Azure는 어떻게 보안할 수 있나요?

Azure 보안을 낱낱이 파헤쳐보자! 파사삭~

Sejun Kim

슬기로운 Azure생활 운영진
클라우드메이트 Azure 사업부장
Azure MVP

Microsoft의 보안

Azure는 어떻게 보안할 수 있나요?

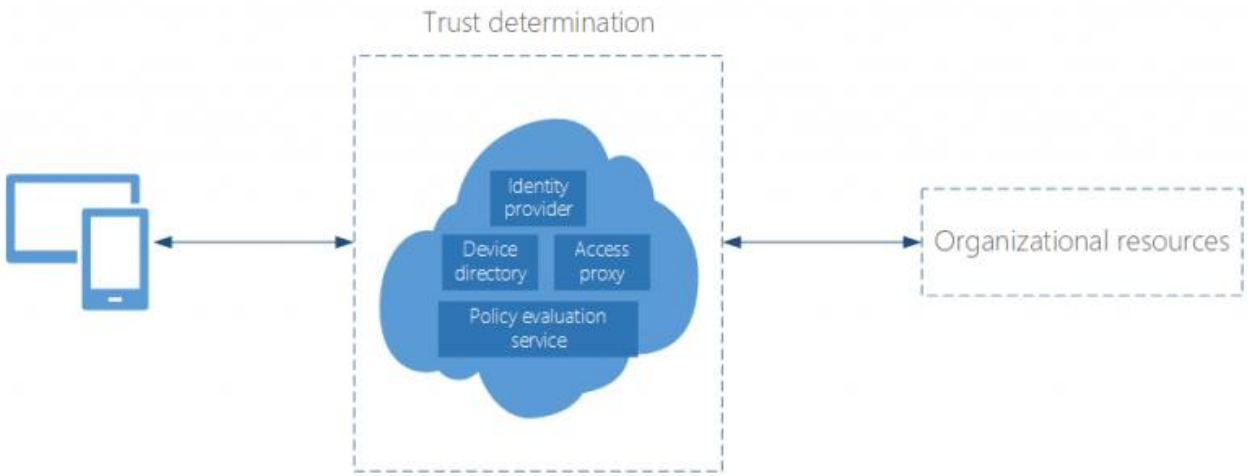
제로 트러스트 모델

제로 트러스트 모델은 트러스트를 가정하지 않는 대신 트러스트를 지속적으로 검증

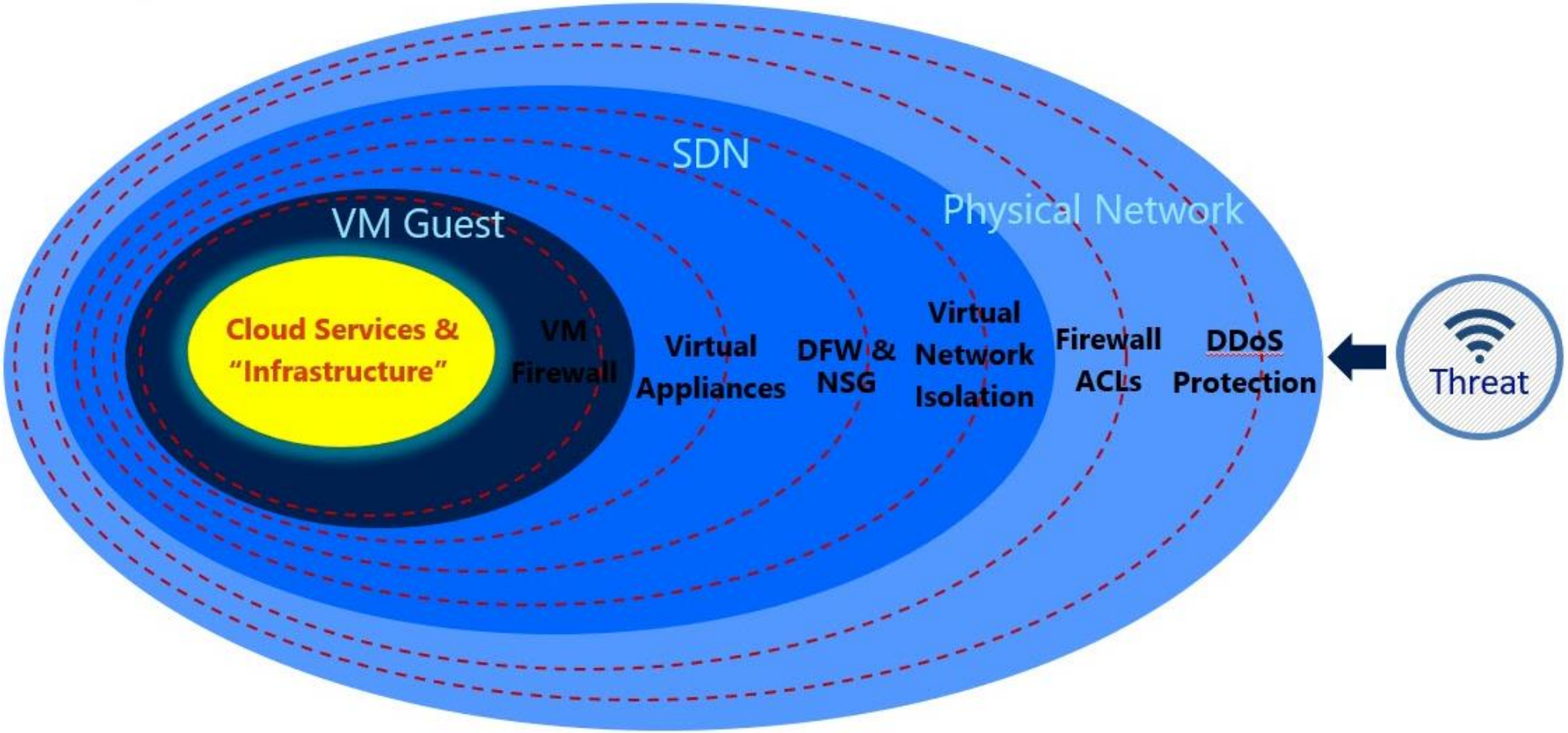
대부분의 사용자가 인터넷에서 앱과 데이터에 액세스함으로 많은 트랜잭션 구성 요소가 조직의 통제를 받지 않게 됨

트러스트 구성 요소:

- ID 공급자
- 디바이스 디렉토리
- 정책 평가 서비스
- 액세스 프록시



Azure의 보안 계층



Azure는 어떻게 보안할 수 있나요?

공유 책임 모델

책임	On-Premises	IaaS	PaaS	SaaS
데이터 거버넌스 및 권한 관리	사용자	사용자	사용자	사용자
엔드포인트	사용자	사용자	사용자	사용자
계정 및 액세스 관리	사용자	사용자	사용자	사용자
아이디와 디렉토리 인프라	사용자	사용자	Microsoft/사용자	Microsoft/사용자
응용프로그램	사용자	사용자	Microsoft/사용자	Microsoft
네트워크 컨트롤	사용자	사용자	Microsoft/사용자	Microsoft
운영체제	사용자	사용자	Microsoft	Microsoft
물리 호스트	사용자	Microsoft	Microsoft	Microsoft
물리 네트워크	사용자	Microsoft	Microsoft	Microsoft
물리 데이터센터	사용자	Microsoft	Microsoft	Microsoft

계정 보안 편

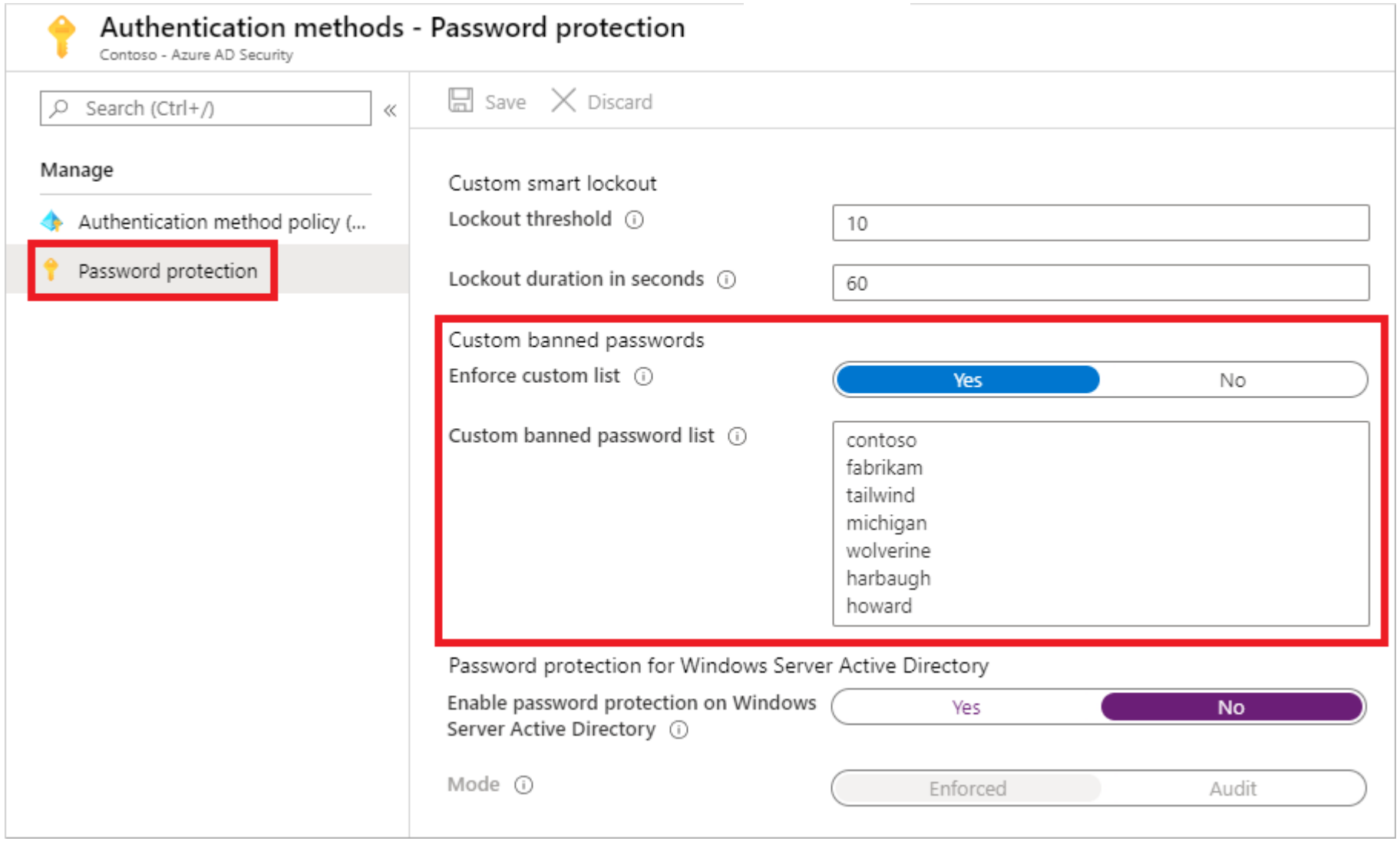
Azure는 어떻게 보안할 수 있나요?

비밀번호 정책 설정

Azure AD는 기본적으로 다음과 같은 정책을 가짐 (수정 가능)

- 최소 8자, 최대 256자
- 대/소문자, 숫자, 기호 중 3개 혼합
- 기본 암호 만료기간: 90일
- 기본 암호 만료 알림: 14일
- 암호 변경 기록: 최근 사용한 비밀번호 사용 불가
- 계정 잠금: 10회 실패 시 1분 동안 계정 잠김

사용자 지정 암호 설정


Authentication methods - Password protection
Contoso - Azure AD Security
Search (Ctrl+/)
Save
Discard
Manage
Authentication method policy (...
Password protection
Custom smart lockout
Lockout threshold
10
Lockout duration in seconds
60
Custom banned passwords
Enforce custom list
Yes
No
Custom banned password list
contoso
fabrikam
tailwind
michigan
wolverine
harbaugh
howard
Password protection for Windows Server Active Directory
Enable password protection on Windows Server Active Directory
Yes
No
Mode
Enforced
Audit

Azure MFA

로그인 프로세스 중에 OTP와 같은 추가 식별을 요구하는 프로세스

다음 세가지를 사용:

- 당신이 알고 있는 것
- 당신이 가지고 있는 것
- 당신에게 있는 것

Passwordless

Windows Hello나 Microsoft Authenticator 앱을 이용한 Passwordless

비밀번호를 입력하지 않고 로그인

Azure MFA와 연동하여 기기 인증 시 패스워드를 묻지 않음

사용자 계정과 서비스 계정

사용자 계정 (User Principal)

- 사용자를 식별하기 위한 계정
- ID/PW를 이용한 로그인 또는 Azure MFA 사용

서비스 계정 (Service Principal)

- 서비스 또는 Application을 식별하기 위한 계정
- Secret Key 또는 인증서로 로그인

Azure AD 조건부 액세스

Azure AD에 접근할 수 있는 조건을 정의

다음을 통해 제어 가능:

- IP 기반
- 위치
- MFA 활성화 여부
- 디바이스

Azure AD PIM

Azure AD를 통해 로그인한 계정의 권한을 할당

Azure AD가 아닌 Azure AD PIM에서 계정에 권한 할당 필요

Just-in-time Role Activate를 통해 특정 시각에만 권한 활성화

권한 사용 및 접근 현황 등을 주기적으로 리포트

네트워크 보안 편

Azure는 어떻게 보안할 수 있나요?

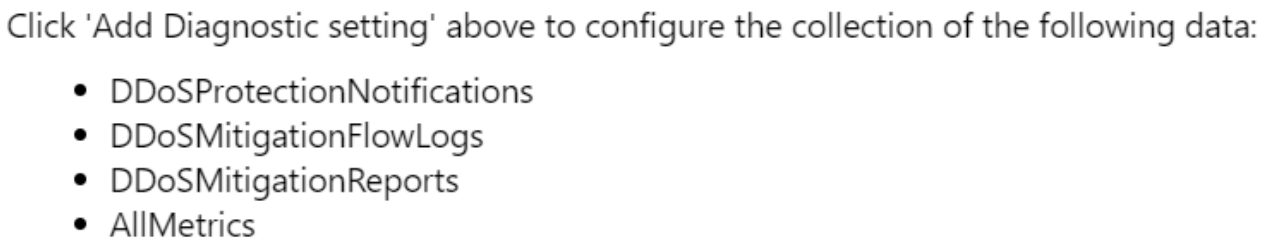
DDoS Protection

Azure내에 들어오는 트래픽에 대한 DDoS 공격 방어

다음 계층으로 나눠짐:

Basic – 기본적으로 활성화 되어있으며 무료. 일반적인 공격을 차단하기 때문에 산업에 특화된 공격에 반응이 느림

Standard – 유료 Plan으로 Microsoft 보안 전문팀이 관리. Public Facing 서비스에 활성화 되며, Public IP에 DDoS Log가 생성됨



Network Security Group

vNIC 또는 Subnet에 연결할 수 있는 Network Access Control List(ACL)

우선 순위 기반 Allow 또는 Deny 설정

CIDR, Tags, Application Gateway를 대상으로 구성

기본 설정이 있으며 수정 불가능

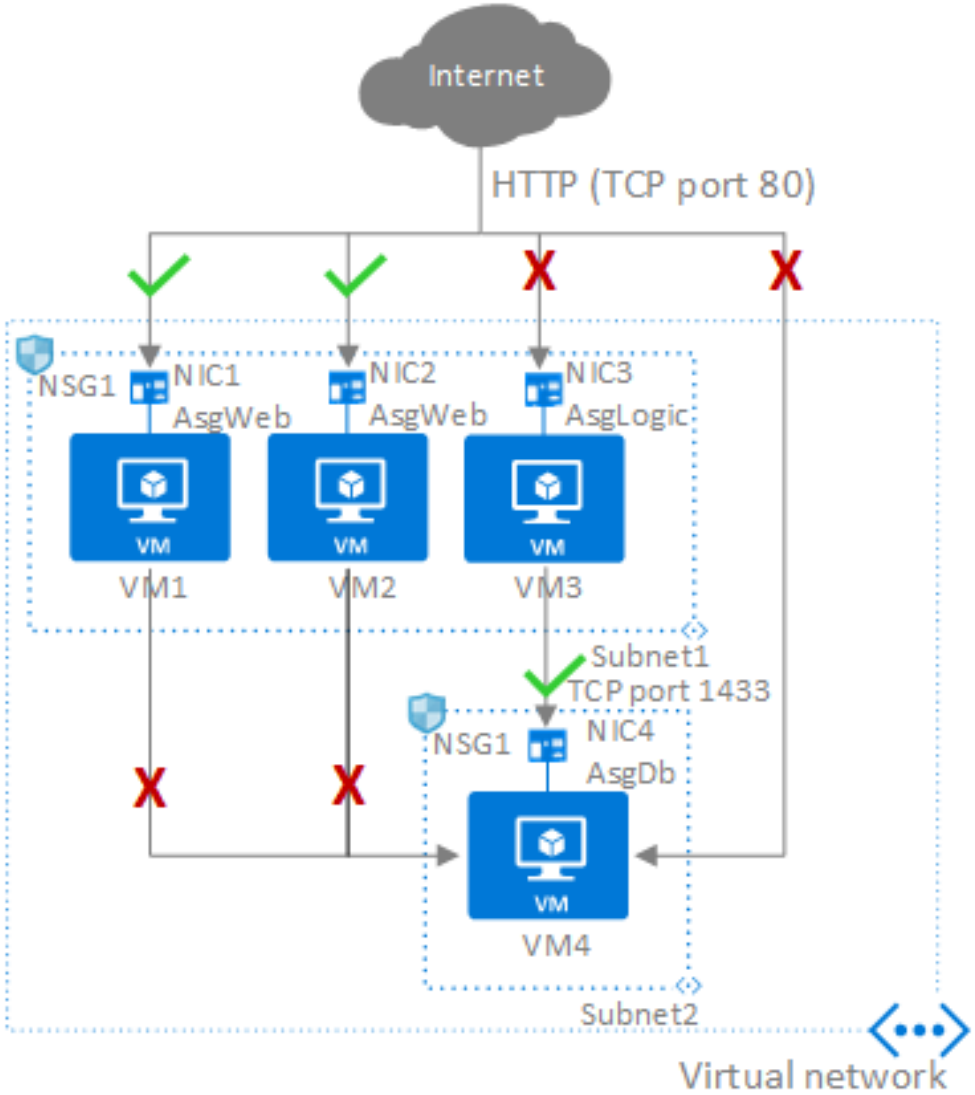
Network Security Group

Priority	Name	Port	Protocol	Source	Destination	Action
500	a7511e1d439014de38765d2c01155676...	80	TCP	Internet	20.41.72.177	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Priority	Name	Port	Protocol	Source	Destination	Action
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

Application Security Group

Azure VM을 Group으로 묶어 Network Security Group의 대상으로 설정할 수 있도록 지원하는 기능



Endpoint와 Private Link 

Azure 서비스 중 Public Facing 서비스를 Virtual Network와 직접 통신

다음과 같은 옵션으로 설정 가능:

Endpoint – Subnet에 Endpoint를 생성하여 Azure 서비스와 직접 통신할 수 있도록 Azure에서 Route 처리

Private Link – Azure 서비스를 Private IP와 맵핑하여 Network 내 통신을 지원

16:00 ~ 16:50 성공적인 하이브리드 클라우드를 위한 Azure 네트워크와 서비스 – 고재성 참고!

Azure Firewall 

CIDR과 Service Tag 그리고 Domain 기반 접근 제어 가능

- 그룹으로 지정하여 관리

최대 30Gbps까지 처리할 수 있으며 Azure Support를 이용하여 증설 가능

10,000개의 규칙(Rule)을 정의할 수 있음

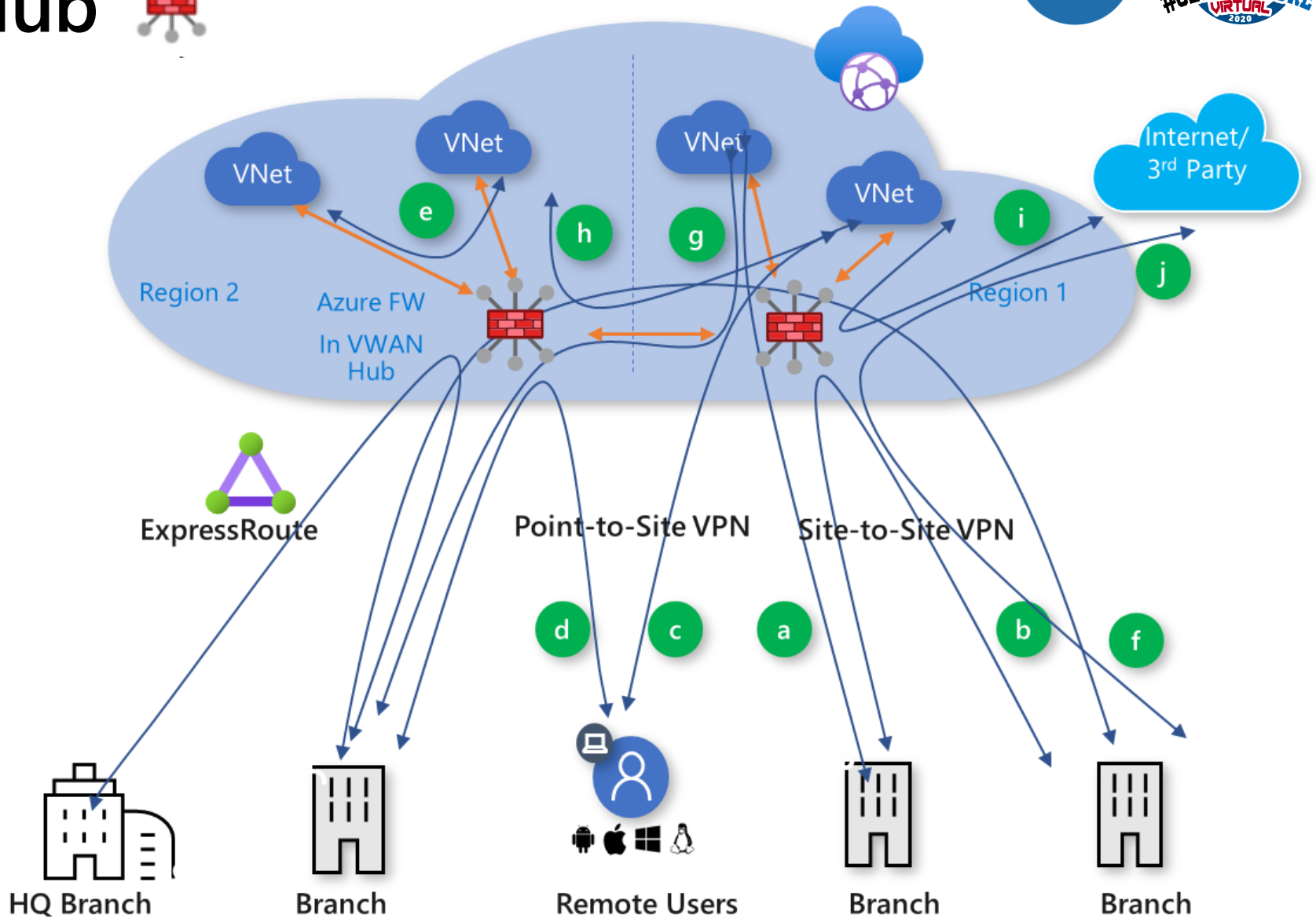
DANT 규칙의 경우 299개 까지 가능

최대 100개의 Public IP 연결 가능

Azure Firewall Threat Intelligence를 이용하여 지능적인 트래픽 제어

Secured Virtual Hub

Azure Firewall을 Hub Network에 생성하여 모든 트래픽을 제어



WAF Policies 

WAF 정책을 선언하여 OSI 7 Layer 기반 접근 제어

AFD(Azure Front Door)와 AGW(Application Gateway) v2에 연결

Diagnostic logs를 이용하여 필터링 정책 확인 가능

https://docs.microsoft.com/en-us/azure/application-gateway/application-gateway-diagnostics#firewall-log

서버와 서비스 보안 편

Azure는 어떻게 보안할 수 있나요?

Azure Bastion 

Azure VM에 RDP 또는 SSH 접속 시 연결을 중개

Virtual Network에 직접 생성하여 VM과 통신

Public Facing 서비스로 Azure Portal에서 접속 가능

세션 현황, 연결된 세션 관리/강제 종료 등 설정

Agentless로 동작

Update Manager

Azure VM에 Update를 관리할 수 있는 서비스

지원 운영체제:

Windows Server

CentOS 6 (x86/x64) and 7 (x64)

Red Hat Enterprise 6 (x86/x64) and 7 (x64)

SUSE Linux Enterprise Server 11 (x86/x64) and 12 (x64)

Ubuntu 14.04 LTS, 16.04 LTS, and 18.04 (x86/x64)

PaaS Firewall

각 Azure 관리형 서비스에 연결되어 있는 Firewall

Internet 차단 및 Endpoint 설정, 특정 IP 허용 등 설정

Azure 서비스간 통신도 명시적으로 허용해야지만 통신

Key Vault 

Key, Secrets, 인증서, HSM 등 저장

CA 인증서 또는 관리형 서비스 Key의 경우 자동 갱신 지원

격리된 저장소에 Key를 저장해야 할 시 HSM SKU 선택 (추가 과금 필요)

App Settings

Web App 등 관리형 서비스에 응용프로그램 구동시 사용

환경변수를 Azure Portal에서 설정하여 Application에 민감정보 저장을 최소화

Slot 고정 가능

Application settings

Application settings are encrypted at rest and transmitted over an encrypted channel. You can choose to display them in plain text in your browser by using the controls below. Application Settings are exposed as environment variables for access by your application at runtime. Learn more

+ New application setting | Show values | Advanced edit | Filter

Name	Value	Source	Deployment slot setting
DATABASE_HOST	Hidden value. Click show values button a	App Config	
DATABASE_NAME	Hidden value. Click show values button a	App Config	
DATABASE_PASSWORD	Hidden value. Click show values button a	App Config	
DATABASE_USERNAME	Hidden value. Click show values button a	App Config	
DOCKER_REGISTRY_SERVER_URL	Hidden value. Click show values button a	App Config	
GIT_BRANCH	Hidden value. Click show values button a	App Config	
GIT_REPO	Hidden value. Click show values button a	App Config	
WEBSITES_ENABLE_APP_SERVICE_STORAGE	Hidden value. Click show values button a	App Config	

Resource Lock

Azure의 모든 리소스 또는 리소스 그룹은 잠금을 설정할 수 있음

Owner가 생성한 잠금은 Contributor가 삭제할 수 없음

Read-Only: 수정과 삭제가 불가능

Delete: 삭제 불가능

데이터 보안 편

Azure는 어떻게 보안할 수 있나요?

Storage Encryption for Data at Rest

기본적으로 Azure에 저장되는 모든 데이터는 암호화 저장

- Storage Account, SQL Database, CosmosDB 등

필요시 사용자 정의 인증서를 통한 암호화 가능

Azure Disk의 경우 Key Vault를 이용하여 암호화 가능

OS Disk는 암호화 권장

Storage Account 권장 설정 

Container(Blob)은 Private Access 설정

Container(Blob) 암호화 사용

보안 강화 전송 필요

Access Key를 주기적으로 재생성

한 시간 내에 SAS (공유 액세스 서명) 토큰이 만료 되도록 요구

SAS 토큰은 HTTPS를 통해서만 공유

Azure File 암호화 사용

Azure Databases ATP

의심스러운 데이터베이스 활동, 잠재적 취약성, 사이버 공격 및 비정상적인 액세스 패턴을 탐지하고 이에 대응

Azure Security Center와 통합

위협 조사 및 완화 지원

다음을 포함하는 Advanced Data Security 오퍼링의 일부로 사용 가능:

- 데이터 발견 및 분류
- 취약점 평가
- 위협 탐지

이벤트 감사 편

Azure는 어떻게 보안할 수 있나요?

Security Center

Azure Architecture Center를 비롯한 많은 보안 권장설정을 모니터링

Azure Policy와 연계되어 설정을 감사 또는 제어

Standard 사용시 다음과 같은 기능 추가 제공

- Compliance 모니터링
- ATP 가시성 제공
- Log 기반 보안 권장사항 감사
- Just-in-time VM Access 구성 가능

Security Center

Overview 및 기능 설명
Just-in-time VM Access

Sentinel 

Azure SIEM(Security Information and Event Management)

약 64개의 Connector 지원

AWS Cloudtrail을 비롯한 Windows Event, Linux Syslog, Cisco ASA, Fortinet, Trend Micro 지원

Microsoft Azure

Search resources, services, and docs

admin@contoso.com
CONTOSO

Home > Azure Sentinel

Azure Sentinel - Overview

Search (Ctrl+/)

GENERAL

- Overview
- Logs

THREAT MANAGEMENT

- Incidents
- Dashboards
- User analytics
- Hunting
- Notebooks

CONFIGURATION

- Getting started
- Data collection
- Analytics
- Playbooks
- Community
- Workspace

Last week (1/21/2018-1/27/2018)

8.2M ↗978.4K
EVENTS

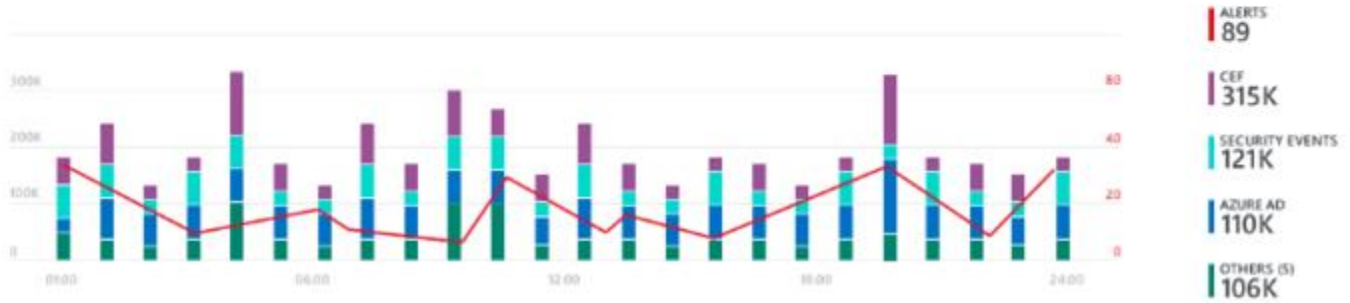
39 ↗6
ALERTS

18 ↗4
INCIDENTS

INCIDENTS BY STATUS

NEW (7) | IN PROGRESS (4) | CLOSED (RESOLVED) (4) | CLOSED (DISMISSED) (3)

Events and alerts over time



ALERTS 89
CEF 315K
SECURITY EVENTS 121K
AZURE AD 110K
OTHERS (5) 106K

Potential malicious events

MALICIOUS IPS EVENTS 82K
OUTBOUND 4K ▲
INBOUND 78K ▼

Recent incidents

User logged in to critical assets	9 Alerts
Suspicious process execution after co...	9 Alerts
Computers with cleaned event logs	8 Alerts
Remote procedure call (RPC) attempts	8 Alerts

Most anomalous data sources

Azure AD
Office
SecurityEvents

Democratize ML for your SecOps

Unlock the power of AI for security professionals by leveraging MS cutting edge research and best practices in ML, regardless of your current investment level in ML

Learn more >

Azure Policy

Azure 리소스에 대한 규칙과 효과를 적용

회사 표준과 서비스 수준 계약(SLA)를 준수할 수 있음

추가 비용 없이 사용

정책을 준수하지 않는 리소스 평가 및 식별

정책이 적용 후 정책을 준수하지 않는 리소스 배포 불가

정책 참고: docs.microsoft.com/azure/governance/policy/samples/