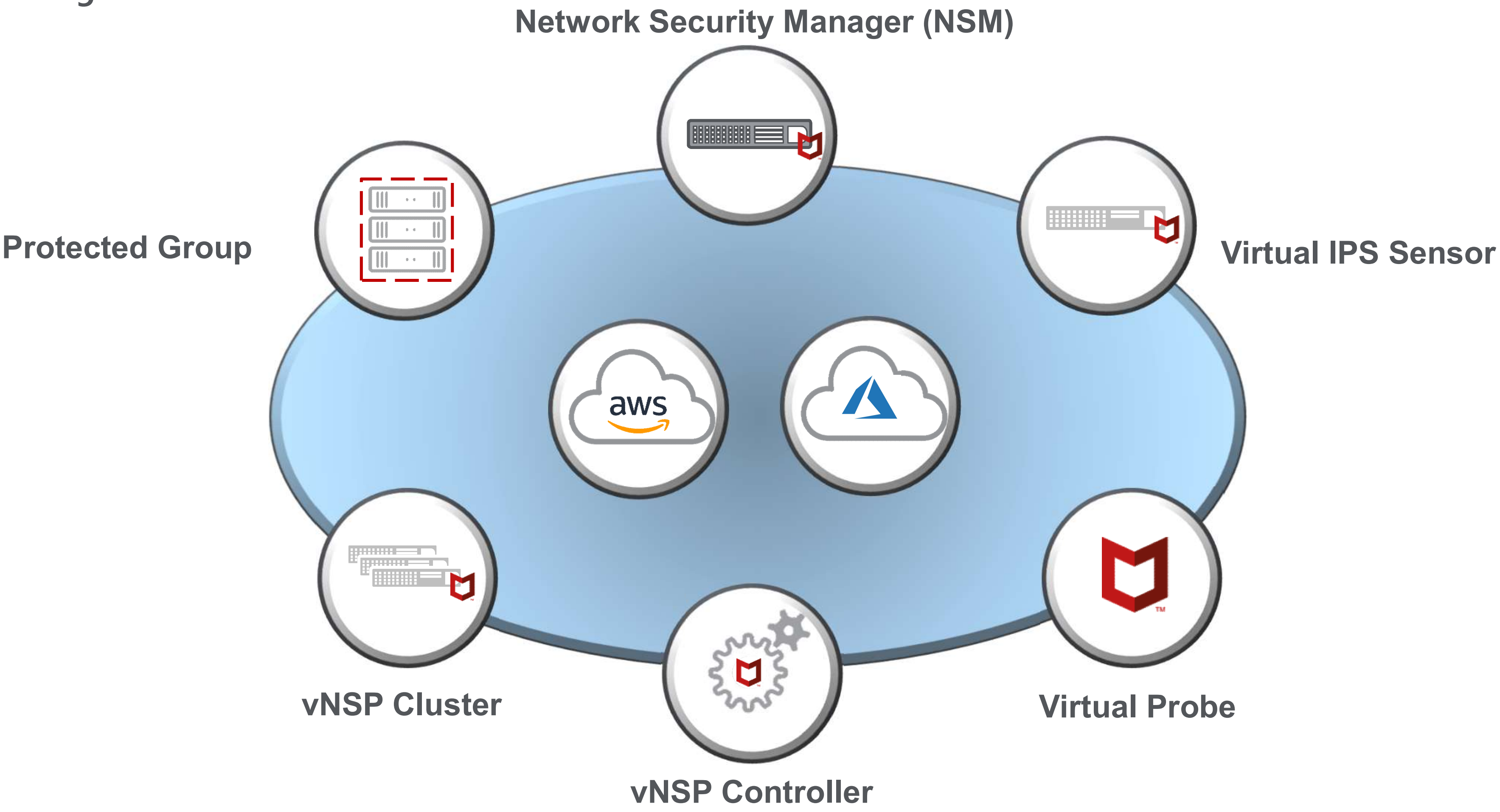
A single pane of glass that provides visibility and the ability to control workloads across the environment

- McAfee vNSP는 보안 관리자에게 단일 화면에서 모든 클라우드 환경에서 Workload를 가시화하고 제어
- AWS ID 및 액세스 관리 (IAM)를 지원하므로 관리자는 특정 사용자 및 그룹에 할당 된 권한에 따라 AWS 서비스 및 리소스에 대한 액세스를 쉽고 안전하게 관리

  (AWS only)
- 노이즈 수준의 경고를 처리하는 대신 사전 구성된 Workflow를 통해 실행 가능한 Security Intelligence를 표시

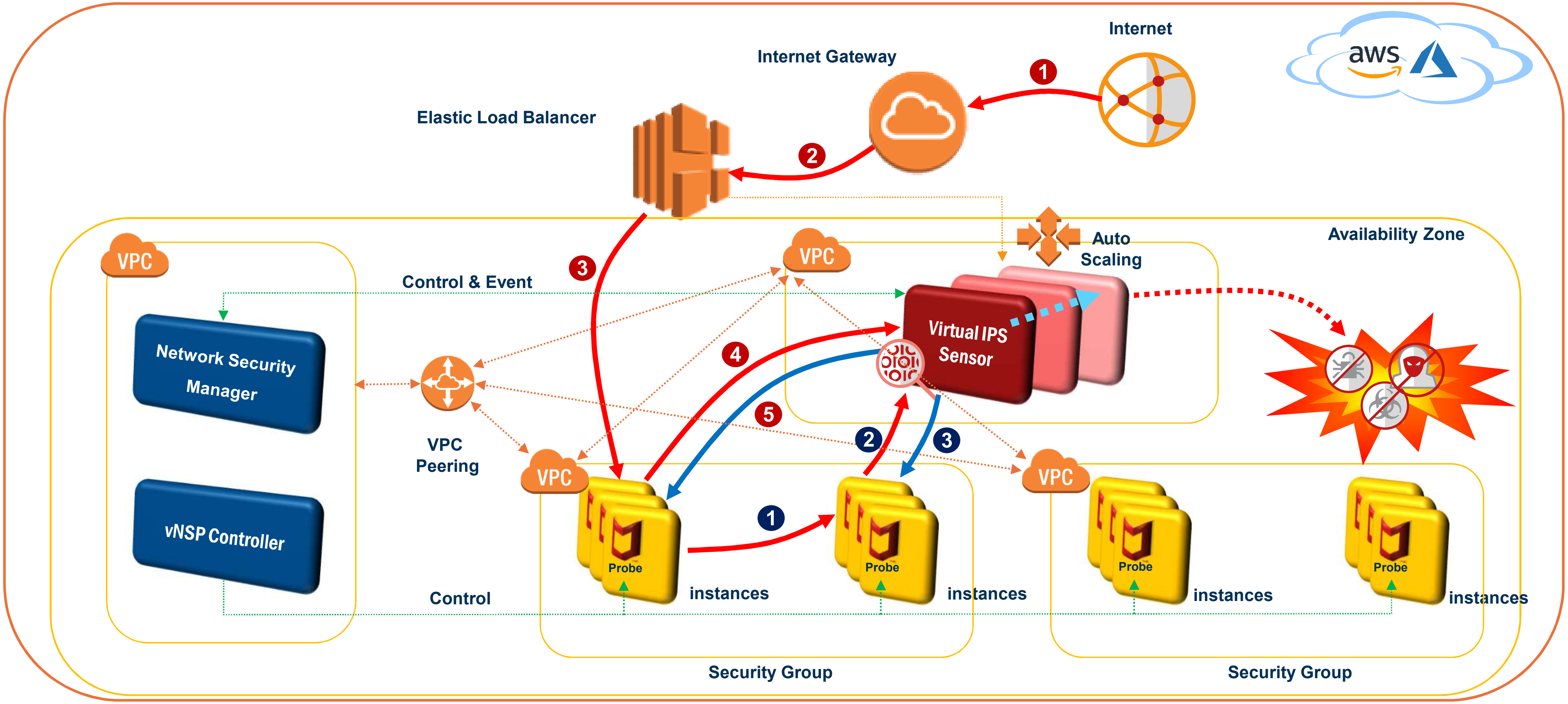
McAfee vNSP Components

Terminologies



McAfee vNSP Functions to Protect Public Cloud

Protection Flow

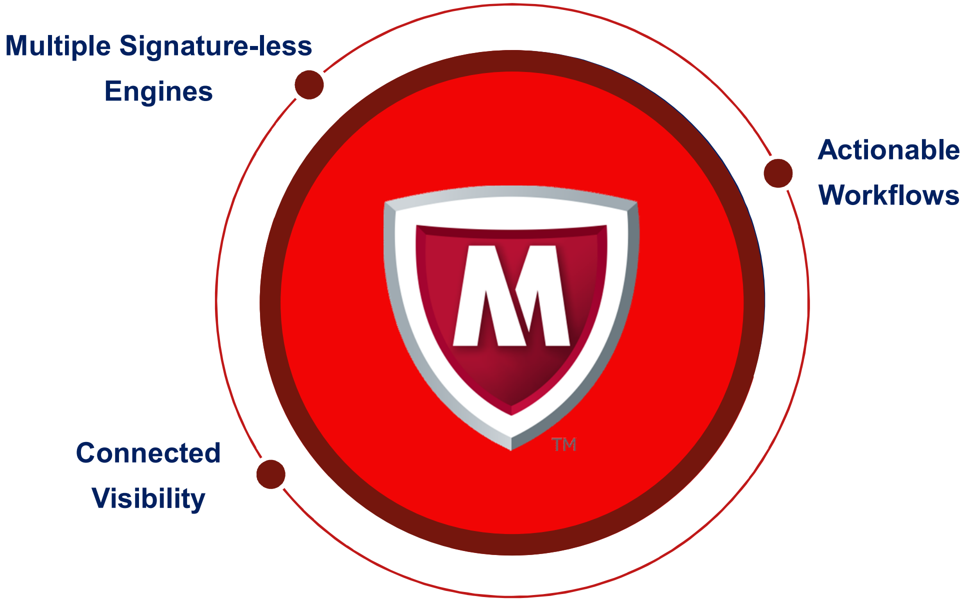


McAfee vNSP Solution

Intelligent IPS

- **Next-generation Inspection Architecture**
  - Application Awareness (Full stack visibility)
  - Context Awareness (External intelligence)
  - Content Awareness (Advanced malware protection)

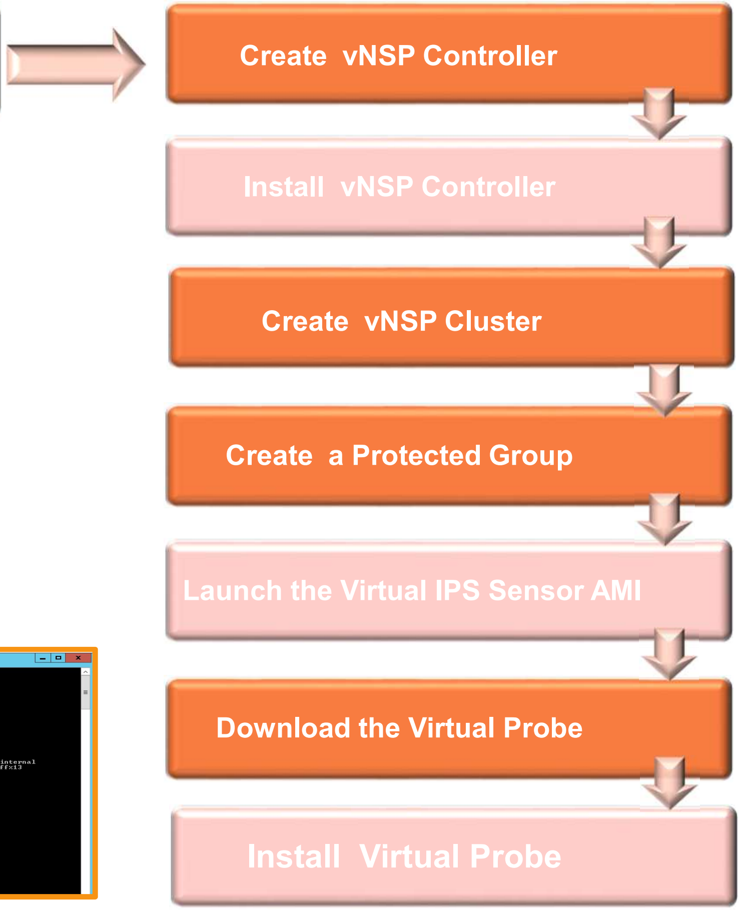
- **Advanced Threat Protection**
  - Signature-less Detection Engine
    - Sophisticated Bot Detection
    - Deep file analysis
    - Global threat intelligence
    - Advanced Threat Defence
    - Network Behavior Analysis
    - Endpoint Intelligence Agent



McAfee vNSP Deployment

Installation Flow

Install Network Security Manager
(Virtual / On-premises)



Create vNSP Controller

Install vNSP Controller

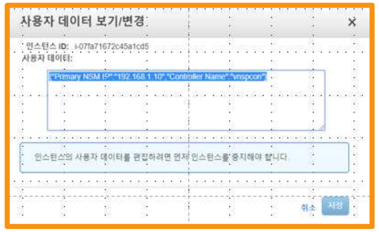
Create vNSP Cluster

Create a Protected Group

Launch the Virtual IPS Sensor AMI

Download the Virtual Probe

Install Virtual Probe



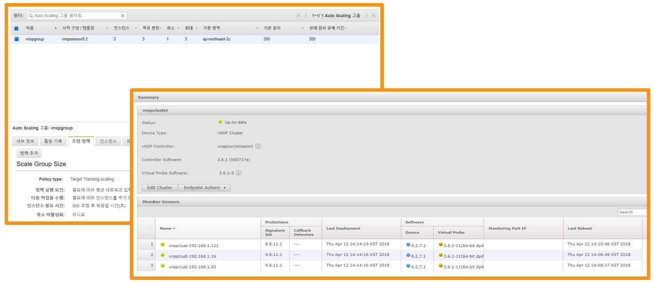
사용자 데이터 보기/변경

인스턴스 ID: i-07fa71672c45a1cd5

사용자 데이터:

```
"Primary NSM IP":"192.168.1.10","Controller Name":"vnspcon"
```

인스턴스의 사용자 데이터를 편집하려면 먼저 인스턴스를 중지해야 합니다.



필터: Auto Scaling 그룹 필터링... 1~1/ 1 Auto Scaling 그룹

이름	시작 구성 / 템플릿	인스턴스	목표 용량	최소	최대	가용 영역	기본 휴지	상태 검사 유예 기간
vnspgroup	vnspsensor9.2	3	3	1	3	ap-northeast-2c	300	300

Auto Scaling 그룹: vnspgroup

Scale Group Size

Policy type: Target Tracking scaling

정책 실행 요건: 필요에 따라 평균 네트워크 입

다음 작업을 수행: 필요에 따라 인스턴스를 추가

인스턴스 필요 시간: 300 조정 후 워밍업 시간(초)

축소 비활성화: 아니요

Summary

vnspcluster

Status: Up-to-date

Device Type: vNSP Cluster

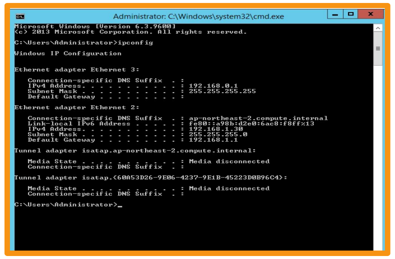
vNSP Controller: vnspcon(Amazon)

Controller Software: 3.6.1 (060717a)

Virtual Probe Software: 3.6.1-5

Member Sensors

	Name	Protections		Last Deployment	Software		Monitoring Port IP	Last Reboot
		Signature Set	Callback Detectors		Device	Virtual Probe		
1	vnspclust-192.168.1.121	9.8.11.1	---	Thu Apr 12 14:14:19 KST 2018	9.2.7.1	3.6.1-11(64-bit dpd		Thu Apr 12 14:10:46 KST 2018
2	vnspclust-192.168.1.16	9.8.11.1	---	Thu Apr 12 14:14:16 KST 2018	9.2.7.1	3.6.1-11(64-bit dpd		Thu Apr 12 14:06:49 KST 2018
3	vnspclust-192.168.1.83	9.8.11.1	---	Thu Apr 12 14:14:16 KST 2018	9.2.7.1	3.6.1-11(64-bit dpd		Thu Apr 12 14:08:27 KST 2018



Administrator: C:\Windows\system32\cmd.exe

```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet 3:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.0.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.255
   Default Gateway . . . . . . . . . :

Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . : ap-northeast-2.compute.internal
   Link-local IPv6 Address . . . . . : fe80::a98b:d2e0:6ac8:f8ff%13
   IPv4 Address. . . . . . . . . . . : 192.168.1.30
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1

Tunnel adapter isatap.ap-northeast-2.compute.internal:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter isatap.{60A53D26-9E06-4237-9E1B-45223D0B96C4}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\Administrator>_
```

🟧	Performed on Network Security Manager
▨	Performed in AWS /Azure

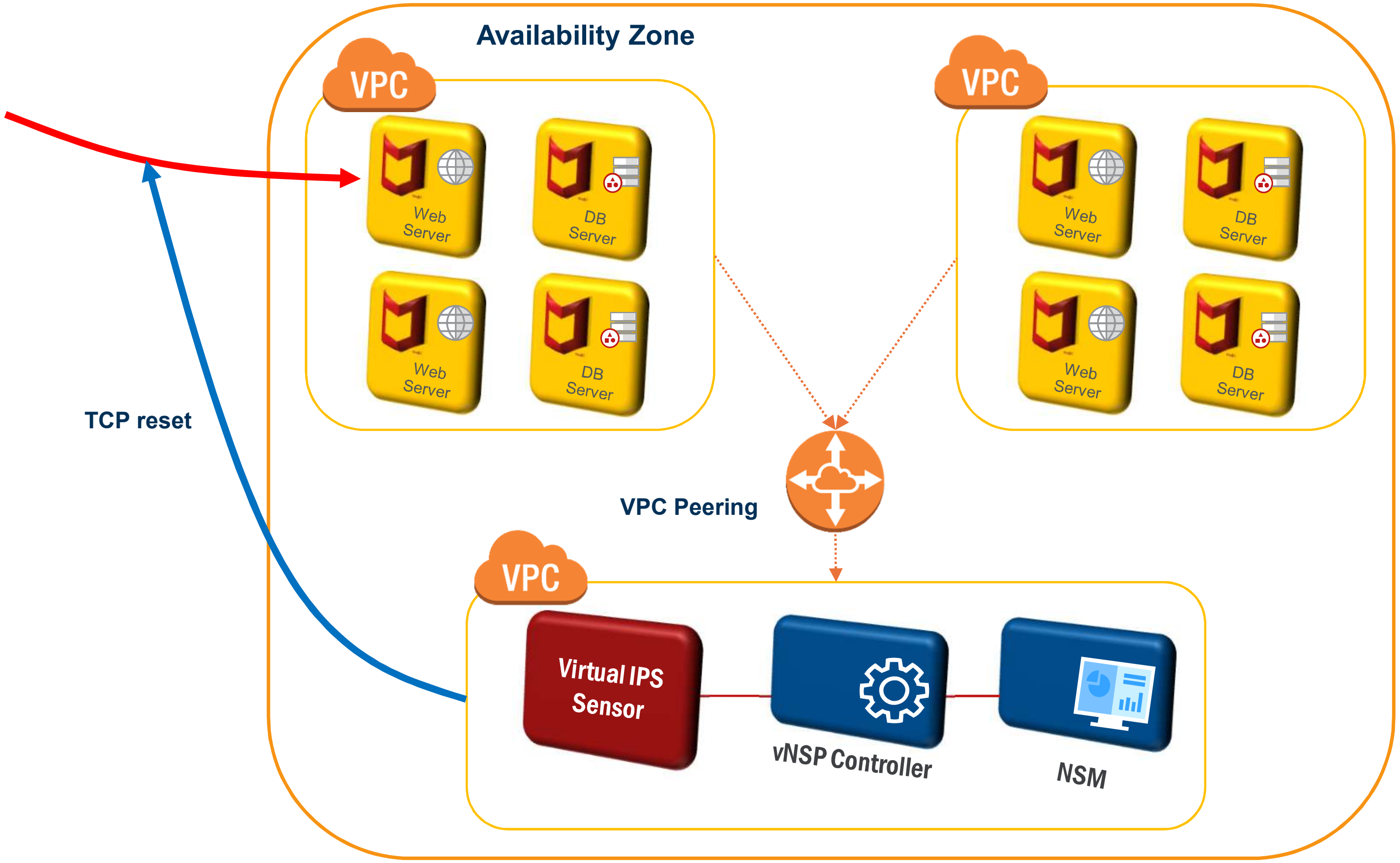
McAfee vNSP Deployment

Components Requirements

Component	AWS Instance Type	Software Requirement	Network Requirement	Azure Virtual Machine Type	Software Requirements	Network Requirement
Network Security Manager	m4.xlarge	Windows 2012 R2 Server	1 Network interface (management subnet)	D4S_V3 Standard (4 vCPUs, 16 GB memory)	Windows 2012 R2 Server	1 Network interface (management subnet)
vNSP Controller	c4.xlarge	vNSP Controller AMI	1 Network Interface (management subnet)	E2S_V3 Standard (2 vCPUs, 16 GB memory)	vNSP Controller Image	1 Network Interface (management subnet)
Virtual IPS Sensor	c4.xlarge	NSP instance AMI	2 Network Interfaces (primary: management subnet, second: data subnet) or 1 Network Interface (management and data subnet)	F8S Standard (8vCPUs, 16 GB memory)	Virtual IPS Sensor Image	2 Network Interfaces (primary: management subnet, second: data subnet) or 1 Network Interface (management and data subnet)
Protected VM Instance	Any	Customer Supplied	1 or more (see deployment) Use public IP address or NAT gateway to access Controller EIP	Any	Customer Supplied	1 or more (see deployment)

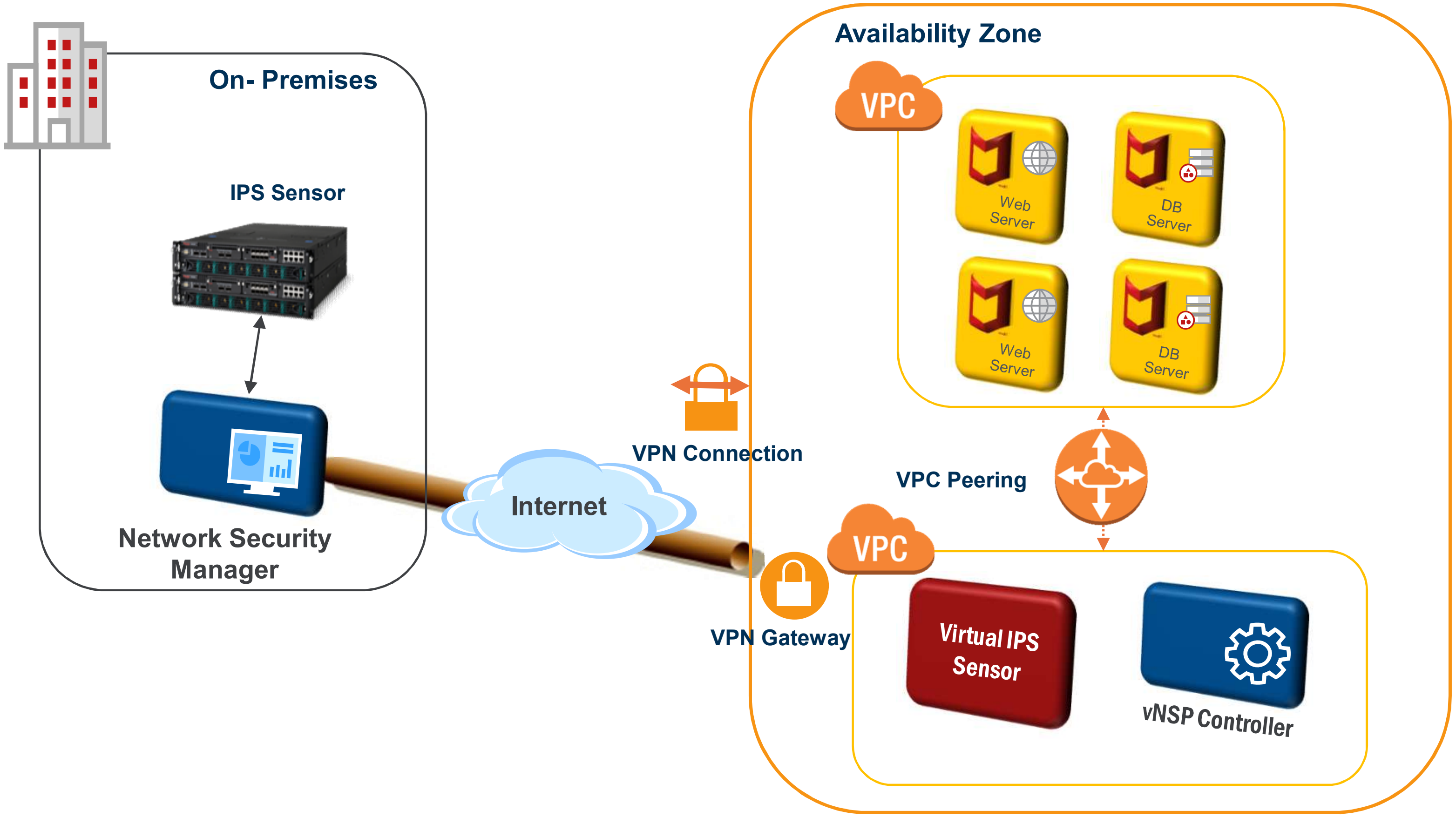
McAfee vNSP Case Scenarios

Deployment of Virtual IPS Sensors in IDS mode



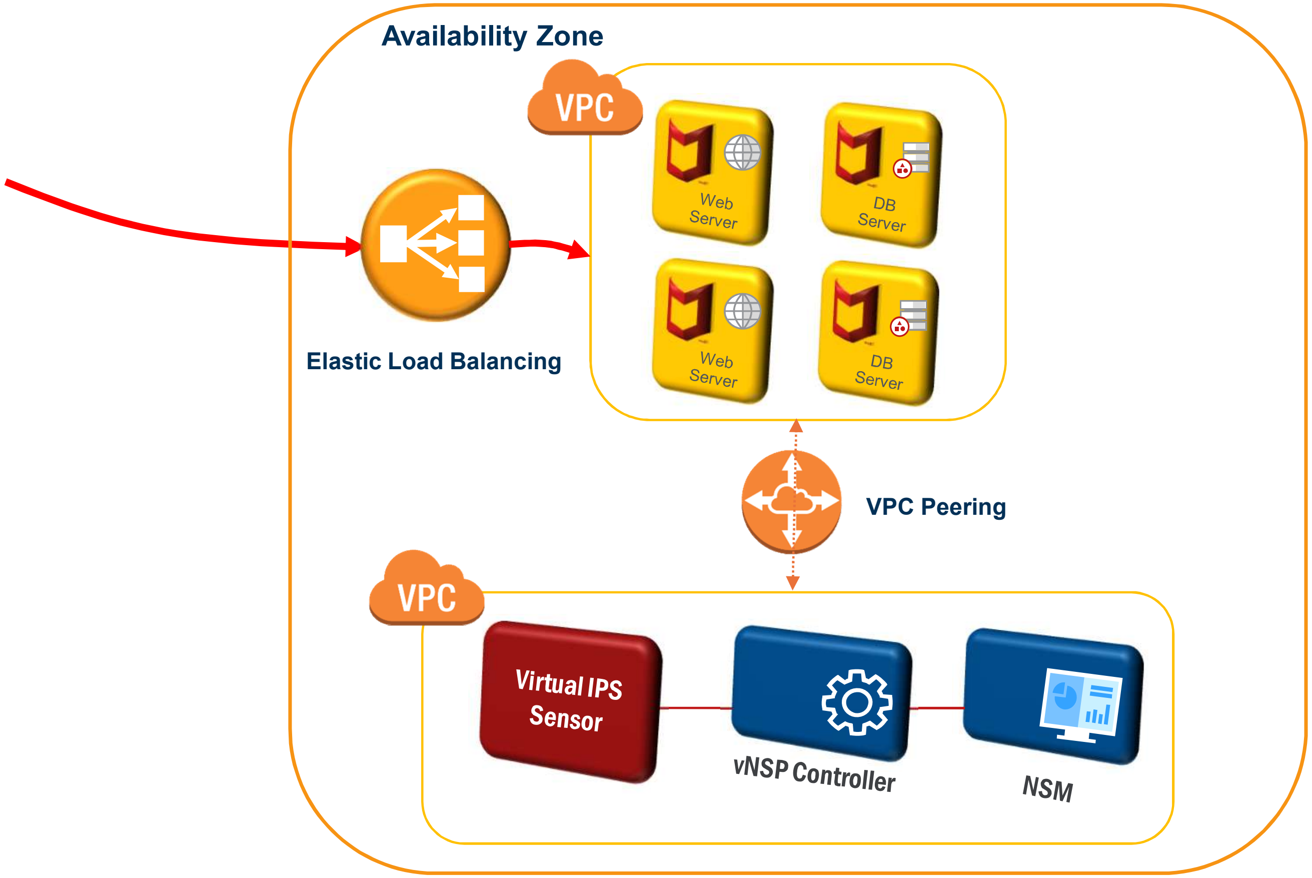
McAfee vNSP Case Scenarios

On-premises Network Security Manager managing Sensors in AWS environment



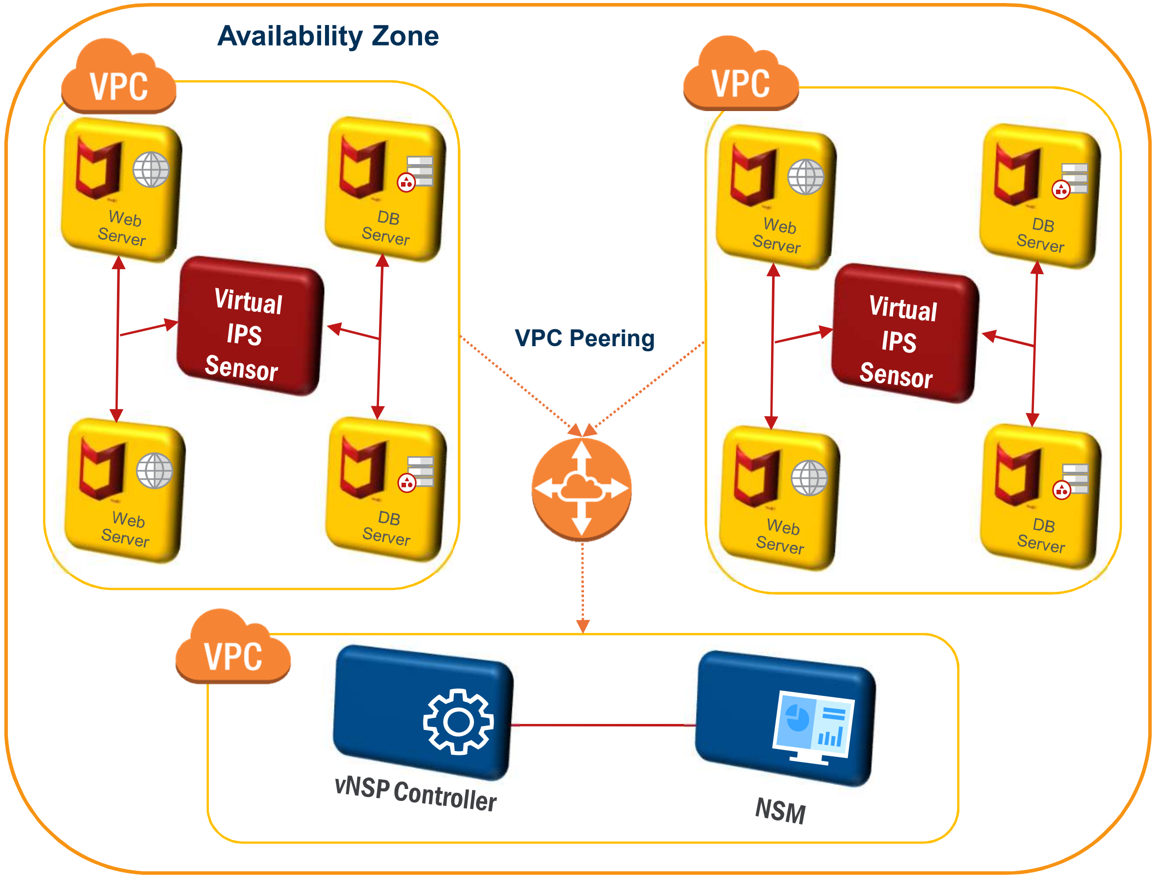
McAfee vNSP Case Scenarios

Virtual IPS Sensor with AWS load balancer deployment



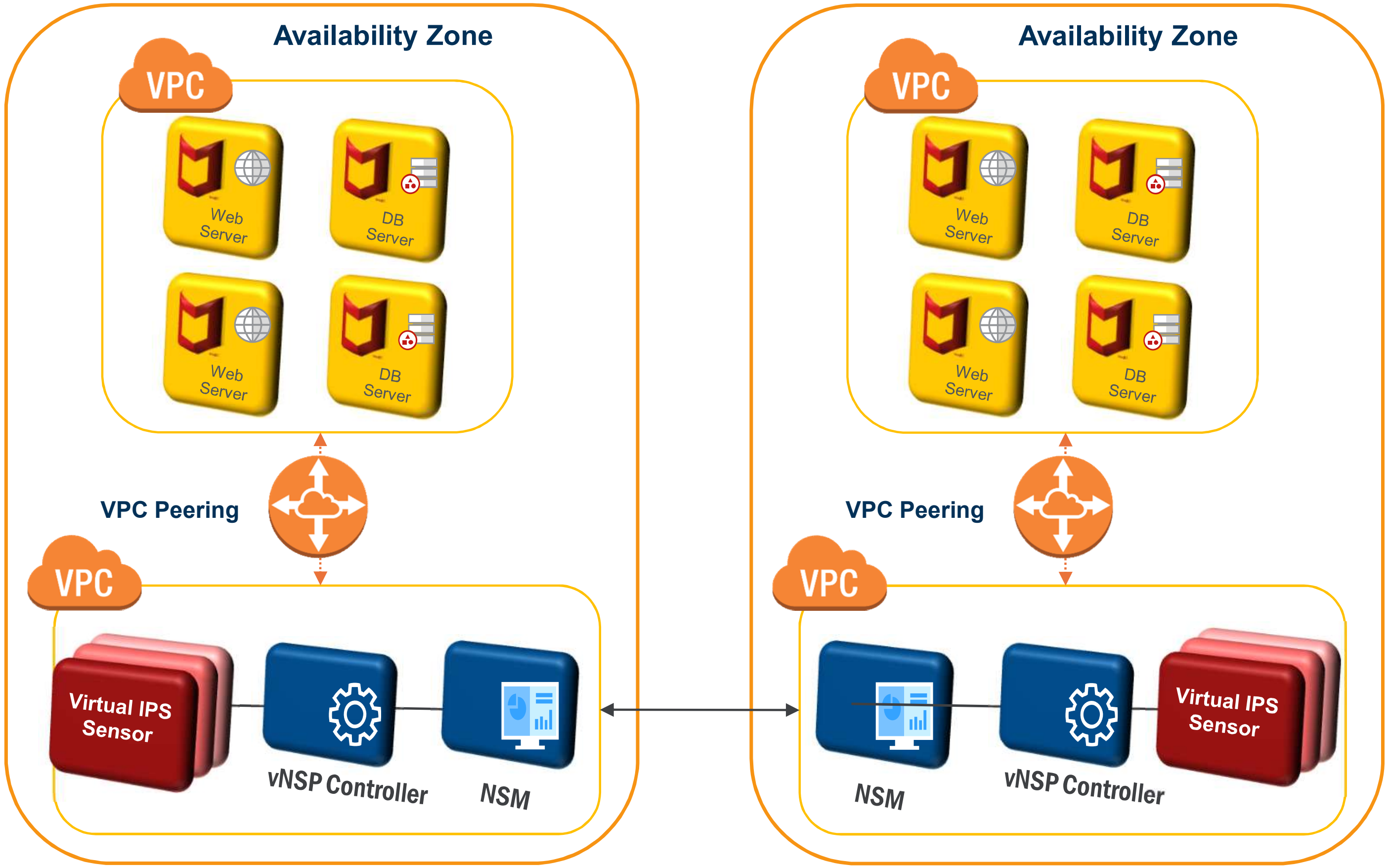
McAfee vNSP Case Scenarios

Single Sensor per protected VPC deployment



McAfee vNSP Case Scenarios

Multi-zone deployment with auto scaling of Virtual IPS Sensors



감사합니다.

chorok st

SECURITY TECHNOLOGY