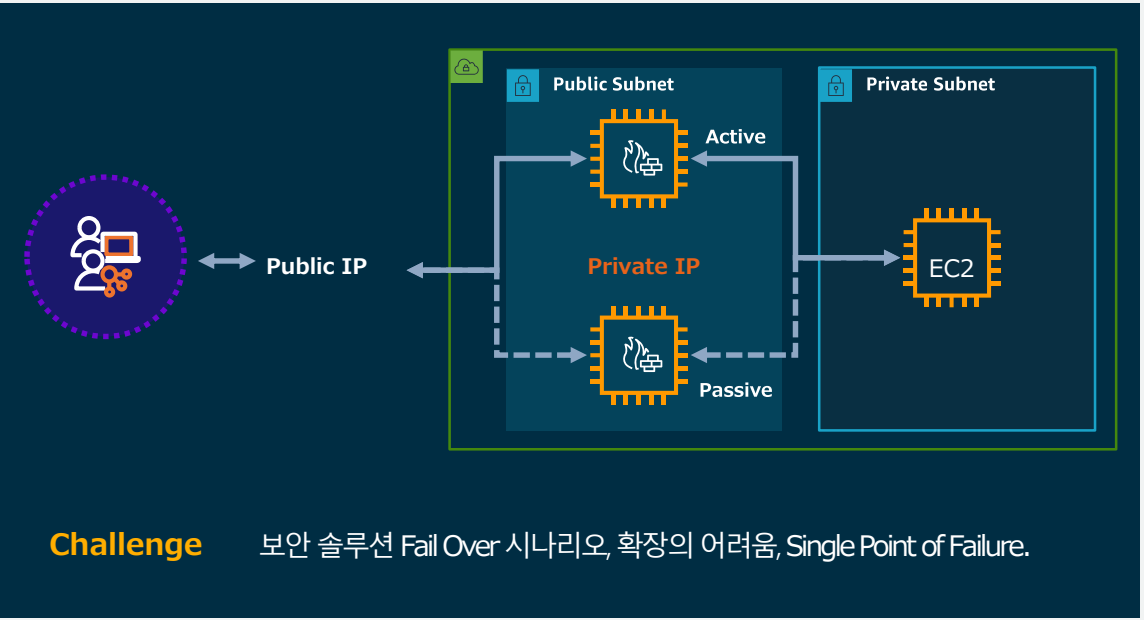
AWS Network Firewall

김수종
2025/01

AWS Network Firewall
- 개요 및 구성요소

AWS 네트워크 보안 - Active-Passive 구성

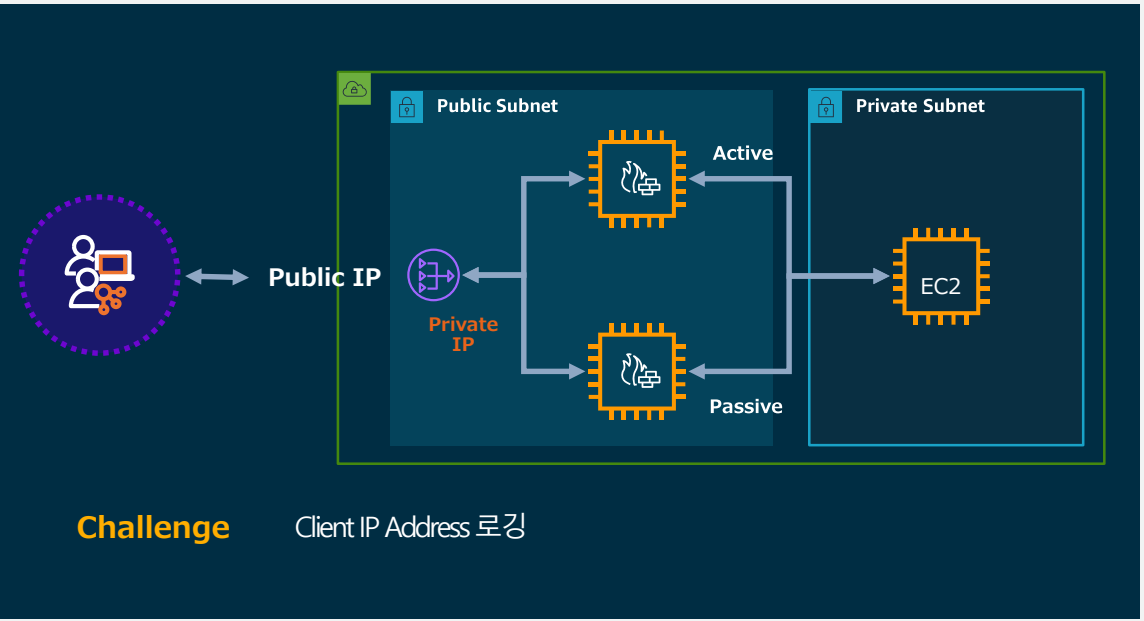
Active-Passive구성을 통해 N-IDS를 구현할 수 있으나, Fail Over 시나리오, 확장의 어려움, Single Point of Failure 단점 존재



- 구성방식
  - 두 개의 IPS 인스턴스를 서로 다른 AZ에 배치
  - VPC 라우팅 테이블을 통한 트래픽 우회
  - 페일오버 시, EIP를 Stanby IPS EC2로 변경
  - 페일오버 및 장애감지를 위해서 Lambda필요
  - 아웃바운드를 위해 NAT서버로 동작하게설정
- 단점
  - 복잡한 라우팅 설정 필요
  - 페일오버 시 일시적 서비스 중단 가능
  - 확장성 제한적
  - 라우팅 테이블 관리 부담
  - Active-Passive 구성으로 인한 리소스 낭비

AWS 네트워크 보안 - ELB 구성

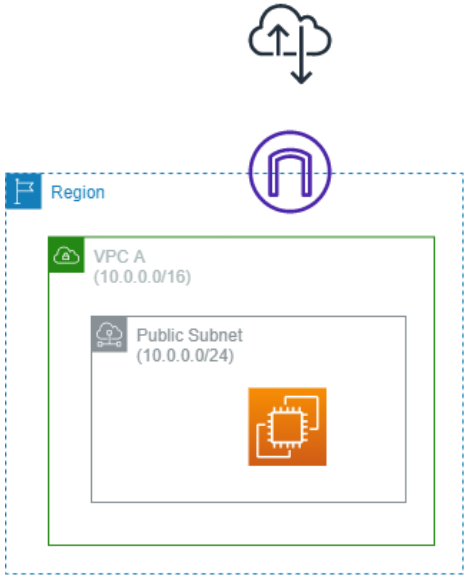
ELB 구성을 통해 N-IDS를 구현할 수 있으나, Client IP 로깅 어려운 단점 존재



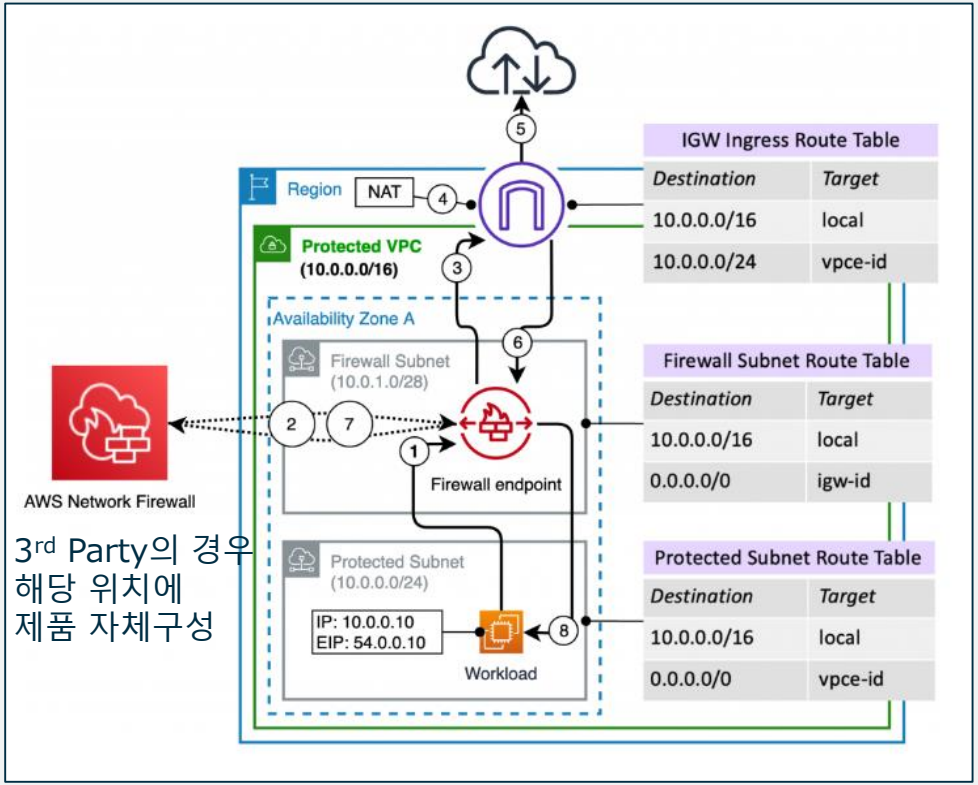
- 구성방식
  - ELB를 앞단에 배치
  - IPS 인스턴스들을 TargetGroup으로 등록
  - ELB의 Health Check로 IPS 상태 모니터링
  - 아웃바운드를 위해 NAT서버로 동작하게설정
- 단점
  - ELB 설정에 따라서 방화벽에서 Real Client IP확인 안될 수 도잇음(ALB를 쓰거나 NLB Src IP보존이 안되었을때 - 타겟그룹 IP주소로 설정안됨)

AWS 네트워크 보안 - ELB 구성

Network Firewall, GWLB 출시로 인해 확장성, 가용성이 보장되는 IDS 구축 가능

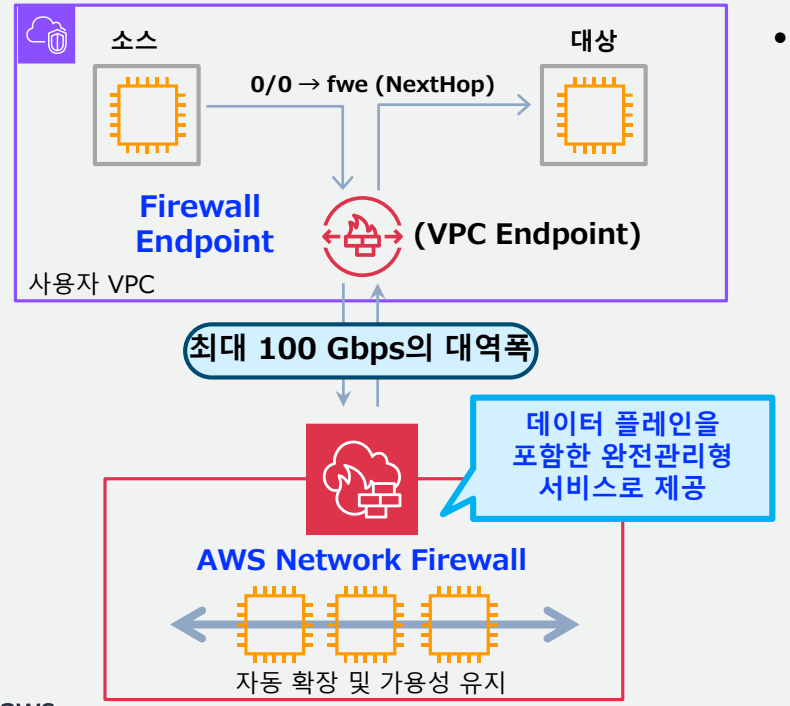


Destination	Target
10.0.0.0/16	local
0.0.0.0	igw



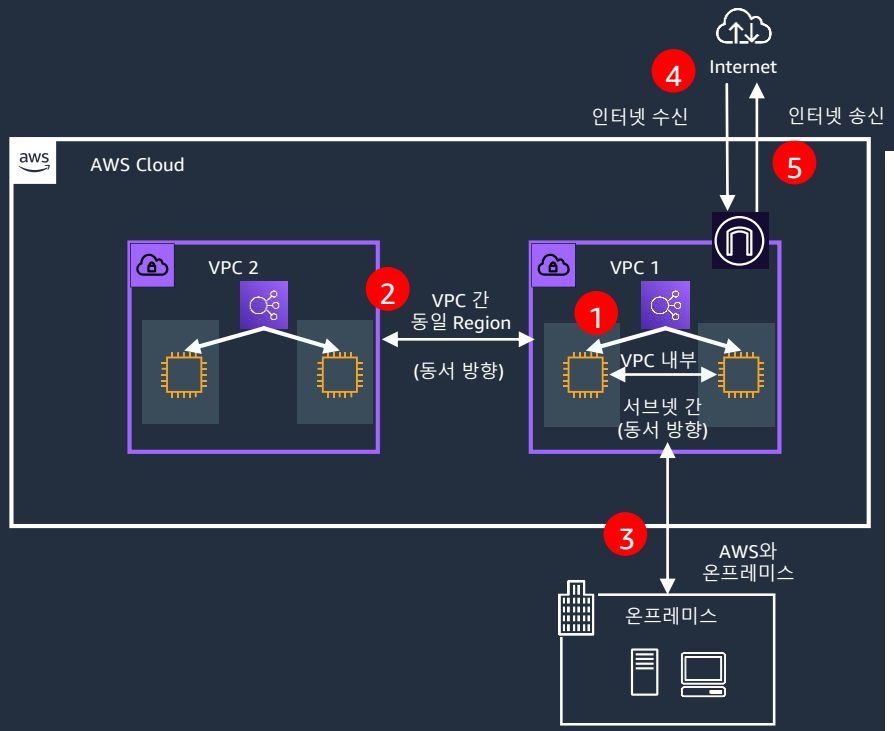
AWS Network Firewall - 개요

VPC의 완전관리형 네트워크 방화벽



- **주요 특징과 이점**
  - 완전관리형 서비스로서 확장성과 가용성 제공 (자체 관리형 EC2 인스턴스 기반 어플라이언스 관리 불필요)
  - 최대 100Gbps의 처리량 성능
  - 네트워크 트래픽에 대한 투명한 검사
  - 상태 기반 규칙의 한 종류로 HTTP/HTTPS 통신의 도메인 이름 기반 필터링 사용 가능
  - S3나 CloudWatch Logs 등 용량 제한이 없는 관리형 서비스로 방화벽 로그 출력

트래픽 검사 패턴



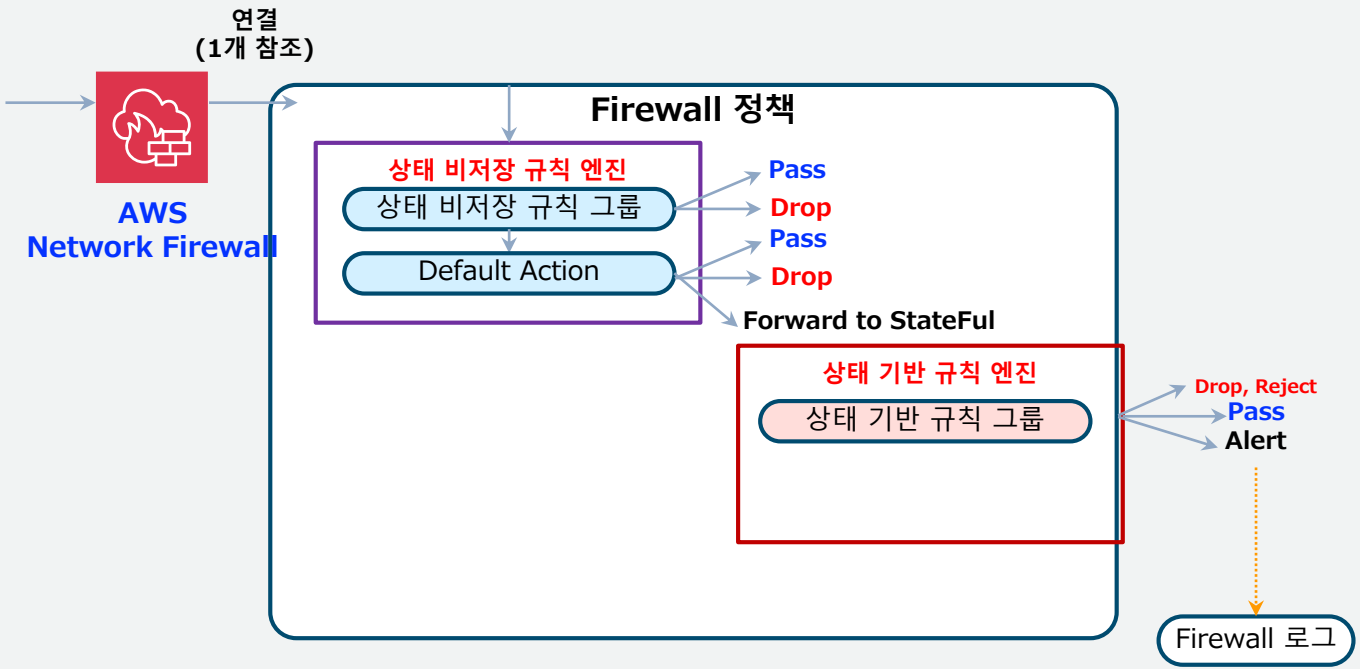
구간별 통제 방법 정의 (샘플)

순번	구간	서브넷	통제 방법
1	동 ↔ 서 [동일 VPC 내부]	WEB	Security Group(느슨한 설정)
		WAS	Security Group(느슨한 설정)
		DB	Security Group(타이트한 설정)
2	동 ↔ 서 [다른 VPC 간]	WEB	Security Group(느슨한 설정)
		WAS	Security Group(느슨한 설정)
		DB	Security Group(타이트한 설정)
3	동 ↔ 서 [데이터센터/오피스 ↔ VPC]	WEB	WAF, Onprem Firewall, Security Group
		WAS	Onprem Firewall, Security Group(타이트한 설정)
		DB	Onprem Firewall, Security Group(타이트한 설정) OR 라우팅 격리
4	남 → 북 [AWS VPC → 외부 인터넷]	WEB	Security Group(느슨한 설정)
		WAS	Security Group(느슨한 설정)
		DB	라우팅 격리
5	북 → 남 [외부 인터넷 → AWS VPC]	WEB	WAF, Network Firewall(Option)
		WAS	라우팅 격리
		DB	라우팅 격리

AWS Network Firewall
- 방화벽 정책

Network Firewall - Firewall 정책

하나의 Firewall은 하나의 Firewall 정책과 연결하여 사용
→ 통과하는 트래픽을 두 개의 규칙 엔진(Stateless/Stateful)으로 평가



상태 비저장 규칙 그룹

- 규칙 유형: 5-tuples 규칙만 사용 가능
  - 프로토콜
  - 출발지 IP
  - 출발지 포트
  - 목적지 IP
  - 목적지 포트
- 각 규칙 일치 시 액션:
  - Pass / Drop / Reject / 전송 지정

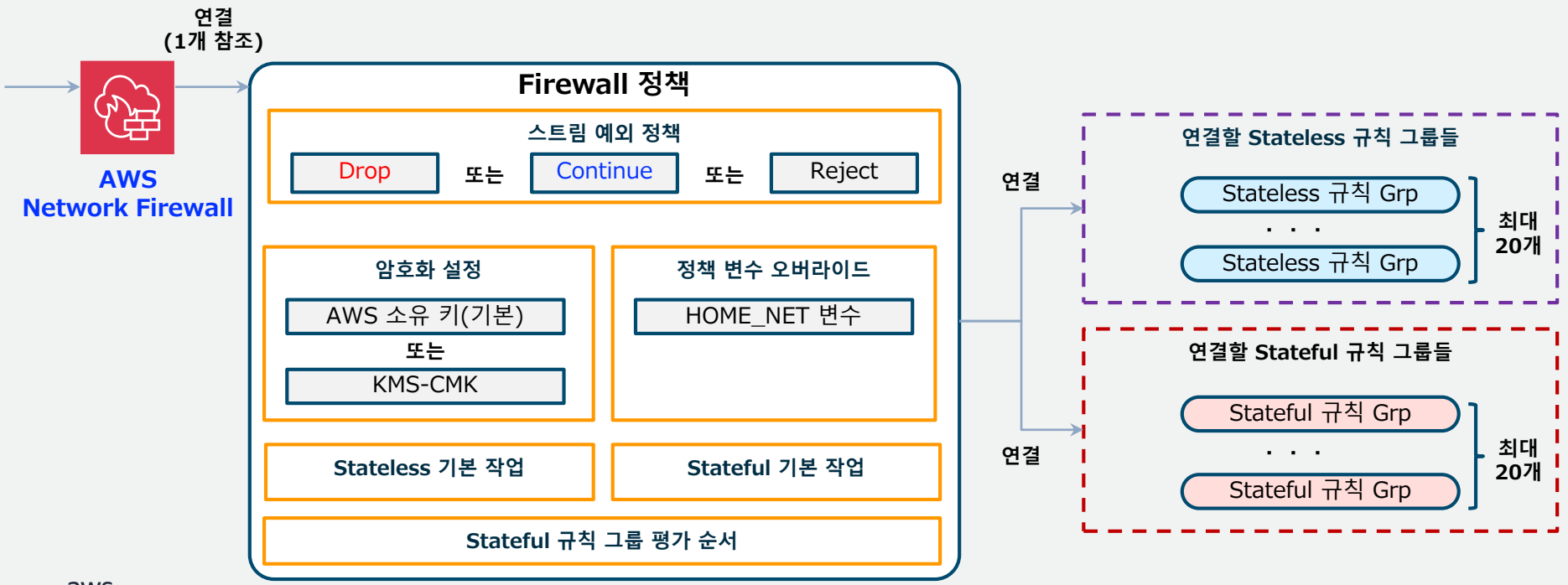
상태 기반 규칙 그룹

- 규칙 유형: 다음 3가지 유형 사용 가능
  1. 표준 (5-tuples 규칙)
  2. 도메인 리스트 - 허용/거부
  3. (HTTP, HTTPS 지원)
  4. Suricata 호환 IPS 규칙
- 각 규칙 일치 시 액션:
  - Pass / Drop / Reject / Alert 지정

※일치 시 액션 "Reject"는 프로토콜 "TCP" 선택 시에만 사용 가능

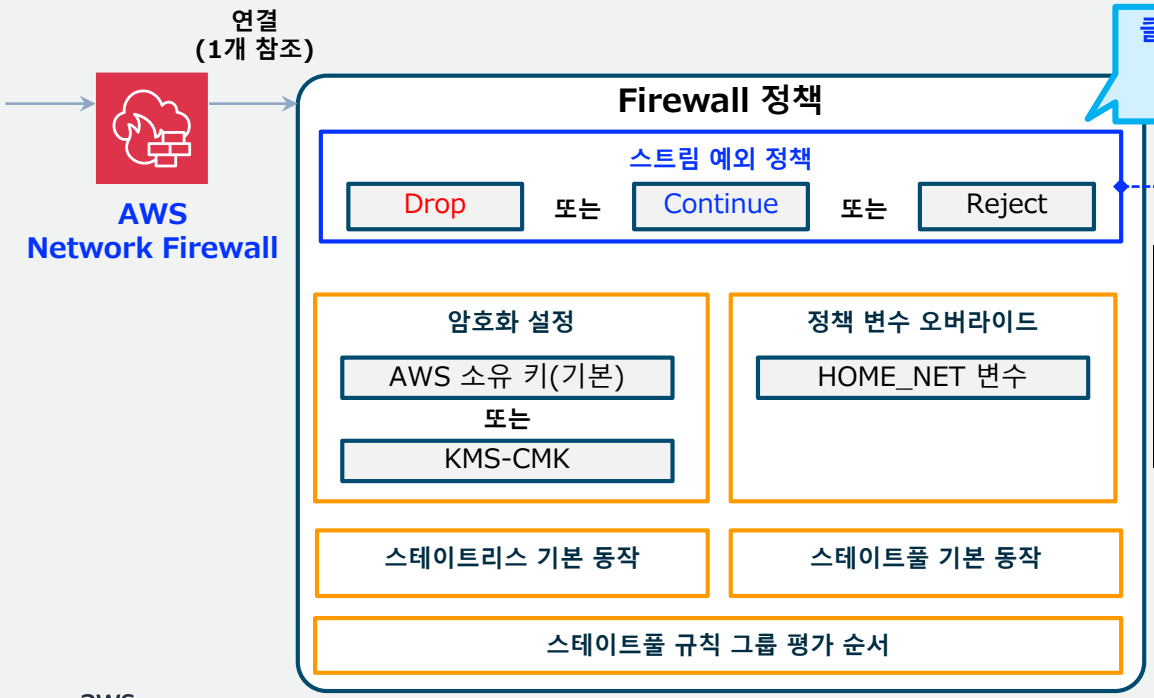
Network Firewall - Firewall 정책 설정

Firewall 정책은 여러 설정 항목을 가지고 있으며, 이와 연결된 Firewall의 전반적인 동작을 설정

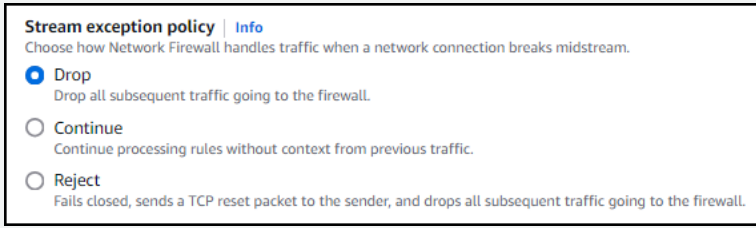


Network Firewall - Firewall 정책/기타 설정(1)

스트림 예외 정책에서 Firewall의 "트래픽 처리에서의 예외적 상황 처리"를 설정



클라이언트나 Network Firewall 측의 어떤 이유로 트래픽이 중단된 경우의 처리를 선택 (기본값은 "Drop")

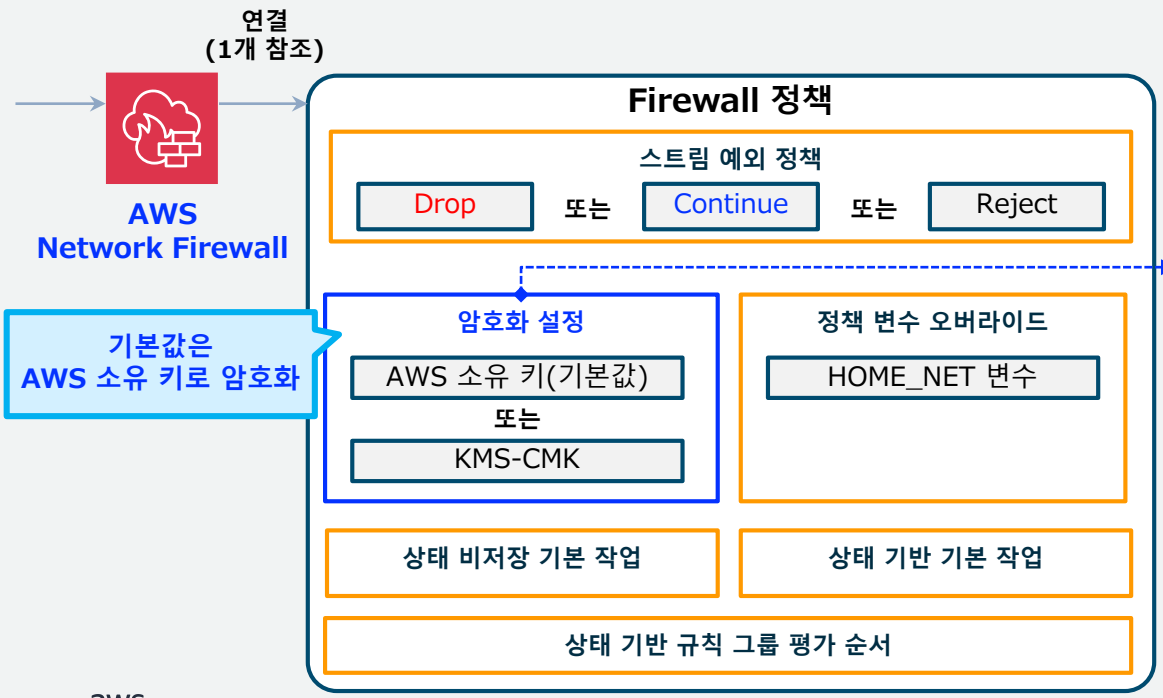


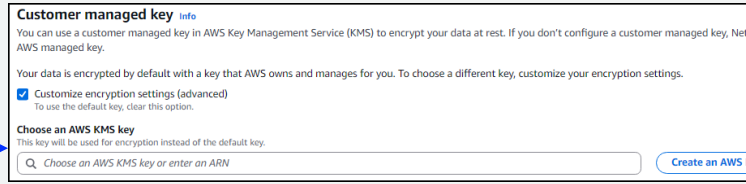
※스트림 예외 정책의 설정은 사용자의 보안 요구사항/정책에 따라 설정해야 할 값이 달라짐:

- Drop: 기본값이지만 아래 2개 중 하나를 검토
- (클라이언트가 타임아웃 대기하므로)
- Continue: 통과 (※스테이트풀 규칙도 통과)
- **Reject: 클라이언트 측 재시도에 맡김**

Network Firewall - Firewall 정책/기타 설정(2)

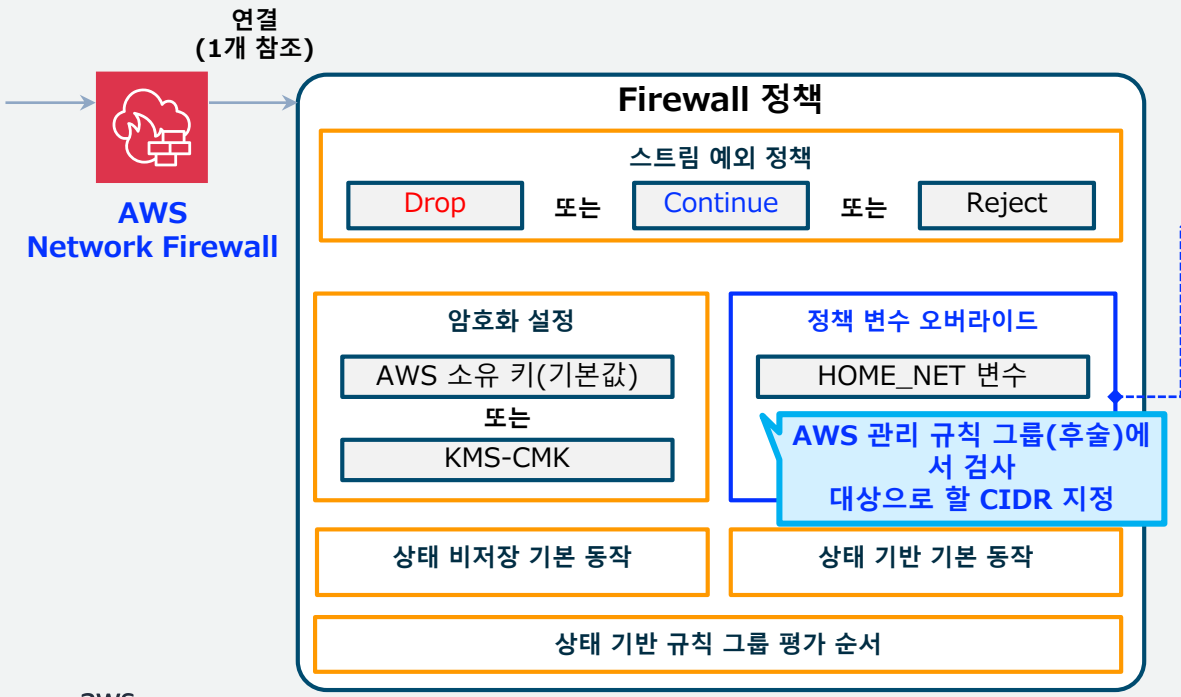
※Network Firewall의 설정과 저장 데이터의 암호화에 사용하는 키를 설정 가능
(※기본값은 AWS 소유 키를 사용)

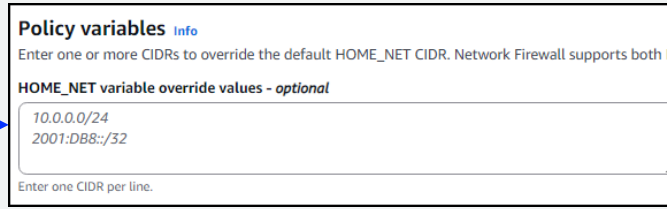




Network Firewall - Firewall 정책/기타 설정(3)

규칙 내부에서 참조하는 변수의 재정의(오버라이드) 지정 가능 (현재는 HOME_NET 변수만 지원)



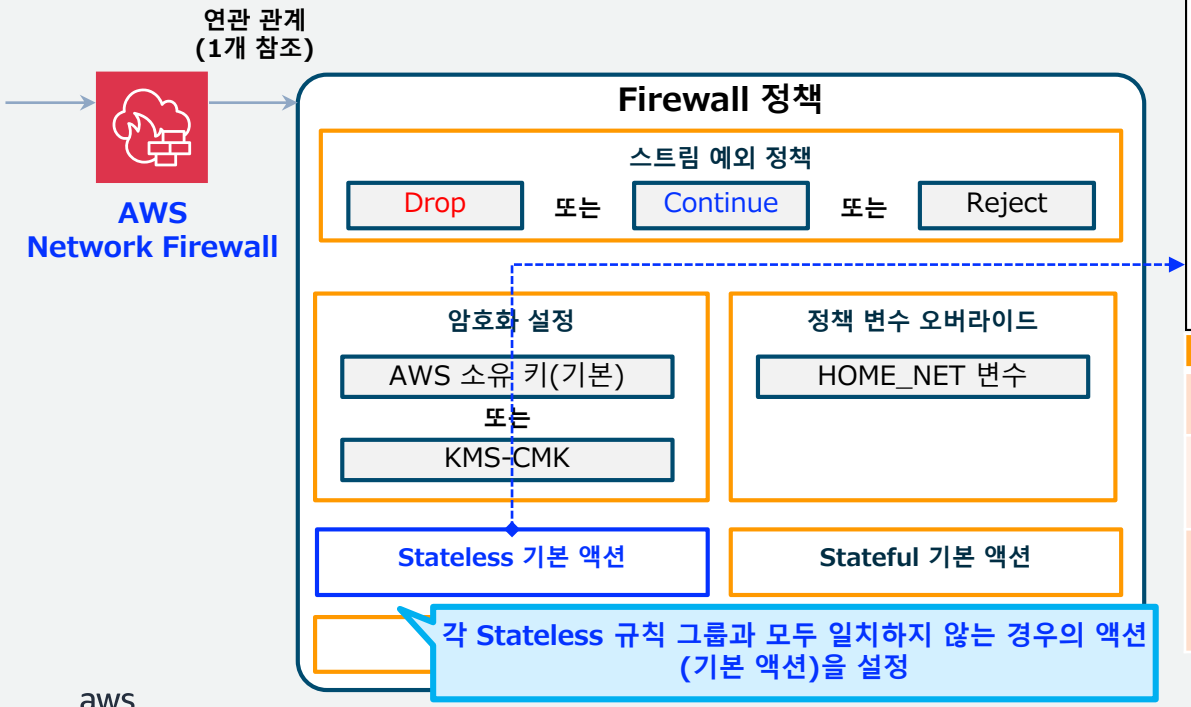


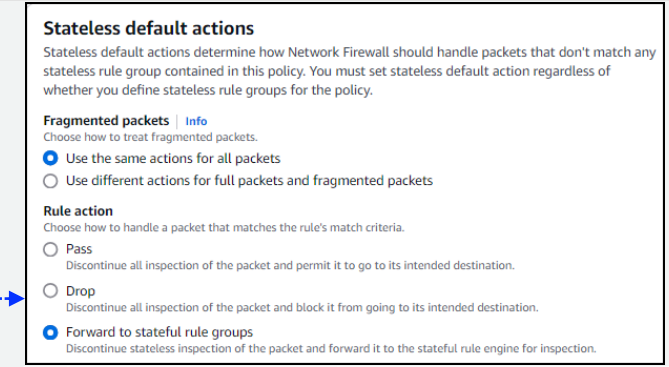
※HOME_NET 변수는 Suricata 호환 규칙에서 참조되는 변수 중 하나 (AWS 관리 규칙 그룹 내 규칙 포함)

→ 각 규칙에서 트래픽 검사 대상으로 하고 싶은 "모든 인바운드 트래픽의 소스 IP 범위" =CIDR을 지정 (※중앙 검사 구성의 경우, 여러 VPC나 온프레미스의 CIDR 모두를 지정)
(기본값은 "Firewall 엔드포인트가 생성된 VPC의 CIDR"만 자동으로 설정되므로, 필요에 따라 설정을 재정의할지 여부를 검토)

Network Firewall - Firewall 정책/기타 설정(4)

Stateless 엔진 내에서 "Stateless 규칙 그룹 중 어느 것과도 일치하지 않은 경우 "의 액션을 설정 가능

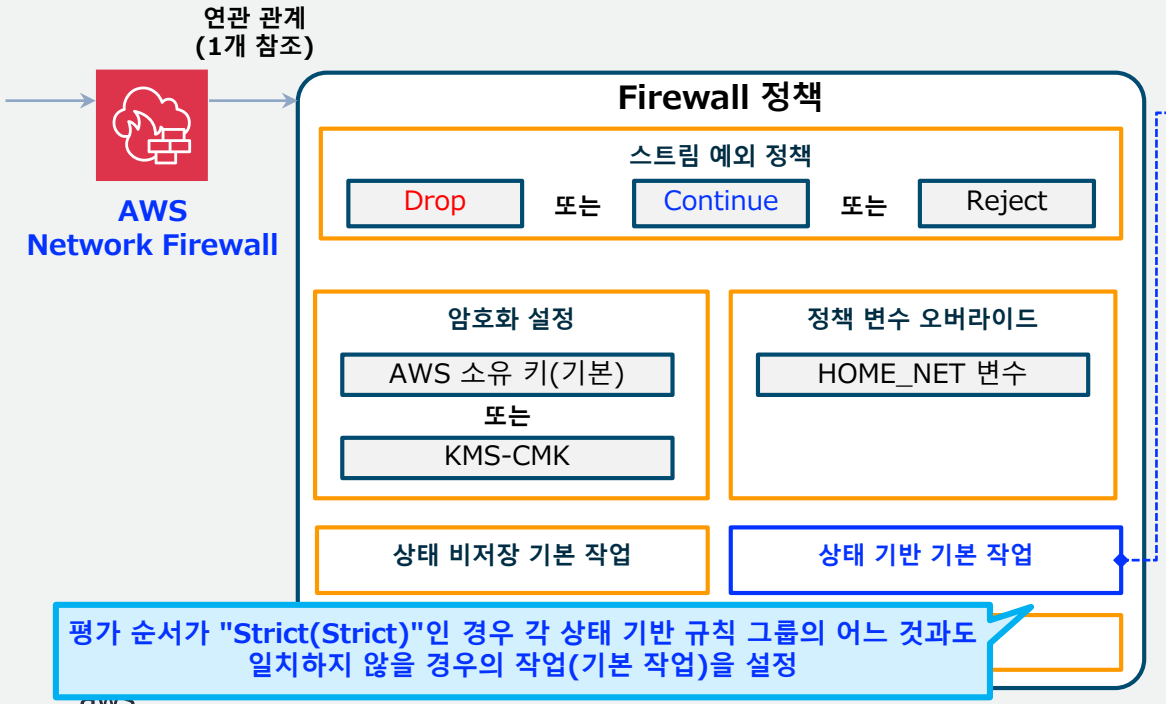


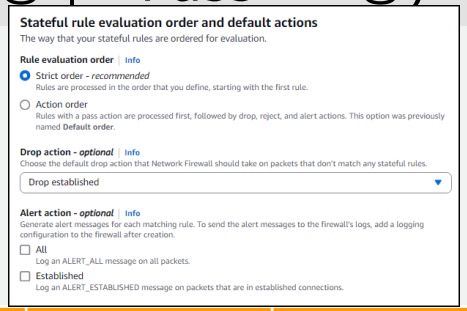


#	설정 항목	설명
1	단편화된 패킷	UDP Fragmentd packet 처리방식 결정
2	규칙 액션	"Drop", "Pass", "Stateful 규칙 엔진으로 전송(기본값)" 중 하나를 지정
3	메트릭 발행	Stateless 규칙 그룹용 CloudWatch 메트릭을 발행할지 여부 & 활성화 시 차원 이름을 지정

Network Firewall - Firewall 정책/기타 설정(5)

Firewall 정책의 "평가 순서"가 Strict(Strict)인 경우에만 상태 기반 기본 작업 설정 (※Action의 경우 "Pass" 고정)



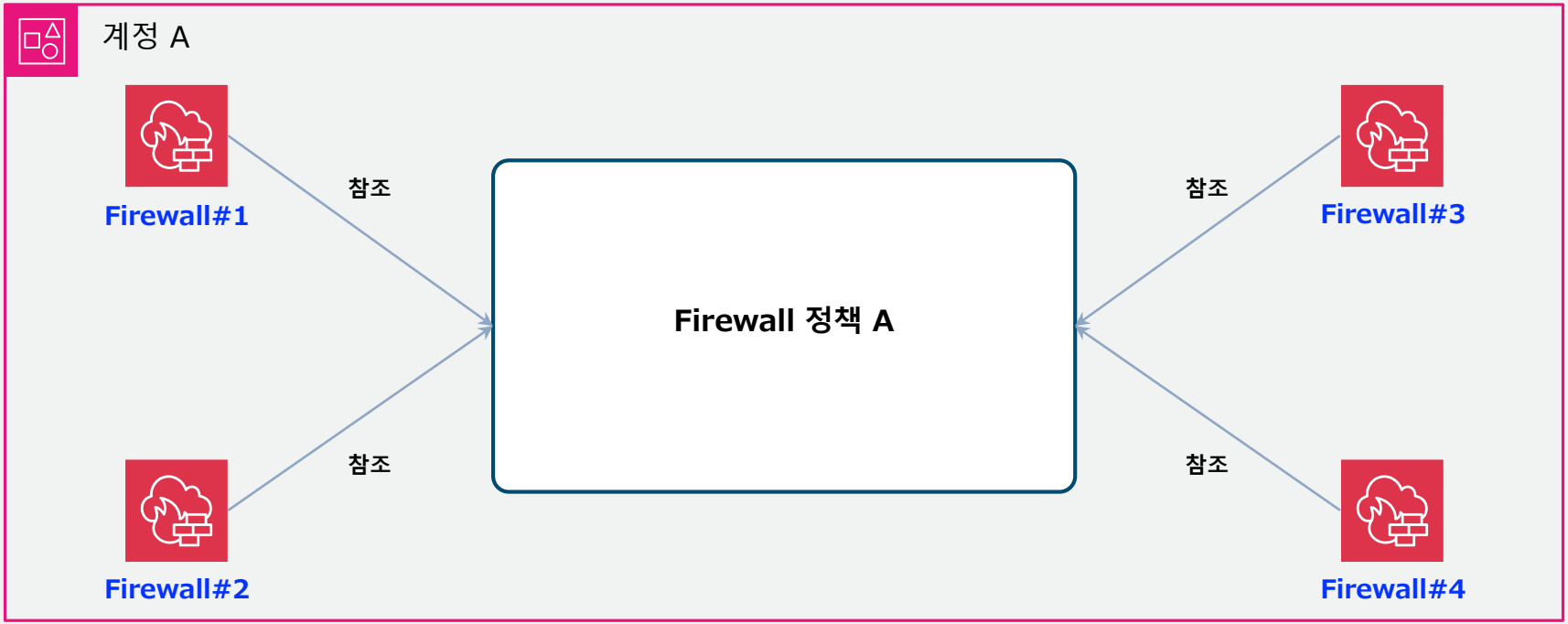


#	설정 항목	설명
1	Drop All?	어떤 상태 기반 규칙 그룹과도 일치하지 않는 경우 Drop **(모든 패킷이 차단됨)**
2	**Drop Established?**	어떤 상태 기반 규칙 그룹과도 일치하지 않는 경우, TCP 세션 수립 후라면 Drop **(TCP 3-handshake 패킷은 통과)**
3	Alert All?	어떤 상태 기반 규칙 그룹과도 일치하지 않는 경우, 로그 기록하고 Pass **(도메인 정보 안남음!)**
4	Alert Established?	어떤 상태 기반 규칙 그룹과도 일치하지 않는 경우, TCP 세션 수립 후라면 로그 기록하고 Pass **(허용된 로그는 안남음!)**

※ 주요로깅문제 https://repost.aws/ko/questions/QUOCuaTA5NRUa4xWpHON25Eg/aws-network-firewall-logging

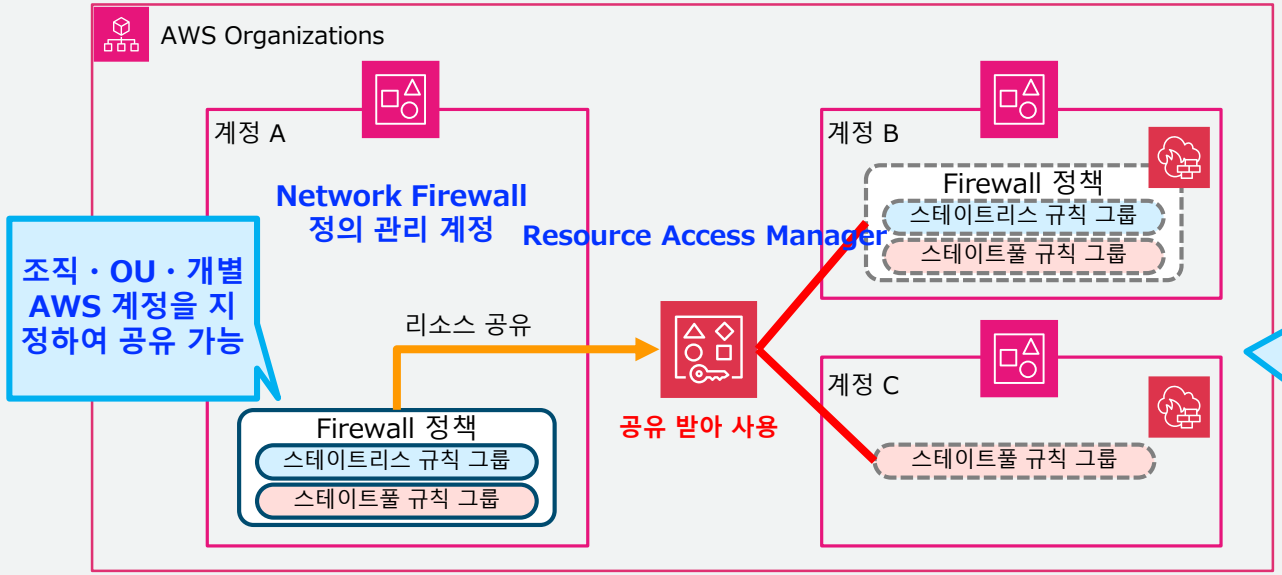
Network Firewall - 계정 내 정책 참조

여러 Firewall에서 단일 Firewall 정책을 공통적으로 참조 가능
→ 동일 계정 내 공통 설정 적용 가능



Network Firewall - 멀티 계정 공유

"Firewall 정책"과 "Firewall 규칙 그룹"은 Resource Access Manager (RAM)를 통해 다른 AWS 계정과 "공유" 가능



"Firewall 정책" 또는 "Firewall 규칙 그룹" 단위로 다른 계정과 공유 가능
→ Resource Access Manager를 통한 Network Firewall 설정의 중앙 관리 실현

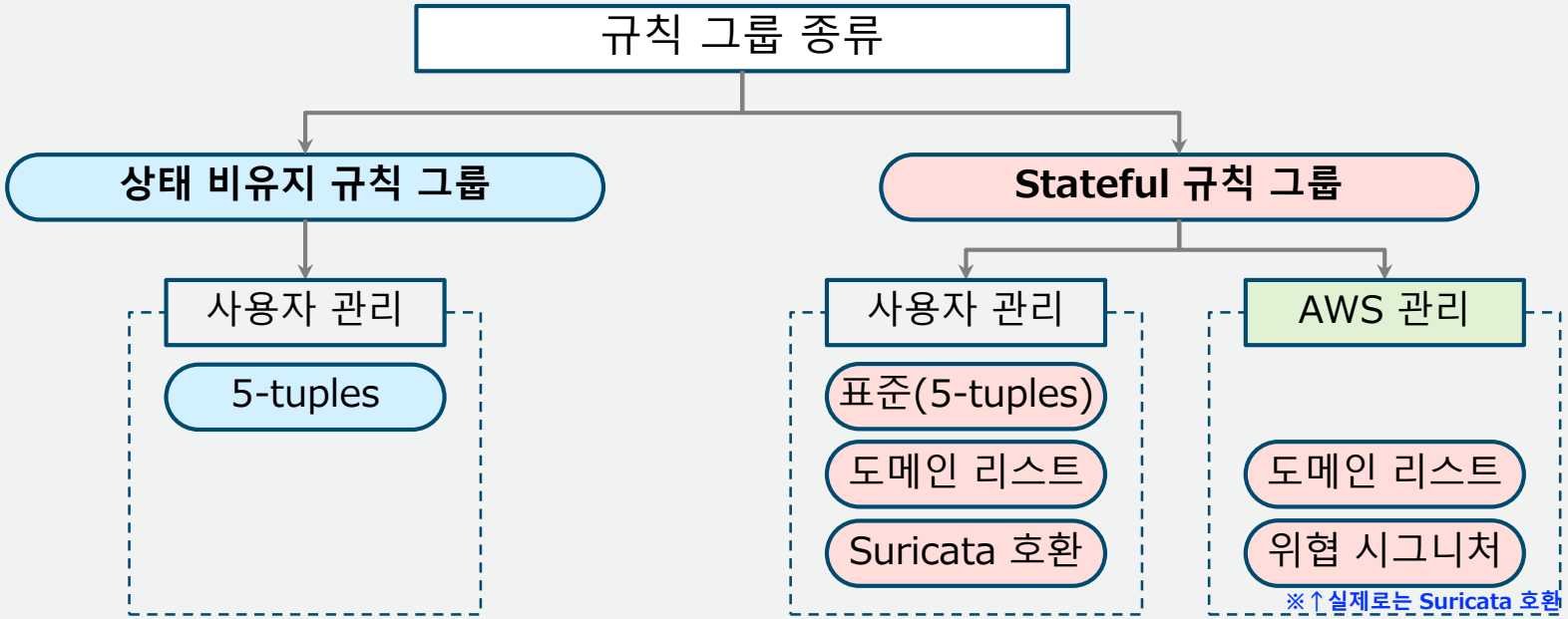
※AWS Firewall Manager를 함께 사용하면 Organization 내의 더 강력한 통제도 가능

※"Firewall 인스턴스" 자체는 계정 간 또는 VPC 간 직접 공유 불가
※"TLS 검사 설정"은 RAM 공유 대상 제외

AWS Network Firewall
- 규칙 그룹

Network Firewall - 규칙 그룹의 분류

Firewall 정책 내에 등록하는 규칙 그룹은,
'Stateful(Stateful)'와 '상태 비유지(Stateless)'로 크게 구분되며, 더 나아가 여러 종류가 존재합니다

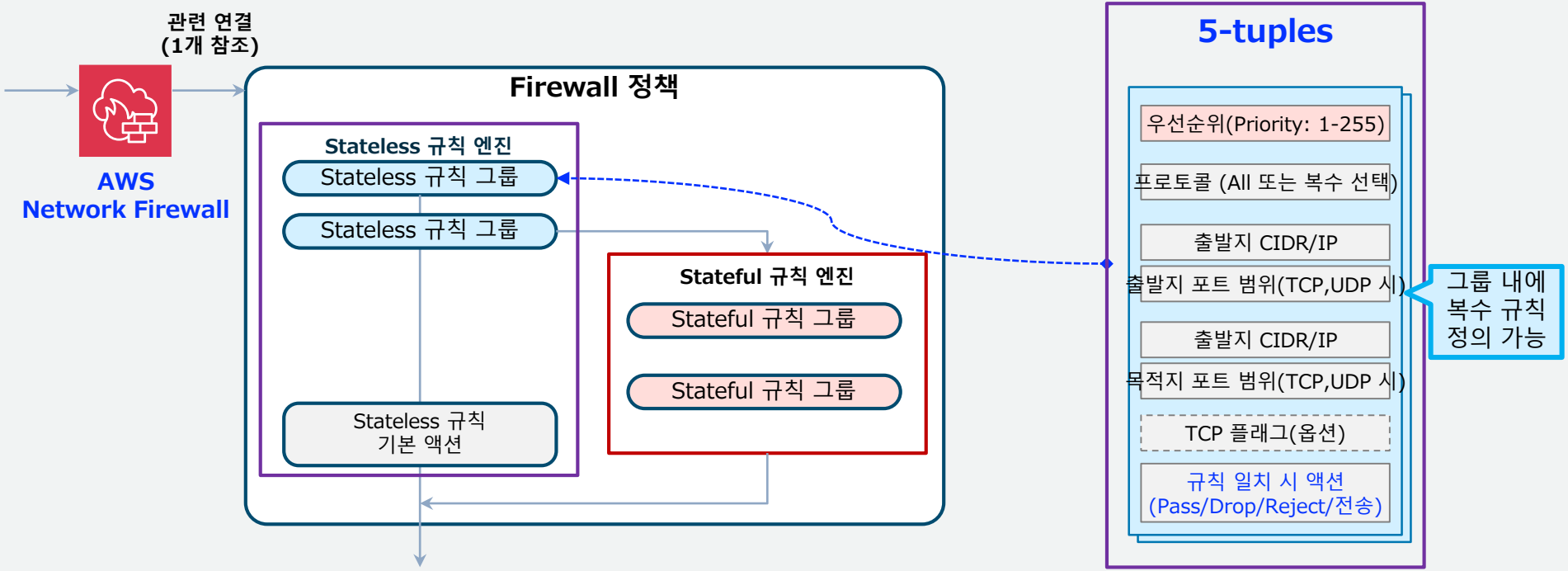


Network Firewall은 TCP 세션 상태를 고려하지 않음
→ 송신 허용 후의 '응답' 트래픽도 명시적인 허용 설정이 필요

Network Firewall은 TCP 세션 상태를 고려함
→ 송신 허용 후의 '응답' 트래픽은 자동으로 허용됨

보충: 규칙 그룹 종류 - 5-tuples(Stateless용)

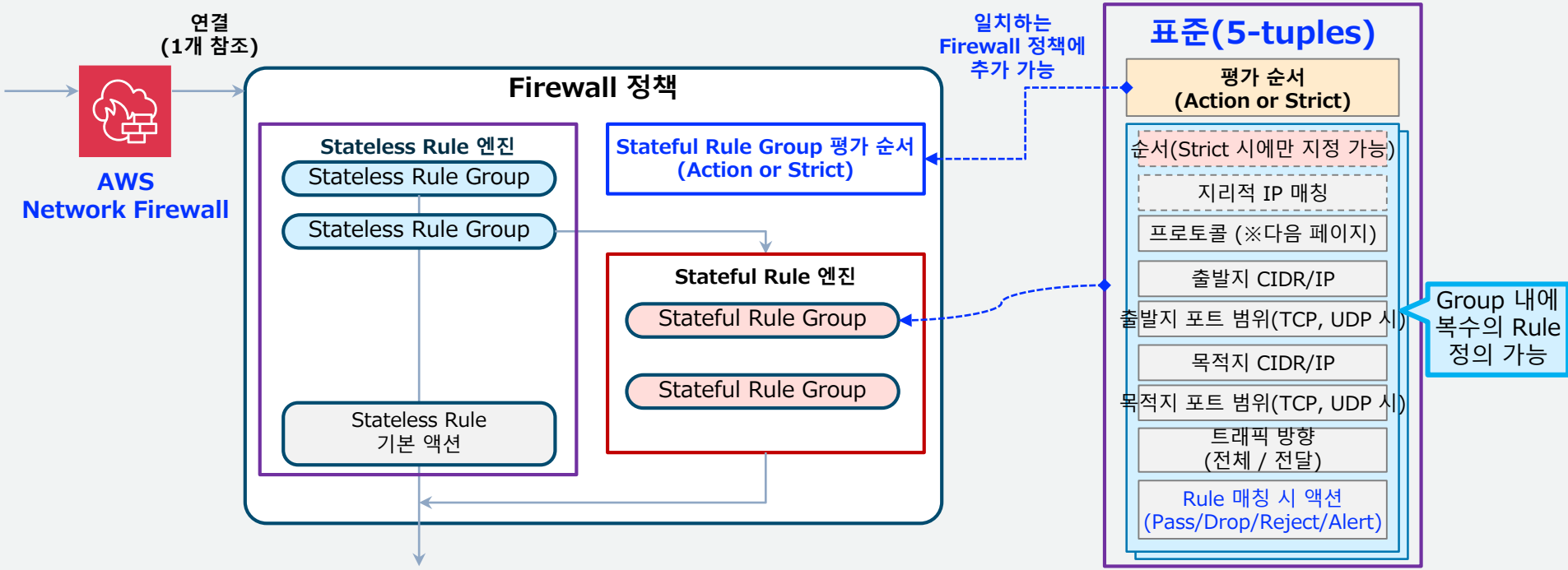
5-tuples를 기본으로 하는 매칭에 의해 액션을 평가함
→ Stateless 규칙 그룹에서 이용 가능한 유일한 규칙 그룹 종류



※동일한 5-tuples 상당의 규칙이라도, Statelessㅇ용 규칙과 Statefulㅇ용 "표준" 규칙에서는 설정 항목이 다름

보충: Rule Group 유형 - 표준(Stateful용)

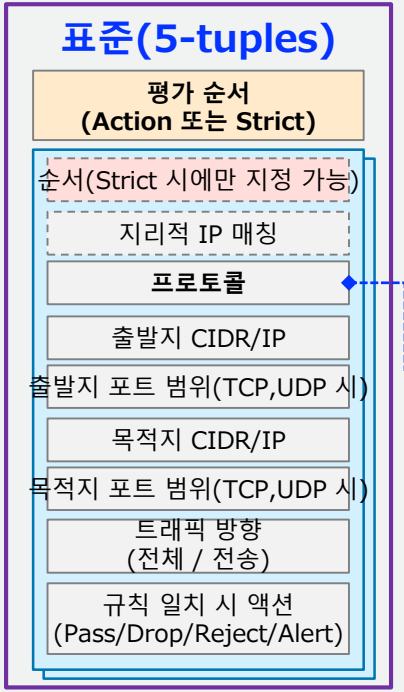
5-tuples 매칭을 통한 액션 평가
→ Stateful Rule Group에서 사용 가능한 Rule Group



※동일한 "표준" 규칙이라도 Stateless용과 Stateful용에서 설정 항목이 다름
※매칭 시 액션 "Reject"는 프로토콜 "TCP" 선택 시에만 사용 가능
※지리적 IP 매칭(geoip 키워드) 등 일부 Suricata 호환 규칙 키워드 설정도 가능

보충: 규칙 그룹 유형 - 표준(Stateful용)

Network Firewall Stateful 규칙 그룹의 "표준(5-tuples)" 유형은 아래 표의 전송 프로토콜을 지원



지원되는 전송 프로토콜

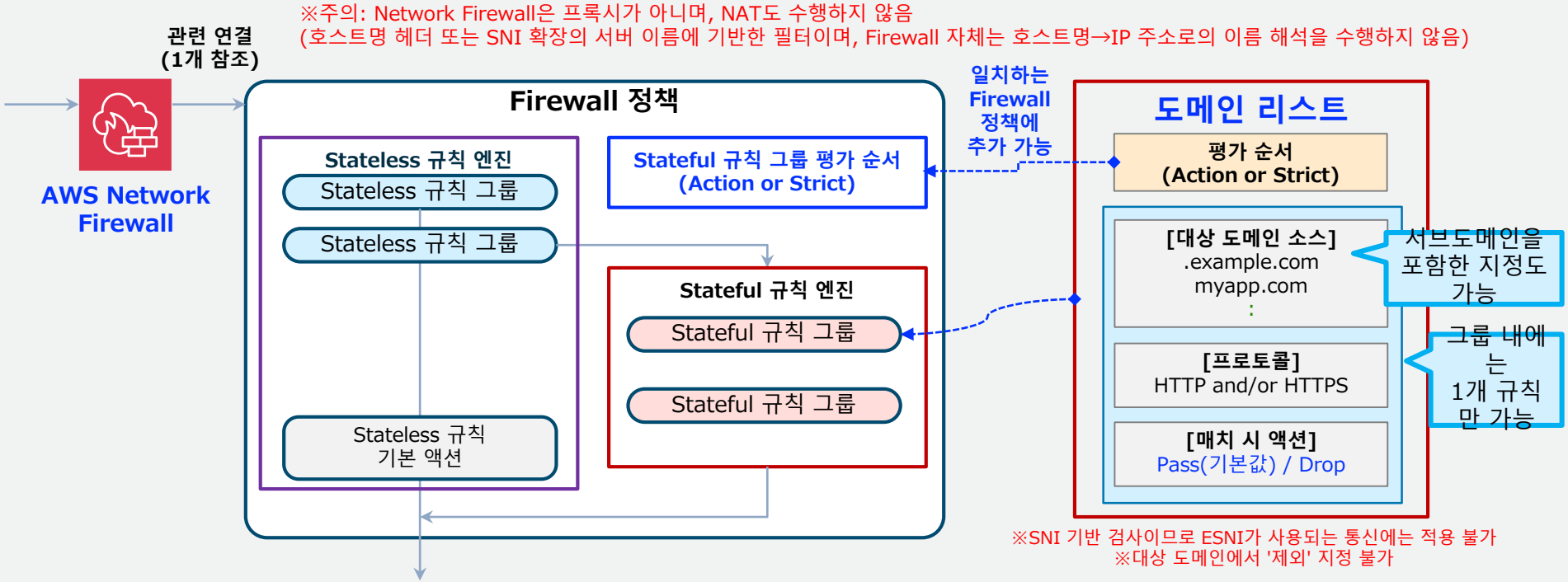
#	지원 프로토콜
1	IP
2	TCP
3	UDP
4	ICMP
5	HTTP
6	FTP
7	TLS
8	SMB
9	DNS
10	DCERPC

#	지원 프로토콜
11	SSH
12	SMTP
13	IMAP
14	MSN
15	KRB5 (Kerberos)
16	IKEV2 (IKEv2)
17	TFTP
18	NTP
19	DHCP

※상태 비저장용 규칙 그룹의 "프로토콜"과는 선택 가능한 범위가 다르며 단일 선택임

보충: 규칙 그룹 유형 - 도메인 리스트

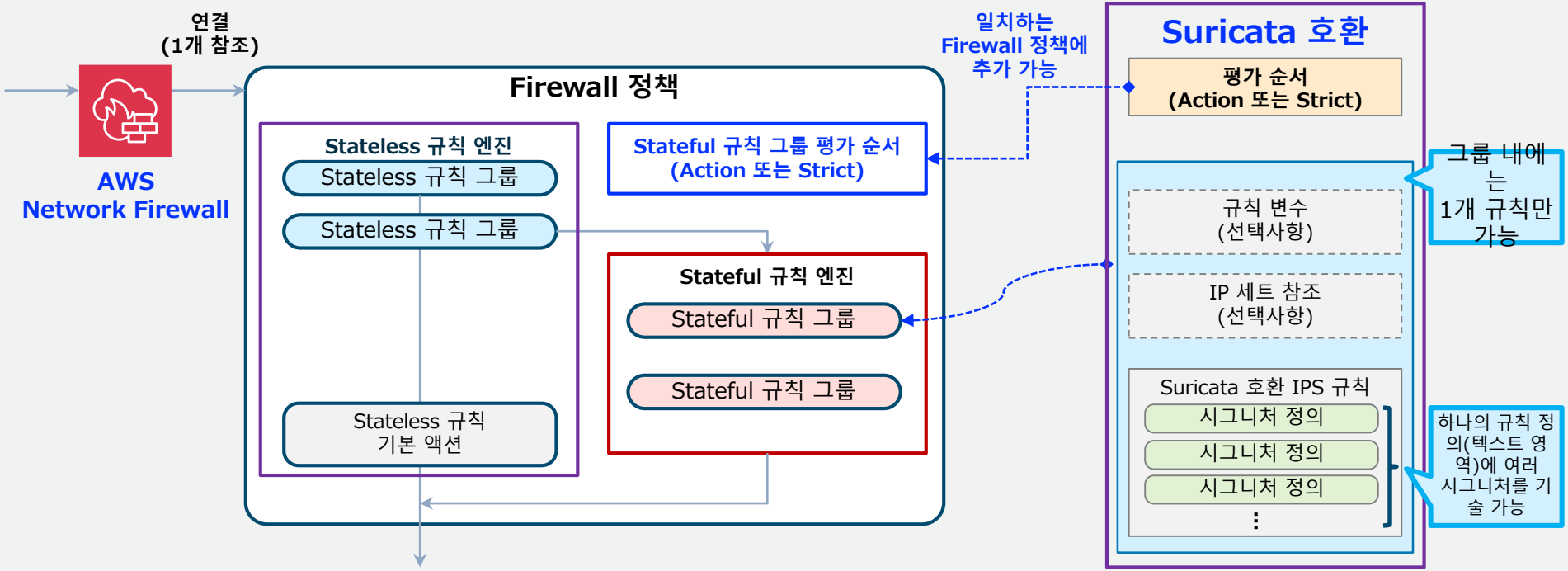
HTTP/HTTPS 통신 대상 도메인 이름의 매칭을 통한 평가와 액션
※거부 리스트・허용 리스트 모두 표현 가능



SNI: Server Name Indication / 암호화 세션 수립 전(Client Hello)에 도메인 이름이 전송됨(=도메인 이름은 암호화 대상 외)
ESNI: Encrypted SNI (=TLS 확장 구현 등의 수단을 통한 서버 측의 대응을 전제로 도메인 이름도 암호화됨)

보충: 규칙 그룹 유형 - Suricata 호환

Suricata 호환 IPS 규칙 정의 (가장 유연한 설정이 가능하나 전문성 필요)
→ Stateful 규칙 그룹에서만 사용 가능한 규칙 그룹



보충: 규칙 그룹 유형 - Suricata 호환 규칙 예시

송신원이 192.168.0.0/24이고 모든 IP 주소 대상의 HTTP/HTTPS 통신에 대해 "example.com" 및 그 하위의 모든 서브도메인 대상 통신을 허용

"평가 순서: Strict(Strict)" & "기본 액션: Drop Established" 설정의 경우

```
pass http 192.168.0.0/24 any -> any 80 (http.host; dotprefix; content:".example.com"; endswith; msg:"Allowed HTTP domain"; sid:102120; rev:1;)
pass tls 192.168.0.0/24 any -> any 443 (tls.sni; dotprefix; content:".example.com"; endswith; msg:"Allowed HTTP domain"; sid:102121; rev:1;)
```

"평가 순서: Strict(Strict)" & "기본 액션: Drop All" 설정의 경우

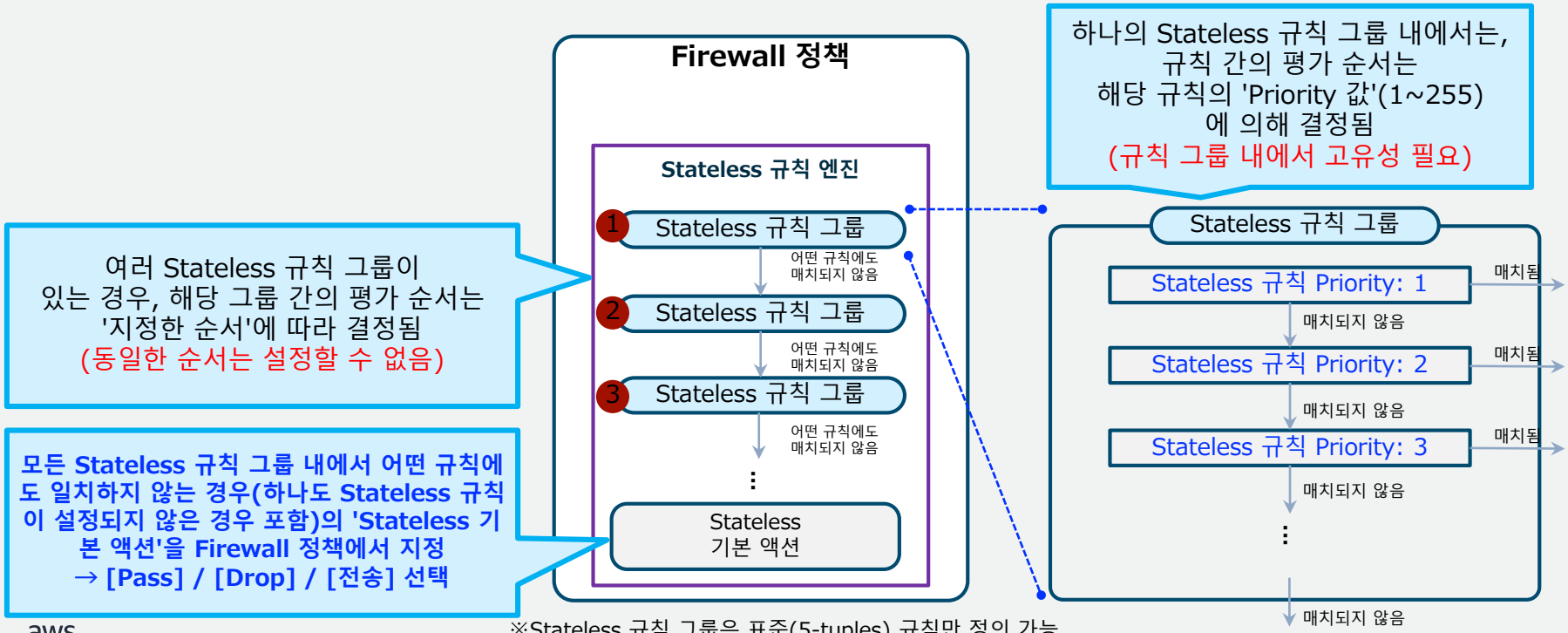
```
pass http 192.168.0.0/24 any -> any 80 (http.host; dotprefix; content:".example.com"; endswith; msg:"Allowed HTTP domain"; sid:102120; rev:1;)
pass tls 192.168.0.0/24 any -> any 443 (tls.sni; dotprefix; content:".example.com"; endswith; msg:"Allowed HTTP domain"; sid:102121; rev:1;)
pass tcp 192.168.0.0/24 any <> any 80 (flow:not_established; sid:102122; rev:1;)
pass tcp 192.168.0.0/24 any <> any 443 (flow:not_established; sid:102123; rev:1;)
```

지리적 IP 매치 이용 설정의 규칙 예시(러시아에서/러시아로의 모든 트래픽을 Alert)

```
alert ip any any -> any any (msg:"GeoIP is RU, Russia"; geoip:any,RU; sid:55555555; rev:1;)
```

Network Firewall - 평가 순서(Stateless 엔진)

Stateless 엔진 내에서는 규칙 그룹 간 지정된 순서대로 평가
규칙 그룹 내에서는 규칙의 Priority 값(1~255) 작은 순서대로 평가



※Stateless 규칙 그룹은 표준(5-tuples) 규칙만 정의 가능
※Stateless 규칙 그룹에서는 Stateful 규칙 그룹과 달리, '반환 트래픽'에 대한 허용을 명시적으로 정의해야 함

Network Firewall - 평가 순서(Stateful 엔진)

Stateful 규칙 그룹(5-tuples형과 Suricata 호환형)은 정책의 '평가 순서 유형(Action 또는 Strict)'에 따라 규칙 평가 순서가 변화합니다

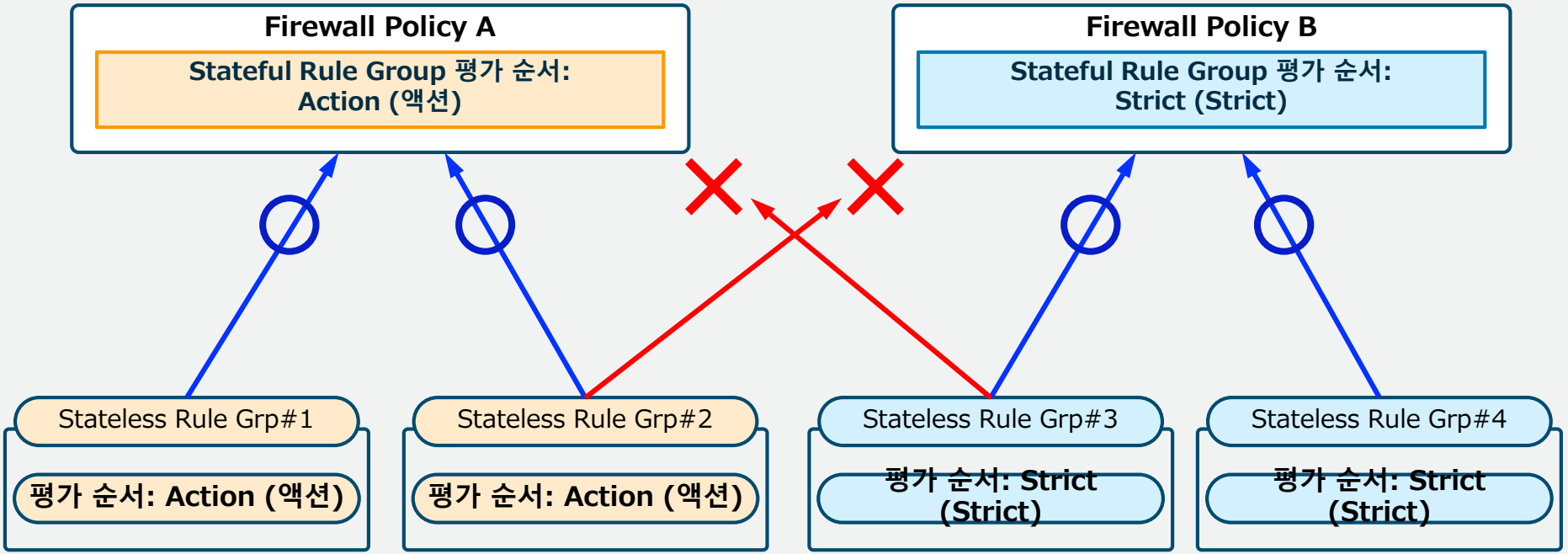
※'평가 순서' 설정은 Firewall 정책 레벨의 설정으로, Firewall 정책 생성 시에만 설정이 가능함(생성 후 변경 불가)

	평가 순서: Action (액션)	평가 순서: Strict (Strict) ※권장
평가 순서	모든 Stateful 규칙 그룹을 횡단하여 액션 종류별로, Suricata 사양의 다음 액션 종류 순서로 평가됩니다 [1. pass]→[2. drop]→[3. reject]→[4. alert] ※Stateful 규칙 그룹 간의 순서 개념이 없음 → 각 pass / drop / alert 액션 종류 내에서는 각 규칙의 priority 값(1~255) 순으로 평가 (1이 가장 우선순위가 높음 → 1, 2, 3, ... 순서로 평가) ※어느 것에도 일치하지 않은 경우는 pass	Stateful 규칙 그룹마다 순서를 정의함 + 각 Stateful 규칙 그룹 내에서 (액션 종류와 무관하게) 순수하게 priority 값(1~255)이 작은 것부터 순서대로 평가됨 → 'Action'과 달리, pass / drop / alert의 액션 종류에 영향을 받지 않음 ※각 규칙 그룹 내의 규칙은 '정의된 순서대로' 처리됨 (1이 가장 우선순위가 높음 → 1, 2, 3, ... 순서로 평가)

※평가 순서 'Action(액션)'은 이전에는 'Default(기본값)'이라는 명칭이었으나 변경됨

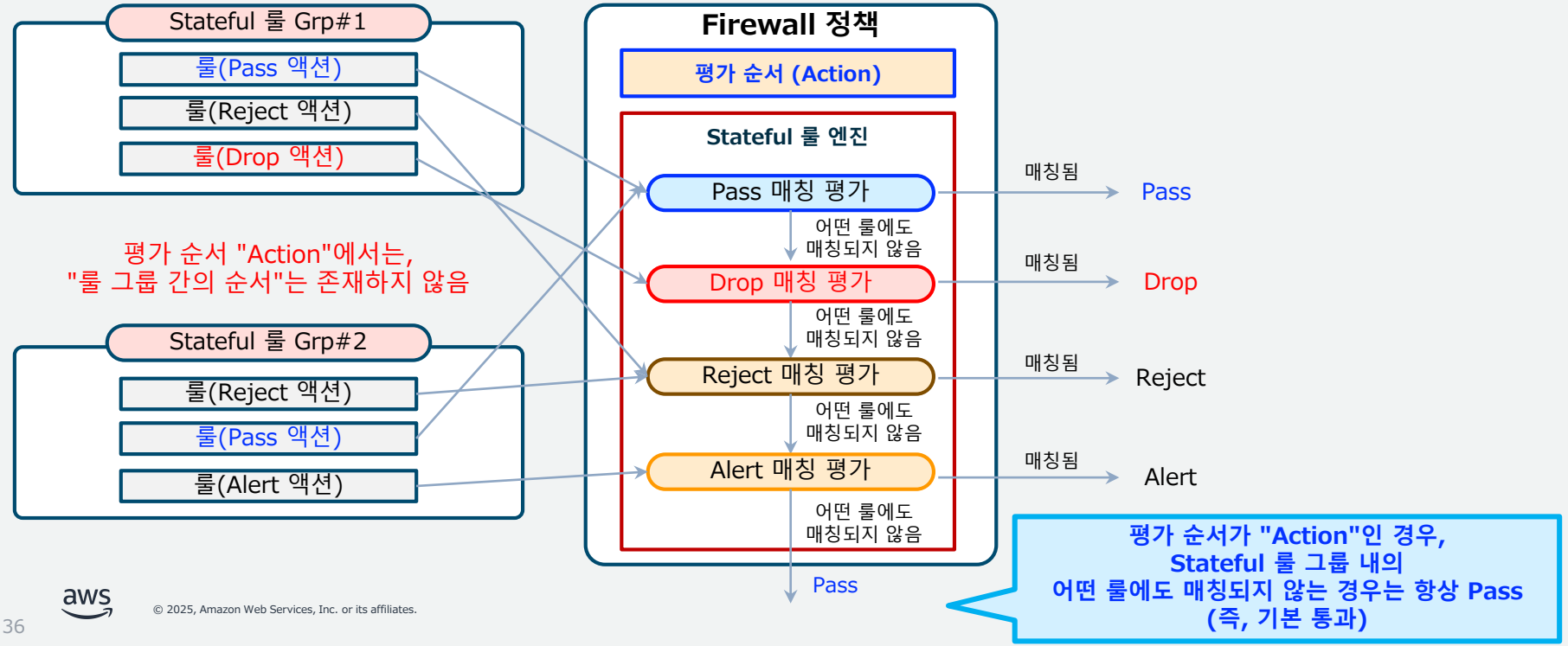
보충: Policy와 Rule Group 평가 순서의 관계

Stateful Rule Group은 "동일한 평가 순서 유형"으로 생성된 Firewall Policy에만 추가 가능



Network Firewall - 평가 순서(Stateful/Action)

Action 평가 순서 타입에서는 룰 그룹을 횡단하여
Pass → Drop → Reject → Alert 순서로 평가하고, 매칭되지 않는 경우는 Pass



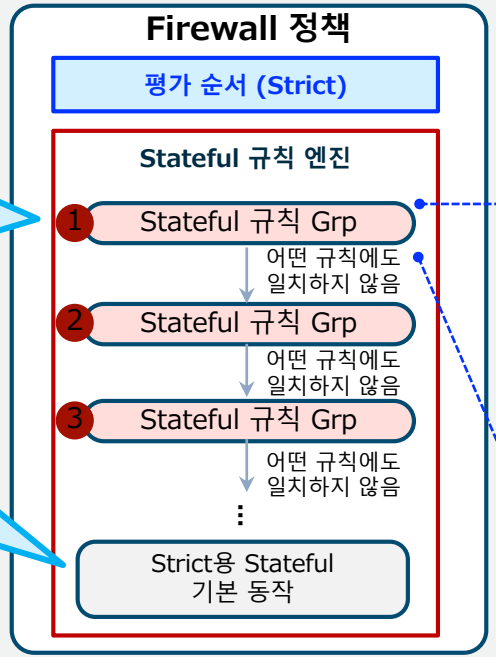
Network Firewall - 평가 순서(Stateful/Strict)

Strict 평가 순서 유형에서는 규칙 그룹 간 지정된 순서대로 평가 & 규칙 그룹 내에서는 평가 순서 설정(다음 페이지 참조)에 따라 평가 순서가 변화

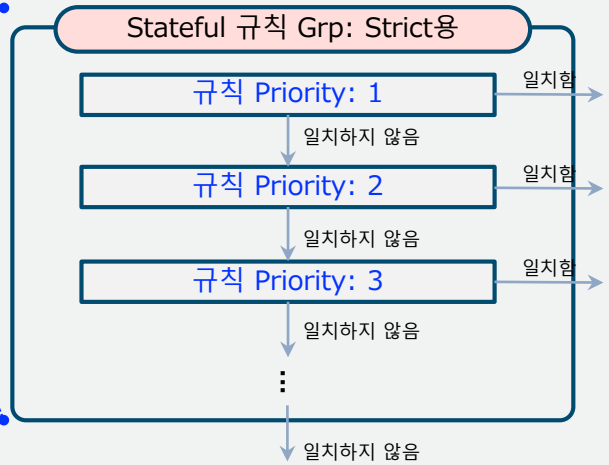
여러 Stateful 규칙 Grp가 있는 경우, 해당 그룹 간의 평가 순서는 "지정된 순서"에 따라 결정됨
(동일한 숫자는 설정할 수 없음)

모든 Stateful 규칙 그룹 내의 어떤 규칙에도 일치하지 않는 경우(Stateful 규칙 Grp가 하나도 설정되지 않은 경우 포함)는 Firewall 정책에서 설정한 "Stateful 기본 동작"을 따름

※기본 동작의 Alert는 개별 규칙의 Drop이나 Alert와 중복되어 작동함

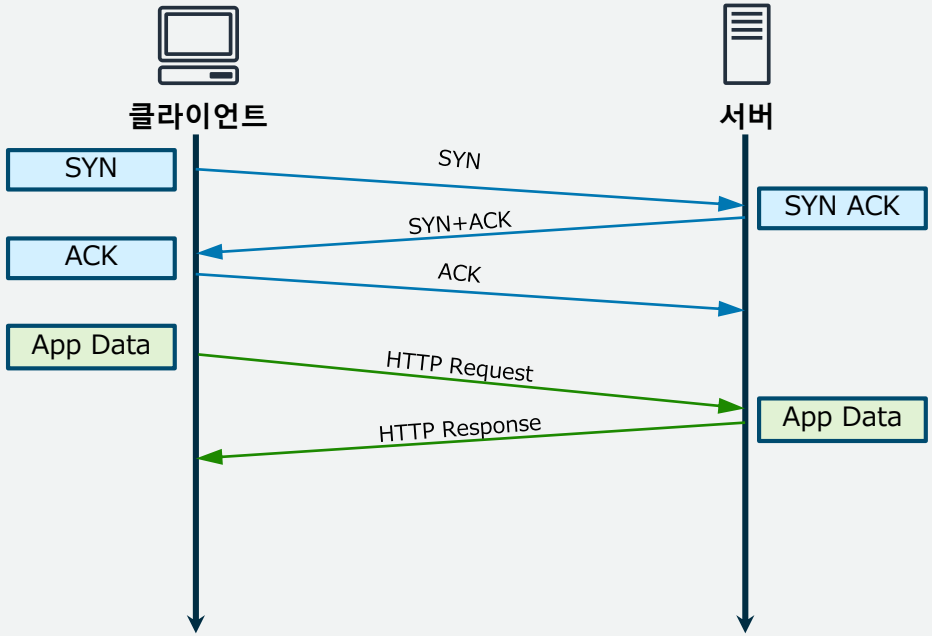


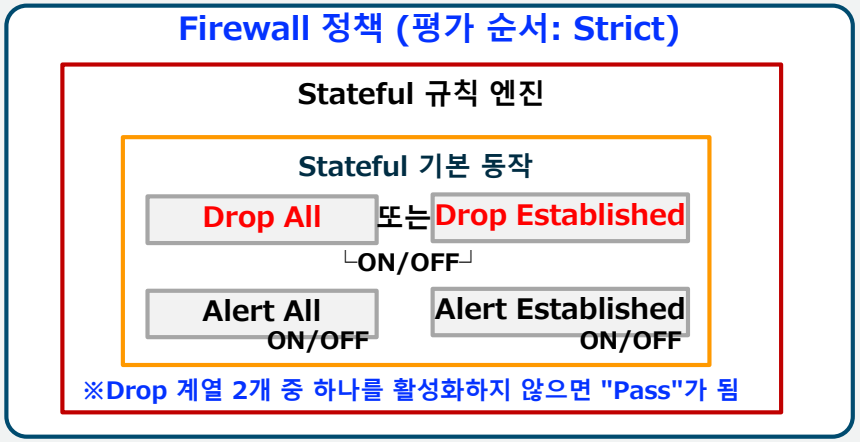
하나의 상태 비저장 규칙 Grp 내에서는, 규칙 간의 평가 순서는 해당 Stateful 규칙 Grp의 "평가 순서" 설정에 따름



Network Firewall - 평가 순서(Stateful/Strict)

"평가 순서: Strict(Strict)" 시 설정 가능한 "Stateful 기본 동작"의 설정값 의미와 동작에 주의

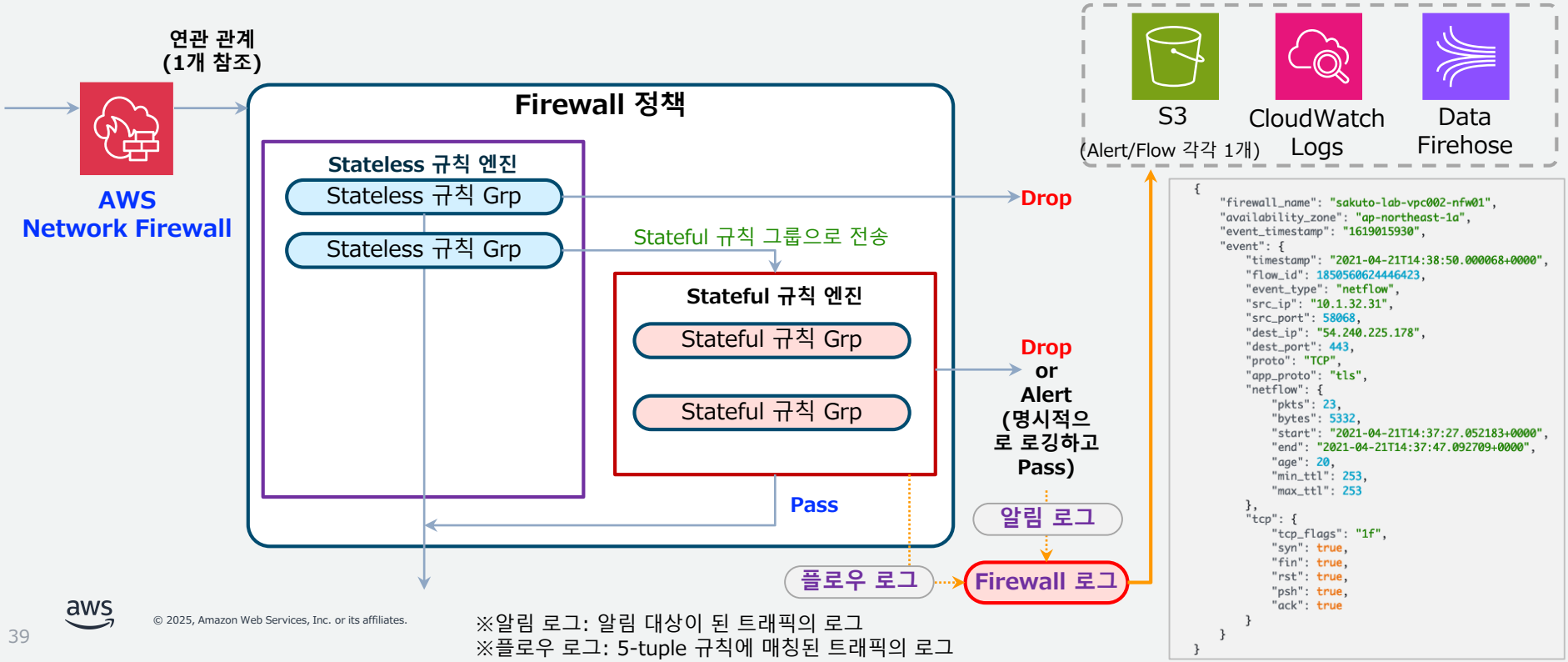




#	활성화/비활성화	설명
1	**Drop All** **(모두 드롭)**	TCP 3-way handshake 트래픽에도 매칭되므로 이들도 Drop함 → HTTP 등의 TCP 연결 후 검사는 수행되지 않음
2	**Drop Established** (연결이 수립된 트래픽을 드롭하고, 그 외는 Pass 함)	TCP 3-way handshake는 제외하고 TCP 세션 수립은 실행함(수립된 것을 Drop) (※대부분의 경우 직관적이고 사용하기 쉬운 설정) 결과적으로 HTTP 등의 상위 레이어 검사를 수행하고, 그 위에서 기본값을 Drop으로 설정할 수 있음. ※Suricata 호환 규칙에서는 TCP 핸드셰이크만 허용하는 규칙을 작성 가능

Network Firewall - Firewall 로그

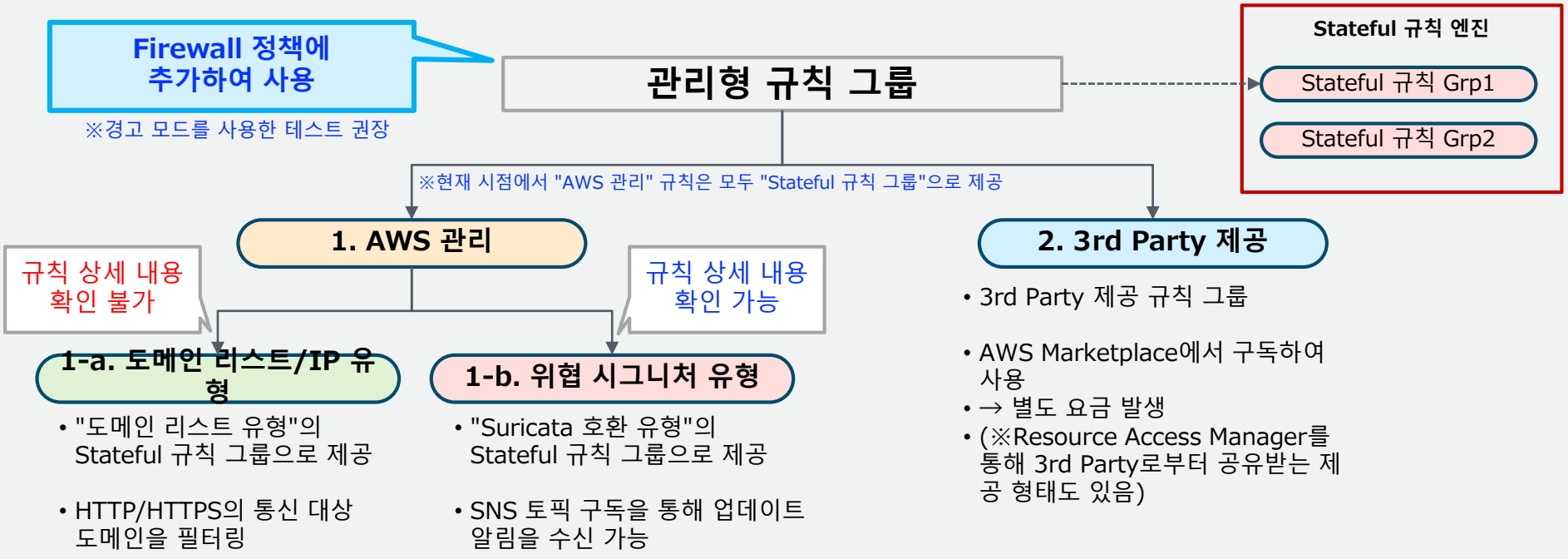
Stateful 규칙 그룹의 로그(알림/플로우 2종류)를 개별적으로 출력 가능 (※Stateless 규칙 그룹의 로그는 출력 불가)



※알림 로그: 알림 대상이 된 트래픽의 로그
※플로우 로그: 5-tuple 규칙에 매칭된 트래픽의 로그

Network Firewall - 관리형 규칙 그룹

사용자가 직접 정의하는 규칙 그룹 외에도, AWS와 3rd Party에서 "관리형 규칙 그룹"을 제공합니다



※AWS 관리 규칙은 기본적으로 HOME_NET 변수가 "해당 Firewall 엔드포인트가 생성된 VPC의 CIDR"로 설정되어 있어, Transit Gateway를 통한 중앙 집중식 트래픽 검사를 하고자 할 경우 이를 재설정해야 함

Network Firewall - 매니지드 룰 그룹

매니지드 룰 그룹은 알림 모드 설정이 일부 가능
(사용자 관리 룰 그룹에서는 "알림 모드" 개념 없음)

"알림 모드"의 ON/OFF로 동작을 제어 가능
→ 테스트 용도(테스트용 모드)로 활용 가능

"알림만(=로그 기록+트래픽은 Pass)"
동작을 수행
(매니지드 룰 그룹에서는 해당 룰 내용을
편집할 수 없기 때문에, 동작 모드로 제공됨)

Network Firewall - AWS 관리 규칙 그룹

도메인 리스트 유형의 AWS 관리 Stateful 규칙 그룹
→ 현재 시점에서는 봇넷과 멀웨어 관련 통신을 차단

1-a. 도메인/IP 유형

#	AWS 관리 규칙 그룹(도메인 리스트)	평가 순서	설명
1	AbusedLegitBotNetCommandAndControlDomainsActionOrder	Action	"봇넷을 호스팅하고 있을 가능성이 있는 도메인" 클래스에 대한 요청을 차단
2	AbusedLegitBotNetCommandAndControlDomainsStrictOrder	Strict	(상동)
3	AbusedLegitMalwareDomainsActionOrder	Action	"봇넷 호스팅으로 알려진 도메인"에 대한 요청을 차단
4	AbusedLegitMalwareDomainsStrictOrder	Strict	(상동)
5	BotNetCommandAndControlDomainsActionOrder	Action	"멀웨어 호스팅으로 알려진 도메인"에 대한 요청을 차단
6	BotNetCommandAndControlDomainsStrictOrder	Strict	(상동)
7	MalwareDomainsActionOrder	Action	"멀웨어를 호스팅할 가능성이 있는 도메인" 클래스에 대한 요청을 차단
8	MalwareDomainsStrictOrder	Strict	(상동)

※ Firewall 정책 설정의 "평가 순서"에 따라 추가할 수 있는 규칙 그룹이 영향을 받기 때문에, 각각 2종류씩 준비되어 있음

Network Firewall - AWS 관리 규칙 그룹

위협 시그니처 유형의 AWS 관리 상태 기반 규칙 그룹

1-b. 위협 시그니처 유형

#	카테고리	AWS 관리 규칙 그룹(위협 시그니처)	평가 순서	설명
1	Botnet	ThreatSignaturesBotnetActionOrder	Action	몇 가지 알려진 리소스에서 생성된 봇 제어와의 통신 감지
2		ThreatSignaturesBotnetStrictOrder	Strict	(상동)
3	Botnet Web	ThreatSignaturesBotnetWebActionOrder	Action	HTTPS 봇넷과의 통신 감지
4		ThreatSignaturesBotnetWebStrictOrder	Strict	(상동)
5	Botnet Windows	ThreatSignaturesBotnetWindowsActionOrder	Action	Windows 봇넷 통신 감지
6		ThreatSignaturesBotnetWindowsStrictOrder	Strict	(상동)
7	DoS	ThreatSignaturesDoSActionOrder	Action	서비스 거부 공격(DoS)의 위협 감지
8		ThreatSignaturesDoSStrictOrder	Strict	(상동)
9	Emerging Threats	ThreatSignaturesEmergingEventsActionOrder	Action	최근 보안 이벤트 기반 위협 감지
10		ThreatSignaturesEmergingEventsStrictOrder	Strict	(상동)

※ Firewall 정책 설정의 '평가 순서'에 따라 추가할 수 있는 규칙 그룹이 영향을 받기 때문에, 각각 2종류씩 준비되어 있음

Network Firewall - AWS 관리 규칙 그룹

위협 시그니처 유형의 AWS 관리 Stateful 규칙 그룹

1-b. 위협 시그니처 유형

#	카테고리	AWS 관리 규칙 그룹(위협 시그니처)	평가 순서	설명
11	Exploits	ThreatSignaturesExploitsActionOrder	Action	ActiveX, FTP, ICMP, NetBIOS, RPC, ShellCode, SNMP, SQL, Telnet, TFTP, VoIP 등의 취약점으로 인한 위협 탐지
12		ThreatSignaturesExploitsStrictOrder	Strict	(상동)
13	Fair Use Policy	ThreatSignaturesFUPActionOrder	Action	공정 사용 정책에 대한 위협 탐지 (예: 유명 게임에 대한 공격, P2P, ...)
14		ThreatSignaturesFUPStrictOrder	Strict	(상동)
15	Compromised	ThreatSignaturesIOCActionOrder	Action	익스플로잇 킷에 의한 위협 탐지
16		ThreatSignaturesIOCStrictOrder	Strict	(상동)
17	Malware	ThreatSignaturesMalwareActionOrder	Action	멀웨어 행위에 관한 위협 탐지
18		ThreatSignaturesMalwareStrictOrder	Strict	(상동)
19	Malware Web	ThreatSignaturesMalwareWebActionOrder	Action	멀웨어의 HTTP 및 SSL 등 웹 관련 위협 탐지
20		ThreatSignaturesMalwareWebStrictOrder	Strict	(상동)

Network Firewall - AWS 관리 규칙 그룹

위협 시그니처 유형의 AWS 관리 Stateful 규칙 그룹

1-b. 위협 시그니처 유형

#	카테고리	AWS 관리 규칙 그룹(위협 시그니처)	평가 순서	설명
21	Scanner	ThreatSignaturesScannersActionOrder	Action	Scanner 도구로부터의 접근으로 인한 위협 탐지
22		ThreatSignaturesScannersStrictOrder	Strict	(상동)
23	Suspect	ThreatSignaturesSuspectActionOrder	Action	JA3 해시를 사용한 의심스러운 SSL 인증서를 이용한 위협 탐지
24		ThreatSignaturesSuspectStrictOrder	Strict	(상동)
25	Attacks	ThreatSignaturesWebAttacksActionOrder	Action	웹 클라이언트/서버/앱의 취약점과 관련된 위협 탐지
26		ThreatSignaturesWebAttacksStrictOrder	Strict	(상동)

Network Firewall - AWS 관리 규칙 그룹

위협 시그니처 유형의 AWS 관리 Stateful 규칙 그룹

1-b. 위협 시그니처 유형

#	카테고리	AWS 관리 규칙 그룹(위협 시그니처)	평가 순서	설명
27	Coin Mining	ThreatSignaturesMalwareCoinminingActionOrder	Action	코인 마이닝 도구 멀웨어 감지
28		ThreatSignaturesMalwareCoinminingStrictOrder	Strict	(상동)
29	Mobile OS	ThreatSignaturesMalwareMobileActionOrder	Action	모바일 OS 멀웨어 위협 감지
30		ThreatSignaturesMalwareMobileStrictOrder	Strict	(상동)
31	Phishing	ThreatSignaturesPhishingActionOrder	Action	인증 정보 피싱 위협 감지
32		ThreatSignaturesPhishingStrictOrder	Strict	(상동)

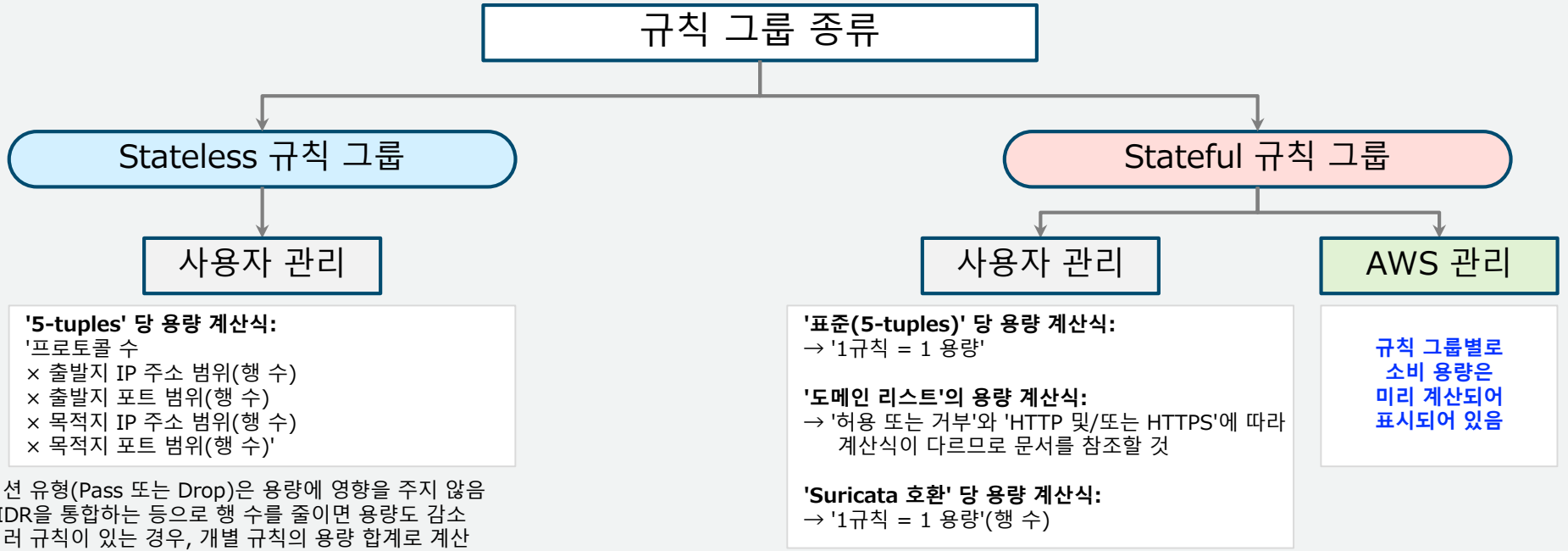
Network Firewall - 3rd Party 룰 그룹

3rd Party가 제공하는 룰 그룹
(내용은 3rd Party가 관리하며, 기본적으로 AWS Marketplace에서 구매)

#	3rd Party	관리형 룰 그룹(AWS Marketplace)	설명
1	Fortinet	Managed IPS Rules for AWS Network Firewall	Enterprise Subscription (링크)

Network Firewall - 규칙 그룹의 용량

Firewall은 정의된 규칙 내용에 기반하여 '용량'을 소비함
→ 규칙 그룹별로 내부 규칙 정의에서 사용 가능한 최대 용량을 선언



※액션 유형(Pass 또는 Drop)은 용량에 영향을 주지 않음
※CIDR을 통합하는 등으로 행 수를 줄이면 용량도 감소
※여러 규칙이 있는 경우, 개별 규칙의 용량 합계로 계산

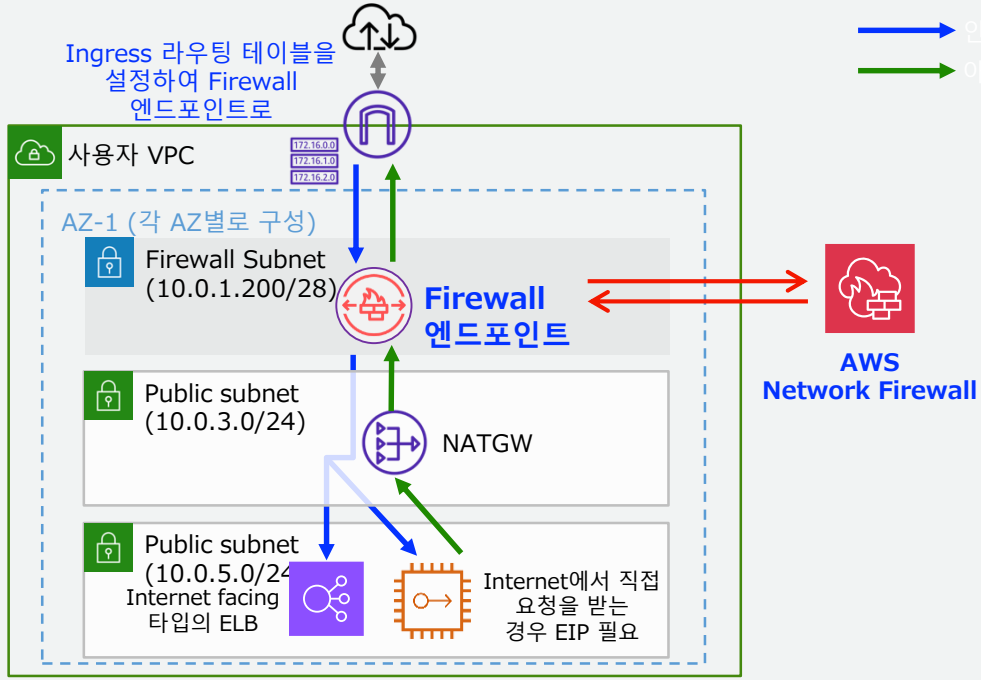
※규칙 그룹 내에 여러 규칙이 있는 경우, 개별 규칙의 용량 합계로 계산
※Stateless/Stateful 규칙 그룹 각각에 대해 '계정 & 리전' 별로 하드 리미트가 존재함

AWS Network Firewall
- 구성 이미지

Network Firewall - 구성 이미지

개별 VPC의 엣지 서비스로서, 또는 South-North나 East-West 트래픽 검사에 사용 가능

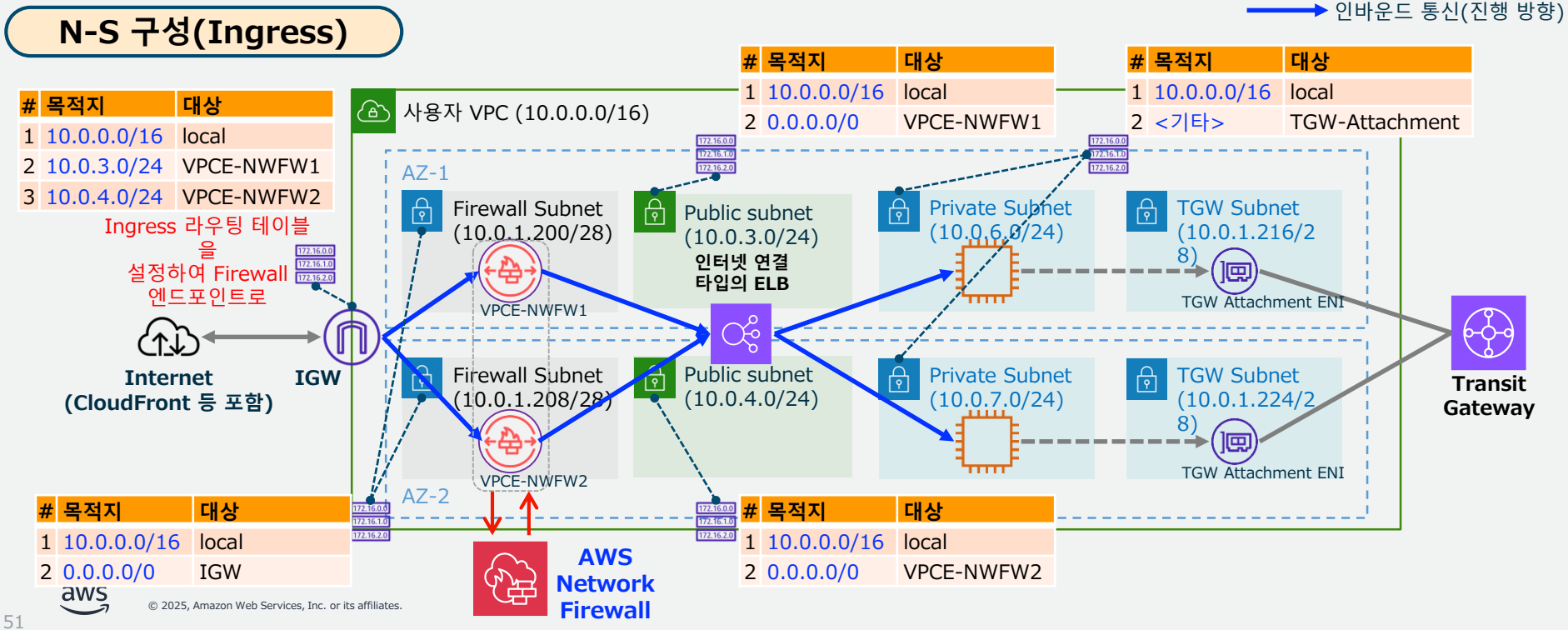
N-S 구성



※Network Firewall(인스턴스)을 여러 VPC에서 직접 공유하는 것은 불가능(→ 검사용 VPC를 두어 공통적으로 라우팅하는 방식으로 대응 가능)
※NAT Gateway의 Public 서브넷과 Private 서브넷 사이에 별도의 Network Firewall을 배치하는 구성도 가능

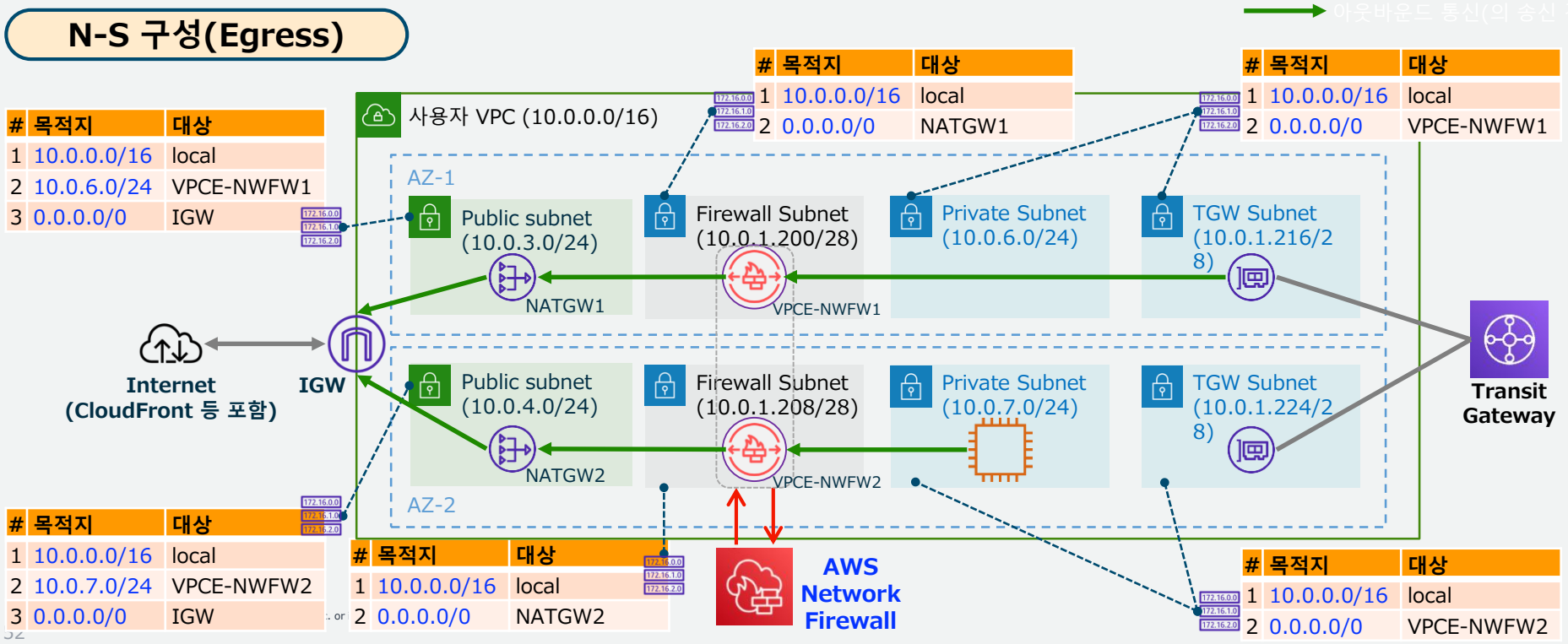
Network Firewall - 구성 예시 (1)

남북 트래픽 검사 (Inbound)



Network Firewall - 구성 예시 (2a)

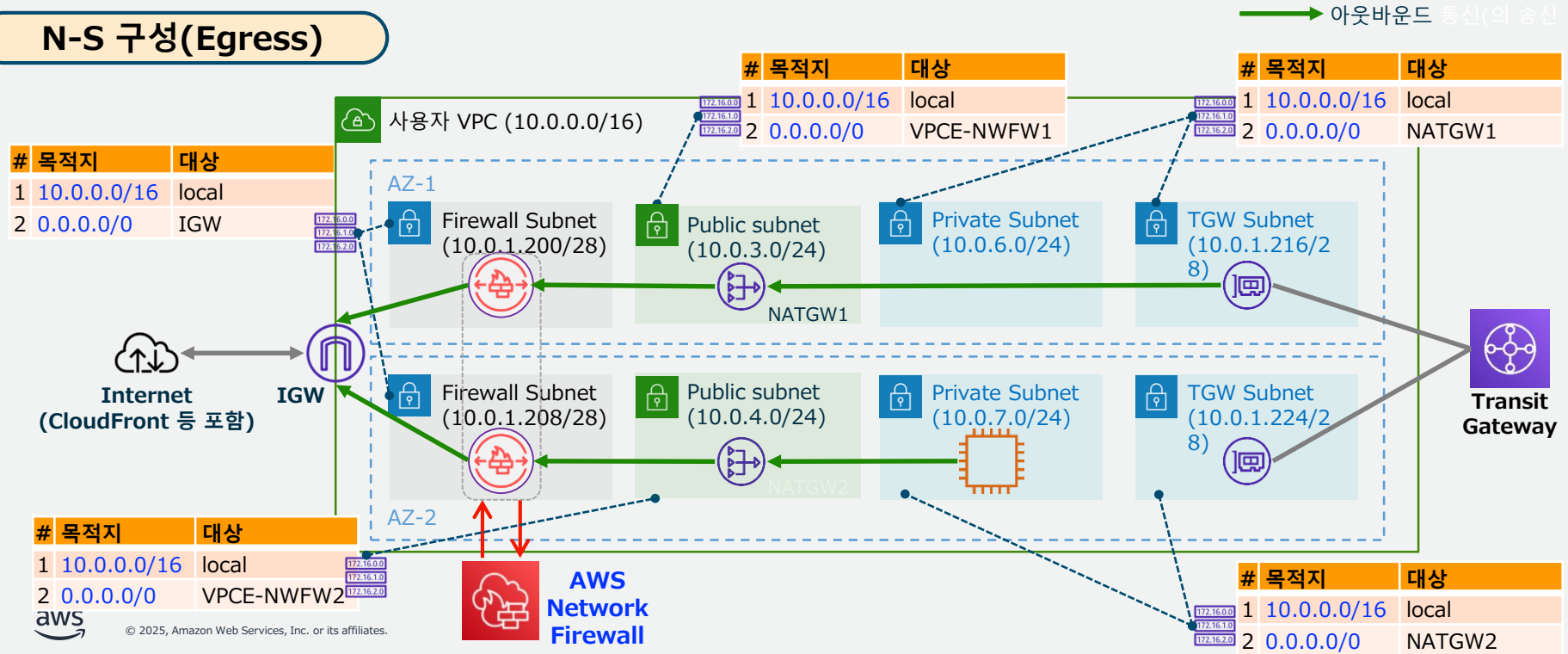
남북 트래픽 검사 (아웃바운드)
(NAT Gateway에 의한 NAT "이전"에 Network Firewall을 배치하는 구성 예시)



Network Firewall - 구성 예시 (2b)

남북 트래픽 검사 (아웃바운드)
(NAT Gateway에 의한 NAT '이후'에 Network Firewall을 배치하는 구성 예시)

N-S 구성(Egress)



#	목적지	대상
1	10.0.0.0/16	local
2	0.0.0.0/0	IGW

#	목적지	대상
1	10.0.0.0/16	local
2	0.0.0.0/0	VPCE-NWFW1

#	목적지	대상
1	10.0.0.0/16	local
2	0.0.0.0/0	NATGW1

#	목적지	대상
1	10.0.0.0/16	local
2	0.0.0.0/0	VPCE-NWFW2

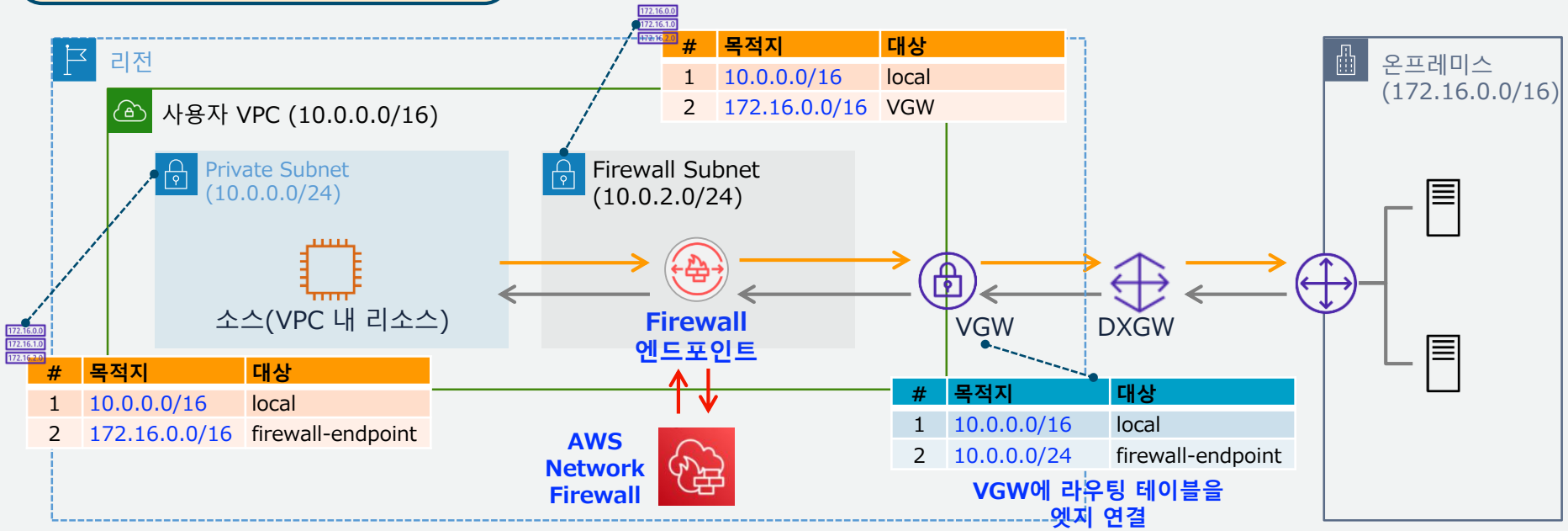
#	목적지	대상
1	10.0.0.0/16	local
2	0.0.0.0/0	NATGW2

※이 구성의 경우, NAT 이후 트래픽이므로 Firewall에서 보는 트래픽 송신원은 NAT Gateway의 IP 주소로 집약됨

Network Firewall - 구성 예시 (3)

개별 VPC와 온프레미스 간의 보안 서비스로 활용 가능
(아래 그림은 Transit Gateway를 사용하지 않고, VGW로 개별 VPC와 연결하는 구성 예시)

VPC ⇔ Direct Connect 구성



#	목적지	대상
1	10.0.0.0/16	local
2	172.16.0.0/16	VGW

#	목적지	대상
1	10.0.0.0/16	local
2	172.16.0.0/16	firewall-endpoint

#	목적지	대상
1	10.0.0.0/16	local
2	10.0.0.0/24	firewall-endpoint

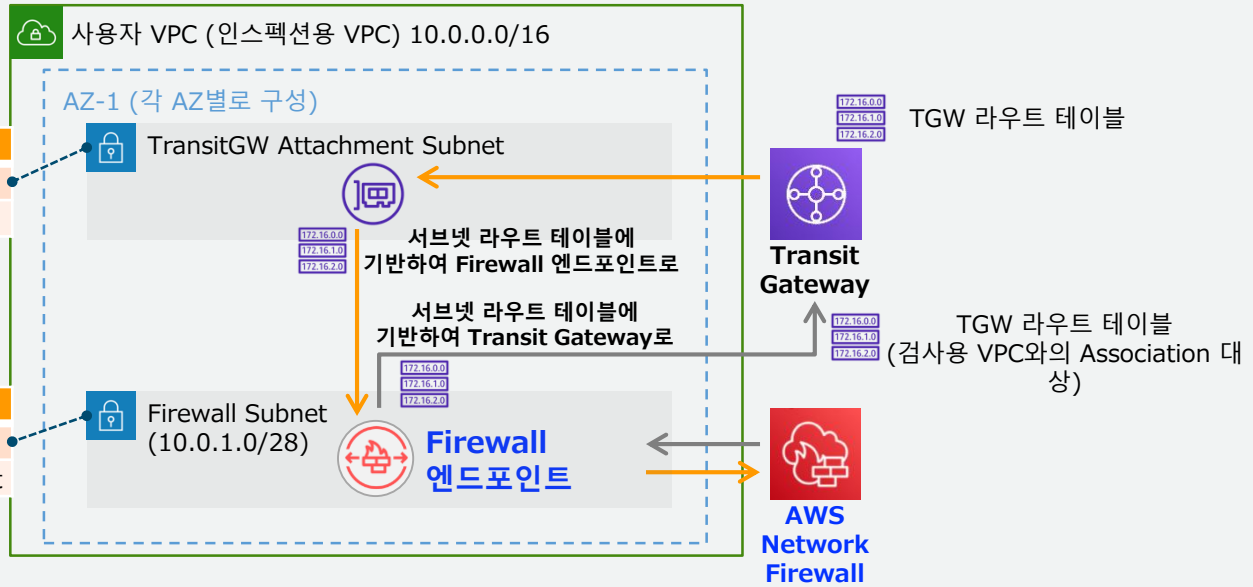
Network Firewall - 구성 예시 (4)

개별 VPC의 엣지 서비스로서, 또는 North-South나 East-West 보안 서비스로 활용 가능

E-W 구성 (=Transit Gateway 이용)

#	목적지	타겟
1	10.0.0.0/16	local
2	0.0.0.0/0	firewall-endpoint

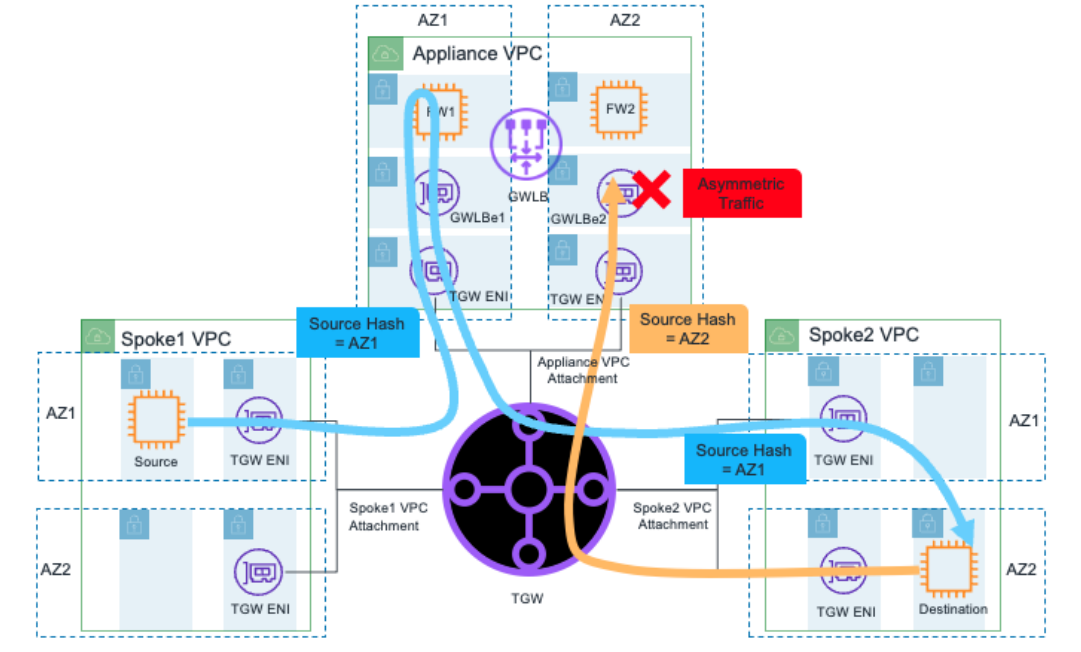
#	목적지	타겟
1	10.0.0.0/16	local
2	0.0.0.0/0	TGW-Attachment



※AWS 관리형 매니지드 룰 그룹을 이용할 경우, Firewall 정책에서 HOME_NET 변수의 덮어쓰기 설정이 필요
(기본값은 Firewall 엔드포인트가 생성된 VPC의 CIDR로부터의 트래픽으로 고정됨)
→ Transit Gateway 경유 트래픽을 집중 검사하려면 HOME_NET 변수의 적절한 설정이 필요

보충: Network Firewall - 주의 사항

TGW Attachment의 어플라이언스 모드 지정 필요



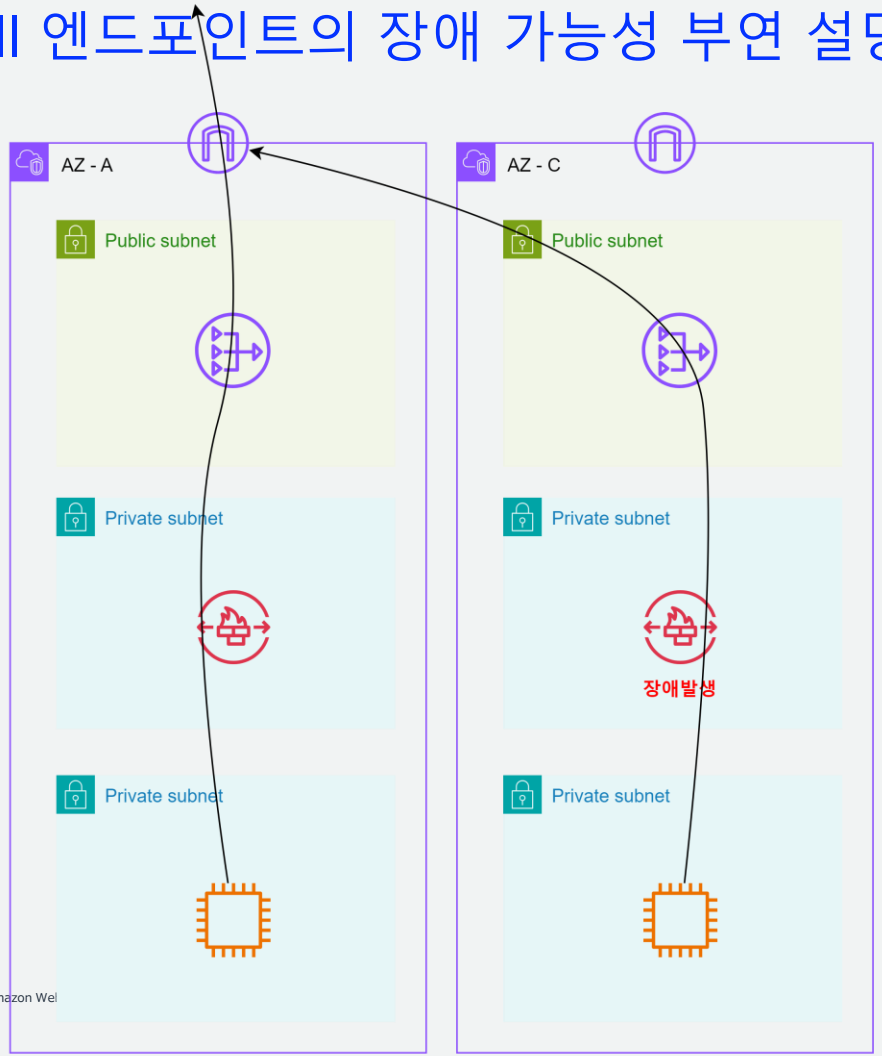
https://aws.amazon.com/ko/blogs/networking-and-content-delivery/best-practices-for-deploying-gateway-load-balancer/

Network Firewall - 이용 시 참고사항 (1/2)

Network Firewall 이용 시에는 주로 다음과 같은 고려사항에 주의가 필요
→ 반드시 사전에 요건과의 정합성을 확인할 것

#	주요 사양・고려사항	설명
1	Firewall 정책 전환 시 동작	• 새로운 Firewall 정책을 생성하고 다른 정책으로 연결을 전환하는 경우, 트래픽 단절이 발생함
2	Firewall 엔드포인트의 장애 가능성	• Firewall 엔드포인트는 AZ 단위로 생성되는 GWLB 타입 VPC 엔드포인트이며, VPC 엔드포인트 및 그 내부 컴포넌트는 AWS에 의해 이중화되어 있습니다. 하지만, Network Firewall 자체에 장애가 발생하지 않는다는 것을 의미하지는 않습니다 • **[Firewall 엔드포인트 내부 컴포넌트의 장애/문제 발생 시]:** • **내부 인스턴스 교체로 인해 후속 TCP 트래픽이 다른 인스턴스로 전환됩니다. 이때 스트림 예외라고 불리는 현상이 발생하며, 해당 트래픽은 "스트림 예외 정책"의 설정에 따라 처리됩니다** • **[Firewall 엔드포인트를 포함한 Network Firewall 서비스의 장애/문제 발생 시]:** • **서브넷의 라우트 테이블에 의해 각각의 Firewall 엔드포인트가 라우팅 대상으로 구성되어 있기 때문에, 하나의 AZ의 Firewall 엔드포인트가 일시적으로 정상적으로 이용할 수 없는 상태가 된 경우에는, 멀티 AZ 구성을 하고 있더라도 AWS가 자동으로 서브넷 측의 라우트 테이블 내용을 변경하는 전환은 수행할 수 없습니다(수행하지 않습니다) → 이러한 상황에서 문제를 사용자 판단으로 회피하기 위해서는, 사용자가 명시적으로 VPC 서브넷의 라우트 테이블을 변경하여 "이용 가능한 다른 AZ의 Firewall 엔드포인트"를 라우팅 대상으로 변경해야 합니다**

Firewall 엔드포인트의 장애 가능성 부연 설명



dest	target
10.1.0.0/16	local
0.0.0.0/0	IGW

dest	target
10.1.0.0/16	local
0.0.0.0/0	NAT-A

dest	target
10.1.0.0/16	local
0.0.0.0/0	vpce-A

dest	target
10.1.0.0/16	local
0.0.0.0/0	IGW

dest	target
10.1.0.0/16	local
0.0.0.0/0	NAT-C

dest	target
10.1.0.0/16	local
0.0.0.0/0	vpce-C

- Firewall 엔드포인트는 각 AZ마다 생성됨
- GWLB(Gateway Load Balancer) 타입의 VPC 엔드포인트임
- AWS가 자체적으로 이중화 구성을 제공
- 장애 발생 시 주의사항
- AWS의 이중화에도 불구하고 Network Firewall 자체 장애 가능성 존재
- **한 AZ의 Firewall 엔드포인트에 문제 발생 시 AWS는 자동 전환을 하지 않음**

[장애 대응 방법]

- **사용자가 직접 라우트 테이블을 수정해야 함**
- **문제가 있는 엔드포인트에서 정상 작동하는 다른 AZ의 엔드포인트로 수동 전환 필요**

Network Firewall - 이용 시 팁 (2/2)

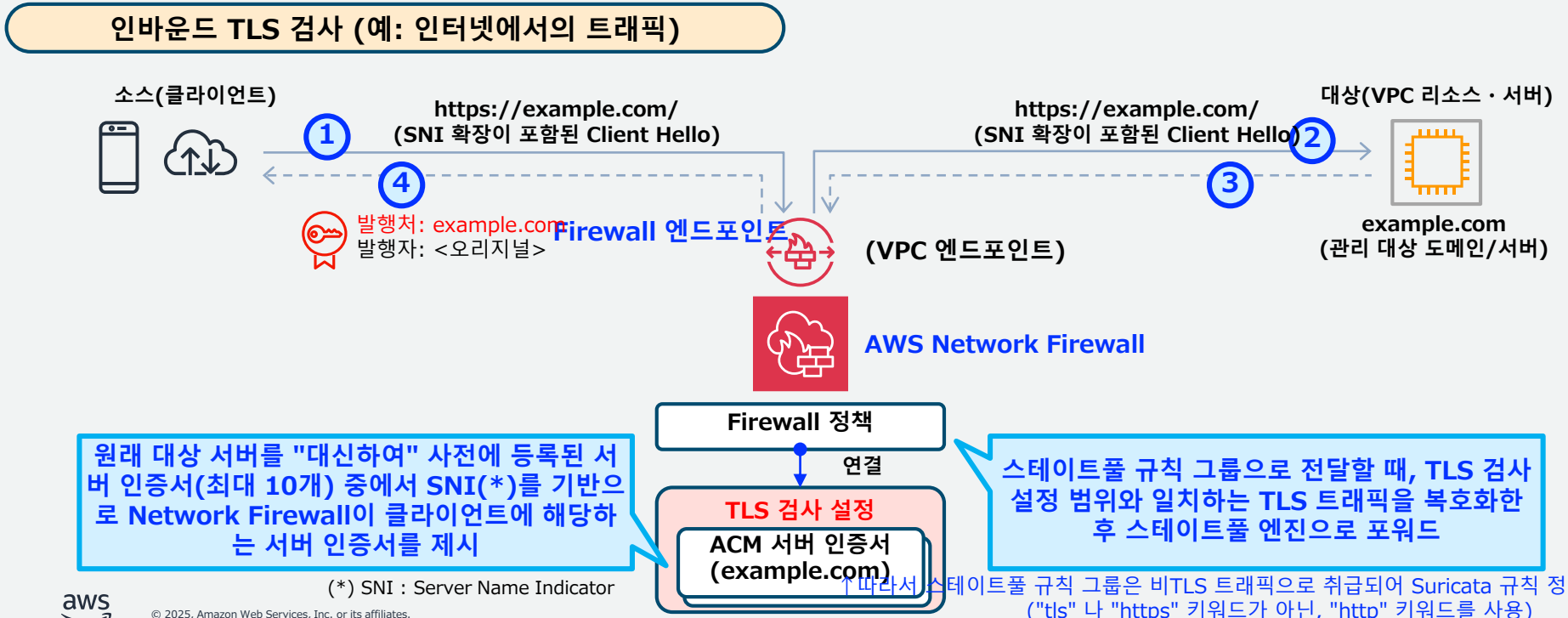
Network Firewall 이용 시 주로 다음과 같은 고려사항에 주의가 필요
→ 반드시 사전에 요건과의 정합성을 확인할 것

#	주요 사양・고려사항	설명
3	AWS 관리 정책의 적용 가능 범위	• AWS 관리 정책의 대부분은 규칙 적용 대상의 소스 IP 범위로 "HOME_NET 변수"를 참조하는 사양입니다. • 해당 변수는 Firewall 정책 레벨에서만 설정 가능하므로, 단일 Firewall 내에서 규칙별로 그 내용을 조정할 수 없습니다 • 이러한 경우에는 다음 중 하나의 대응이 필요: 1. AWS 관리 정책(실제로는 Suricata 호환 규칙)을 복사하여, 내용을 요건에 맞게 커스터마이즈하여 사용자 관리 규칙으로 생성・이용 2. Firewall 인스턴스 및 참조하는 Firewall 정책을 별도로 배포하고, 트래픽의 소스와 목적지에 따라 적절한 Firewall 인스턴스가 이용되도록 라우팅을 구성
4	AWS 관리 규칙의 내용 변경	• AWS 관리 정책은 새로운 위협에 대응하기 위해 사전 통지 없이 변경됨 • (AWS WAF의 관리 규칙과 같은 "버전 개념"이나 "명시적 버전 지정 기능"은 제공되지 않음) • → 위협 시그니처 유형은 내용이 항상 공개 제공되므로, 복사 이용・반영하여 셀프 관리형으로 운영함으로써 업데이트 타이밍을 자체 관리 가능
5	Transit Gateway와의 조합 이용 시 어플라이언스 모드의 적절한 이용	• 검사용 VPC 내에 멀티 AZ 구성으로 Firewall 엔드포인트를 배치할 때는 Transit Gateway 측의 어플라이언스 모드를 활성화해야 함

AWS Network Firewall - TLS 검사

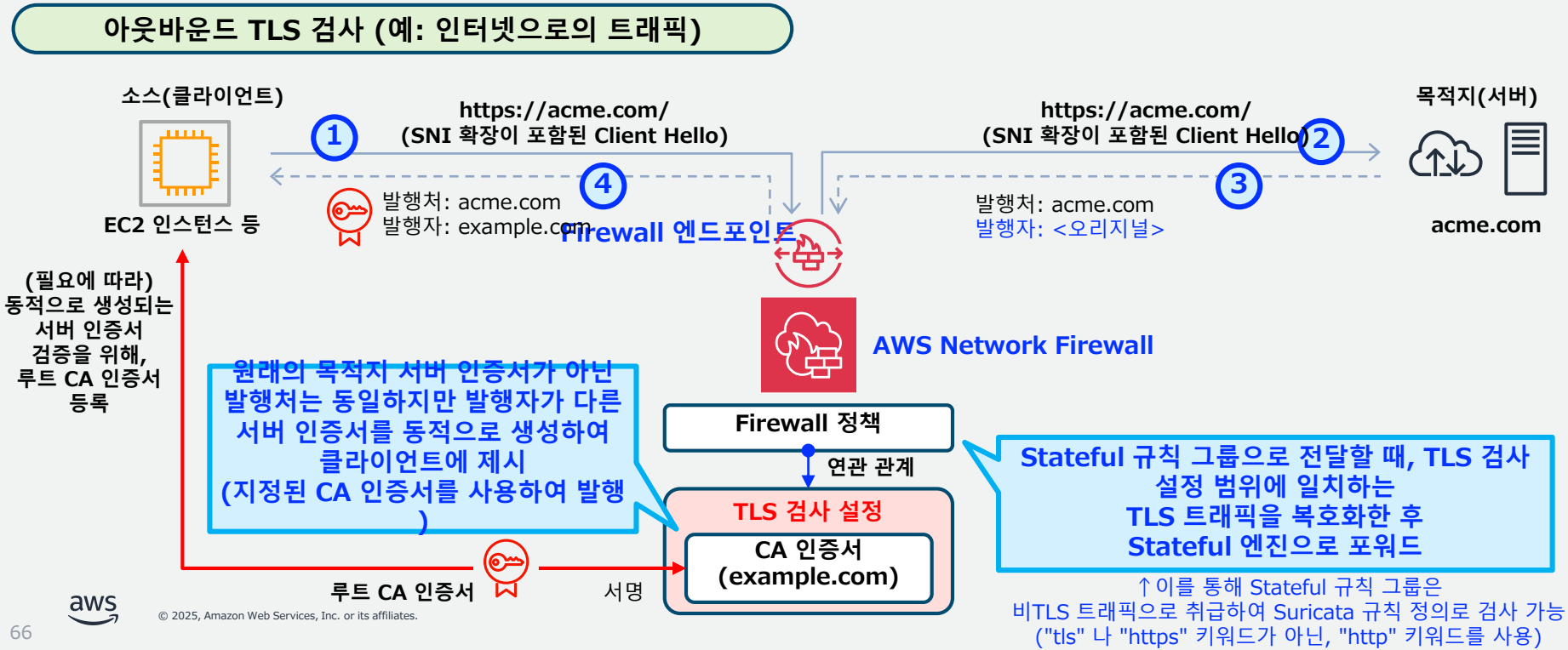
Network Firewall - TLS 검사

인바운드(Ingress)와 아웃바운드(Egress) 양방향 TLS 검사 지원
→ Network Firewall이 개입하여 TLS 세션을 복호화하고 검사 후 재암호화



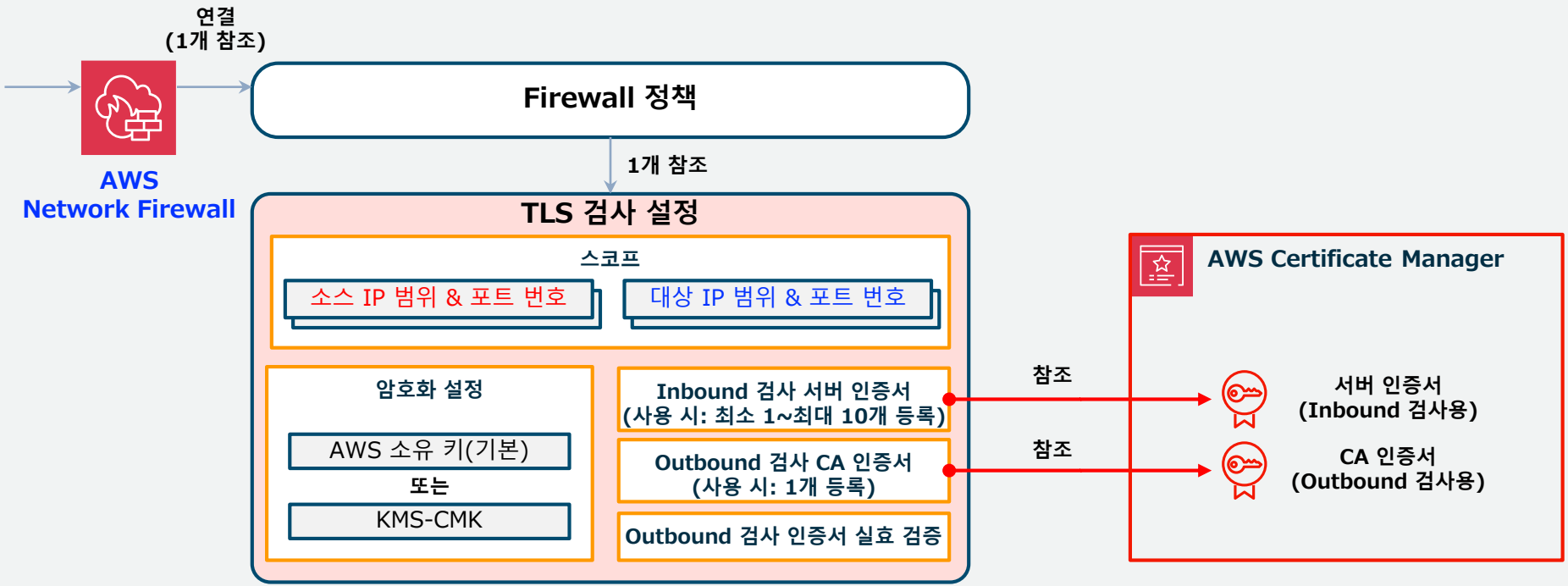
Network Firewall - TLS 검사

인바운드(Ingress)와 아웃바운드(Egress) 양방향 TLS 검사 지원
→ Network Firewall이 개입하여 TLS 세션을 복호화하고 검사 후 재암호화



Network Firewall - TLS 검사 설정

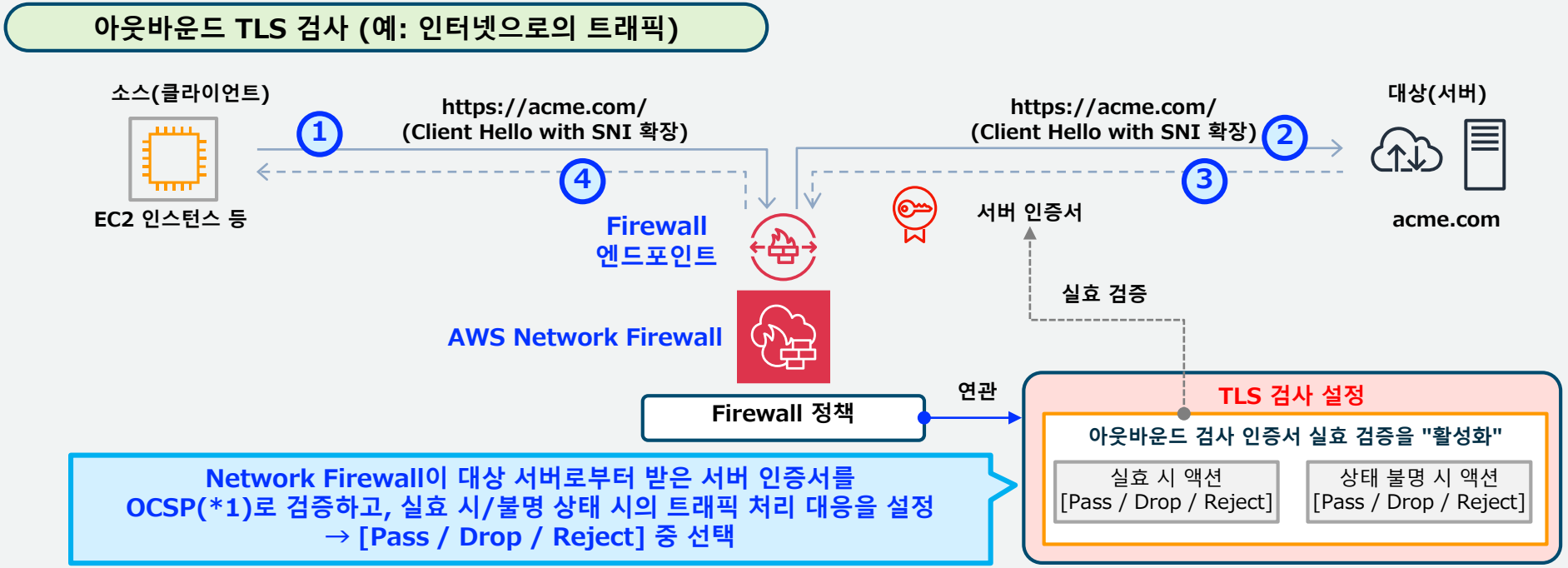
TLS 검사 설정에서는 스코프로서 소스와 대상의 IP 주소 & 포트를 정의
→ 스테이트풀 룰 엔진에서 비 TLS 트래픽으로서 검사 가능



※TLS 검사가 가능한 트래픽은 Client Hello에서 SNI extension에 대응한 클라이언트 요청만
(SNI extension에 비대응 트래픽은 RST 응답)

Network Firewall - TLS 검사 설정 인증서 실효 검증

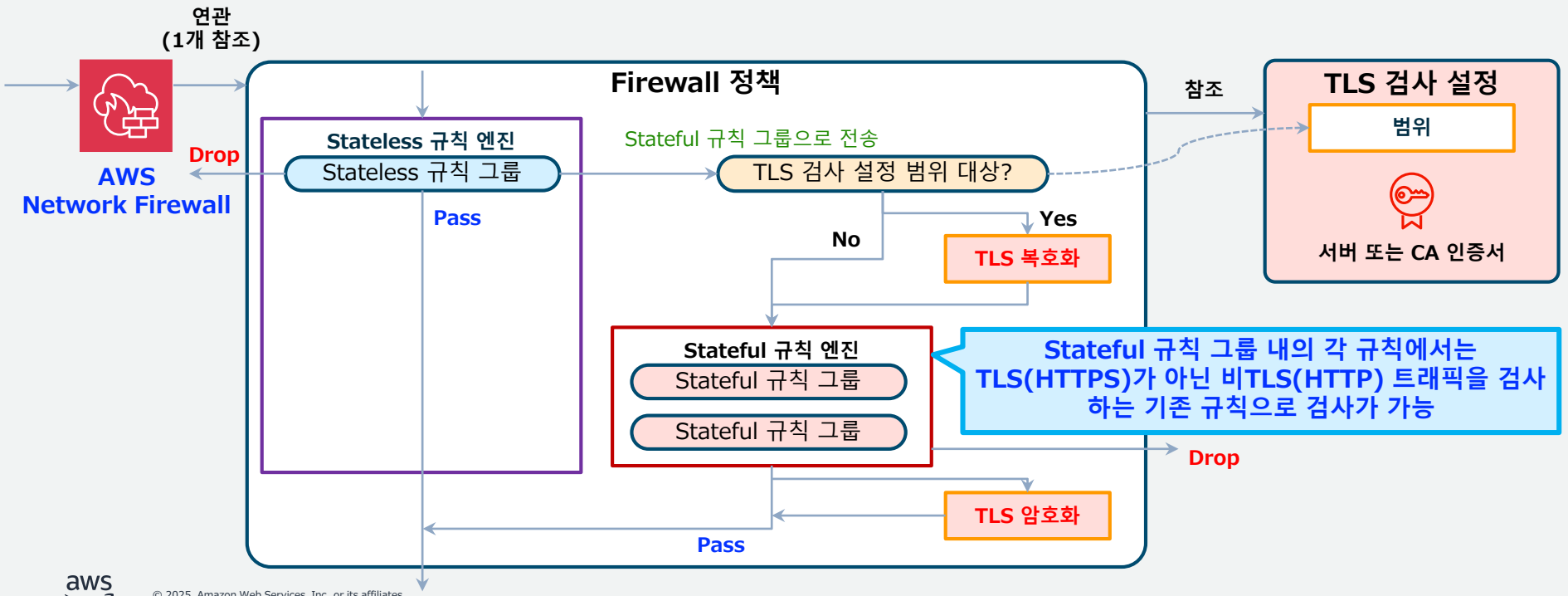
아웃바운드 TLS 검사에서 대상 서버의 인증서 실효 여부를 검증
→ OCSP를 통한 실효 판정과 실효 상태에서의 트래픽 처리를 결정 가능



(*1) OCSP: Online Certificate Status Protocol

Network Firewall - 규칙 엔진과의 관계

Stateless 규칙 그룹에서 Stateful 규칙 그룹으로 전송할 때,
TLS 검사 설정 범위에 일치하는 TLS 트래픽을 자동으로 복호화



Network Firewall - TLS 검사 이용 시 힌트 (1/2)

TLS 검사 이용 시 주로 다음 고려사항에 주의가 필요
→ 사전에 요건과의 정합성 확인

https://docs.aws.amazon.com/network-firewall/latest/developerguide/tls-inspection-configurations.html

#	주요 사양・고려사항	설명
1	지원하는 TLS 버전	• TLS 1.1/1.2/1.3 (※TLS1.0은 미지원)
2	지연시간에 대한 영향	• 왕복으로 2회의 TLS 복호화・암호화가 이루어지므로 필연적으로 지연시간 증가

3	비암호화 SNI extension이 전제	• Client Hello에서 SNI extension에 대응하지 않는 트래픽은 지원되지 않음 (TLS 세션은 강제로 종료됨)
		  • 예: ALB의 TLS 리스너에서 TLS 종단 후, 타겟 그룹에 HTTPS 프로토콜을 지정하여 ALB가 TLS 클라이언트가 되는 경우가 해당
		  • ※스테이트리스 룰 그룹의 룰 정의에서, 스테이트풀 룰 엔진으로 전송하지 않고(=TLS 검사하지 않고), pass시키는 것은 가능
		• 확장판 TLS1.3에 의한 '암호화 SNI'는 지원되지 않음

4	추가 서비스 요금 발생	• 'Advanced 검사' 요금이 추가로 발생(※'서비스 요금' 참조)
5	TLS 암호화 알고리즘	• 클라이언트는 Network Firewall이 지원하는 알고리즘에 대응 필요
6	StartTLS에 의존한 TLS 프로토콜 미지원	
7	HTTP2 또는 WebSocket의 TLS 검사 미지원	
8	TCP 기반 TLS가 전제	• UDP 기반(QUIC) 또는 도중에 UDP로 전환하는 TLS 세션은 미지원
9	크로스 서명(Cross-signed) 루트 인증서 미지원	• 예: Let's Encrypt가 발행하는 서버 인증서가 해당

※크로스 서명: 크로스 루트용 중간 인증서를 설정함으로써 기존 트리와는 별도의 루트 인증서에도 연결 가능하게 하는 구조

Network Firewall - TLS 검사 이용 시 힌트 (2/2)

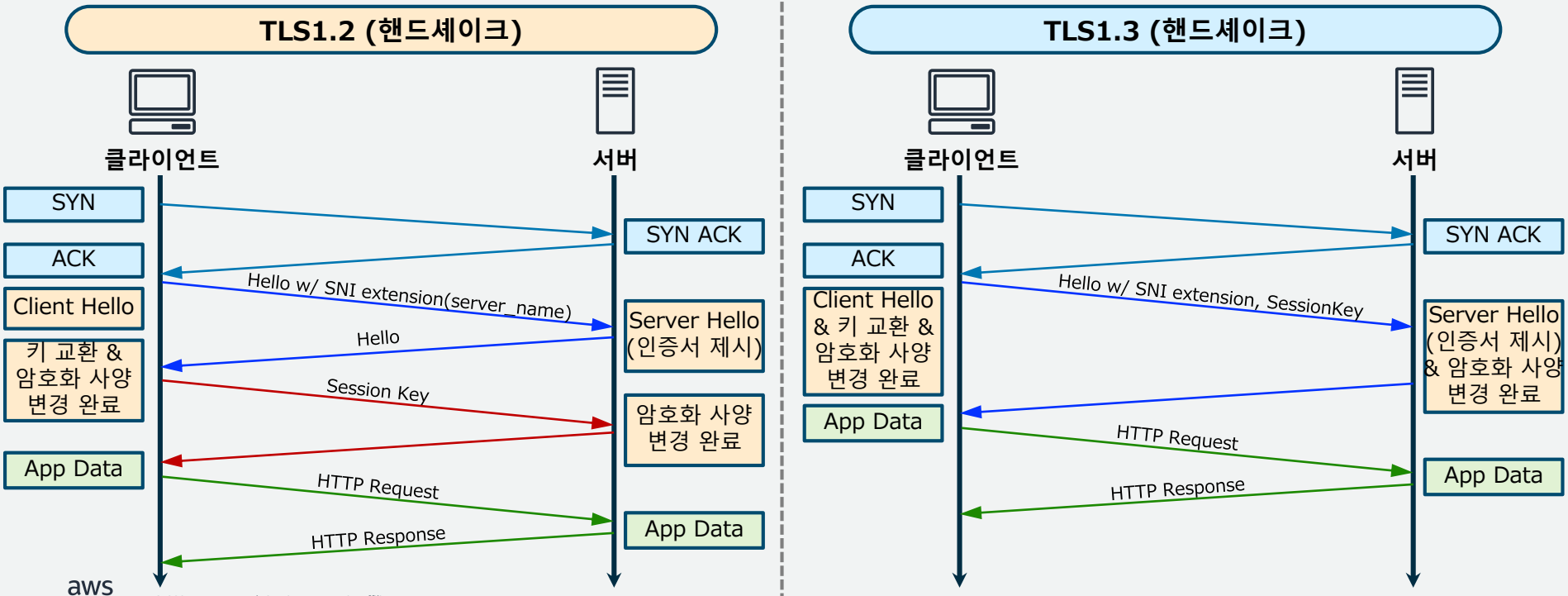
TLS 검사 이용 시에는 주로 다음과 같은 고려사항에 유의가 필요
→ 사전에 요건과의 정합성을 확인

https://docs.aws.amazon.com/network-firewall/latest/developerguide/tls-inspection-configurations.html

#	주요 사양・고려사항	설명
10	Firewall 정책에 TLS 검사 설정 연결	• Firewall 정책 생성 시에만 가능 • ※Firewall 정책 생성 후 TLS 검사 설정의 연결이나 연결 해제는 불가 • → 새로운 Firewall 정책을 생성하여 정책 자체를 전환하여 대응) • ※연결된 Firewall 정책 전환 시에는 트래픽 단절이 발생
11	TLS 검사 설정 업데이트 시의 동작	• 반영 전파 과정에서 불일치 상태가 짧은 시간 동안 발생 • (수 초 정도로 해소될 것으로 예상됨)
12	인바운드 TLS 검사용 서버 인증서 요건	• 자체 서명 인증서를 사용한 서버 인증서는 지원되지 않음
13	아웃바운드 TLS 검사용 CA 인증서 요건	• 루트 CA로는 Mozilla Included CA Certificate List에 표시된 것을 사용해야 하며, 그 중 하나에 의해 서명된 CA 인증서여야 함 • 그렇지 않은 경우, 클라이언트는 해당 루트 CA 인증서를 신뢰 저장소에 추가해야 함 • AWS Private Certificate Authority에서 발행된 인증서는 지원되지 않음
14	인바운드/아웃바운드 검사 선택	• 반드시 둘 다 사용해야 하는 것은 아님 • (선택적 사용 가능 = 둘 다 또는 둘 중 하나)

보충: TLS 검사 - TLS Client Hello

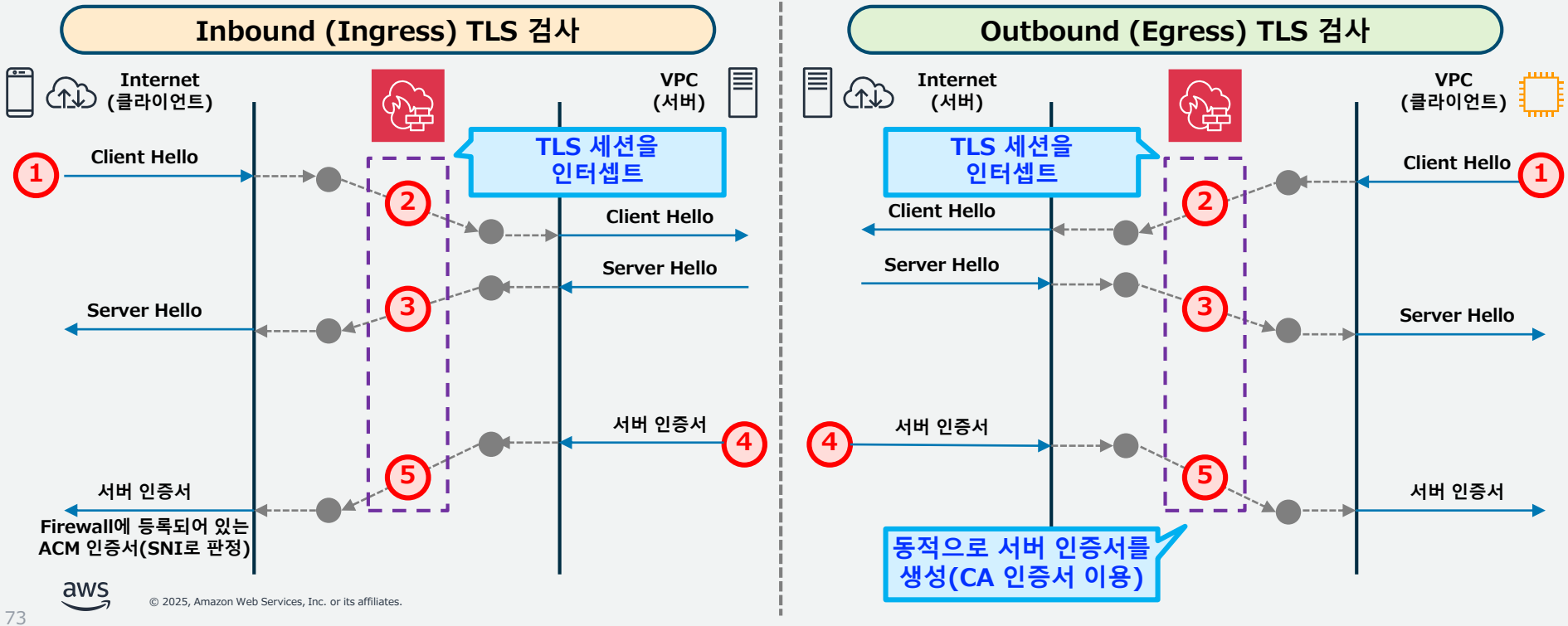
TLS에서는 클라이언트와 서버 간에 암호화 채널을 확립하기 위해 핸드셰이크가 수행됨 (※TLS1.3에서는 핸드셰이크가 고속화됨)



※Network Firewall은 확장 TLS1.3 프로토콜의 '암호화된 Client Hello'를 지원하지 않음

보충: TLS 검사 - 동작 이미지

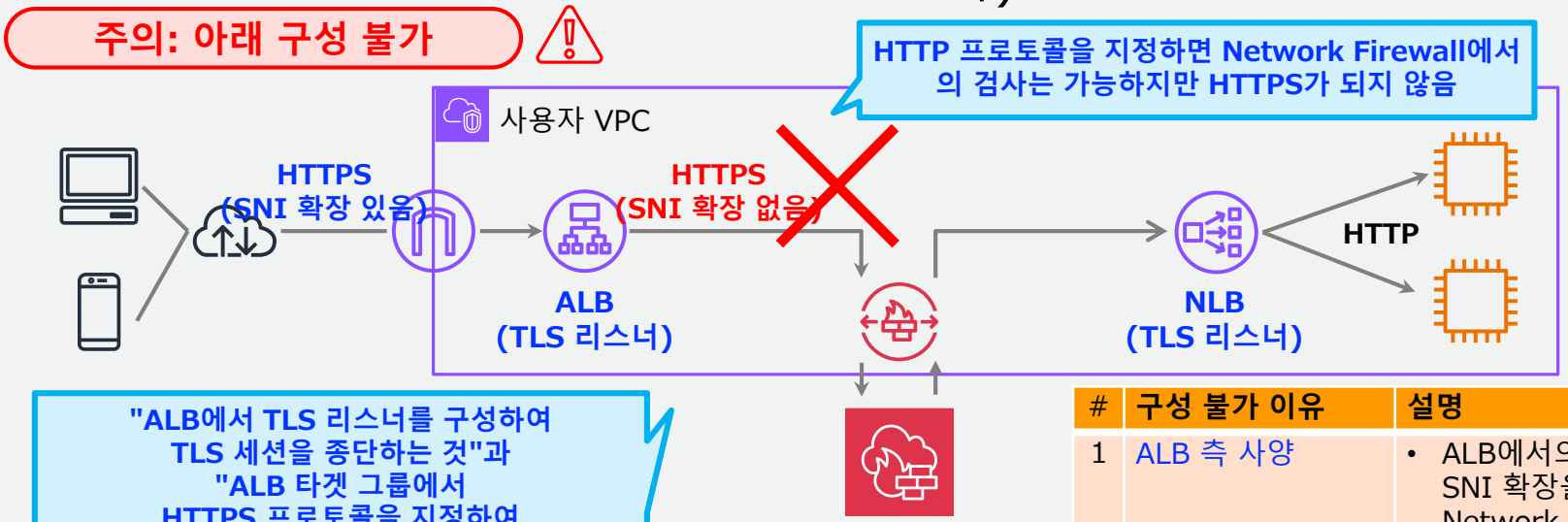
TLS 검사는 클라이언트와 서버 사이에 Network Firewall이 개입하여 각각에 대해 클라이언트/서버로서 세션을 확립함



보충: TLS 검사 - ALB→타겟 간 트래픽

ALB 자체가 HTTPS 클라이언트로서 타겟 그룹과 통신하는 경우,
TLS 검사 불가 (→ 대응: ALB 이전 단계에서 TLS 검사 또는 NLB 후단에서 비 TLS 검사)

주의: 아래 구성 불가



"ALB에서 TLS 리스너를 구성하여
TLS 세션을 종단하는 것"과
"ALB 타겟 그룹에서
HTTPS 프로토콜을 지정하여
다시 ALB가 클라이언트가 되어 HTTPS 통신을
하는 것"은 ALB 기능으로는 가능. 하지만,
그 후단의 HTTPS 통신을 Network Firewall에
서 TLS 검사하는 것은 실현 불가

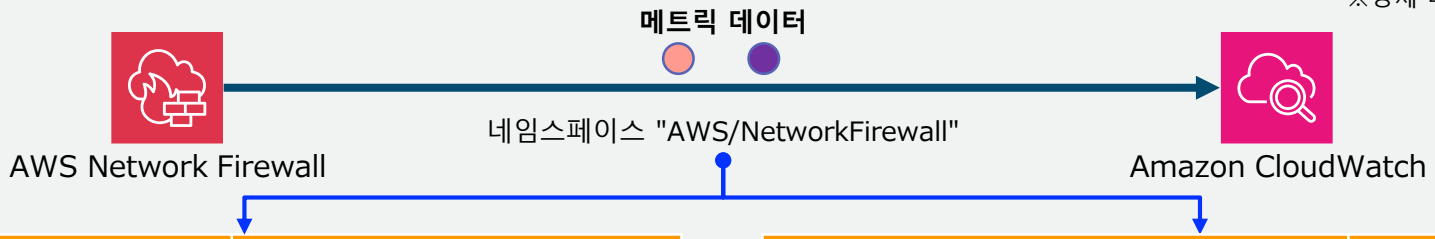
#	구성 불가 이유	설명
1	ALB 측 사양	• ALB에서의 HTTPS 요청은 SNI 확장을 지원하지 않아 Network Firewall 전제 사양을 만족하지 않음
2	Network Firewall 측 사양	• 본래 ALB 발신 요청은 자체 서명 인증서를 허용하지만, Network Firewall은 자체 서명 인증서의 서버는 대상으로 지원하지 않음

AWS Network Firewall - 기타

Network Firewall - 모니터링 (메트릭)

아래 표의 CloudWatch 메트릭을 발행
→ 이를 활용한 모니터링과 CloudWatch 알람을 통한 자동화가 가능

※상세 내용은 문서 참조



메트릭	내용
DroppedPackets	규칙에 의해 Drop된 패킷 수
InvalidDroppedPackets	패킷 측 문제로 Drop된 수
OtherDroppedPackets	위 이외의 이유로 Drop된 수
Packets	검사한 패킷 수
PassedPackets	허용(Pass)된 패킷 수
ReceivedPackets	수신한 패킷 수
RejectedPackets	거부(Reject)된 패킷 수
StreamExceptionPolicyPackets	스트림 예외 정책에 매치된 패킷 수

메트릭	내용
TLSDroppedPackets	TLS 검사에서 Drop된 수
TLSErrors	TLS에서의 에러 수
TLSPassedPackets	TLS 검사에서 Pass된 수
TLSReceivedPackets	TLS 검사에서 수신한 수
TLSRejectedPackets	TLS 검사에서 거부된 수
TLSRevocationStatusOKConnections	TLS 폐기 검사 OK 연결 수
TLSRevocationStatusRevokedConnections	TLS 폐기 검사 NG 연결 수
TLSRevocationStatusUnknownConnections	TLS 폐기 검사 알 수 없음 연결 수

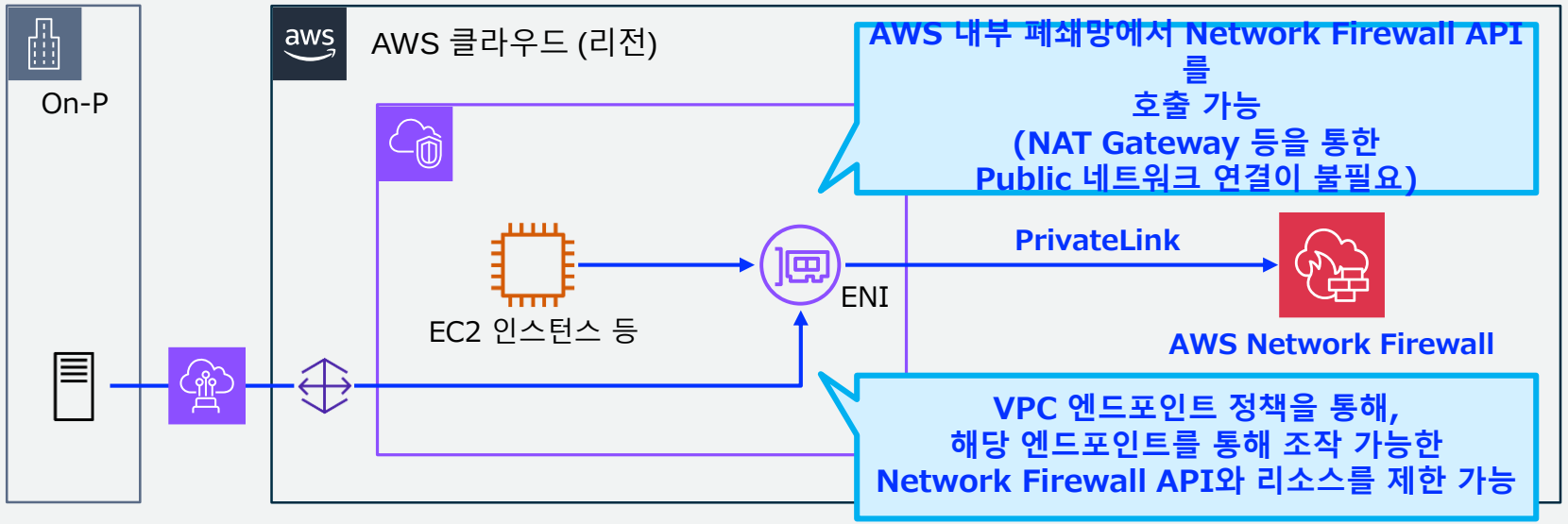
Network Firewall - AWS PrivateLink 지원

Network Firewall이 PrivateLink 지원

→ 사용자 VPC에서 AWS 내부 폐쇄망으로 API(*) 호출 가능

엔드포인트 서비스 이름:
com.amazonaws.<region>.network-firewall

(*) Network Firewall 관리 API 호출이며,
검사 트래픽은 아닙니다



Network Firewall - 할당량 (1/2)

Network Firewall 사용 시 아래 표의 할당량에 유의

https://docs.aws.amazon.com/network-firewall/latest/developerguide/quotas.html

리전 &
계정 레벨 할당량

항목	기본 할당량	상한 완화 가능 ?
Network Firewall 최대 수	5	Yes
Firewall 정책 최대 수	20	Yes
Stateful 규칙 그룹 최대 수	50	Yes
Stateless 규칙 그룹 최대 수	50	Yes
Stateful 규칙 그룹 용량 최대값	30,000 (*1)	Yes
TLS 검사 설정 최대 수	20	Yes
TLS 검사 설정당 CA 인증서 최대 수(Outbound 검사용)	1	Yes
TLS 검사 설정당 서버 인증서 최대 수(Inbound 검사용)	10	Yes

(*1) 최대 50,000까지 완화 신청 가능

Network Firewall - 할당량 (2/2)

Network Firewall 사용 시 아래 표의 할당량에 주의

https://docs.aws.amazon.com/network-firewall/latest/developerguide/quotas.html

리전 &
계정 레벨 할당량

항목	할당량	상한 완화 가능 ?
Suricata 규칙당 최대 문자 수(변수값도 제한에 포함)	8,192	No
규칙 그룹당 Suricata 호환 규칙의 최대 수	2,000,000	No
Suricata 호환 Stateful 규칙 그룹의 IP 세트 최대 수	5	No
Firewall 정책당 Stateful 규칙 그룹의 최대 수	20	No
Firewall 정책당 Stateful 규칙의 최대 수	30,000	No
상태 비저장 규칙 그룹 용량의 최대값	30,000	No
상태 비저장 규칙 그룹당 사용자 지정 작업 최대 수	10	No
Firewall 정책당 상태 비저장 규칙 그룹의 최대 수	20	No
Firewall 정책당 상태 비저장 규칙의 최대 수	30,000	No
Firewall 엔드포인트당 최대 네트워크 대역폭 (각 서브넷에 하나씩 Firewall을 생성하여 분리 가능)	100 Gbps	No
Firewall당 Firewall 정책 수	1	No

※각 Firewall 정책 단위의 할당량이 아닌 점에 특히 주의 (특히 규칙 그룹의 용량)

Network Firewall - 서비스 요금

(*) 도쿄 리전 요금 기재

이하 서비스 요금 구조
(동일 VPC의 NAT GW 시간 요금은 엔드포인트에 대응하여 면제 있음)

AWS Network Firewall 요금

①Firewall 엔드포인트 요금

0.395 USD/시간

+

(Advanced 검사)
1.095 USD/시간

※AZ/서브넷 별로 엔드포인트 생성

+

②Firewall 트래픽 요금

0.0065 USD/GB

+

(Advanced 검사 처리)
0.005 USD/GB

-

(③NAT Gateway 요금)

Network Firewall을 사용하는 VPC에서 NAT GW를 생성하는 경우, 표준 NAT GW 요금(처리 및 시간당 사용 요금)은 1GB당 처리와 Firewall 사용 시간에 대해 1:1로 면제

(※동일 계정 & 리전 기준)

Thank you!