



F5 Distributed Cloud WAAP 構成概要

F5ネットワークスジャパン合同会社

2024/3

本資料の注意点

- 本資料は、資料作成時点のサービス内容およびライセンスに基づいて記載しています。最新の情報は、F5 Distributed Cloud Servicesの[公式サイト](#)を参照ください
- 技術的な内容に関するお問い合わせは、ご契約済みのお客様はサポート窓口、それ以外のお客様は当社営業/SE、または[問い合わせ窓口](#)までご連絡ください。

アジェンダ

















- F5 Distributed Cloud Servicesの概要
- HTTP Load Balancerの概要
- WAAP(WAF)機能の概要

F5 Distributed Cloud Services (略称XC)

1 Application Security Service

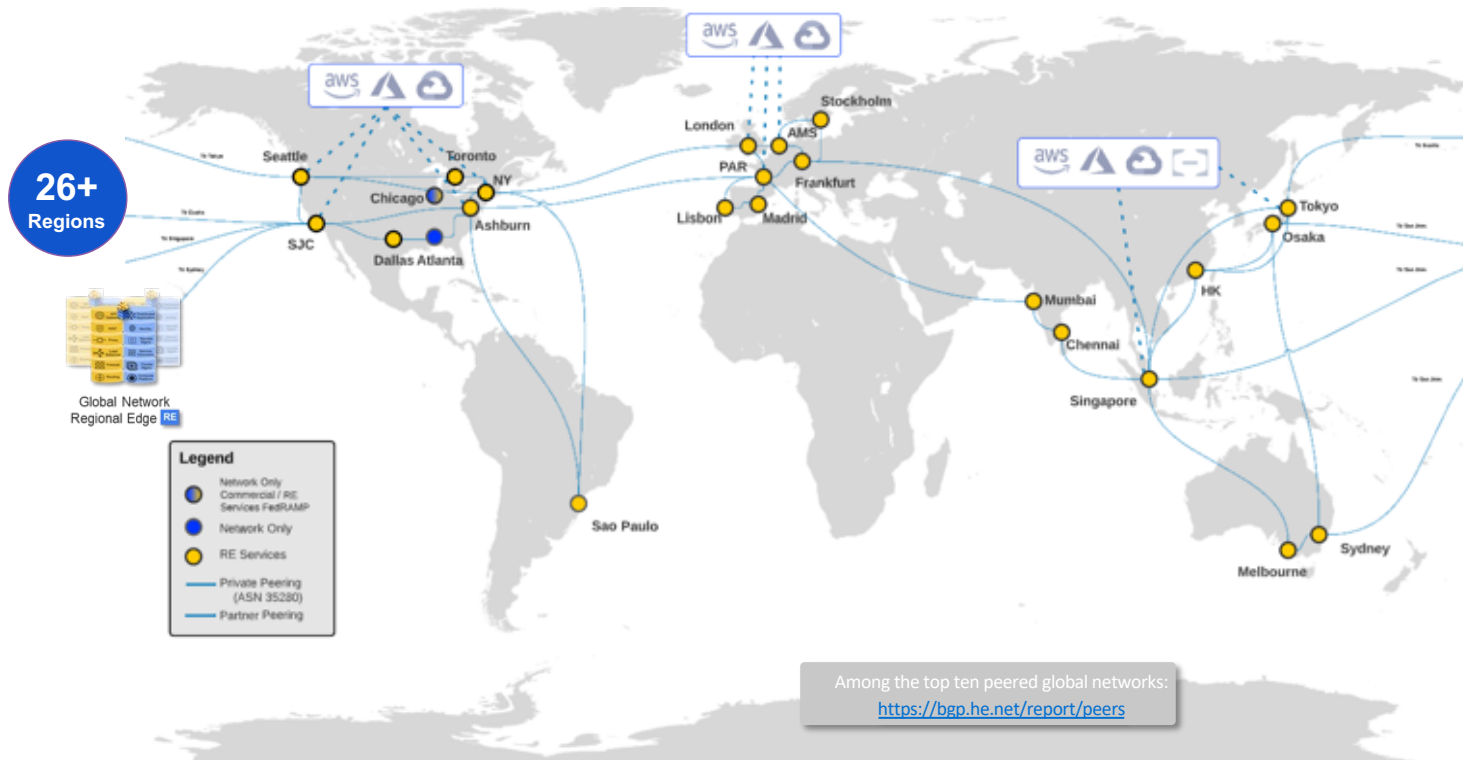
2 Multi Cloud Networking/Network As A Service

3 Managed Kubernetes

 Multi-Cloud Network Connect > Networking & security across clouds, edge and on-premises	 Distributed Apps > Deploy apps in our global PoPs (REs) or your cloud/edge sites	 Content Delivery Network > Optimize asset delivery with content caching	 DNS Management > Configure and manage primary or secondary DNS service
 Multi-Cloud App Connect > Connect apps across clouds, edge and on-premises using Load Balancers	 Web App & API Protection > Create a proxy and configure WAF, Bot, and API security services for your apps	 DDoS & Transit Services > Secure your infrastructure and apps against L3/L4 DDoS attacks	 Bot Defense > Deploy bot mitigation for F5 BIG-IP and other 3rd party services
 Application Traffic Insight > Recognize and monitor all client devices that access your applications	 Client-Side Defense > Preview Monitor and mitigate fraudulent app requests at the client devices	 NGINX One > Private Preview View, monitor, secure, and configure your NGINX fleet.	 Observability > Easily monitor your critical applications and systems from regions around the world
 Shared Configuration > Create and manage shared configuration objects	 Audit Logs & Alerts > Review logs and manage alerts	 Billing > Manage billing and payment settings	 Administration > Manage tenant settings, users and personal account

Additional services available

F5 XC ネットワークの特徴



17+ Tbps capacity
(Tier-1 Carriers: NTT, Telia, Level3)

Multi-Tbps private backbone
(Zayo, Telia, CenturyLink)

Dedicated connectivity
(Cloud providers, SaaS providers)



Customer Edge

お客様の任意のサイト
(オンプレミス/パブリッククラウド) を
F5XCのリージョンとして構成可能

XC WAAPの構成要素

WAAPの各機能は、**HTTP Load Balancer**の上で動作
(※L3/L4DDoS Protectionの機能は、Regional Edge基盤に実装)

App Firewall
(WAF)

Bot Defense
(Shape based
function)

DDoS Protection
(L7)

API Security

HTTP Load Balancer

DDoS Protection
(L3/L4)

HTTP LBの概要

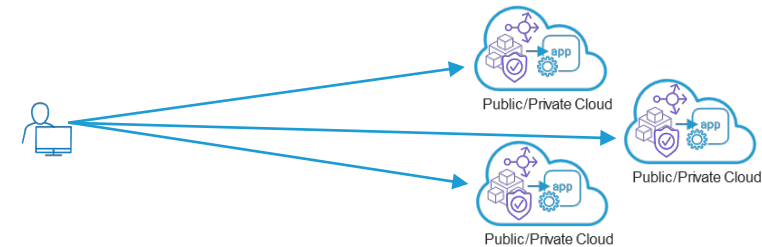
HTTP Load Balancerが動作する場所

Regional Edge (RE)



- F5のRE上で動作
- 使用するIPアドレスは、F5のRE上で提供されるIP
- BGP AnycastによるIP広報
※BYOIPもオプションで提供可能
- L3/L4 DDoS対策が自動的に適応
(モニタリング機能はなし)

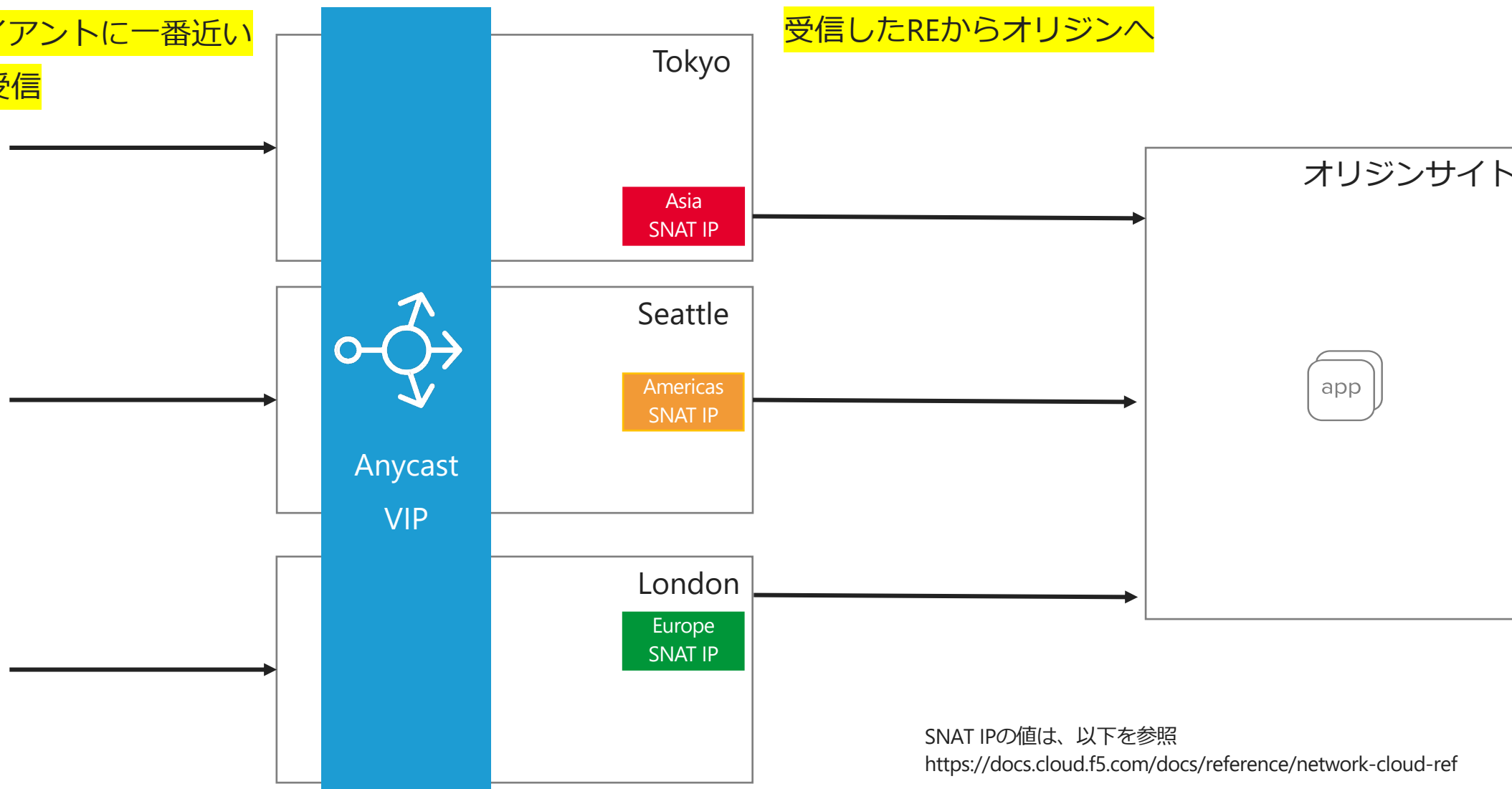
Customer Edge (CE)



- お客様サイト上に構築したXC Meshノード上で動作
- 使用するIPアドレスは、XC Meshノードに割り当てられたお客様サイトのIPアドレス
- L3/L4 DDoS対策機能は無し
オプションのDDoS Protectionサービスが必要
(RE上のDDoS緩和設備を利用するサービス)

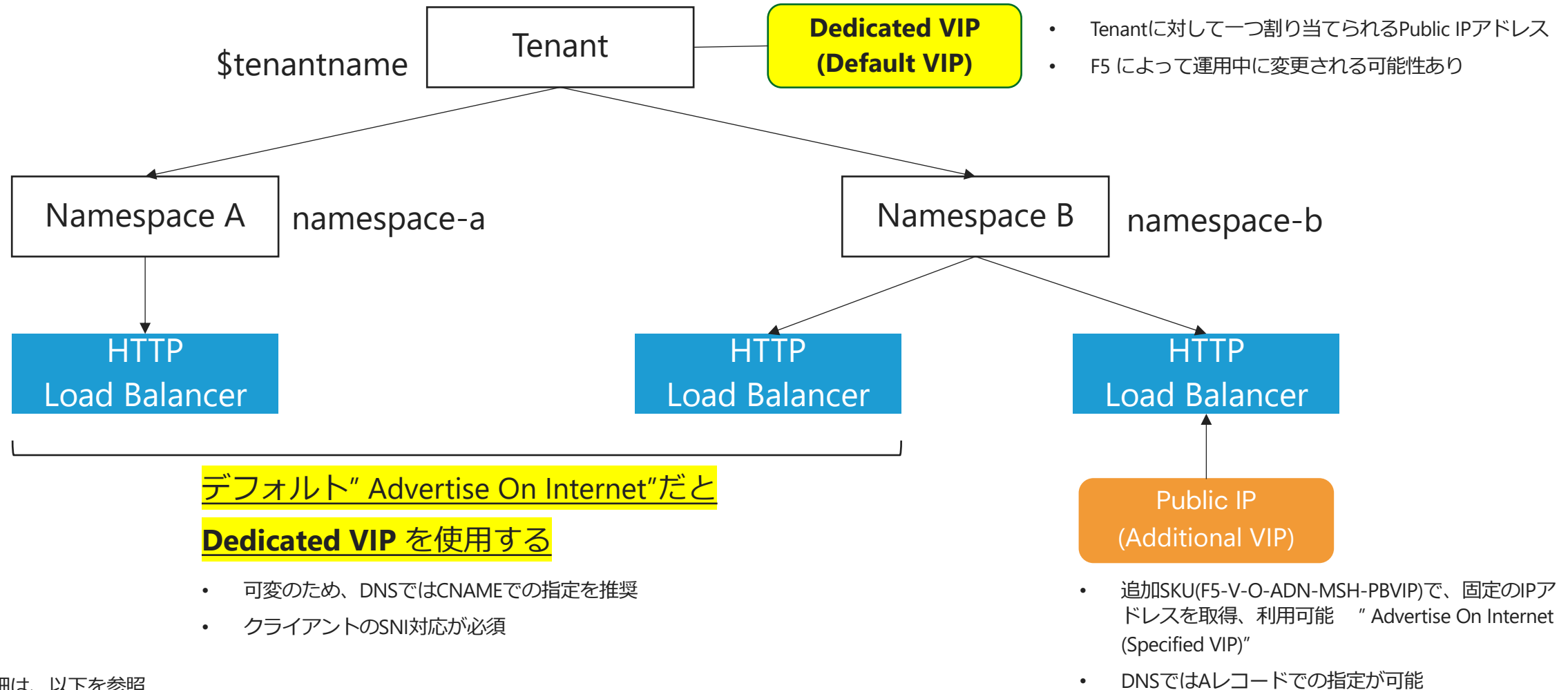
BGP AnycastによるSNAT (HTTP LB on RE)

クライアントに一番近い
REで受信



SNAT IPの値は、以下を参照
<https://docs.cloud.f5.com/docs/reference/network-cloud-ref>

HTTP LBが使用するVIPの種類(HTTP LB on RE)

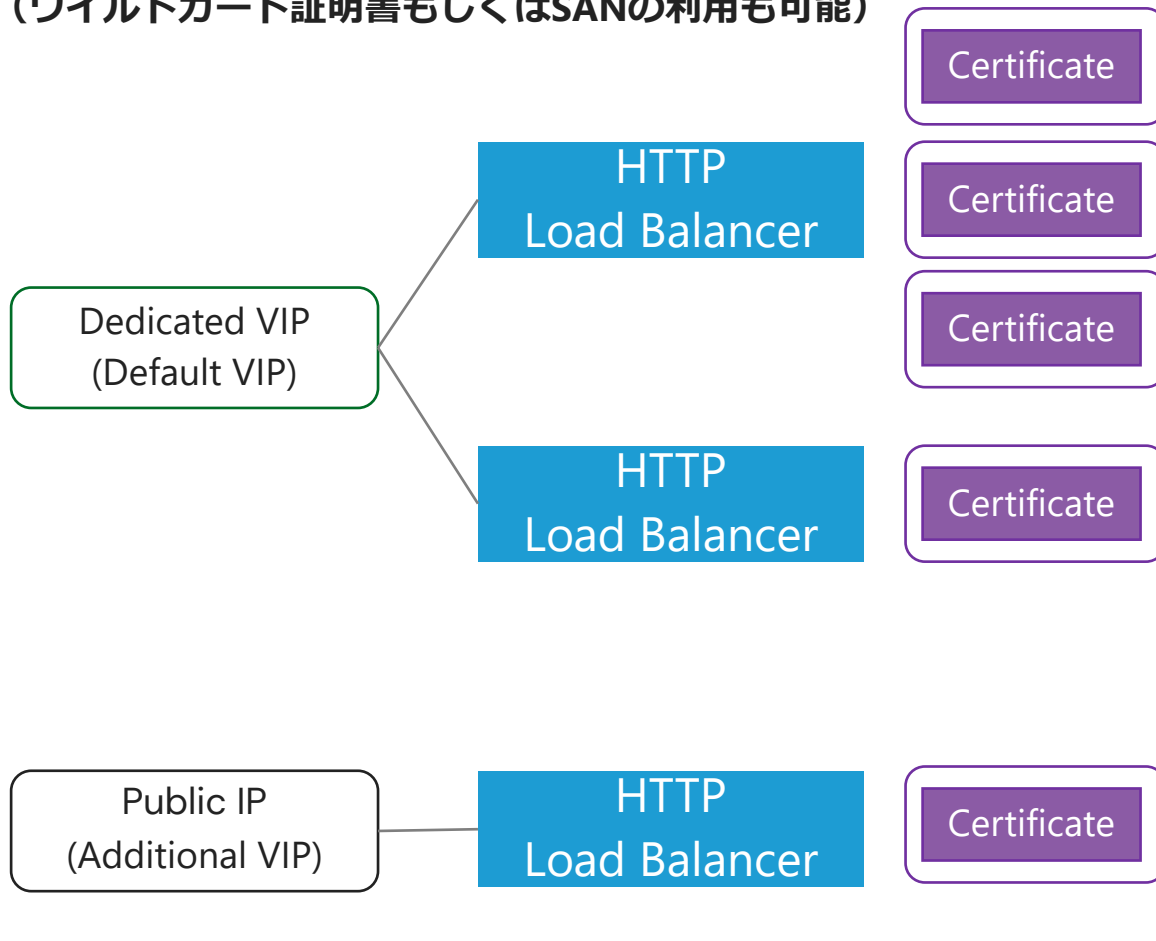


詳細は、以下を参照

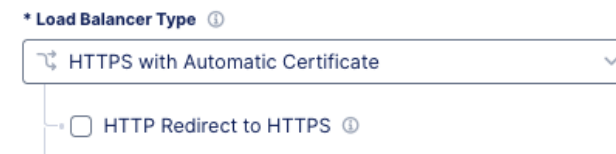
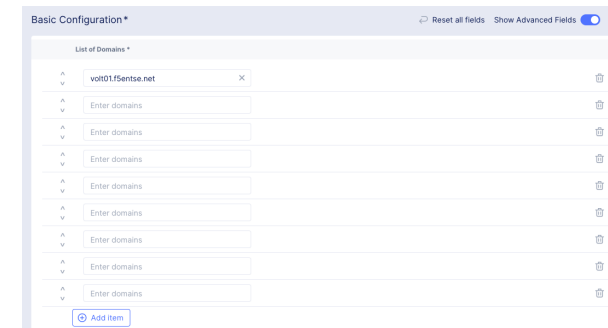
<https://docs.cloud.f5.com/docs/reference/f5dcs-public-vips>

VIP とLoad BalancerとFQDNとSSLサーバ証明書

1つのLBで、複数(32個まで)のSSLサーバ証明書を保持可能
(ワイルドカード証明書もしくはSANの利用も可能)



1つのHTTP Load Balancerに収容できるFQDNは32個まで
(ワイルドカード指定を含む。例: *.domain.com)



一つのLB内で、HTTP/HTTPSの共存は不可(同一プロコルでのマルチポートはサポート)。
HTTPSのLBとして、HTTP->HTTPSリダイレクトさせることは可能

DNSによるトラフィック誘導

お客様DNSサーバでの誘導

- HTTP Load Balancerで使用しているVIPに対応する“Host Name”(ves-io-xxxx.ves.io)をCNAMEレコードとして、お客様が管理するDNSサーバへ登録。

※Public IP(Additional VIP)を使用している場合、もしくはCEで固定IPを使用している場合はAレコードでの登録も可

DNSレコード設定例

<input type="checkbox"/>	volt02.f5entse.net	CNAME	シンプル	-	ves-io-1ab972ff-1e45-4c0b-8e1c-7e6e139e5b3b.ac.vh.ves.io
--------------------------	--------------------	-------	------	---	--

XC Primary DNSへのゾーン委任

- XC Primary DNSにて、対象ドメインのゾーンを作成 (“Allow HTTP Load Balancer Managed Records”を有効)
- 以降、新規作成したHTTP LBに設定した当該ドメインのFQDNのAレコードがXCのDNS内で自動生成される (Aレコードとして生成)
- お客様が管理するDNSサーバ(もしくはレジストラ)へは、対象ドメインのNSレコードとして、F5 XC Primary DNS Nameサーバ群を登録

DNSレコード設定例

<input checked="" type="checkbox"/>	Record name	Type	Routin...	Differ...	Alias	Value/Route traffic to
<input checked="" type="checkbox"/>	volt01.f5entse.net	NS	Simple	-	No	ns1.f5clouddns.com ns2.f5clouddns.com

SSLサーバ証明書管理

Custom Certificate

- サードパーティ認証局で発行されたSSLサーバ証明書と秘密鍵を、HTTP Load Balancerに登録

Automatic Certificate

- F5 XCにて、Let's EncryptのSSLサーバ証明書を発行し管理し、自動更新まで実施
- DNSのゾーンを、XC Primary DNSへ委任しているか、していないかで手順が異なる

<https://docs.cloud.f5.com/docs/ves-concepts/load-balancing-and-proxy#automatic-certificate-generation>

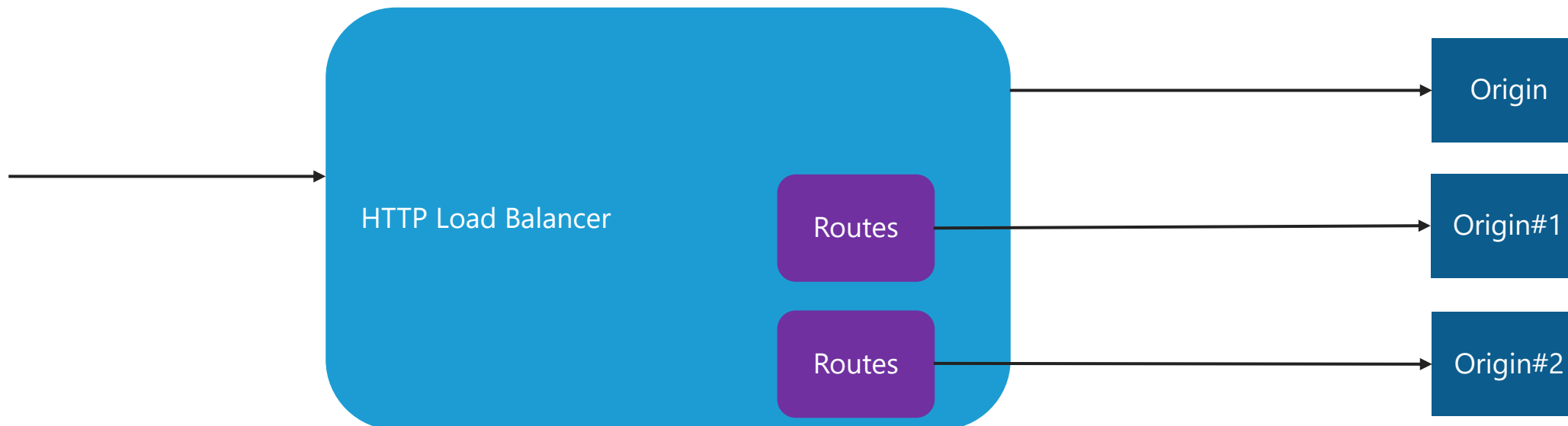
一つのLB内で、Custom Certificateと、Automatic Certificateの共存は不可

Routes機能

基本的な、HTTP-LBとOriginの関係



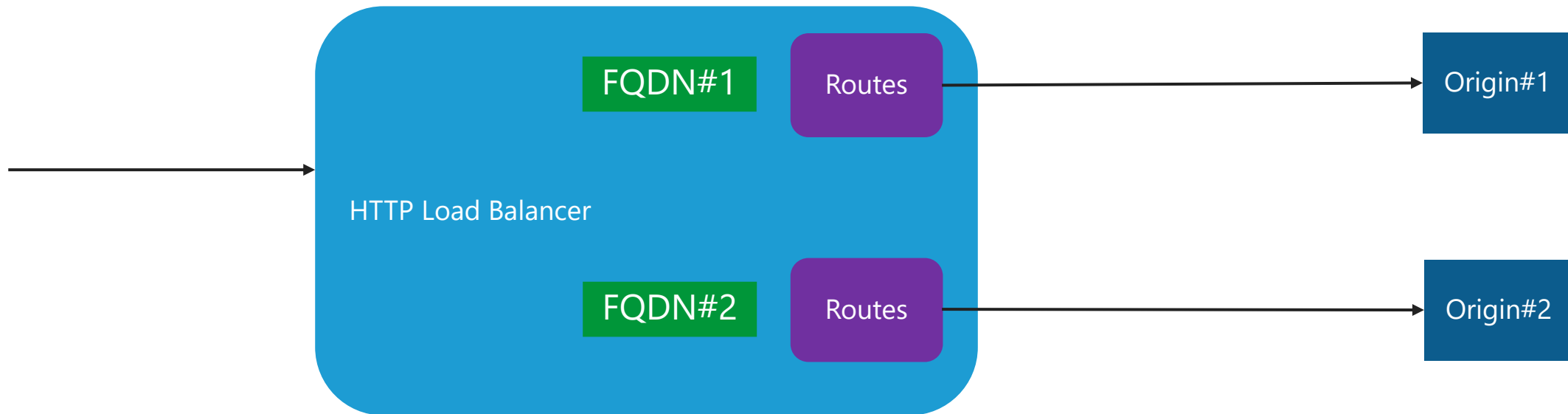
Routes機能を使ったL7条件ベースルーティング
(Method/Path/Header/Port)



Routes機能を使用した複数FQDN収容時のOriginの振り分け

Routes機能で、Host Headerを元に、振り分け先のOriginを決定

本設定により、複数サイトを一つのHTTP Load Balancerに収容し、運用可能



WAAP(WAF)設定の概要

WAAP設定内容と関連オブジェクト

HTTP Load Balancer

Web Application Firewall

- WAF Exclusion Rules
- Data Guard Rules
- Cross-Site Request Forgery Protection
- GraphQL Inspection
- Cookie Protection

Bot Defense

API Protection

DoS Protection

Common Security Controls

- IP Reputation
- Malicious User Detection
- Rate Limiting

App Firewall

Enforcement Mode (Blocking/Monitoring)

Detection Settings

- Security Policy
- Signature-Based Bot Protection

Advanced configuration

- Allowed Response Status Code
- Mask Sensitive Parameters in Logs
- Blocking Response Page

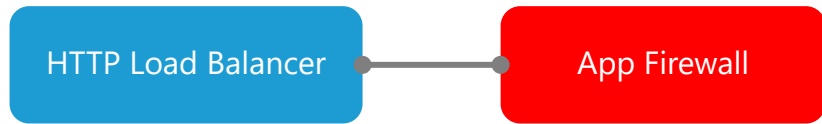
Service Policy

Action

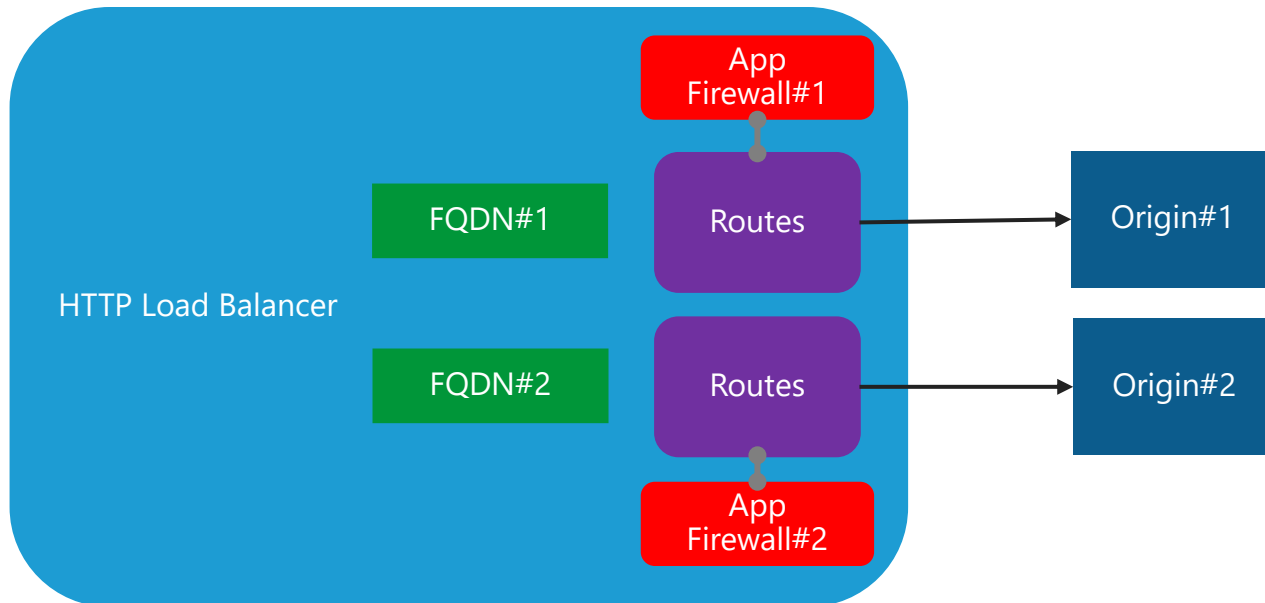
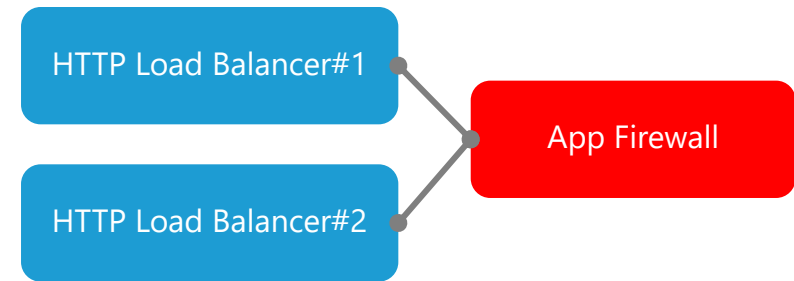
- Allow/Deny
- App Firewall Action
 - Skip
 - Detection Control
- Bot Action(Skip)
- Malicious User Mitigation Action(Skip)

HTTP Load BalancerとApp Firewallの関係

- ① HTTP Load Balancer本体には1つのApp Firewallが設定可能
- ③ App Firewallは複数のHTTP Load Balancer、Routesに設定が可能

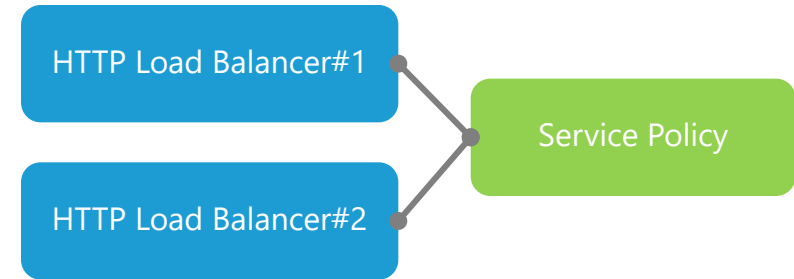
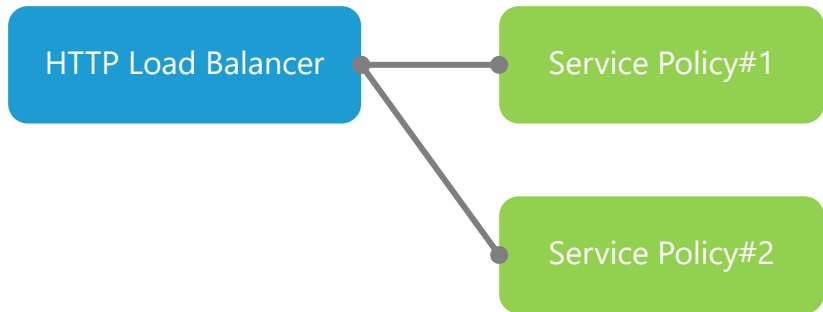


- ② HTTP Load BalancerのRoute設定ごとに、別々のApp Firewallを設定可能



HTTP Load BalancerのService Policyの関係

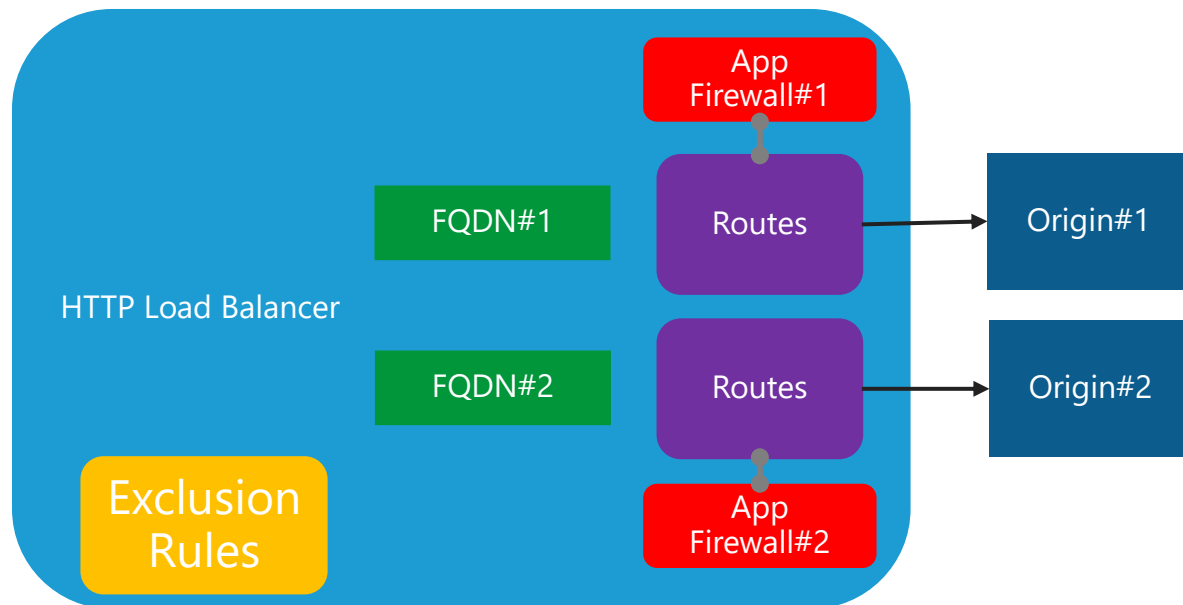
- ① HTTP Load Balancer本体には複数のService Policyが設定可能 ② Service Policyは複数のHTTP Load Balancerに設定が可能



Service Policy自体、または一つのService Policyの中のRuleごとに、適応する条件（Host名や、HTTP Headerや、PATH、送信元など）が指定されるので、実際の設定内容が発動のは条件が合致した場合のみとなる

App Firewallの除外設定

① HTTP Load Balancer本体での除外設定



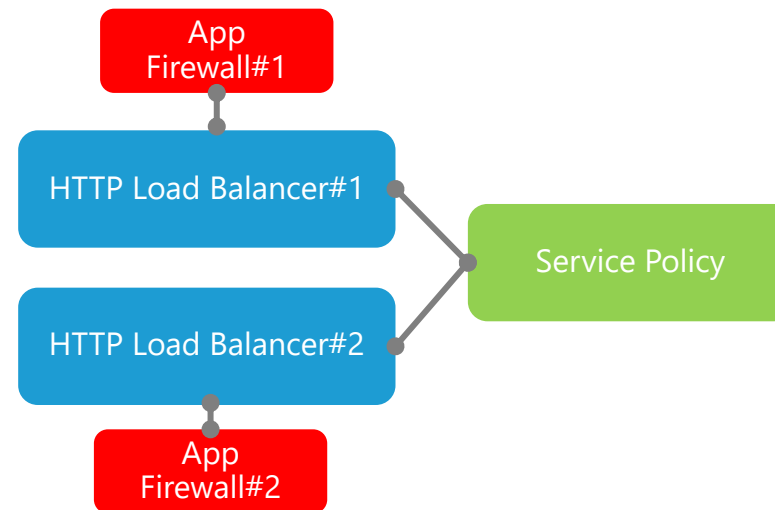
条件: Domain/PATH/Method

Action:

Detection Control (Signature ID / Violation Type / Bot Names)

Skip

② Service Policyでの除外設定



Service Policy内のRuleとして、左と同じ除外設定が定義可能

