AWSKRUG - AWS한국사용자모임

Public group

AWS Network Firewall

박병화 bhpark@amazon.com

Security Risk and Compliance

AWS Proserve

Lv 200~300

목차 :

1. AWS Network Firewall 뭔가요?
2. GWLB 동작 방식 (aka. 3rd party 보안 솔루션 연결 방법)
3. AWS Network Firewall 정책을 세워볼까요?

© 2022, Amazon Web Services, Inc. or its affiliates.

AWS Network Firewall 뭔가요?

© 2022, Amazon Web Services, Inc. or its affiliates.

고객이 클라우드 네트워크를 보호하는 방법

Homegrown

자체 관리형 오픈 소스 또는 맞춤형 솔루션

복잡하고 관리가 어려움

Third party

클라우드의 가상 방화벽 어플라이언스

비용이 많이 드는 통합 문제

On-premises

온-프레미스 하드웨어 방화벽으로 다시 전달되는 클라우드 트래픽

확장성이 부족하고 비용 증가

Cloud Native

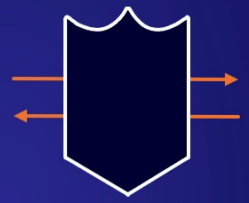
클라우드 제공업체가 제공하는 보안 서비스

클라우드 네이티브 관리 경험, 집중 기능 세트

© 2022, Amazon Web Services, Inc. or its affiliates.

AWS 의 관리형 네트워크 방화벽

AWS Firewall Manager 를 통한 통합 관리



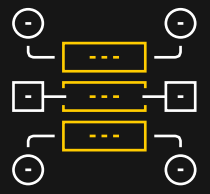
Stateless 정책 + Stateful 정책 동시 적용

Suricata 기반 IDS/IPS 정책

HTTP/HTTPS Domain 필터링

© 2022, Amazon Web Services, Inc. or its affiliates.

AWS Network Firewall



AWS 관리형 인프라의 자동 확장

매우 유연한 대용량 규칙 엔진

중앙 집중식 정책 관리, 실시간 모니터링

사전 확약금이 없으며 **사용한 만큼만 요금 지불**

© 2022, Amazon Web Services, Inc. or its affiliates.

AWS Network Firewall

고객

방화벽 정책 및
규칙 만들기

방화벽 EP로
트래픽 배포
및 라우팅

AWS Firewall
Manger로 중앙
집중식 제어

AWS

트래픽에 따라
자동으로 확장

FW EP당 **100Gbps**
대역폭 처리 성능

리전 선호도 및
세션 대칭 관리

99.99% 의
SLA를 통한 탄력성

© 2022, Amazon Web Services, Inc. or its affiliates.

AWS Network Firewall 세부 기능

패킷 필터링

- Stateless / Stateful 정책

  - 5 Tuples :

    Src/Dst IP | Src/Dst Port | Protocol
- 대규모 IP 차단/허용 목록
- HTTP/HTTPS에서 FQDN 필터링
- 프로토콜 감지, 시행
- 애플리케이션 규칙:

  - IPS/IDS (공통 오픈 소스 규칙 형식)

가시성 및 보고

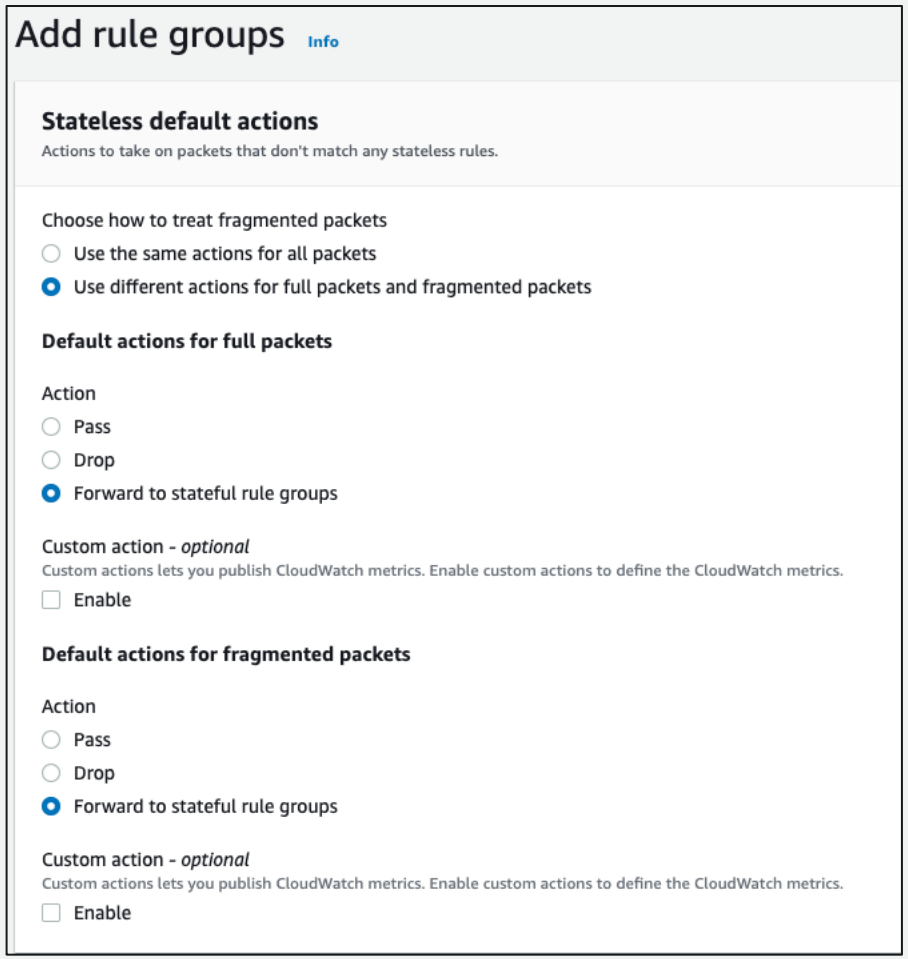
- 클라우드워치 규칙 지표
- 전체 네트워크 흐름 로그
- 이벤트, 규칙 기반 로그
- S3, CloudWatch 로그 또는 Kinesis Firehose 로그 수집

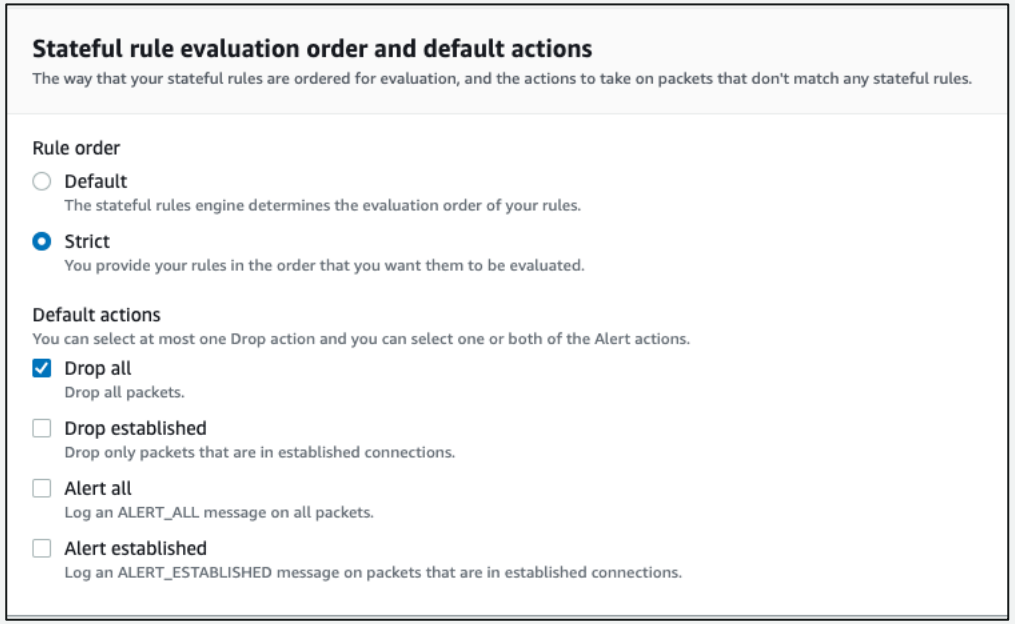
중앙 집중식 관리

- AWS Firewall Manager를 사용한 교차 계정 관리 및 규칙 가시성
- 클라우드포메이션 및 테라폼 템플릿
- AWS 리소스 액세스 관리자(RAM)

aws © 2022, Amazon Web Services, Inc. or its affiliates.

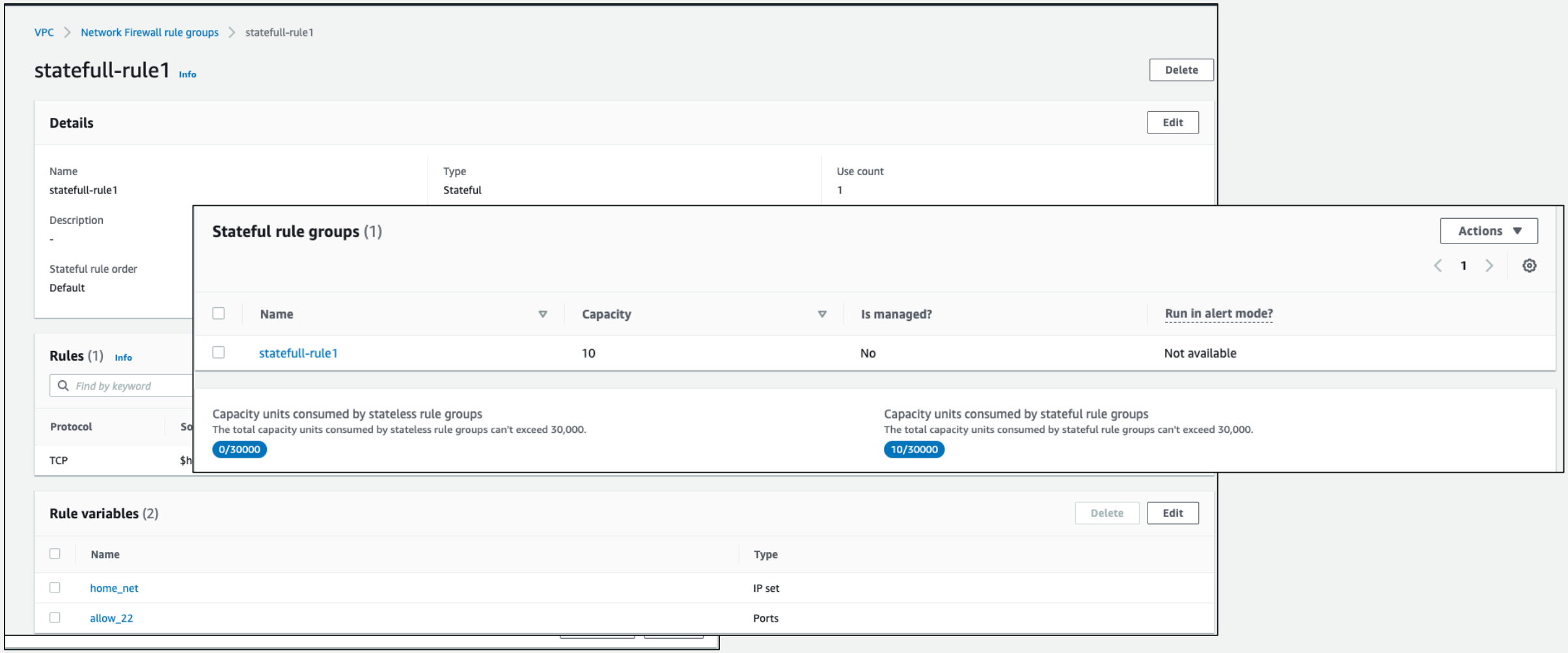
AWS Network Firewall GUI





© 2022, Amazon Web Services, Inc. or its affiliates.

AWS Network Firewall GUI



© 2022, Amazon Web Services, Inc. or its affiliates.

AWS Network Firewall 로그

Timestamp	Message
2021-04-20T12:32:26.000-04:00	{"firewall_name":"ANFW-lab"


```
{
    "firewall_name": "ANFW-lab",
    "availability_zone": "us-east-1a",
    "event_timestamp": "1618936346",
    "event": {
        "timestamp": "2021-04-20T16:32:26.781117+0000",
        "flow_id":
        "event_type": "alert",
        "src_ip": "10.1.3.4",
        "src_port": 43326,
        "dest_ip":
        "dest_port": 80,
        "proto": "TCP",
        "tx_id": 0,
        "alert": {
            "action": "blocked",
            "signature_id": 3,
            "rev": 1,
            "signature": "not matching any HTTP allowlisted FQDNs",
            "category": "",
            "severity": 1
        },
        "http": {
            "hostname": "google.com",
            "url": "/",
            "http_user_agent": "curl/7.61.1",
            "http_method": "GET",
            "protocol": "HTTP/1.1",
            "length": 0
        },
        "app_proto": "http"
    }
}
```


Log events

You can use the filter bar below to search for and match terms, phrases, or values in

View as text | Actions | Create Metric Filter

Timestamp	Message
2021-04-14T15:05:32.000-04:00	{"firewall_name":"anfw-lab


```
{
    "firewall_name": "anfw-lab ",
    "availability_zone": "us-east-1a".
    "event_timestamp":
    "event": {
        "timestamp": "2021-04-14T19:05:32.008127+0000",
        "flow_id"
        "event_type": "netflow",
        "src_ip":
        "src_port"
        "dest_ip":
        "dest_port": 80,
        "proto": "TCP",
        "netflow": {
            "pkts": 4,
            "bytes": 220,
            "start": "2021-04-14T19:04:25.964874+0000",
            "end": "2021-04-14T19:04:31.447200+0000",
            "age": 6,
            "min_ttl": 115,
            "max_ttl": 115
        },
        "tcp": {
            "tcp_flags": "13",
            "syn": true,
            "fin": true,
            "ack": true
        }
    }
}
```

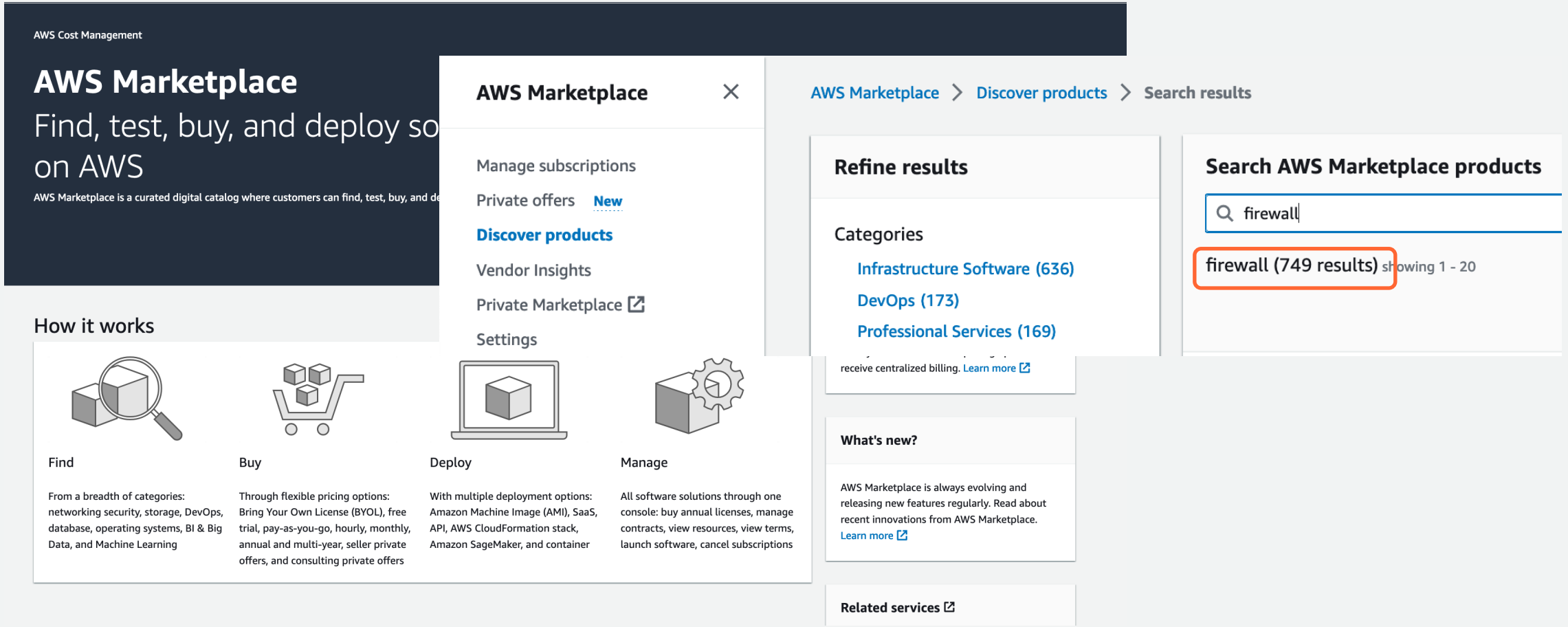
AWS Network Firewall Quotas

Resource	Default quota per account per Region
Maximum number of firewalls.	5
Maximum number of firewall policies.	20
Maximum number of stateful rule groups.	50
Maximum number of stateless rule groups.	50

•A rule with a protocol that specifies 30 different protocols, a source with 3 settings, a destination with 5 settings, and single or no specifications for the other match settings has a capacity requirement of (30*3*5) = 450.

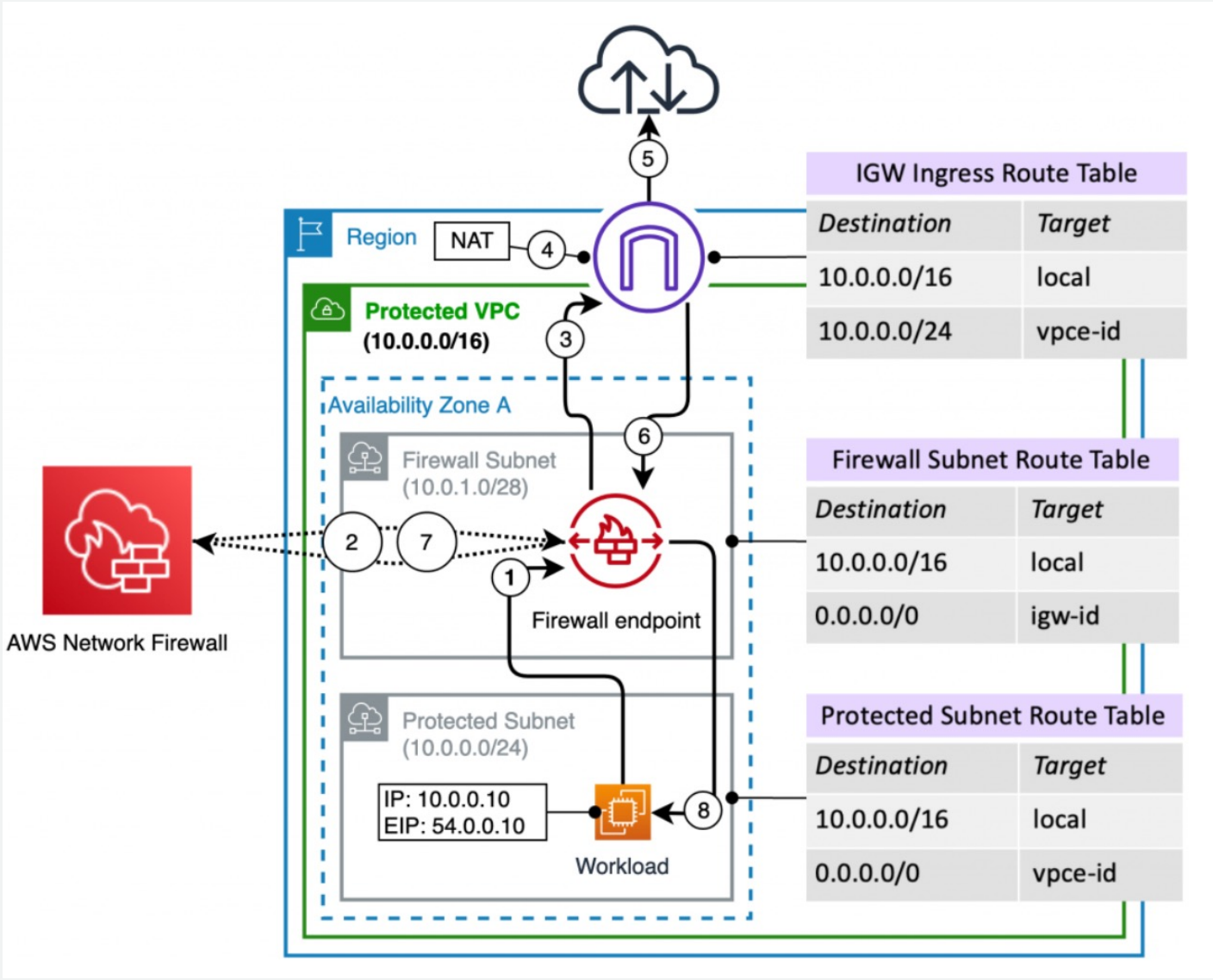
Resource	Quota per account per Region
Maximum character length of a Suricata rule. Each variable value in the rule counts towards this limit.	8,192
Maximum size of a Suricata-compatible rules string for a rule group, in bytes.	2,000,000
Maximum stateful rule group capacity. For more information, see Setting rule group capacity in AWS Network Firewall.	30,000
Maximum number of IP set references per Suricata compatible stateful rule group. For information about IP set references, see Using IP set references in Suricata compatible rule groups.	5
Maximum number of stateful rule groups per firewall policy.	20
Maximum number of stateful rules per firewall policy. This is the total across all rule groups that are referenced by the policy.	30,000
Maximum stateless rule group capacity. For more information, see Setting rule group capacity in AWS Network Firewall.	30,000
Maximum number of stateless rule groups per firewall policy.	20
Maximum number of stateless rules per firewall policy. This is the total across all rule groups that are referenced by the policy.	30,000
Maximum network traffic bandwidth per firewall endpoint. If you require more traffic bandwidth, you can split your resources into subnets and create a firewall in each subnet.	100 Gbps
Required number of firewall policies per firewall.	1
Maximum number of firewalls that can use the same firewall policy.	1,000
Maximum number of firewall policies that can use the same rule group.	1,000

AWS Network Firewall – 파트너 출시



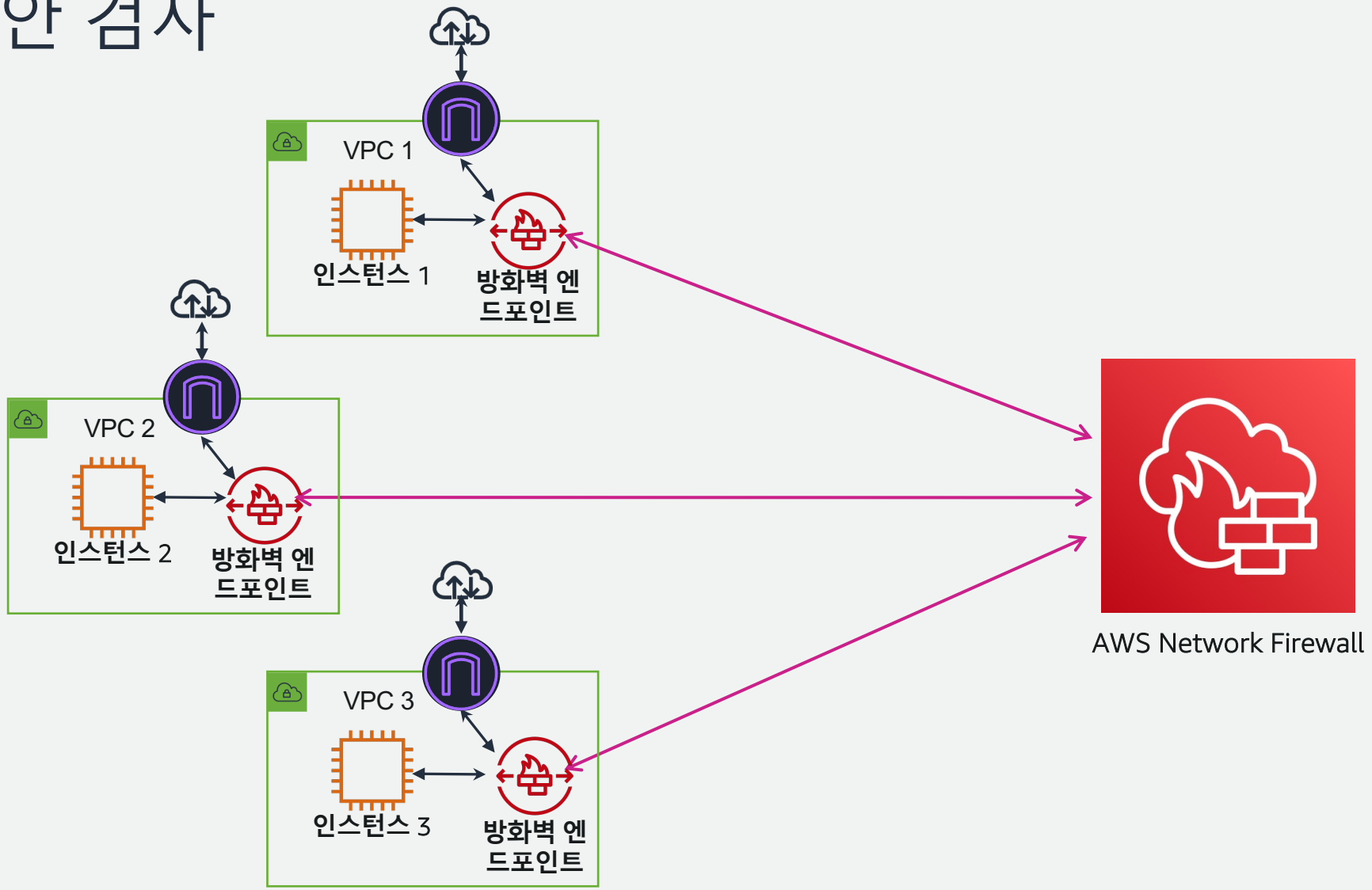
© 2022, Amazon Web Services, Inc. or its affiliates.

Traffic Flow



© 2022, Amazon Web Services, Inc. or its affiliates.

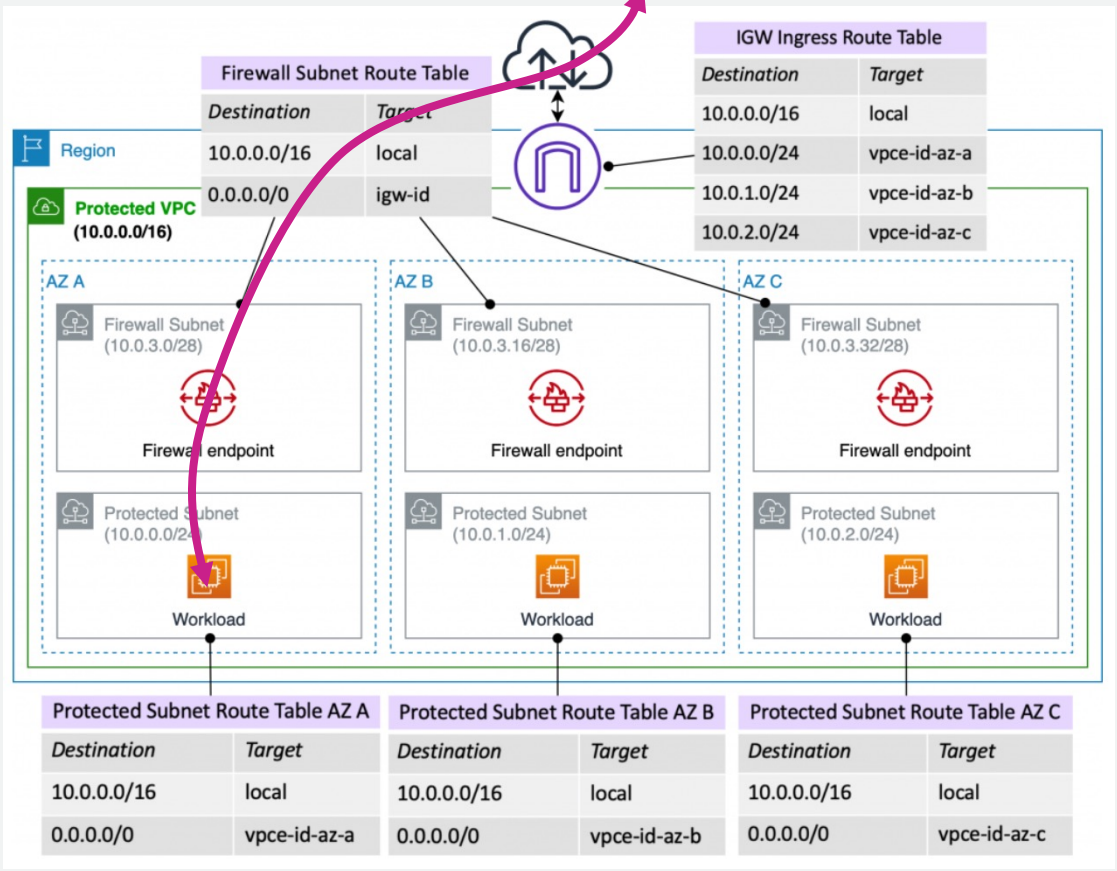
분산 보안 검사



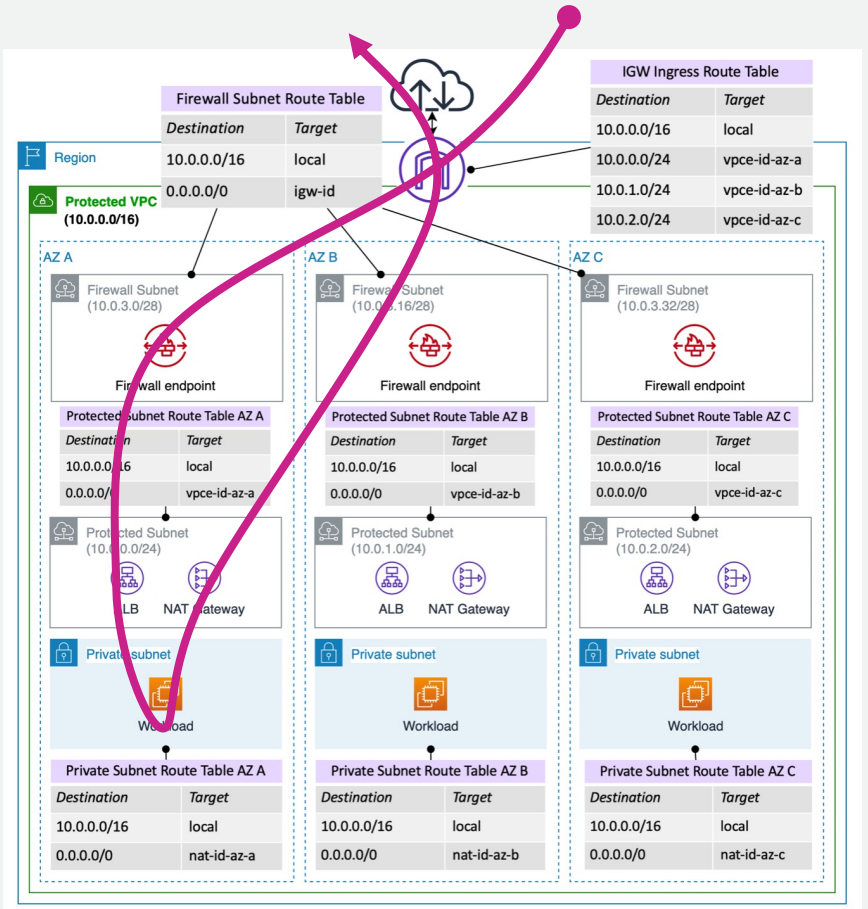
© 2022, Amazon Web Services, Inc. or its affiliates.

분산 보안 검사

Distributed Model, Multi-AZ protecting Public Subnets / between internet & ALB/NATGW



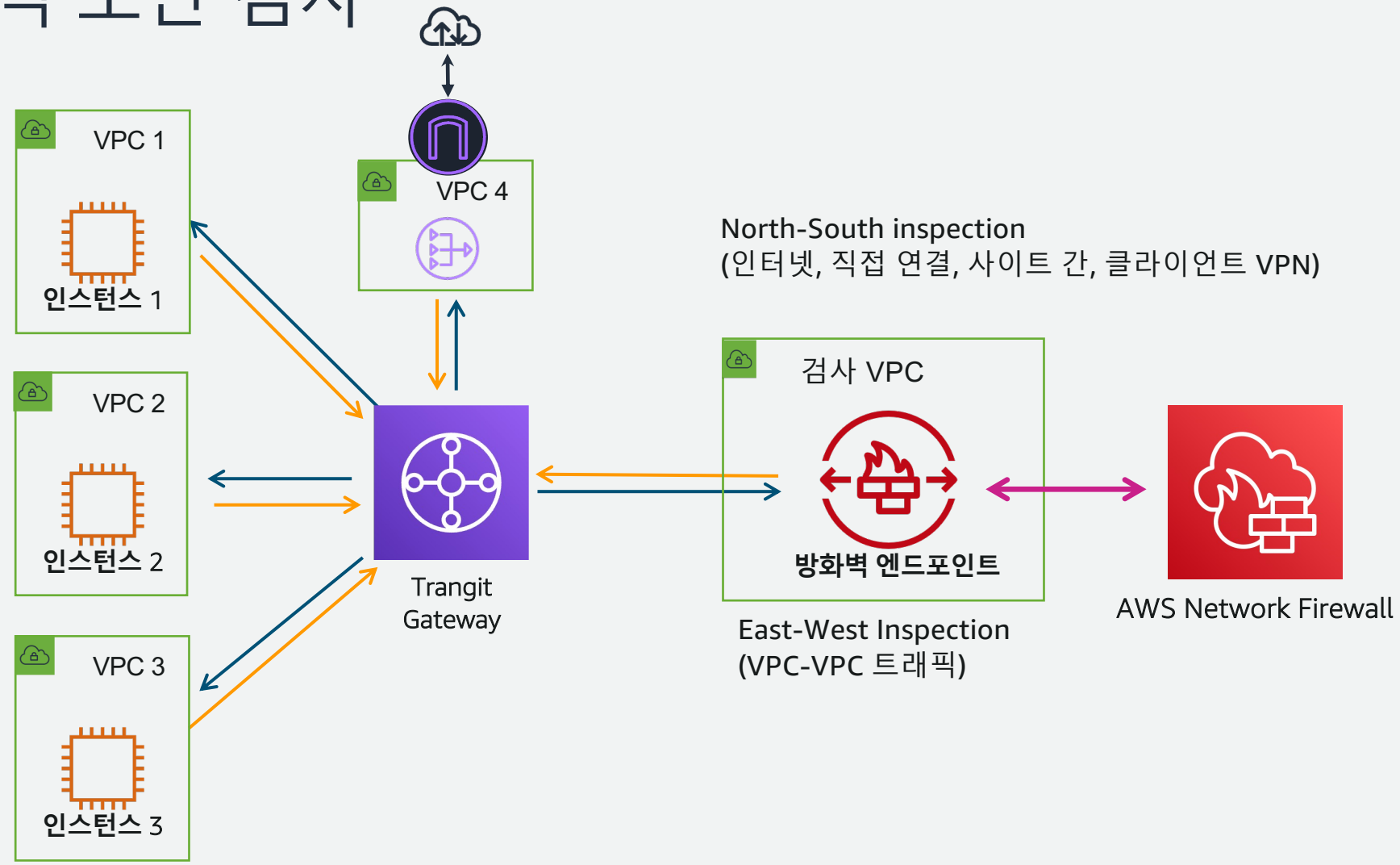
< Multi-AZ protecting Public Subnets >



< between internet & ALB/NATGW >

© 2022, Amazon Web Services, Inc. or its affiliates.

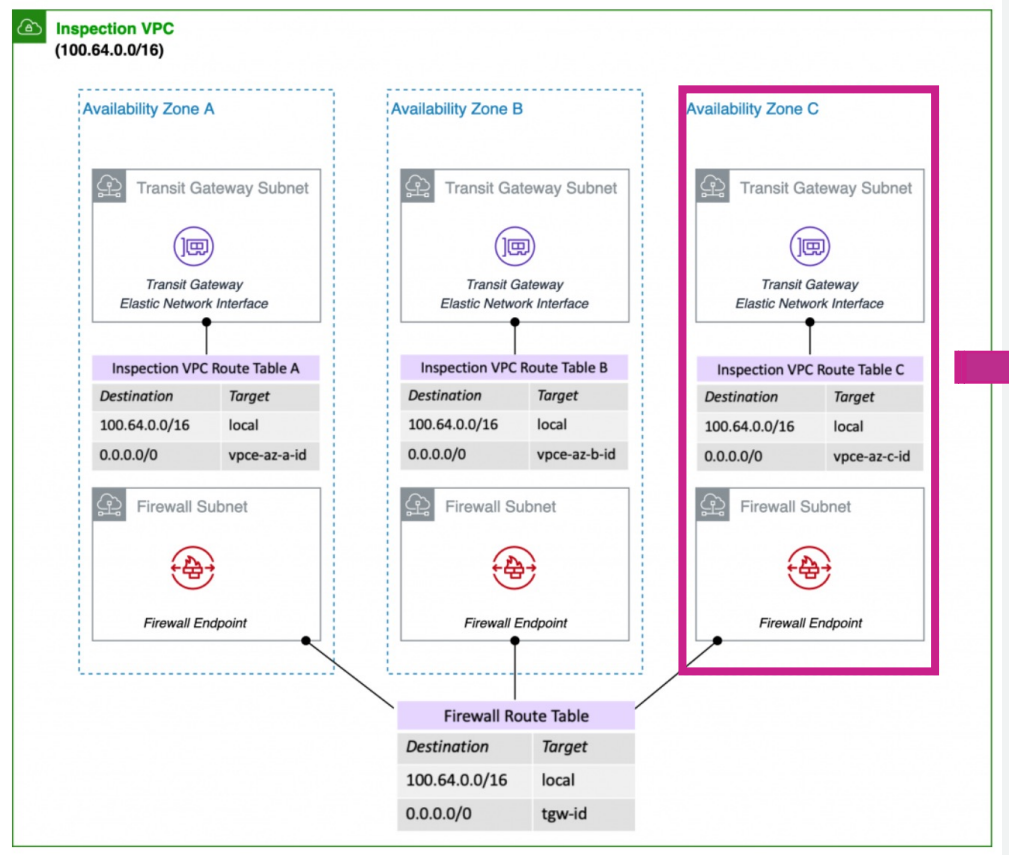
중앙 집중식 보안 검사

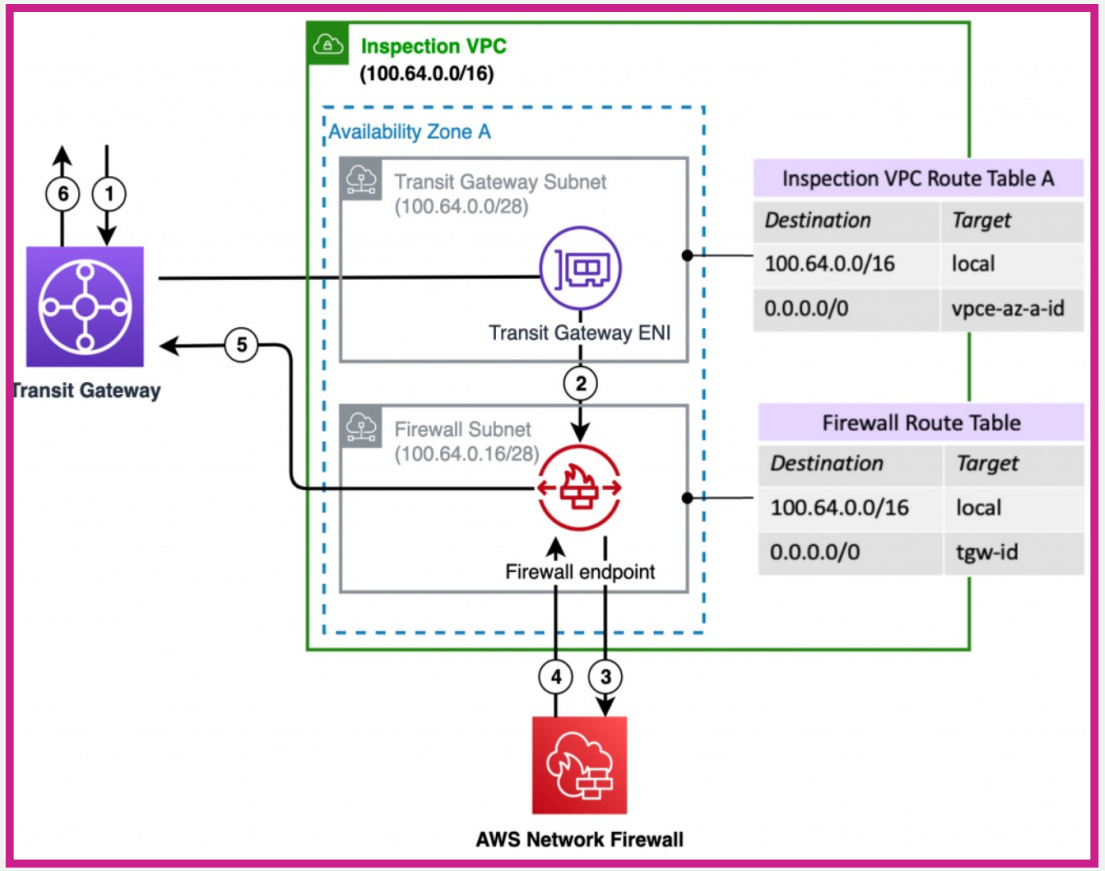


© 2022, Amazon Web Services, Inc. or its affiliates.

중앙 집중식 보안 검사

Centralized Model, AWS Network Firewall deployed in Inspection VPC

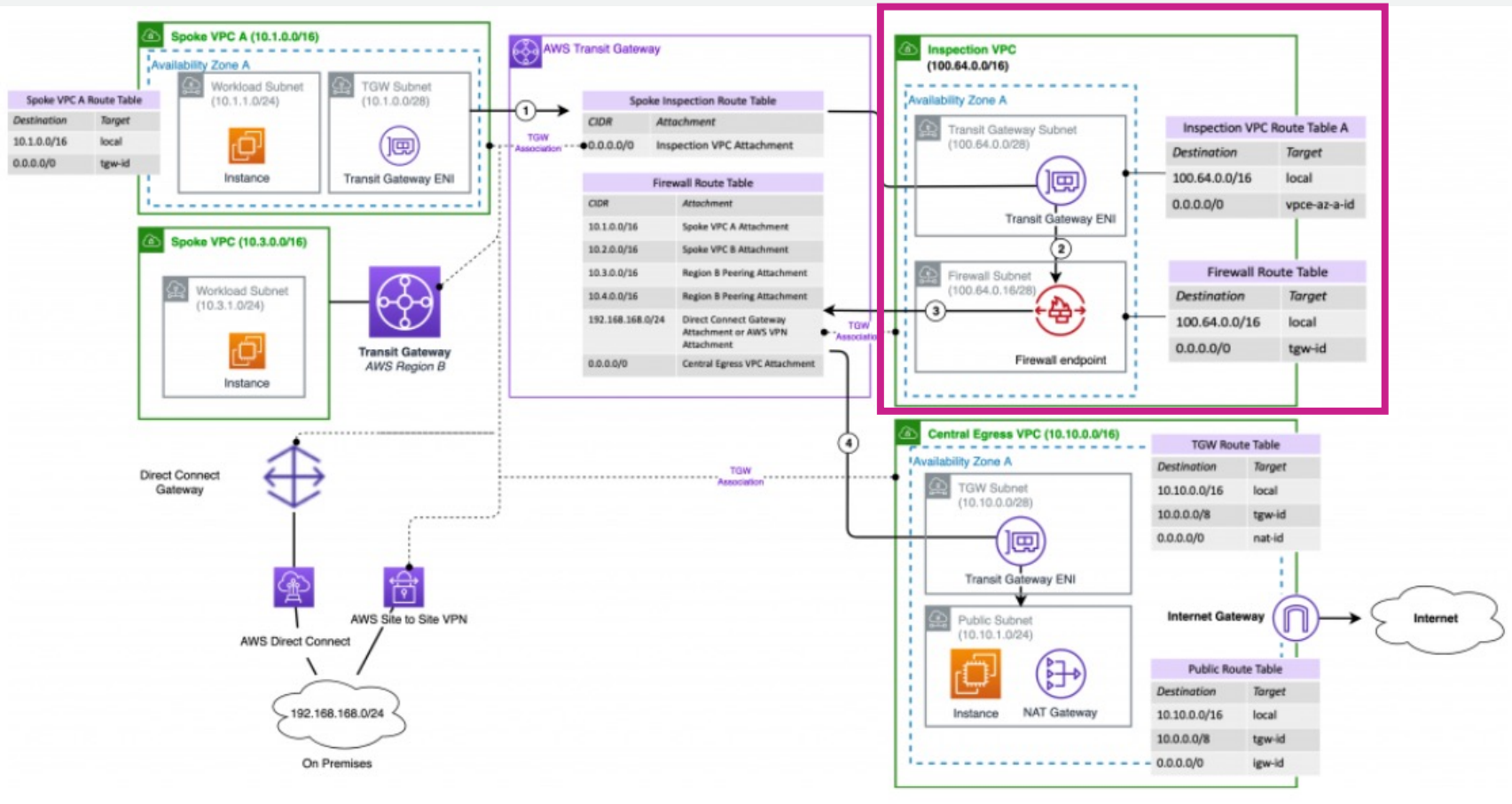




© 2022, Amazon Web Services, Inc. or its affiliates.

중앙 집중식 보안 검사

Centralized Model, Internet Egress and NAT gateway



© 2022, Amazon Web Services, Inc. or its affiliates.

Deployment model comparison

- 권고 모델: AWS 환경 구성에 협의 후 Centralized 혹은 Combined 모델 구성

구분	Distributed AWS Network Firewall deployment model	Centralized AWS Network Firewall deployment model	Combined AWS Network Firewall deployment model
East-West: VPC to VPC traffic flow	Not supported	Supported	Supported
North-South: VPC to Internet traffic flow	Supported	Supported	Supported
North-South: VPC to on-prem via VPN or DX traffic flow	Not supported	Supported	Supported
Prerequisites	AWS Network Firewall subnet	Inspection VPC and AWS Transit Gateway	AWS Network Firewall subnets in each protected VPC; Inspection VPC and AWS Transit Gateway
Centralized management	Through AWS Firewall Manager	Through a single instance of AWS Network Firewall	Through AWS Firewall Manager
Source IP visibility	Configuration dependent	Yes	Configuration dependent
Misconfiguration risk and potential blast radius	Lowest	Medium	Low
Cost	Per AWS Network Firewall endpoint	Per AWS Transit Gateway attachments & AWS Network Firewall endpoints; AWS Transit Gateway data processing	Per AWS Transit Gateway attachments & AWS Network Firewall endpoints (including any additional endpoints per protected VPC); AWS Transit Gateway data processing

© 2022, Amazon Web Services, Inc. or its affiliates.

추가 정보

© 2022, Amazon Web Services, Inc. or its affiliates.

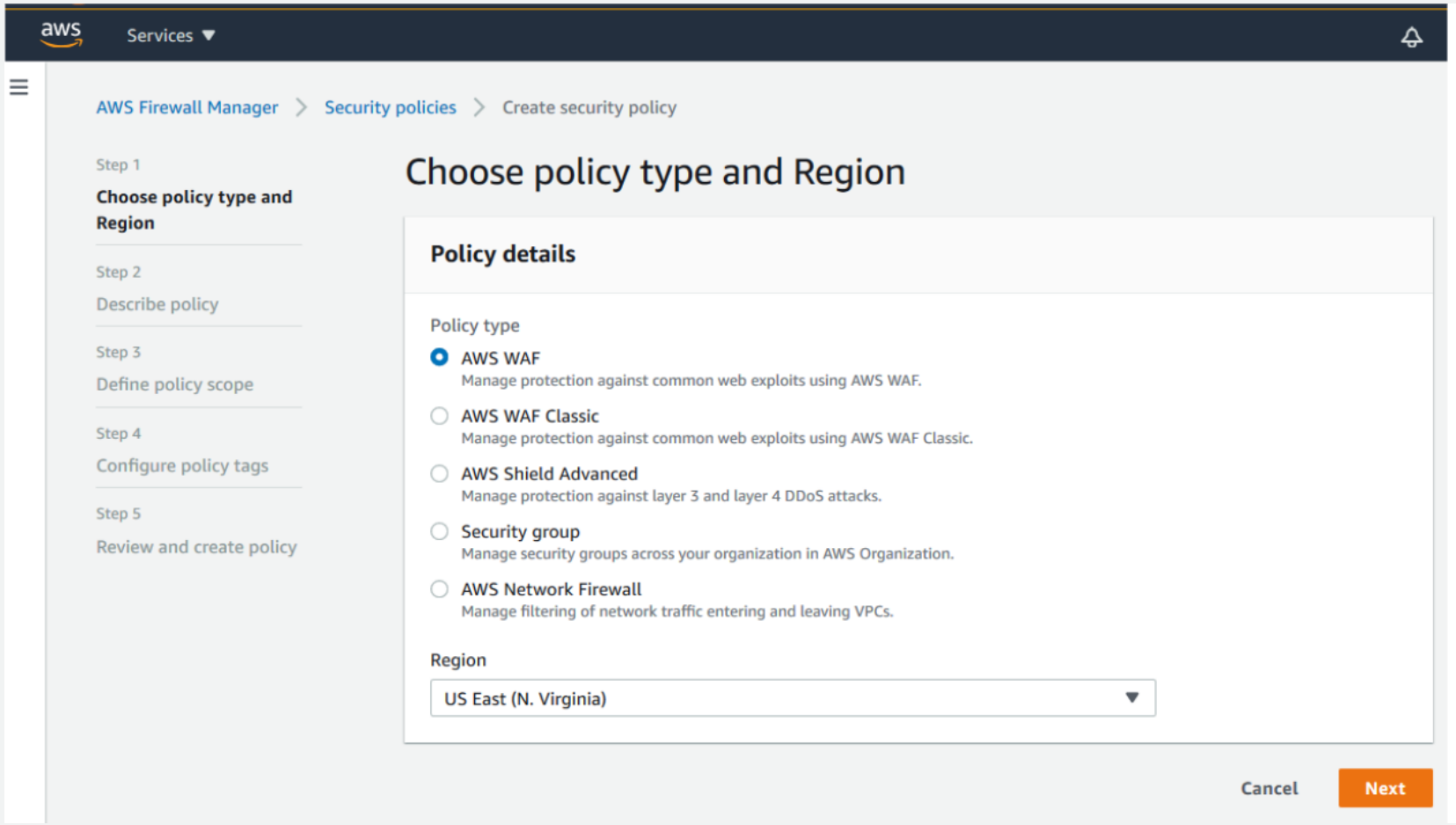
AWS Firewall Manager를 통한 일관된 정책 관리

AWS Network Firewall
VPC에서 라우팅 가능한 엔드포인트로 심층 패킷 검사를 제공하는 L3-7 전체 네트워크 방화벽

AWS WAF
AWS APIGW, AWS ALB 및 AWS 클라우드프론트에 대한 L7 보호

AWS Shield Advanced
클라우드 프론트, ELB, AWS EIP 및 AGA에서 L3-4 DDoS 보호

Security Group
EC2에서의 L3-4 IP 필터링 보호



© 2022, Amazon Web Services, Inc. or its affiliates.

AWS Firewall Manager를 통한 일관된 정책 관리

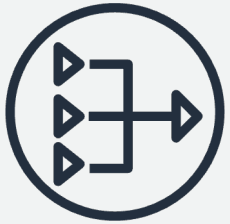
AWS 네트워크 방화벽

각 방화벽 엔드포인트에 대해 시간당 요금을 지불하면 됩니다. 또한 방화벽 끝점에서 처리한 기가바이트 단위로 청구되는 트래픽 양에 대해서도 비용을 지불합니다.

- 시간당 0.395달러
- 기가바이트 당 0.065달러

AWS NAT 게이트웨이

AWS 네트워크 방화벽과 함께 VPC에 NAT 게이트웨이를 생성하도록 선택하는 경우 표준 NAT 게이트웨이 처리 및 시간당 사용 요금이 일대일로 면제됩니다. 이때 AWS 네트워크 방화벽에 대해 요금이 청구된 GB당 처리량 및 사용 시간이 적용됩니다.



aws © 2022, Amazon Web Services, Inc. or its affiliates.

GWLB 동작 방식
(aka. 3rd party 보안 솔루션 연결 방법)

© 2022, Amazon Web Services, Inc. or its affiliates.

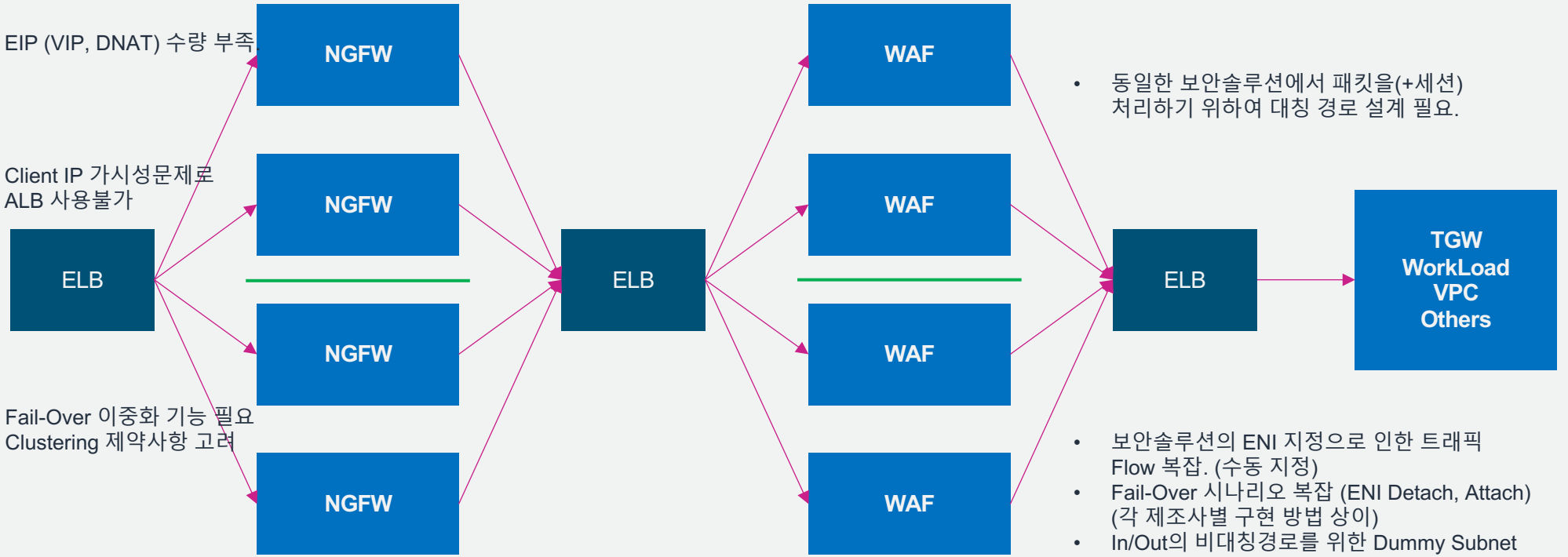
Legacy 3rd party 솔루션 연동 방법과 제약

- 2차 보안솔루션간의 트래픽 연계 방안의 복잡성 (대상 VIP, Health Check, Fail-Over 시나리오 등)
- ELB의 FQDN대상 DNAT 기능 지원 필요.

- 추후 보안솔루션 추가 구축 시 네트워크 설계 전면 재 검토 필요.
- 트래픽 송/송수신 아키텍처 검토.
- 이전 솔루션 도입 절차의 반복. (설계, 검증, 안정화)

- EIP (VIP, DNAT) 수량 부족.

- Client IP 가시성문제로 ALB 사용불가



- Fail-Over 이중화 기능 필요
- Clustering 제약사항 고려

- 동일한 보안솔루션에서 패킷을(+세션) 처리하기 위하여 대칭 경로 설계 필요.

- 보안솔루션의 ENI 지정으로 인한 트래픽 Flow 복잡. (수동 지정)
- Fail-Over 시나리오 복잡 (ENI Detach, Attach) (각 제조사별 구현 방법 상이)
- In/Out의 비대칭경로를 위한 Dummy Subnet 구현 필요. (Routing Conflict 방지)

- 확장 시 Clustering 설정, 구현 복잡
- 복잡한 Fail-Over 시나리오
- AZ Fail시 수동으로 Fail-Over 수행
- 자동 구현 시 Lambda code 후 작업 필요

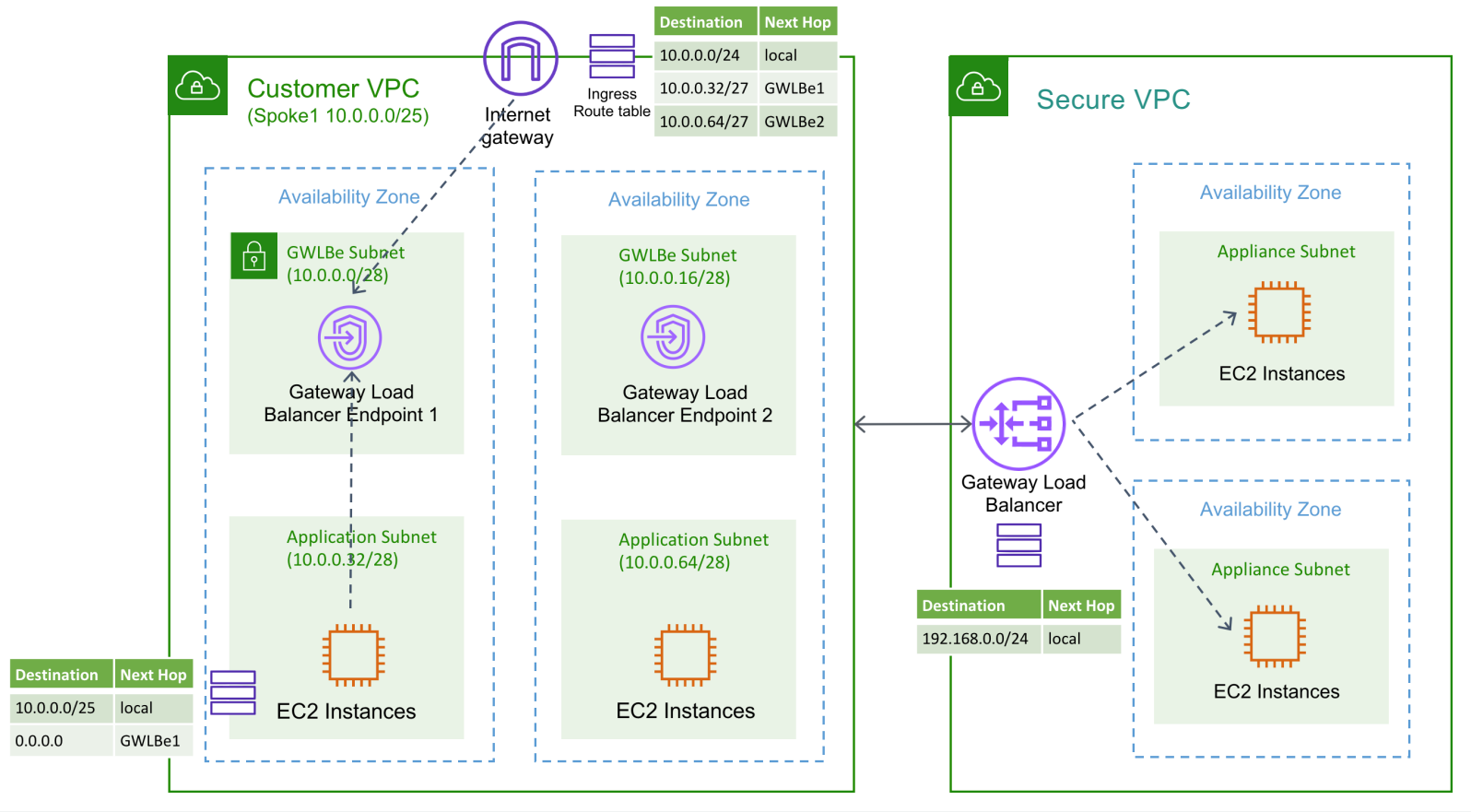
© 2022, Amazon Web Services, Inc. or its affiliates.

GWLB (Gateway Loadbalacer)

- GWLB는 가상 전용 보안솔루션에 대한 **로드 밸런싱 및 확장기능을 제공**하고 **선호하는 솔루션(제조사)의 구축 용이성, 고 가용성, 복원성 제공**.
- 가상 보안솔루션 Pool(Fleet)로 라우팅 하기 위한 게이트웨이를 제공하여 운영 오버헤드와 비용 감소. **(단순하고 능률적인 네트워크 아키텍처 구현)**
- AWS Marketplace에서 주요 보안솔루션을 쉽게 배포할 수 있으며 **처리 용량에 따라 자동으로 확장**되며, 정상동작하는 솔루션으로만 트래픽을 라우팅되도록 함으로써 애플리케이션 및 워크로드의 가용성을 높임.
- **Client IP 유지가 가능한 간결한 설계**로(샌드위치 구조와 비교 시 적은 제약사항) 트래픽 가시성의 확보와 보안솔루션 구축 시 아키텍처 설계의 단순화.
- 워크로드에 따른 서비스 체이닝 구현, 원하는 워크로드에 원하는 보안 솔루션을 묶어 연동하여 워크로드에 특화된 보안 서비스 제공
- 테스트 망 구축 없이 특정 워크로드에 테스트가 필요한 **3rd Party 솔루션을 연동**하여 고객사 운영 효율성 증대

aws © 2022, Amazon Web Services, Inc. or its affiliates.

3rd Party 솔루션 연동을 위한 GWLB 구조



APN - FW

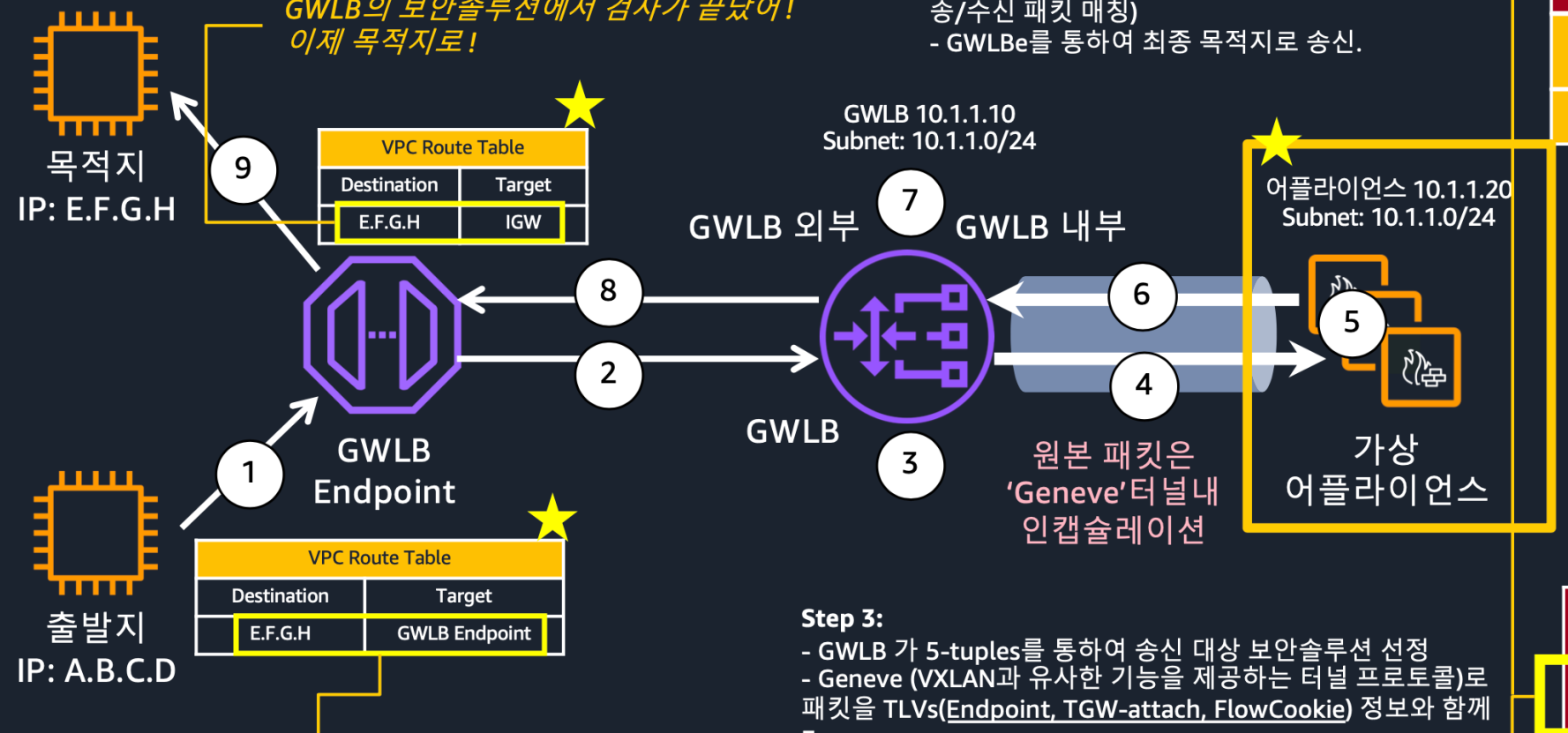
APN - NGFW

APN - WAF

© 2022, Amazon Web Services, Inc. or its affiliates.

GWLB 동작원리

GWLB에 의하여 보안솔루션 Pool이, 보안 VPC로 쉽게 구현될 수 있음 (E/W, N/S, 가용성)



Step 7:
- GWLB 가 Decap (원본 패킷 복원).
- 'Tuple'과 ' FlowCookie' 검증. (이전 송/수신 패킷 매칭)
- GWLBe를 통하여 최종 목적지로 송신.

Step 6: 보안솔루션(검사 후 반환) > GWLB

Outer Src IP: 10.1.1.20		Outer Dst IP: 10.1.1.10
GWLBE ID	ATTACHMENT ID	FLOW COOKIE
Inner Src IP: A.B.C.D		Inner Dst IP: E.F.G.H
Payload		

Step 5:
- 보안솔루션은 원본패킷을 복원
- 고유의 보안기능 수행 (탐지, 차단)
- 검사 후 GWLB로 재송신 (TLV포함)

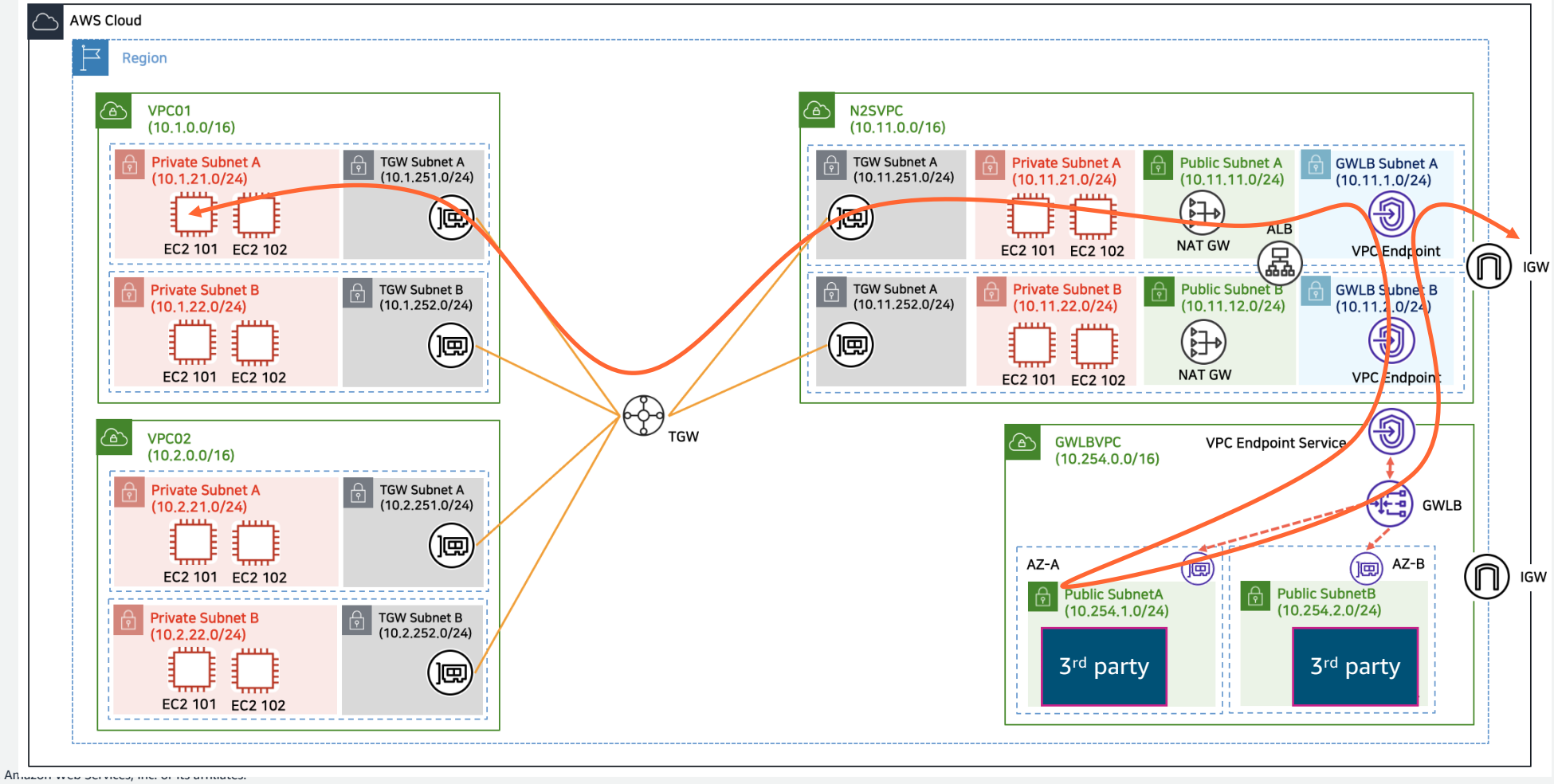
Step 4: GWLB > 보안솔루션

Outer Src IP: 10.1.1.10		Outer Dst IP: 10.1.1.20
GWLBE ID	ATTACHMENT ID	FLOW COOKIE
Inner Src IP: A.B.C.D		Inner Dst IP: E.F.G.H
Payload		

Step 3:
- GWLB 가 5-tuples를 통하여 송신 대상 보안솔루션 선정
- Geneve (VXLAN과 유사한 기능을 제공하는 터널 프로토콜)로 패킷을 TLVs(Endpoint, TGW-attach, FlowCookie) 정보와 함께 Encap

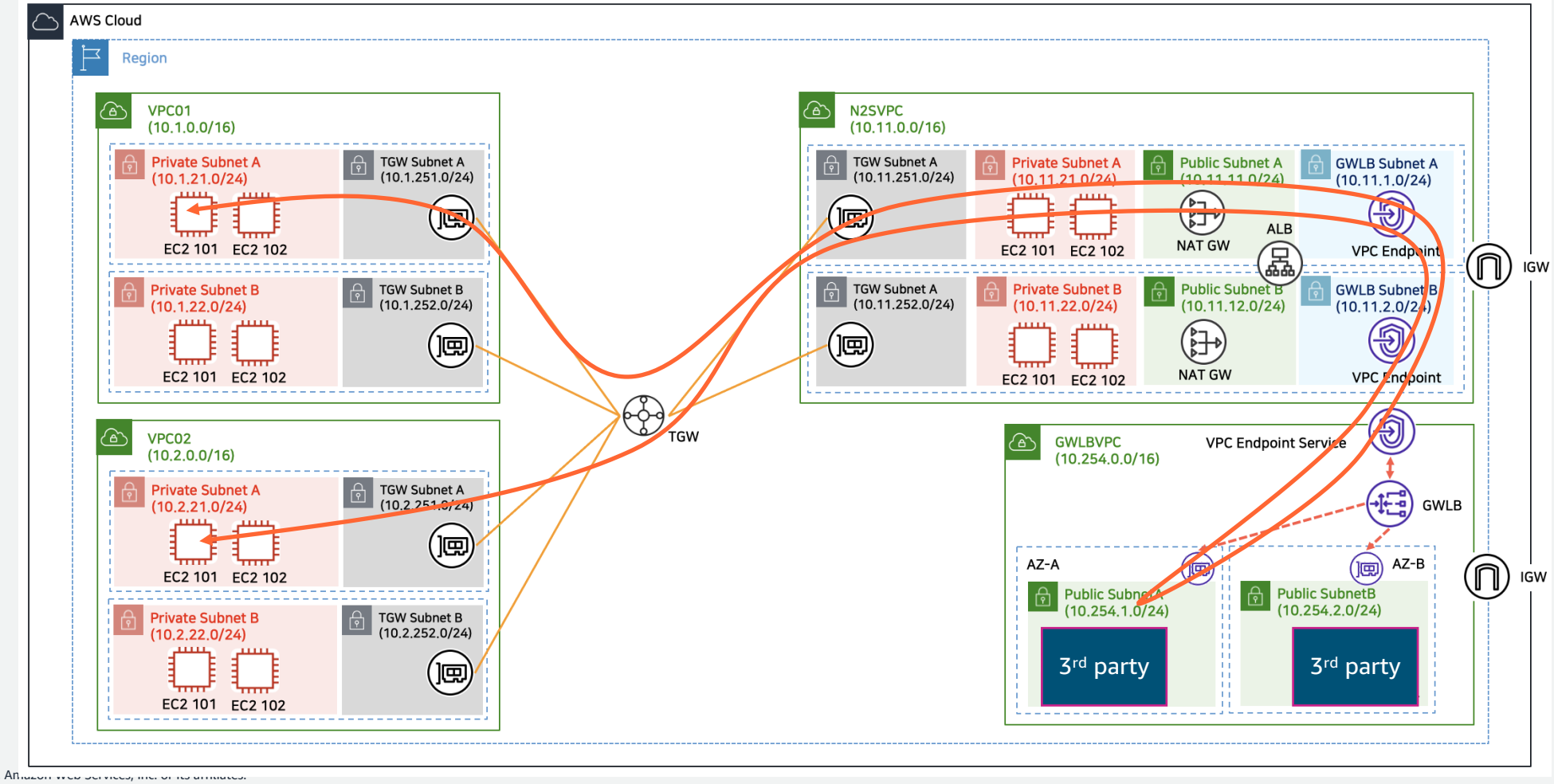
© 2021 Amazon Web Services, Inc. or its affil

전용 보안존 구성을 통해 3rd party 연동 : North - South



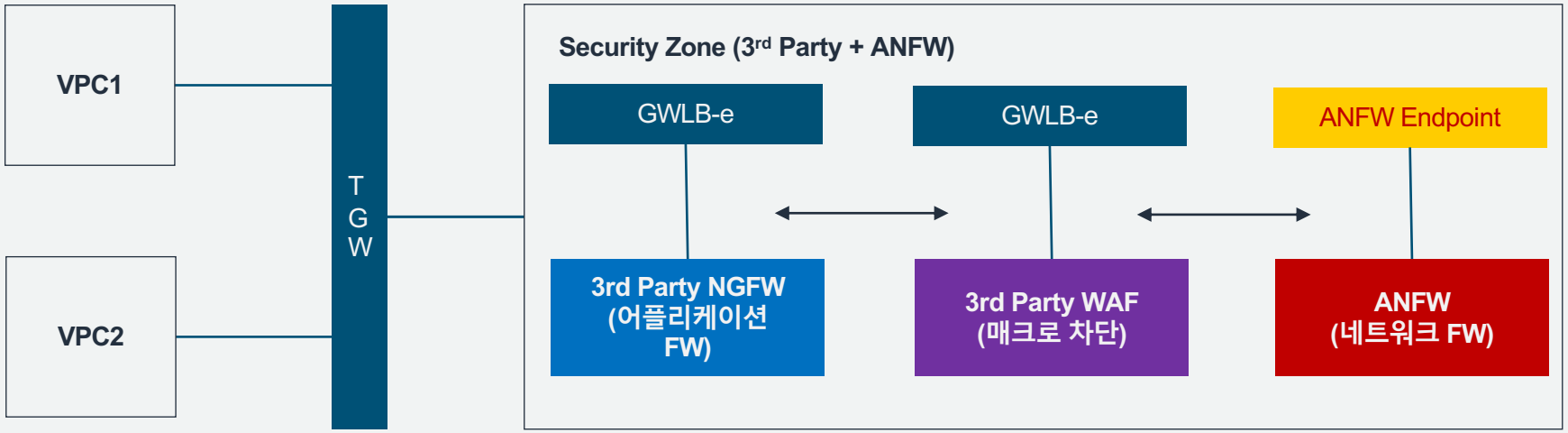
© 2022, Amazon Web Services, Inc. or its affiliates.

전용 보안존 구성을 통해 3rd party 연동 : East - West



© 2022, Amazon Web Services, Inc. or its affiliates.

Multi 3rd Party 솔루션 연동 플로우



트래픽 타입	경로
VPC1 to VPC2 (내부통신)	VPC1 > TGW > ANFW > TGW> VPC2
VPC1 to External (외부통신)	VPC1 > TGW > NGFW > External
External to VPC 1 (외부통신)	External > IGW > NGFW > WAF > VPC1
External to VPC 2 (외부통신)	External > IGW > NGFW > WAF > VPC2

© 2022, Amazon Web Services, Inc. or its affiliates.

AWS Network Firewall 정책을 세워볼까요?

© 2022, Amazon Web Services, Inc. or its affiliates.

ANFW 와 NACL/Security Group 차이점

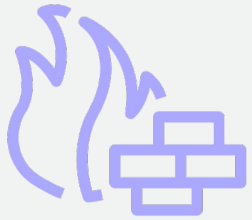
Network ACL

흐름 처리 : Stateless
규칙 검사 : Order
규칙 액션 : Allow, Deny
적용 대상 : Subnet

+

Security group

흐름 처리 : Stateful
규칙 검사 : 모두 검사
규칙 액션 : Allow
적용 대상 : EC2 or ENI



Network Firewall

=

흐름 처리 : Stateless
규칙 검사 : Order
규칙 액션 : Pass, Drop, Forward
적용 대상: Routing 기준

Stateless Engine

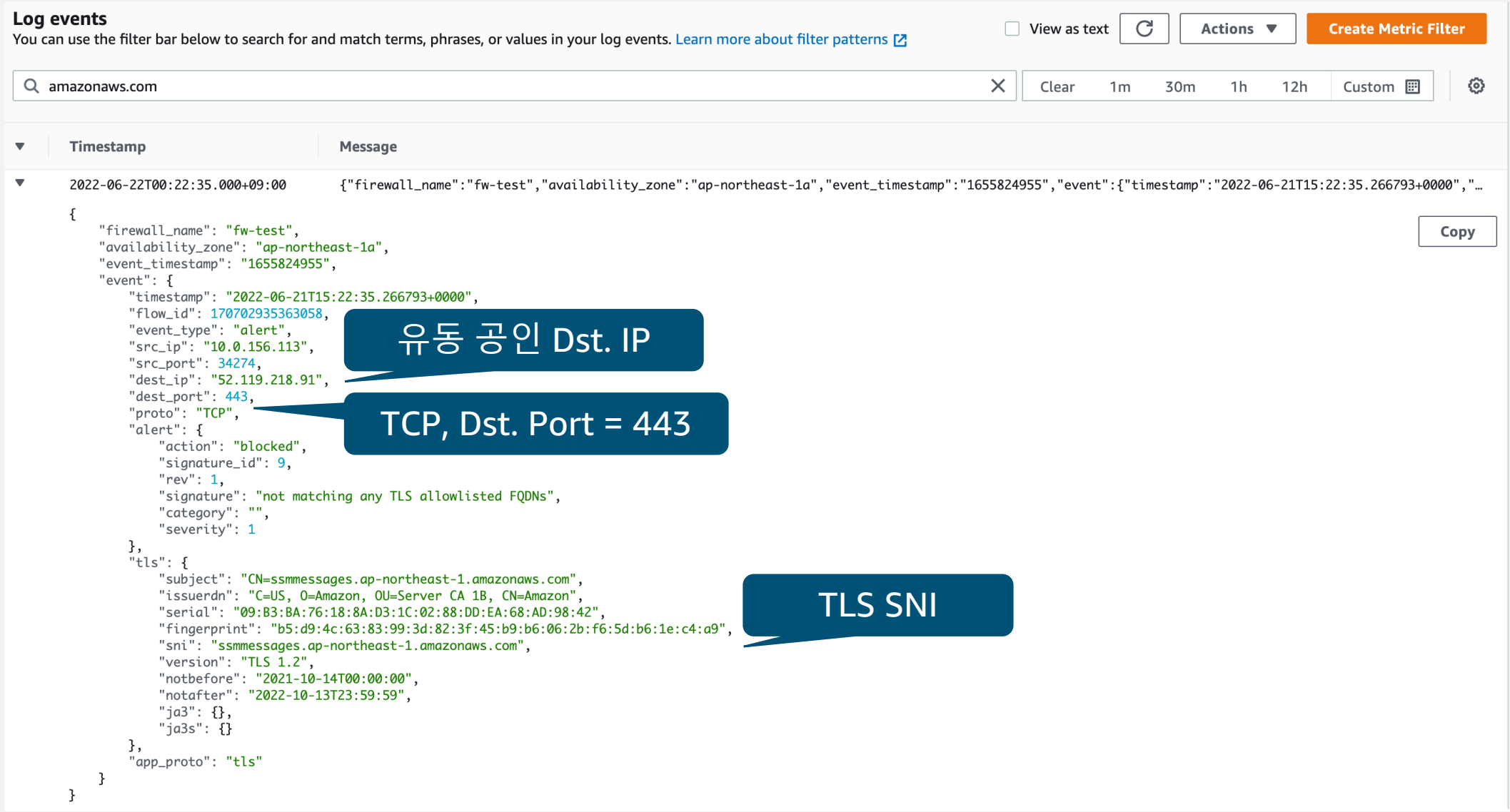
+

흐름 처리 : Stateful
규칙 검사 : 모두 검사
규칙 액션 : Pass, Drop, Alert
적용 대상: Stateless Forward 규칙 기준

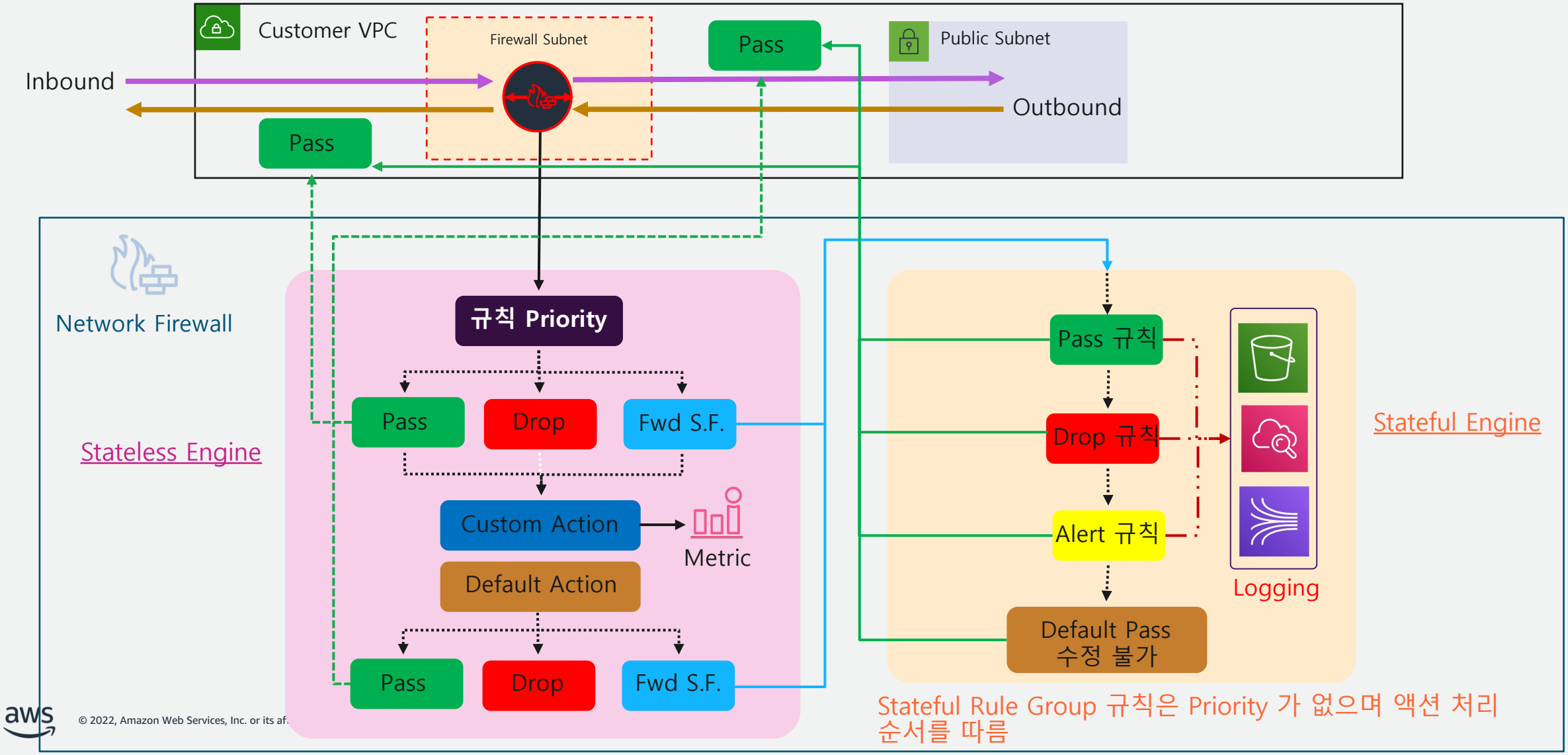
Stateful Engine

aws
© 2022, Amazon Web Services, Inc. or its affiliates.

ANFW TLS 패킷에 대해 제어 방법



Network Firewall Engine의 규칙 검사 흐름도



© 2022, Amazon Web Services, Inc. or its af.

Outbound 트래픽 IP 제어 정책

정책 요건 – VPC 내의 특정 Subnet 혹은 지정된 IP 에 대해서만 인터넷 접근을 허용하고 그 이외에는 차단

IP Stateless Rule Group – Default 값으로 모두 유지

Tip. Stateless Rule Group 은 Default Action 이 Stateful Group 으로 Forwarding 하는 것이므로 별도의 설정이 없다면 모든 트래픽은 Stateful 엔진에서 검사하게 됨

IP Stateful Rule Group – 특정 VPC IP 대역에서 인터넷(Any IP)으로 접근하는 트래픽에 대해 "Pass" 액션 규칙 등록

Protocol	Source IP	Destination IP	Source Port	Destination Port	Action
TCP	10.0.1.0/24	Any	Any	Any	Pass
TCP	10.0.2.0/24	Any	Any	Any	Pass
TCP	Any	Any	Any	Any	Drop

Tip. IP Stateful Rule Group 은 Default 로 Pass 규칙이 적용되므로 Stateful Rule Group 을 White List 기반으로 적용하고자 하는 경우에는 Any-Any Drop 규칙을 생성하여 적용

aws
© 2022, Amazon Web Services, Inc. or its affiliates.

Inbound 트래픽 IP 제어 정책

정책 요건 – 인터넷에서 유입되는 트래픽 중 Source IP 가 Black List IP 인 경우 차단하고 그 이외에는 허용

IP Stateless Rule Group – Black List IP 에서 VPC 로 접근하는 트래픽에 대해 "Drop" 액션 규칙 등록

Priority	Protocol	Source IP	Destination IP	Source Port	Destination Port	Action
1	All	Black List IP	Public Subnet	Any	Any	Drop

IP Stateful Rule Group – Any IP 에서 VPC CIDR 로 접근하는 트래픽에 대해 "Pass" 액션 규칙 등록

Protocol	Source IP	Destination IP	Source Port	Destination Port	Action
TCP	Any	Public Subnet	Any	Any	Pass
TCP	Any	Any	Any	Any	Drop

aws © 2022, Amazon Web Services, Inc. or its affiliates.

Outbound 트래픽 IP 제어 정책 w/ Blacklist

정책 요건 – 특정 VPC IP 대역에서 인터넷으로 접근할 때 모두 허용하되 목적지가 Blacklist IP 인 경우에는 차단

IP Stateless Rule Group – VPC CIDR 에서 Black List IP 로 접근하는 트래픽에 대해 "Drop" 액션 규칙 등록

Priority	Protocol	Source IP	Destination IP	Source Port	Destination Port	Action
1	All	VPC CIDR	Black List IP	Any	Any	Drop

Tip. Stateful Rule Group 은 Pass Action 이 Drop Action 보다 우선하기 때문에 Stateful Rule Group 에서 허용되는 트래픽을 차단하기 위해서는 Stateless Rule Group 사용

IP Stateful Rule Group – 특정 VPC IP 대역에서 인터넷(Any IP)으로 접근하는 트래픽에 대해 "Pass" 액션 규칙 등록

Protocol	Source IP	Destination IP	Source Port	Destination Port	Action
TCP	10.0.1.0/24	Any	Any	Any	Pass
TCP	10.0.2.0/24	Any	Any	Any	Pass
TCP	Any	Any	Any	Any	Drop

aws
© 2022, Amazon Web Services, Inc. or its affiliates.

Outbound Domain White List 정책

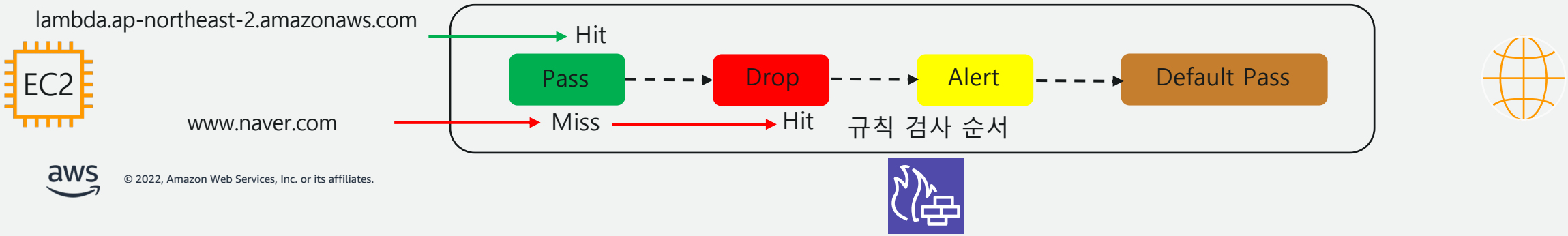
정책 요건 – VPC 에서 인터넷으로 접근하는 모든 HTTP/HTTPS 는 차단하되 White List Domain 에 대해서만 허용

IP Stateful Rule Group – VPC CIDR 에서 인터넷(Any IP)으로 접근하는 Port 80/443 에 대해 "Drop" 액션 규칙 등록

Protocol	Source IP	Destination IP	Source Port	Destination Port	Action
HTTP	VPC CIDR	Any	Any	80	Drop
TLS	VPC CIDR	Any	Any	443	Drop

Domain Rule Group – 접근을 허용하고자 하는 Domain 에 대해 "Allow" 액션 규칙 등록. (예, AWS 서비스 관련 도메인)

Traffic To Inspect	Domain List	Action
HTTP, HTTPS	.amazonaws.com	Allow



© 2022, Amazon Web Services, Inc. or its affiliates.

DX 장애시, Outbound 허용을 통한 임시조치

정책 요건 – DX 장애 발생중 EC2 접속용 Session Manager 허용을 위한 도메인 기반의 임시 정책

Outbound Stateless

Priority	Protocol	Src. IP	Dst. IP	Src. Port	Dst. Port	Action
10	tcp	40.0.0.0 /8	any	any	443	Fwd, SF
1000	all	any	any	any	any	drop

Outbound Stateful

Protocol	Src. IP	Dst. IP	Src. Port	Dst. Port	Action

Protocol	Domain List	Action
HTTPS	ssm.ap-northeast-2.amazonaws.com ssmmessages.ap-northeast-2.amazonaws.com ec2messages.ap-northeast-2.amazonaws.com	Pass

Inbound Stateless

Priority	Protocol	Src. IP	Dst. IP	Src. Port	Dst. Port	Action
10	All	Black List IP	Public Subnet	Any	Any	Drop

Inbound Stateful

Protocol	Src. IP	Dst. IP	Src. Port	Dst. Port	Action

aws © 2022, Amazon Web Services, Inc. or its affiliates.

기타 이것 저것...

© 2022, Amazon Web Services, Inc. or its affiliates.

Stateful에는 Protocol layer Priority 없고, action 순서는..?

Evaluation order for stateful rule groups

PDF | RSS

All of your stateful rule groups are provided to the rule engine as Suricata compatible strings. Suricata can evaluate stateful rule groups by using the default rule group ordering method, or you can set an exact order using the *strict* ordering method. The settings for your rule groups must match the settings for the firewall policy that they belong to.

Default action order

If your firewall policy is set up to use default rule group ordering, the default action order by which Suricata evaluates stateful rules is determined by the following settings, listed in order of precedence:

1. The Suricata `action` specification. This takes highest precedence.

   Actions are processed in the following order:

   a. `pass`
   b. `drop`
   c. `alert`

   For more information about the action specification, see Suricata.yaml: Action-order in the Suricata User Guide.
2. The Suricata `priority` keyword. Within a specific action group, you can use the priority setting to indicate the processing order. By default, Suricata processes from the lowest numbered priority setting on up. The `priority` keyword has a mandatory numeric value ranging from 1 to 255. Note that the `priority` keyword is only valid using the default action order.

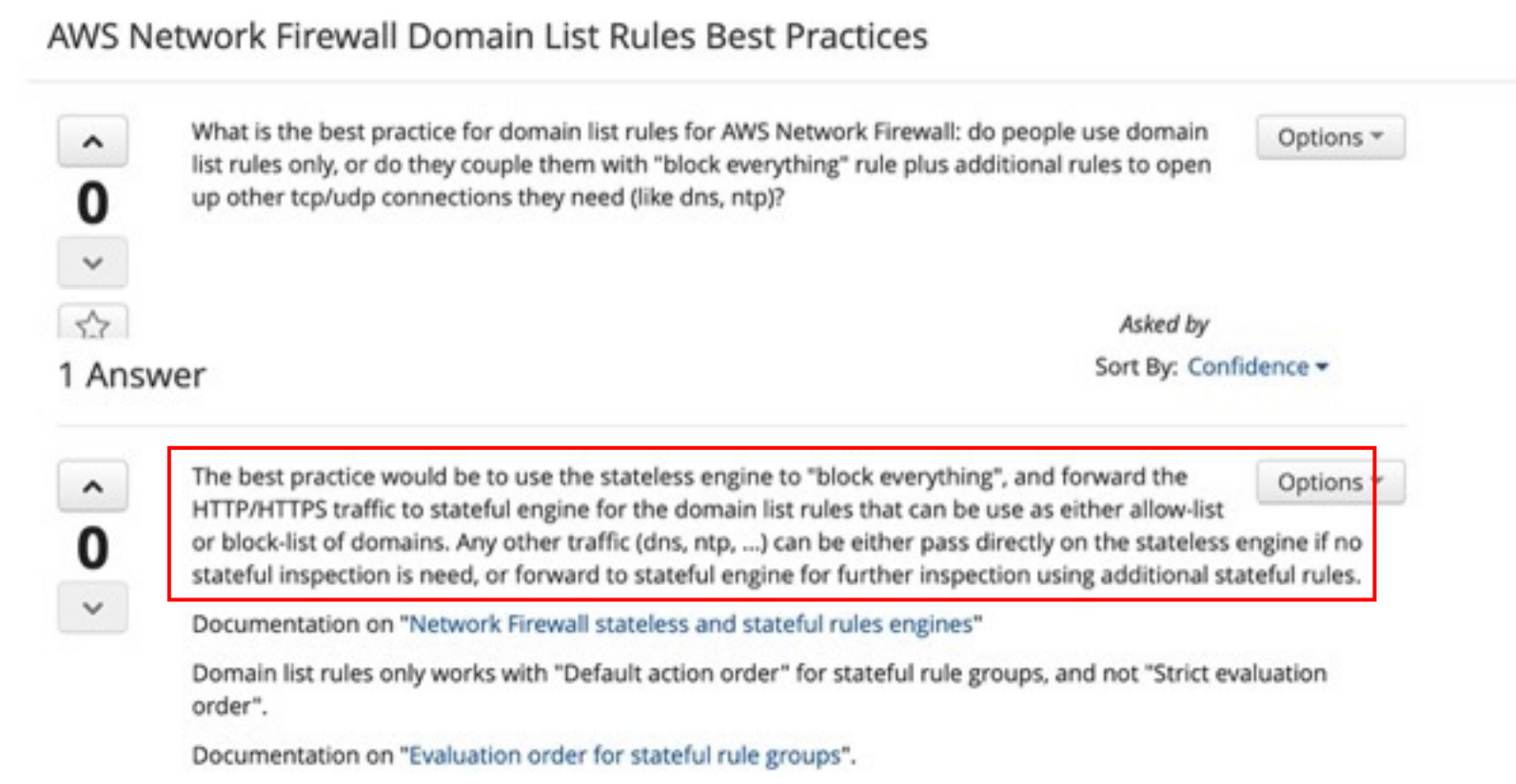
   For more information about priority, see Suricata.yaml: Action-order in the Suricata User Guide.

For example, Suricata evaluates all `pass` rules before evaluating any `drop` or `alert` rules by default, regardless of the value of priority settings. Within all `pass` rules, if priority keywords are present, Suricata orders the processing according to them.

The protocol layer does not impact the rule evaluation order by default. If you want to avoid matching against lower-level protocol packets before higher-level application protocols can be identified, consider using the `flow` keyword in your rules. This is needed because, for example, a TCP rule might match on the first packet of a TCP handshake before the stateful engine can identify the application protocol. For information

aws © 2022, Amazon Web S

Domain-list Best Practice 알려줘..



AWS Network Firewall Domain List Rules Best Practices

0

What is the best practice for domain list rules for AWS Network Firewall: do people use domain list rules only, or do they couple them with "block everything" rule plus additional rules to open up other tcp/udp connections they need (like dns, ntp)?

Options

Asked by

1 Answer

Sort By: Confidence

0

The best practice would be to use the stateless engine to "block everything", and forward the HTTP/HTTPS traffic to stateful engine for the domain list rules that can be use as either allow-list or block-list of domains. Any other traffic (dns, ntp, ...) can be either pass directly on the stateless engine if no stateful inspection is need, or forward to stateful engine for further inspection using additional stateful rules.

Options

Documentation on "Network Firewall stateless and stateful rules engines"

Domain list rules only works with "Default action order" for stateful rule groups, and not "Strict evaluation order".

Documentation on "Evaluation order for stateful rule groups".

© 2022, Amazon Web Services, Inc. or its affiliates.

Domain-list white-list 같이 동작한다는데.. 비정상동작시!?

Domain lists

The domain list rule group has one action setting at the rule group level. You specify one of the following options:

- **Allow** – Indicates that the domain name list is to be used as an allow list for all traffic that matches the specified protocols. For matching packets, discontinue inspection of the packet and permit it to pass to its intended destination. For non-matching packets, discontinue inspection of the packet, block it from going to its intended destination, and send a message to the firewall's alert logs if the firewall has alert logging configured.
- **Deny** – Indicates that the domain name list is to be used as a deny list for traffic that matches the specified protocols. For matching packets, discontinue inspection of the packet, block it from going to its intended destination, and send a message to the firewall's alert logs if the firewall has alert logging configured. For non-matching packets, take no action.

Note. Nonmatching packet에 대해서는 검사 중단하고, 차단 및 alert log인데….

allow 되버리네.. Eg. https://google.com

May 4

add comment

0

I also had a customer who setup their ANFW with asymmetric routing (only had one NAT Gateway in a separate VPC and didn't have appliance mode enabled). What ended up happening was a bit bizarre, the 5 tuple rules and the suricata rules which they applied actually worked, but the domain list rules didn't. So I would definitely speak to your customer and ensure they don't have any Symmetric flows in their environment, as it will cause ANFW not to block or alert for any traffic.

Options

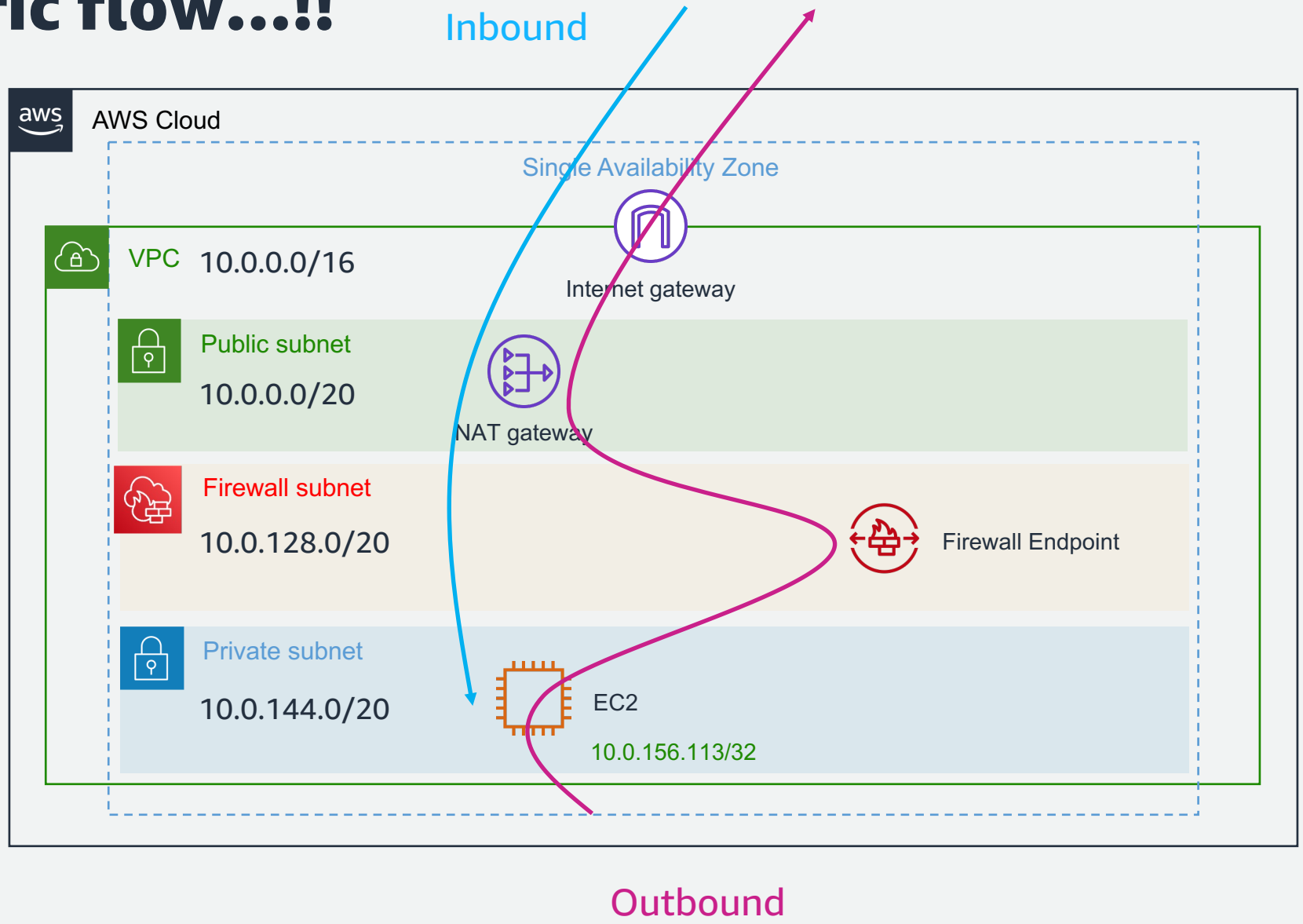
Answered by

Asymmetric flow에서 발생하는 도메인 기반 차단/경고 불가

add comment

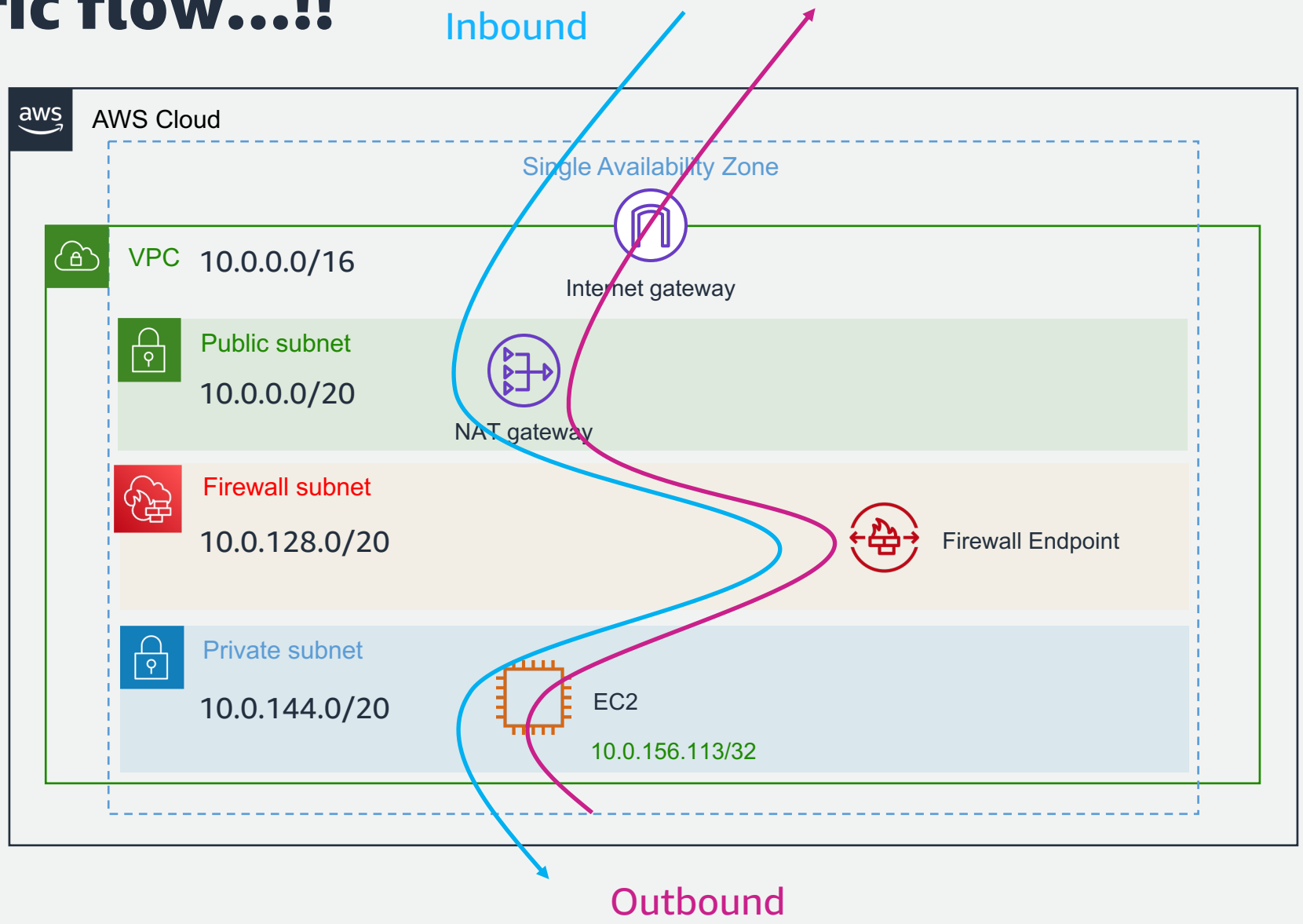
© 2022, Amazon Web Services, Inc. or its affiliates.

문제는 **Asymmetric flow...!!**



aws © 2022, Amazon Web Services, Inc. or its affiliates.

문제는 **Asymmetric flow...!!**



aws © 2022, Amazon Web Services, Inc. or its affiliates.

Logging을 남기고 싶다면 **Stateful Engine**으로..

Logging network traffic from AWS Network Firewall

PDF | RSS

You can configure AWS Network Firewall logging for your firewall's stateful engine. Logging gives you detailed information about network traffic, including the time that the stateful engine received a packet, detailed information about the packet, and any stateful rule action taken against the packet. The logs are published to the log destination that you've configured, where you can retrieve and view them.

> **Note**
>
> Firewall logging is only available for traffic that you forward to the stateful rules engine. You forward traffic to the stateful engine through stateless rule actions and stateless default actions in the firewall policy. For information about these actions settings, see Stateless default actions in your firewall policy and Defining rule actions in AWS Network Firewall.
>
> Metrics provide some higher-level information for both stateless and stateful engine types. For more information, see AWS Network Firewall metrics in Amazon CloudWatch.

You can record flow logs and alert logs from your Network Firewall stateful engine.

- Flow logs are standard network traffic flow logs. Each flow log record captures the network flow for a specific 5-tuple.
- Alert logs report traffic that matches your stateful rules that have an action that sends an alert. A stateful rule sends alerts for the rule actions `DROP` and `ALERT`.

aws © 2022, Amazon Web Services, Inc. or its affiliates.

마무리 :

오늘로 끝내지 말고 좀 더 욕심내보세요.

© 2022, Amazon Web Services, Inc. or its affiliates.

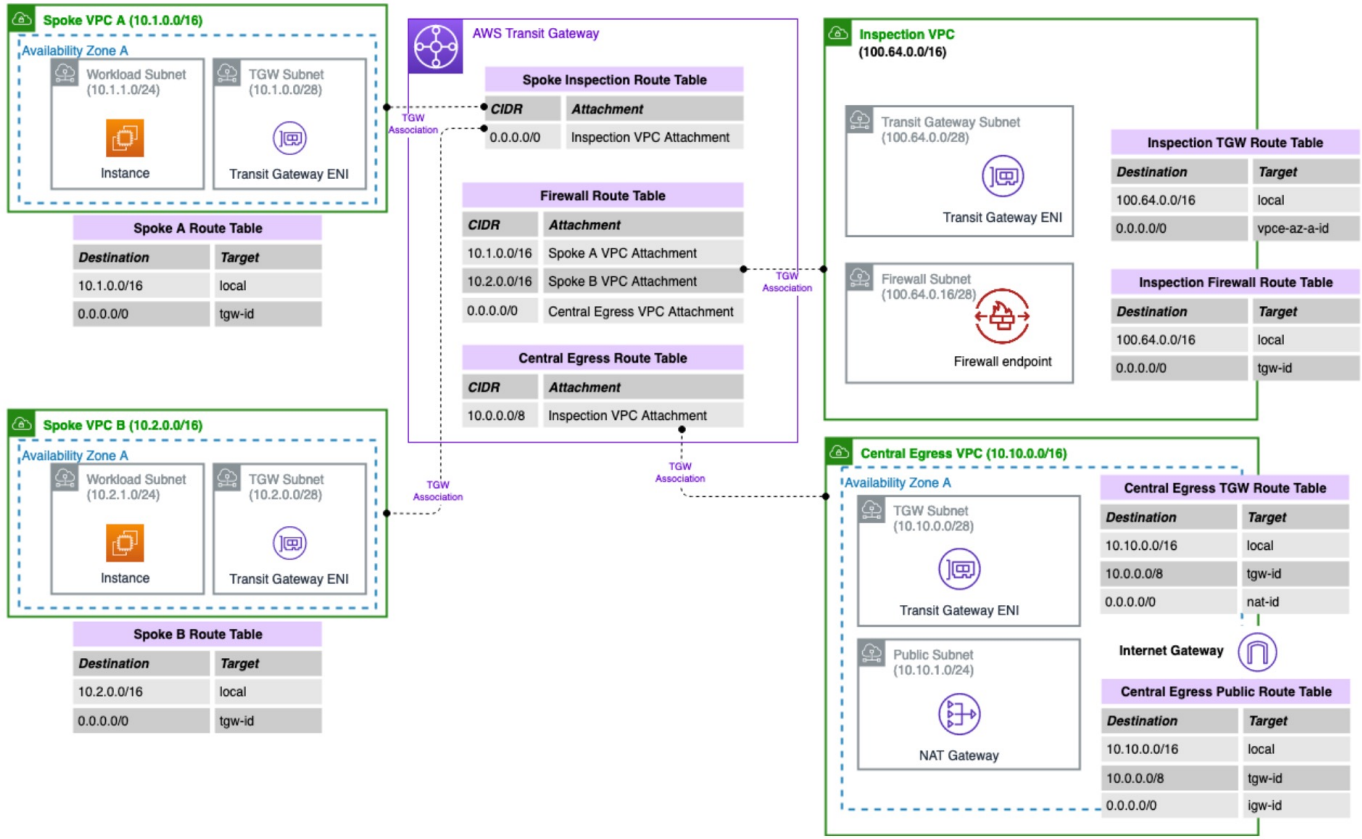
네트워크 방화벽을 익히기 좋은 워크샵 - 아키텍처편# 1

https://catalog.us-east-1.prod.workshops.aws/workshops/d071f444-e854-4f3f-98c8-025fa0d1de2f/en-US/lab-three

Hands-on Network Firewall Workshop

- **Step Five:** Configure the Transit Gateway Route Tables

At the end of this lab you will have created the architecture in the diagram below.



aws ©

네트워크 방화벽을 익히기 좋은 워크샵 - 방화벽 정책# 2

https://catalog.workshops.aws/networkfirewall/en-US

AWS Network Firewall Workshop

- Introduction
- Setup
  - Distributed Deployment Model
  - Centralized Deployment Model
- Labs
  - **Lab 1 - Verify Firewall Resources**
  - Lab 2 - Egress Web Filtering
  - Lab 2.1 - Egress DNS Query filtering
  - Lab 3 - Using Open Source rules with AWS Network Firewall
  - Lab 4 - Threat Hunting with AWS Network Firewall
  - Lab 5 (Optional): Ingress Traffic Inspection - DIY
  - Lab 6 (Optional): Custom Surricata rules with Strict Rule ordering
- Cleanup

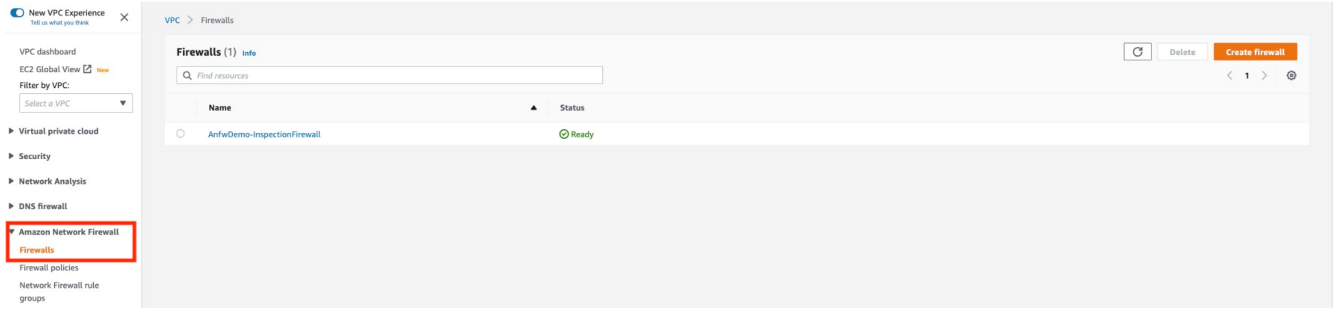
AWS Network Firewall Workshop > Labs > Lab 1 - Verify Firewall Resources

Lab 1 - Verify Firewall Resources

Step 1 - List Firewalls

Since we have already provisioned an AWS Network Firewall as part of our Setup instructions, let's verify the policy and rule groups created by CloudFormation template.

- Amazon Network Firewall is listed under VPC in the AWS web console:



- In the AWS Web Console, click on VPC -> Firewalls to list the currently provisioned Firewalls. If your region is listed below, you can click on the desired region tab below to access the Network Firewall console: