The bridge to possible

Traffic Inspection in Azure using Cisco Secure Firewall and Gateway Load Balancer

Sameer Singh, Technical Marketing Engineer – Network Security

BRKSEC-2109

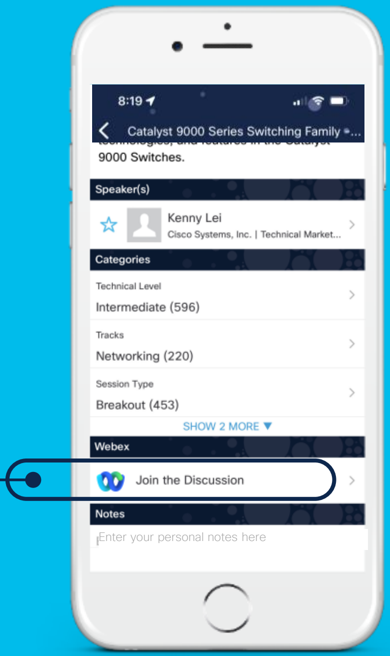
Cisco Webex App

Questions?

Use Cisco Webex App to chat
with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click "Join the Discussion"
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space



8:19

Catalyst 9000 Series Switching Family ...

9000 Switches.

Speaker(s)

Kenny Lei
Cisco Systems, Inc. | Technical Market...

Categories

Technical Level
Intermediate (596)

Tracks
Networking (220)

Session Type
Breakout (453)

SHOW 2 MORE ▼

Webex

Join the Discussion

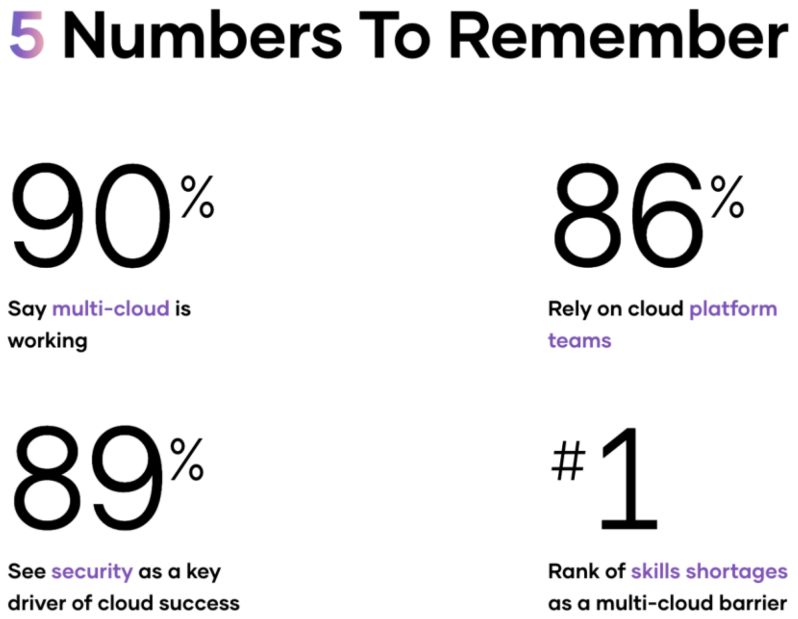
Notes

Enter your personal notes here

Webex spaces will be moderated until February 24, 2023.

Welcome to the Multi-Cloud Era

HashiCorp 2022 State of Cloud Strategy Survey



5 Numbers To Remember

90%
Say multi-cloud is working

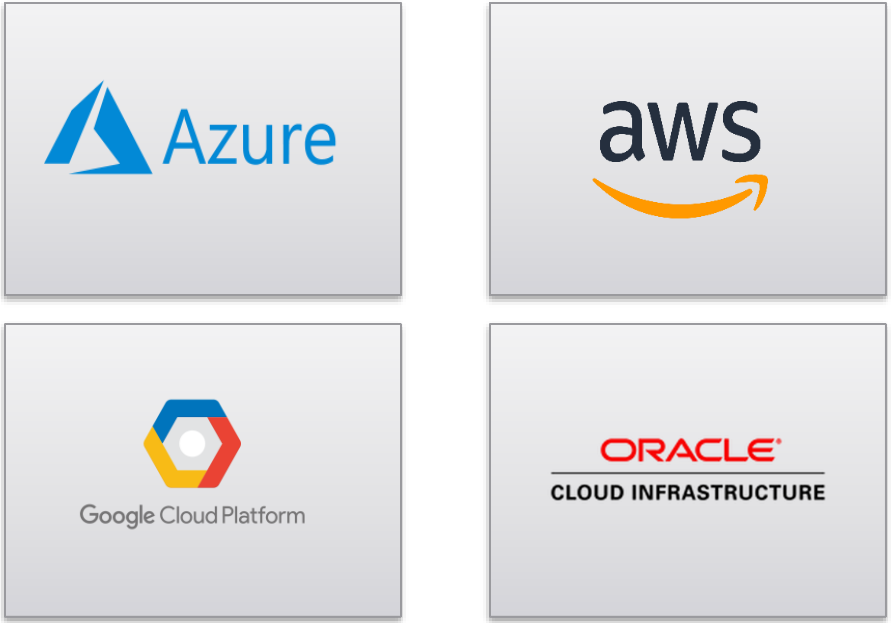
86%
Rely on cloud platform teams

94%
Are wasting money in the cloud

89%
See security as a key driver of cloud success

#1
Rank of skills shortages as a multi-cloud barrier

Major Cloud Providers



Abstract

In this session, we will see how the introduction of Gateway load balancer in Azure **simplifies the insertion** of Cisco Secure firewall in the Azure environment. We will look at the different components of the solution, how it can leverage autoscaling and addresses some of the current challenges.

Agenda

- Azure Load Balancers
- Load Balancer Challenges
- Gateway Load Balancer
- Configuration Overview
- Demo
- Automation and Auto scale Solution Overview
- Key Takeaway

About the Speaker

Sameer Pratap Singh

- Degree in Electronics and Communication Engineering
- Security Solutions Consulting Engineer till 2021
- Technical Marketing Engineer – Network Security
- CCIE Security
- Interested in everything automation

Cisco Webex App

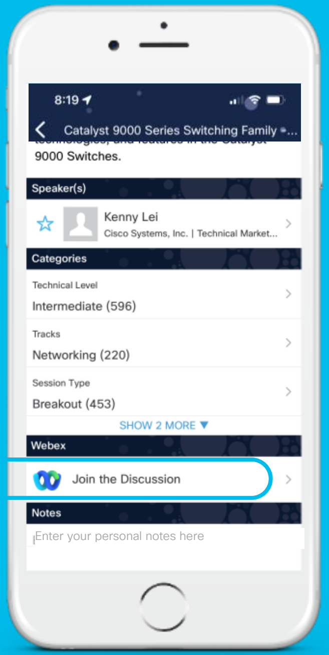
Questions?

Use Cisco Webex App to chat
with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex Spaces will be moderated until February 24, 2023.



8:19

Catalyst 9000 Series Switching Family ...

9000 Switches.

Speaker(s)

☆ Kenny Lei
Cisco Systems, Inc. | Technical Market...

Categories

Technical Level
Intermediate (596)

Tracks
Networking (220)

Session Type
Breakout (453)

SHOW 2 MORE ▼

Webex

Join the Discussion

Notes

Enter your personal notes here

https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2109

Important: Hidden Slide Alert

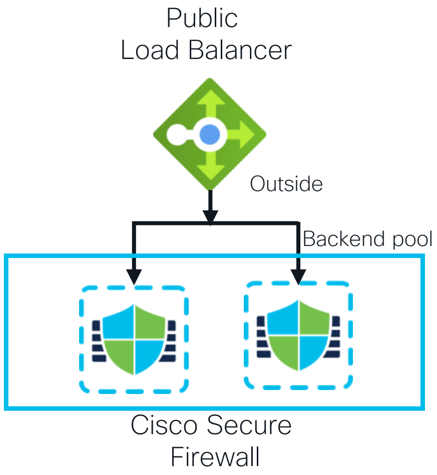
Look for this “For Your Reference” Symbol in your PDF’s

There is a tremendous amount of hidden content, for you to use later!

Azure Load Balancers Overview

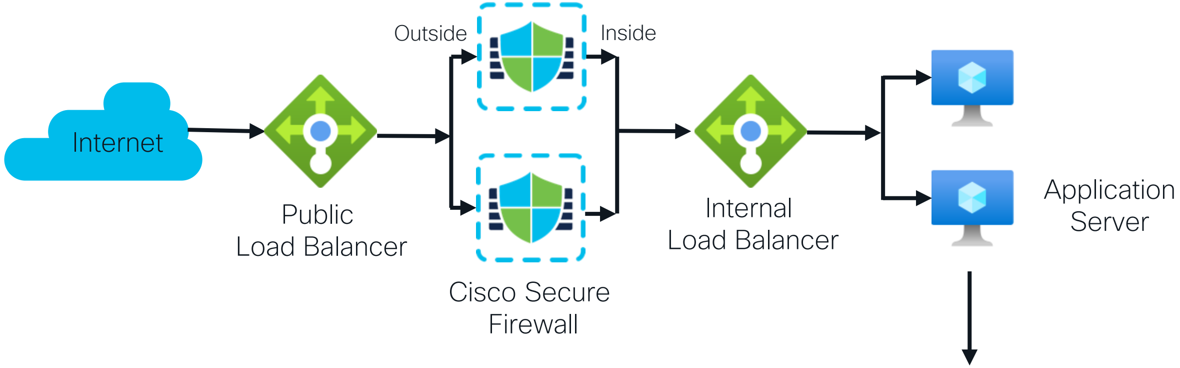
Azure – Standard Load Balancers

- Acts as a single point of contact and distributes incoming traffic across multiple instances
- Load Balancing rules decide traffic flow
- Improves scalability and availability of applications
- Health probes periodically check the health of the backend instances
- Types - Public and Internal Load Balancers



Standard Load Balancer Deployment
with **Cisco Secure Firewall**

- The original Initiator IP Address is unknown to the target application
- NAT and Route need to be configured on the firewall

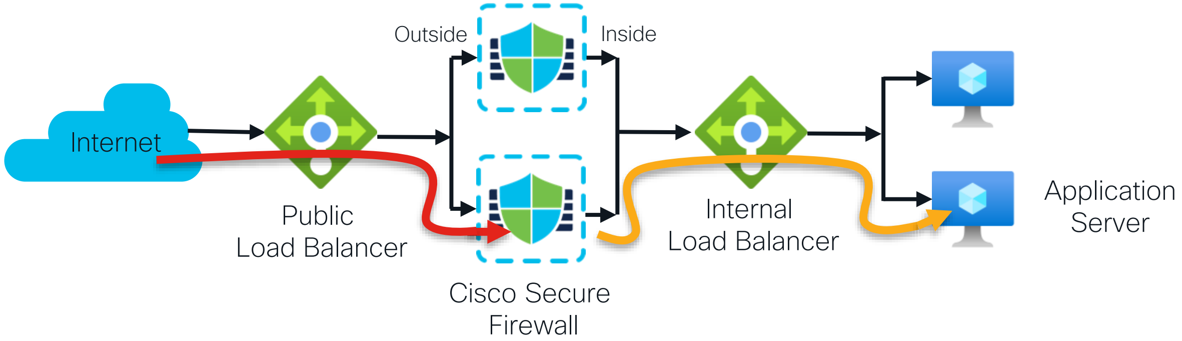


Original Source IP missing

Source IP	Destination IP
FTD Inside Interface IP Address	Application Server IP Address

Standard Load Balancer Deployment

with **Cisco Secure Firewall**



Source IP	Destination IP
Client IP	Public Load Balancer Frontend IP

Source IP	Destination IP
Client IP	Cisco Secure Firewall Outside Interface IP

NAT

Source IP	Destination IP
Cisco Secure Firewall Inside Interface IP	Internal Load Balancer frontend IP

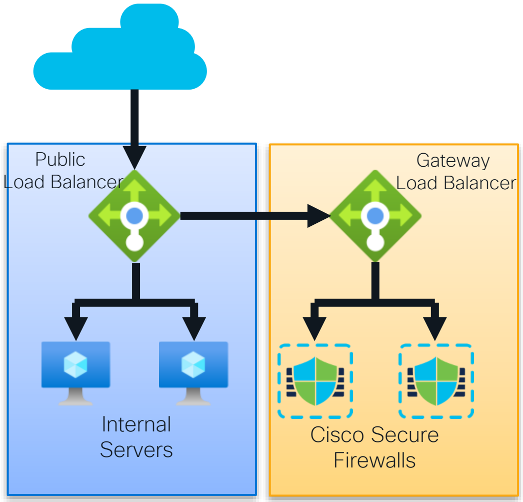
Source IP	Destination IP
Cisco Secure Firewall Inside Interface IP	Application Server IP

Standard Load Balancer Challenges

- Management Overhead
- The Source IP address of the packet is hidden
- Might Require to rearchitect the environment
- Operational Complexity

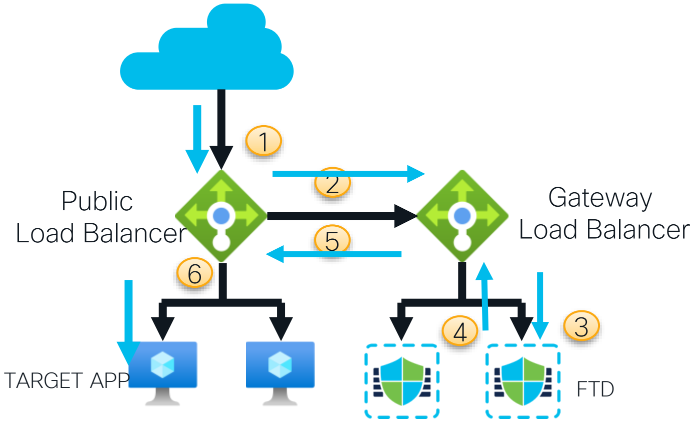
Azure - Gateway Load Balancer

- A load balancer solution which simplifies insertion of network firewall service in Azure environment.
- Transparent insertion of firewalls.
- Redirection with VXLAN protocol
- Firewall receives and forwards traffic through the same interface



Bump-in-the-wire

Traffic Flow



Source IP: Original Initiator IP Address
Destination IP: Application Server IP Address

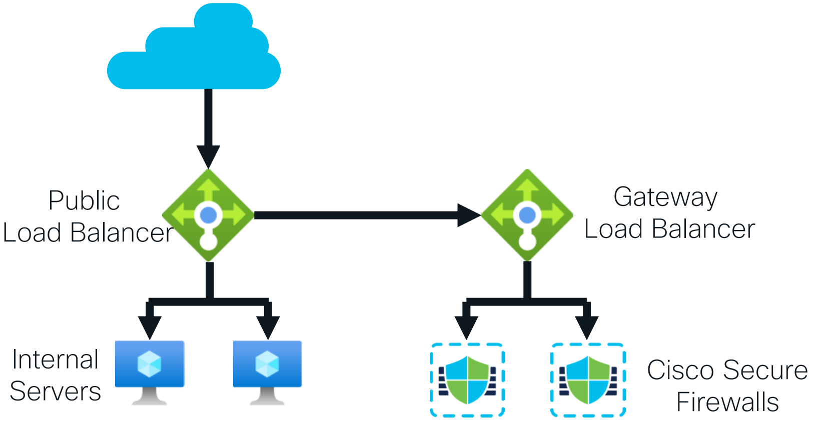
- **NAT not required to be configured on the firewall**
- GWLB maintains flow stickiness to a specific instance in the backend pool

1. Inbound traffic reached the Public IP of the load balancer
2. Load balancer forwards the traffic to the Gateway Load balancer
3. GWLB forwards the traffic to one of the firewall instances in the backend pool for inspection
4. Firewall returns inspected traffic to GWLB
5. GWLB returns traffic to the load balancer
6. Load balancer forwards it to the internal server

Service Chaining

- GWLB can be Chained to

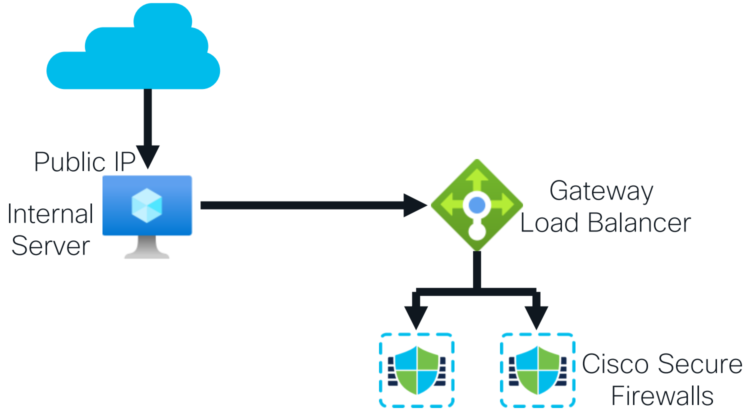
A Standard Public Load Balancer



Service Chaining

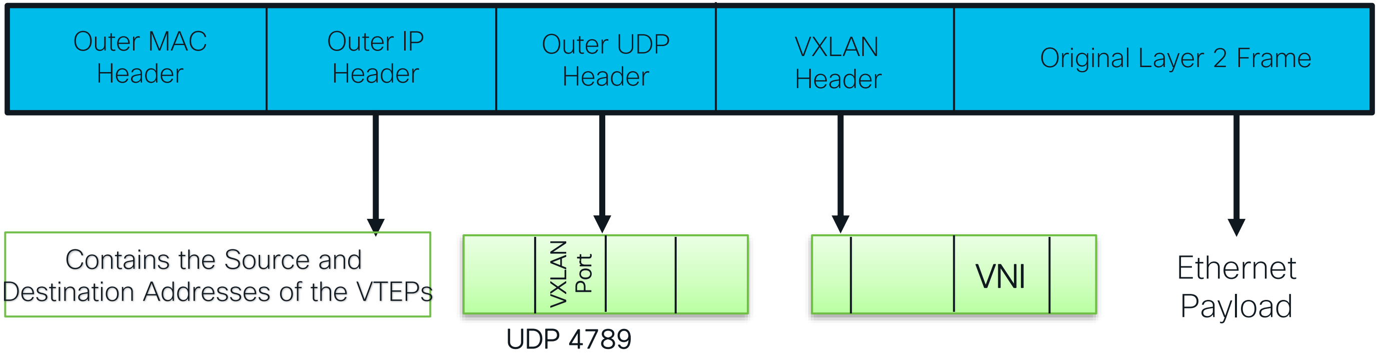
- GWLB can be Chained to

A Standard Public IP attached to a Virtual Machine



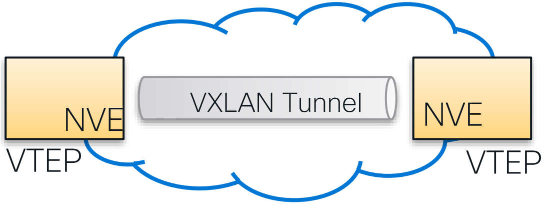
Virtual Extensible LAN (VXLAN) - Overview

- Provide VLAN functionality with greater extensibility and flexibility
- Extends layer 2 segments over the underlying layer 3 network infrastructure
- The transport protocol used is IP plus UDP
- Mac-in-UDP encapsulation scheme



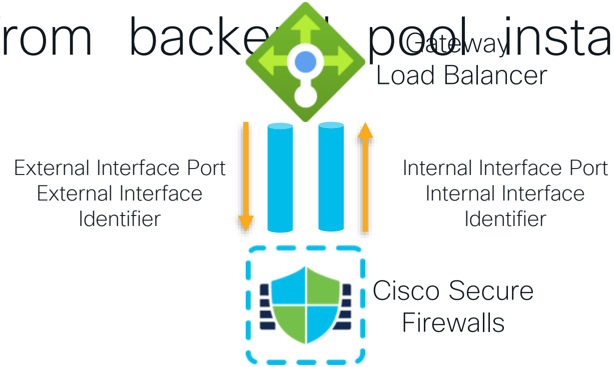
VXLAN Components

- Network Virtualization Edge (NVE) - Logical interface where the encapsulation and decapsulation occur
- VXLAN Tunnel Endpoint (VTEP) - This is the device that does the encapsulation and decapsulation
- VXLAN Network Identifier (VNI) – 24-bit segment ID that defines the broadcast domain. Interchangeable with "VXLAN Segment ID"

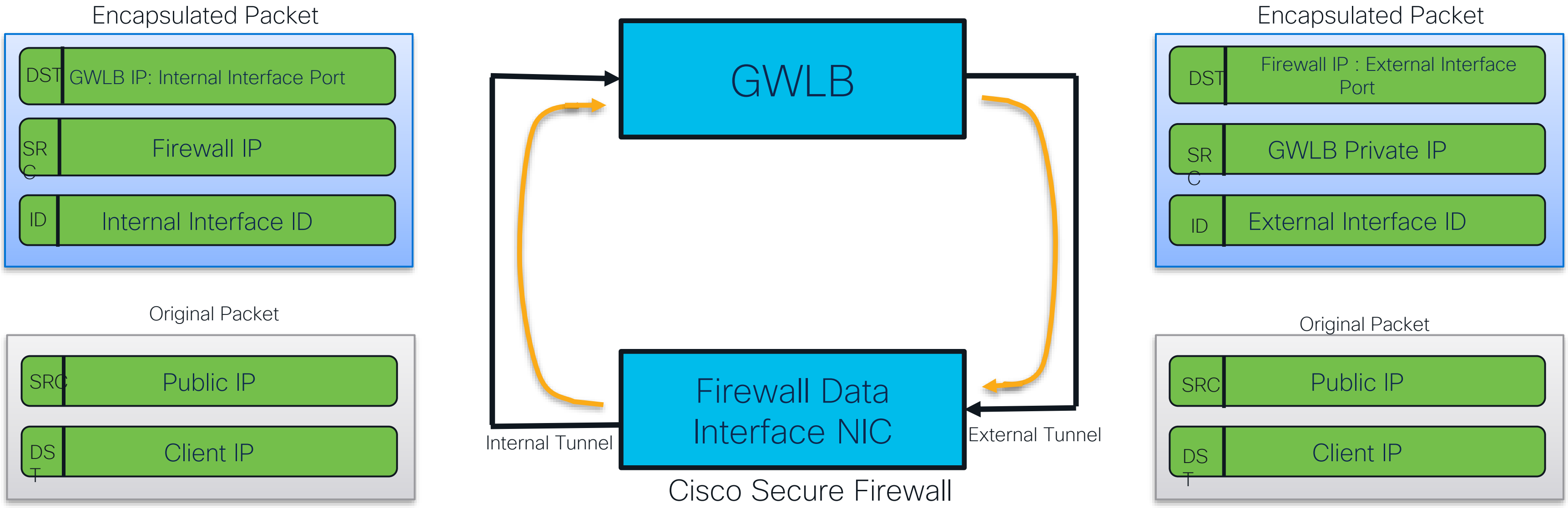


GWLB VXLAN Tunnels

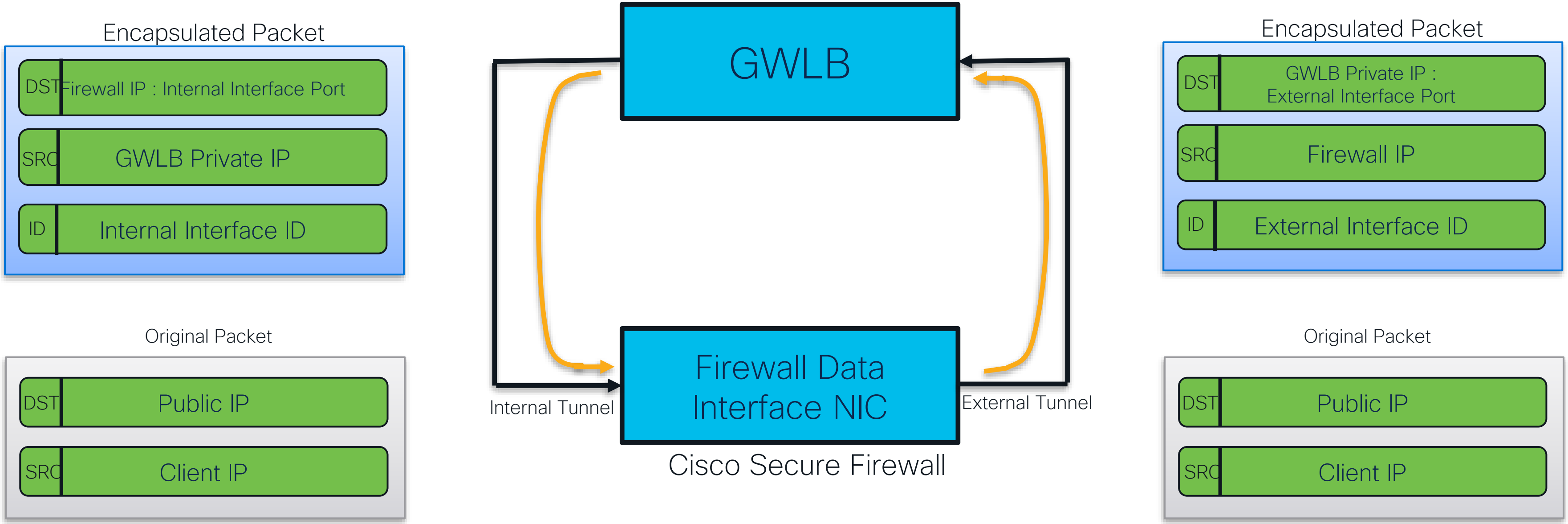
- Azure GWLB uses two VXLAN tunnels to communicate with its backend pool
- External Tunnel for untrusted traffic from GWLB to backend pool instance
- Internal Tunnel for trusted traffic from backend pool instance to GWLB
  - Each Tunnel uses a different UDP Port
  - Each Tunnel uses a different VNI



Traffic to the Client



Traffic from the Client



Encapsulated Packet

DST Firewall IP : Internal Interface Port

SRC GWLB Private IP

ID Internal Interface ID

Original Packet

DST Public IP

SRC Client IP

GWLB

Firewall Data Interface NIC

Cisco Secure Firewall

Internal Tunnel

External Tunnel

Encapsulated Packet

DST GWLB Private IP : External Interface Port

SRC Firewall IP

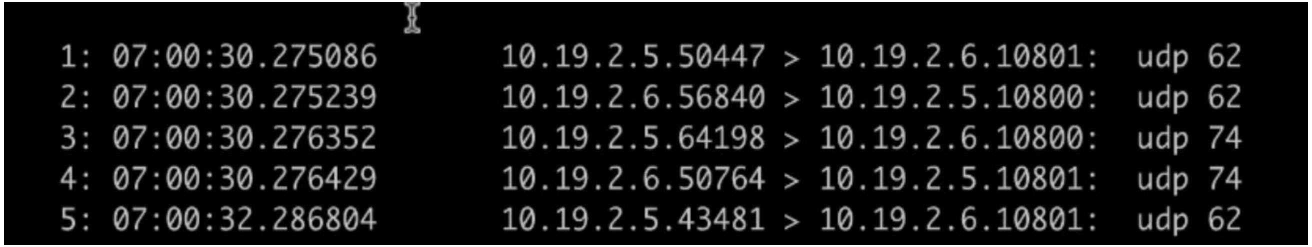
ID External Interface ID

Original Packet

DST Public IP

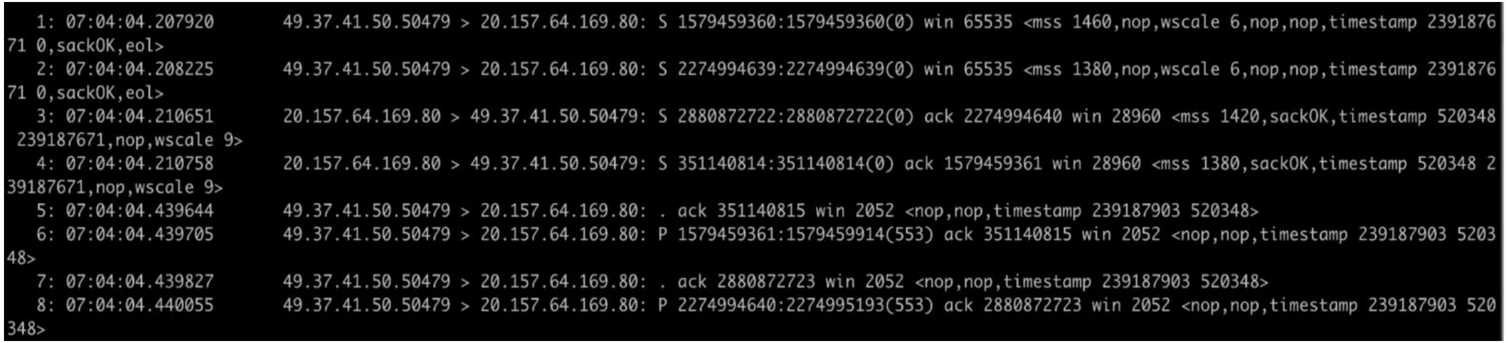
SRC Client IP

Encapsulated packets on the VTEP interface



```
  1: 07:00:30.275086       10.19.2.5.50447 > 10.19.2.6.10801:  udp 62
  2: 07:00:30.275239       10.19.2.6.56840 > 10.19.2.5.10800:  udp 62
  3: 07:00:30.276352       10.19.2.5.64198 > 10.19.2.6.10800:  udp 74
  4: 07:00:30.276429       10.19.2.6.50764 > 10.19.2.5.10801:  udp 74
  5: 07:00:32.286804       10.19.2.5.43481 > 10.19.2.6.10801:  udp 62
```

Original packets on the VNI interface



```
   1: 07:04:04.207920       49.37.41.50.50479 > 20.157.64.169.80: S 1579459360:1579459360(0) win 65535 <mss 1460,nop,wscale 6,nop,nop,timestamp 2391876
71 0,sackOK,eol>
   2: 07:04:04.208225       49.37.41.50.50479 > 20.157.64.169.80: S 2274994639:2274994639(0) win 65535 <mss 1380,nop,wscale 6,nop,nop,timestamp 2391876
71 0,sackOK,eol>
   3: 07:04:04.210651       20.157.64.169.80 > 49.37.41.50.50479: S 2880872722:2880872722(0) ack 2274994640 win 28960 <mss 1420,sackOK,timestamp 520348
 239187671,nop,wscale 9>
   4: 07:04:04.210758       20.157.64.169.80 > 49.37.41.50.50479: S 351140814:351140814(0) ack 1579459361 win 28960 <mss 1380,sackOK,timestamp 520348 2
39187671,nop,wscale 9>
   5: 07:04:04.439644       49.37.41.50.50479 > 20.157.64.169.80: . ack 351140815 win 2052 <nop,nop,timestamp 239187903 520348>
   6: 07:04:04.439705       49.37.41.50.50479 > 20.157.64.169.80: P 1579459361:1579459914(553) ack 351140815 win 2052 <nop,nop,timestamp 239187903 5203
48>
   7: 07:04:04.439827       49.37.41.50.50479 > 20.157.64.169.80: . ack 2880872723 win 2052 <nop,nop,timestamp 239187903 520348>
   8: 07:04:04.440055       49.37.41.50.50479 > 20.157.64.169.80: P 2274994640:2274995193(553) ack 2880872723 win 2052 <nop,nop,timestamp 239187903 520
348>
```

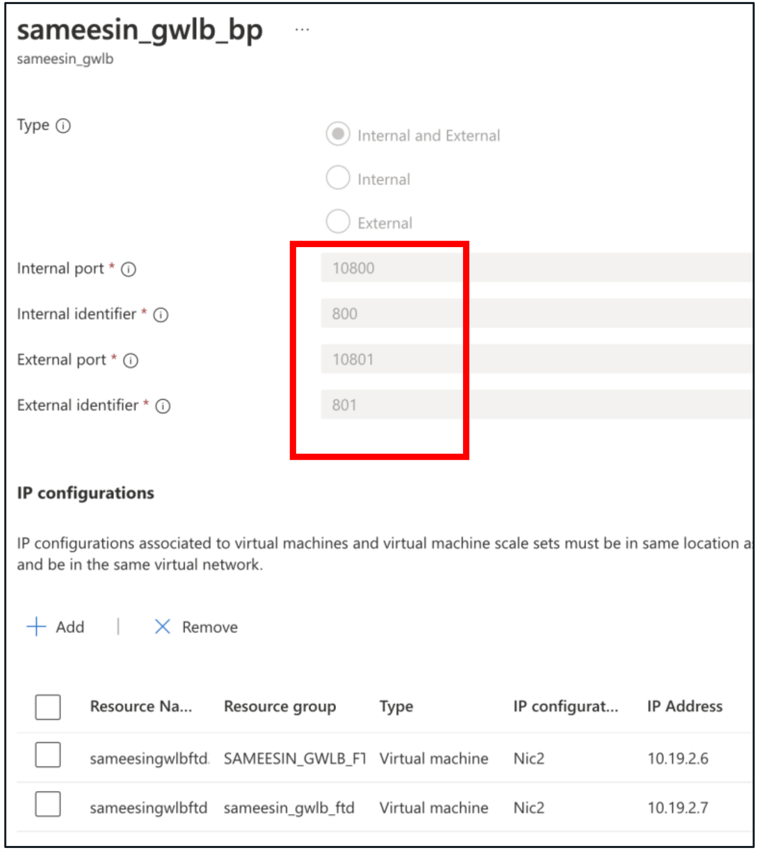
Azure GWLB Components

- **Frontend IP Configuration** – A private IP Address assigned to the Gateway Load balancer
- **Backend Pool** – Group of virtual machines that receive the incoming traffic from the Gateway load balancer
- **Load balancing rules (HA Port rule)** – Enables load balancing on all ports for TCP and UDP protocols.
- **Health Probe** – Used to identify healthy virtual machines in the backend pool to receive load-balanced traffic

Backend Pool

- Defines the group of firewall instances that will inspect traffic for a given load-balancing rule
- Associate the VM that should be part of the backend pool.
- Two VXLAN tunnels are defined for the backend pool

- Internal Port and Internal Identifier
- External Port and External Identifier



sameesin_gwlb_bp ···

sameesin_gwlb

Type ⓘ

● Internal and External

○ Internal

○ External

Internal port * ⓘ	10800
Internal identifier * ⓘ	800
External port * ⓘ	10801
External identifier * ⓘ	801

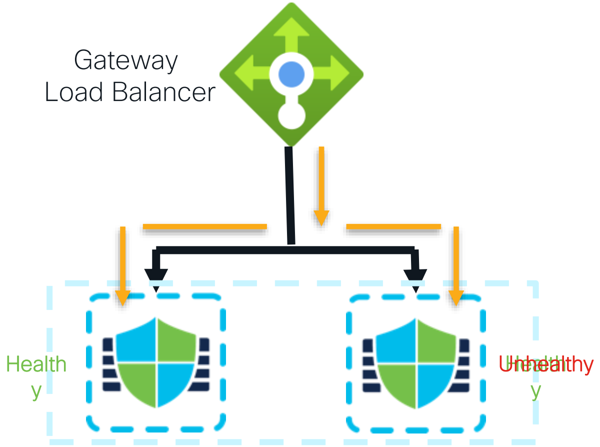
IP configurations

IP configurations associated to virtual machines and virtual machine scale sets must be in same location a and be in the same virtual network.

□	Resource Na...	Resource group	Type	IP configurat...	IP Address
□	sameesingwlbftd	SAMEESIN_GWLB_F1	Virtual machine	Nic2	10.19.2.6
□	sameesingwlbftd	sameesin_gwlb_ftd	Virtual machine	Nic2	10.19.2.7

Health Probe

- Determines which backend pool instance will not receive new connections
- Defines the port and protocol to be used for the probe
- For Cisco Secure firewall, ports TCP/22 or TCP/443 can be used
- Defines the interval between probes



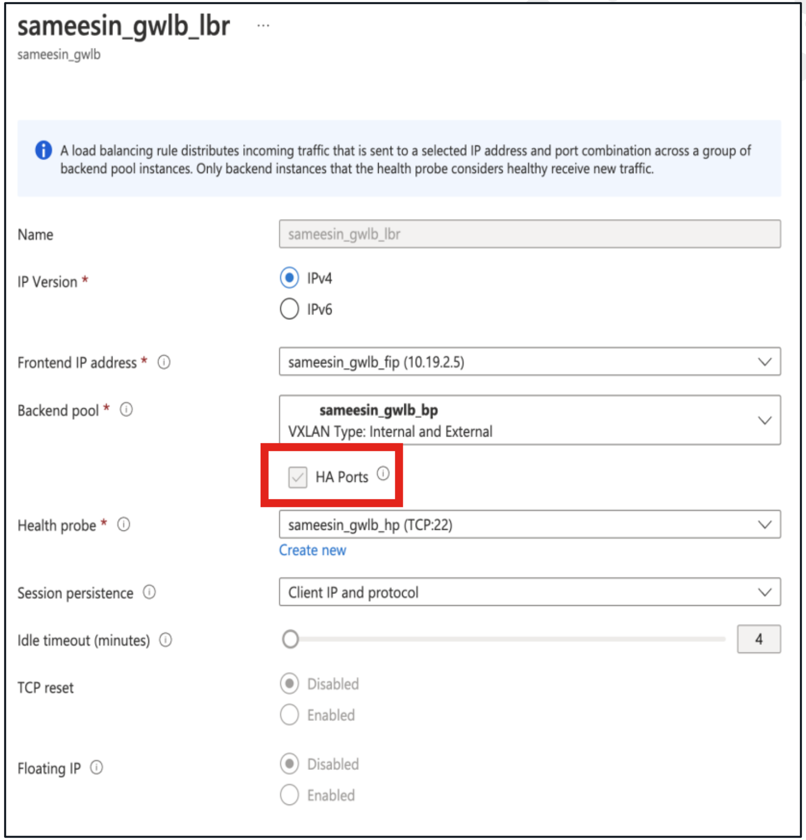
Cisco Secure Firewall Backend Pool

Load Balancer Rule

- Defines forwarding of traffic from the load balancer to instances in the backend pool
- GWLB allows only High Availability Ports rule

  – All forwarded traffic to the load balancer will match this rule

  – protocol – all and port – 0



sameesin_gwlb_lbr ...

sameesin_gwlb

A load balancing rule distributes incoming traffic that is sent to a selected IP address and port combination across a group of backend pool instances. Only backend instances that the health probe considers healthy receive new traffic.

Name: sameesin_gwlb_lbr

IP Version *: ● IPv4 ○ IPv6

Frontend IP address *: sameesin_gwlb_fip (10.19.2.5)

Backend pool *: **sameesin_gwlb_bp** VXLAN Type: Internal and External

☑ HA Ports

Health probe *: sameesin_gwlb_hp (TCP:22)

Create new

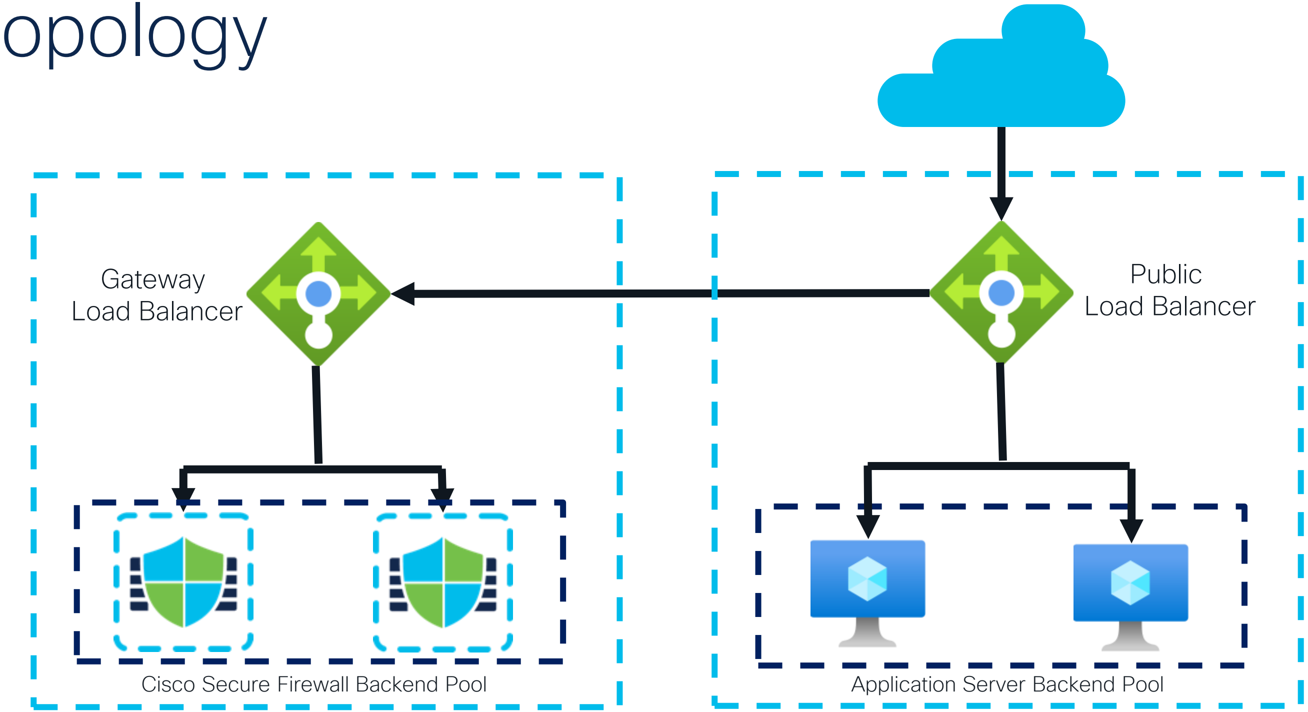
Session persistence: Client IP and protocol

Idle timeout (minutes): 4

TCP reset: ● Disabled ○ Enabled

Floating IP: ● Disabled ○ Enabled

Topology


Gateway
Load Balancer
Public
Load Balancer
Cisco Secure Firewall Backend Pool
Application Server Backend Pool

Prerequisites

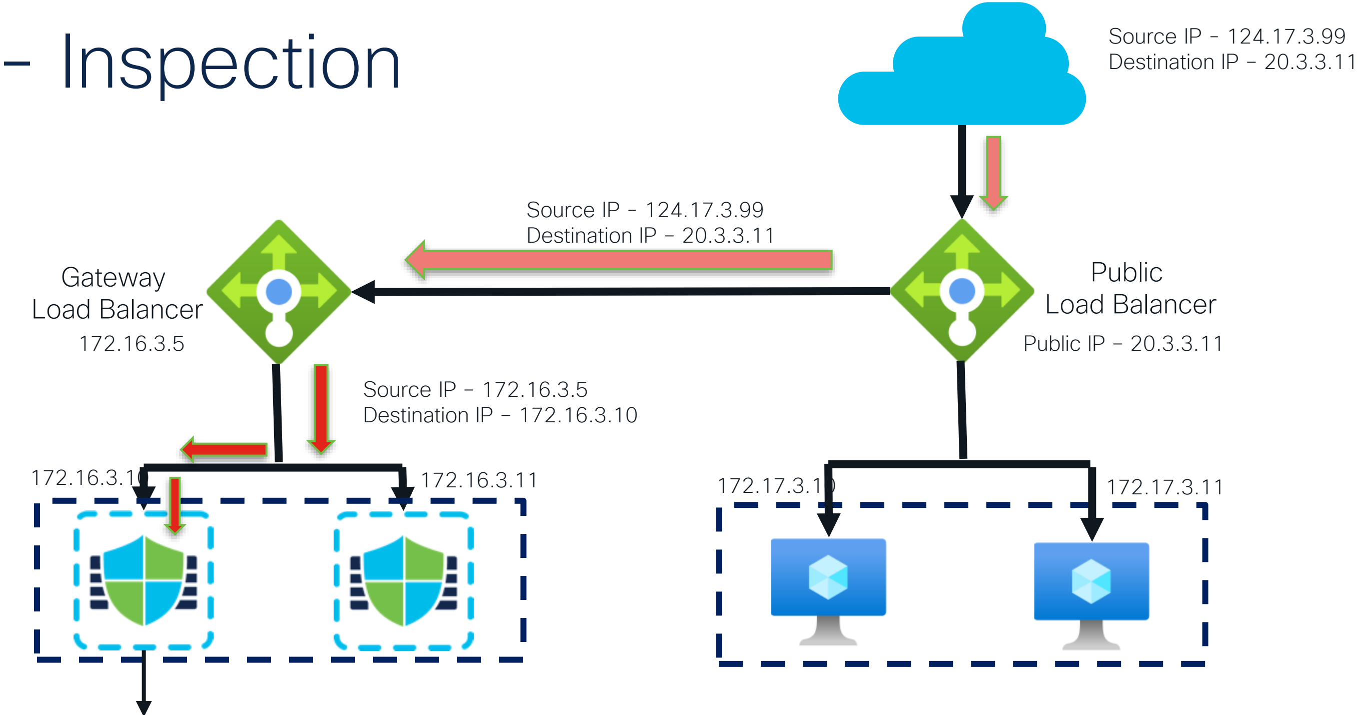
- Public Load Balancers (PLB) frontend IP configurations must be standard SKU.
- The network interface must have a standard SKU public IP address associated to it.

Cisco Secure Firewall Configuration

Prerequisites

- FMC and FTD versions should be 7.3 or above
- Secure Firewalls to be part of the backend pool should be registered to the Secure Firewall Management Center
- Only one data interface is required for this setup

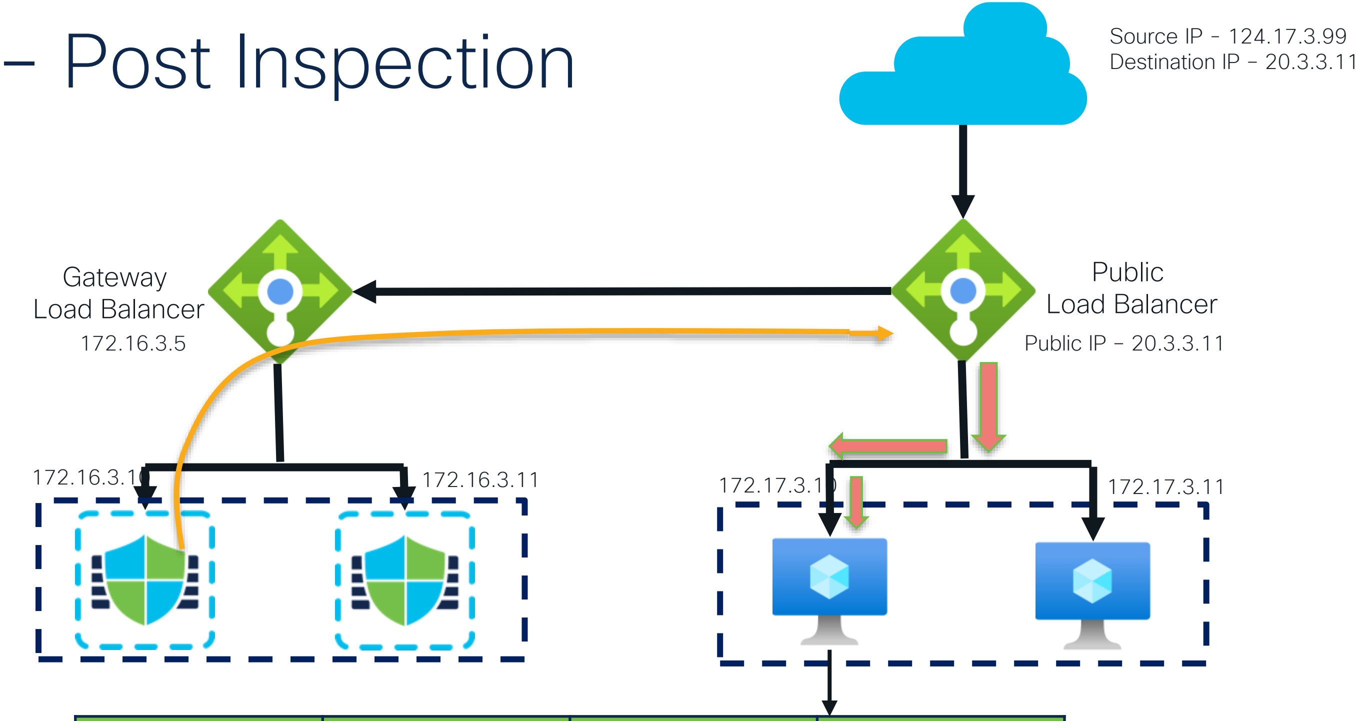
Flow – Inspection



Interface	Source IP	Destination IP	Destination Port
outside	172.16.3.5	172.16.3.10	10801
vni	124.17.3.99	20.3.3.11	80

🟥 Original packet
🟥 Encapsulated packet

Flow – Post Inspection

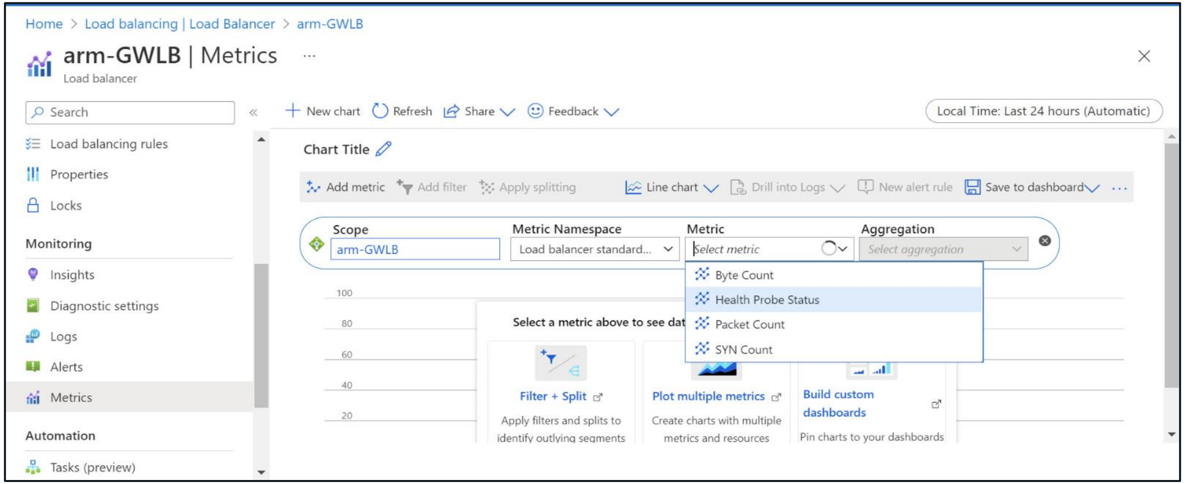


Interface	Source IP	Destination IP	Destination Port
eth0	124.17.3.99	172.17.3.10	80

Demo

Troubleshooting Tips

- Check the health probe status of the firewalls
- Navigate to **Metrics** in the GWLB **Monitoring** section and select **Health Probe Status** as the metric



Home > Load balancing | Load Balancer > arm-GWLB

arm-GWLB | Metrics

Load balancer

Scope: arm-GWLB

Metric Namespace: Load balancer standard...

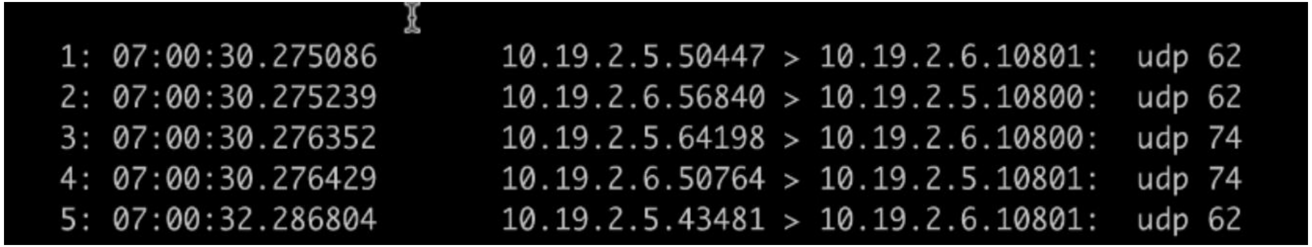
Metric: Select metric

Aggregation: Select aggregation

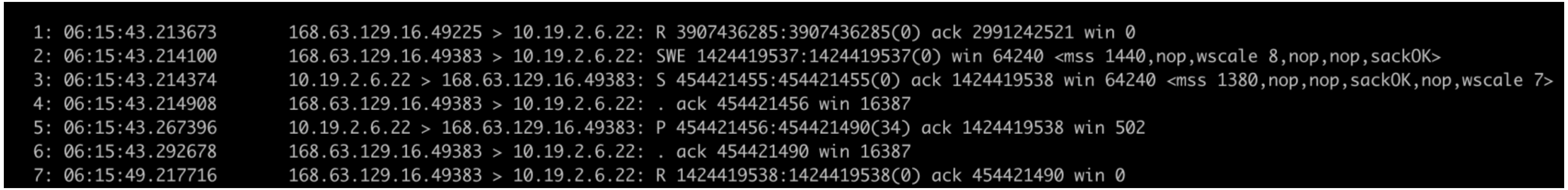
- Byte Count
- Health Probe Status
- Packet Count
- SYN Count

Troubleshooting Tips

- Packet capture on the FTDs
  - Capture traffic on the VTEP interface to verify encapsulated traffic and health probe are being received.



```
1: 07:00:30.275086       10.19.2.5.50447 > 10.19.2.6.10801:  udp 62
2: 07:00:30.275239       10.19.2.6.56840 > 10.19.2.5.10800:  udp 62
3: 07:00:30.276352       10.19.2.5.64198 > 10.19.2.6.10800:  udp 74
4: 07:00:30.276429       10.19.2.6.50764 > 10.19.2.5.10801:  udp 74
5: 07:00:32.286804       10.19.2.5.43481 > 10.19.2.6.10801:  udp 62
```



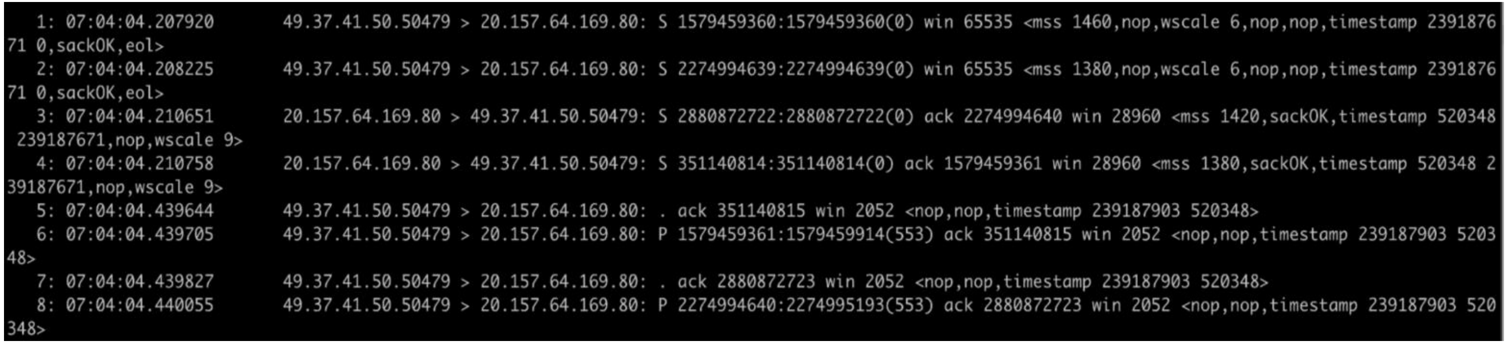
```
1: 06:15:43.213673       168.63.129.16.49225 > 10.19.2.6.22: R 3907436285:3907436285(0) ack 2991242521 win 0
2: 06:15:43.214100       168.63.129.16.49383 > 10.19.2.6.22: SWE 1424419537:1424419537(0) win 64240 <mss 1440,nop,wscale 8,nop,nop,sackOK>
3: 06:15:43.214374       10.19.2.6.22 > 168.63.129.16.49383: S 454421455:454421455(0) ack 1424419538 win 64240 <mss 1380,nop,nop,sackOK,nop,wscale 7>
4: 06:15:43.214908       168.63.129.16.49383 > 10.19.2.6.22: . ack 454421456 win 16387
5: 06:15:43.267396       10.19.2.6.22 > 168.63.129.16.49383: P 454421456:454421490(34) ack 1424419538 win 502
6: 06:15:43.292678       168.63.129.16.49383 > 10.19.2.6.22: . ack 454421490 win 16387
7: 06:15:49.217716       168.63.129.16.49383 > 10.19.2.6.22: R 1424419538:1424419538(0) ack 454421490 win 0
```

Troubleshooting Tips

- If you see no traffic, check
  - GWLB configuration
  - Inbound effective security rules on the VTEP network interface
  - Interface configuration on the firewall
  - Confirm that the GWLB is associated with the firewall
- If you see no response for the health probe
  - check platform settings on the firewall

Troubleshooting Tips

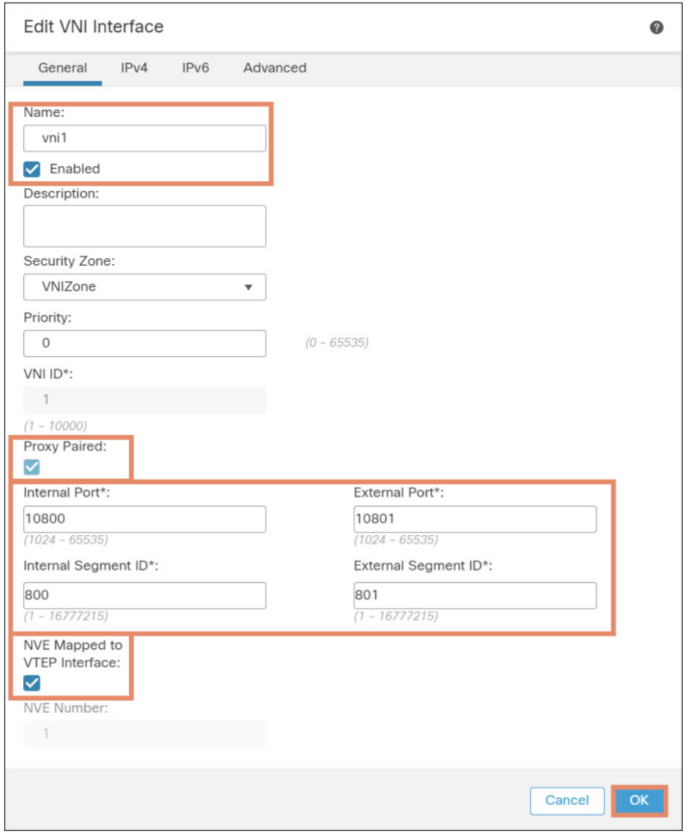
- Packet capture on the FTDs
  - Capture traffic on the VNI interface to verify traffic is received by the firewall.



```
   1: 07:04:04.207920       49.37.41.50.50479 > 20.157.64.169.80: S 1579459360:1579459360(0) win 65535 <mss 1460,nop,wscale 6,nop,nop,timestamp 2391876
71 0,sackOK,eol>
   2: 07:04:04.208225       49.37.41.50.50479 > 20.157.64.169.80: S 2274994639:2274994639(0) win 65535 <mss 1380,nop,wscale 6,nop,nop,timestamp 2391876
71 0,sackOK,eol>
   3: 07:04:04.210651       20.157.64.169.80 > 49.37.41.50.50479: S 2880872722:2880872722(0) ack 2274994640 win 28960 <mss 1420,sackOK,timestamp 520348
 239187671,nop,wscale 9>
   4: 07:04:04.210758       20.157.64.169.80 > 49.37.41.50.50479: S 351140814:351140814(0) ack 1579459361 win 28960 <mss 1380,sackOK,timestamp 520348 2
39187671,nop,wscale 9>
   5: 07:04:04.439644       49.37.41.50.50479 > 20.157.64.169.80: . ack 351140815 win 2052 <nop,nop,timestamp 239187903 520348>
   6: 07:04:04.439705       49.37.41.50.50479 > 20.157.64.169.80: P 1579459361:1579459914(553) ack 351140815 win 2052 <nop,nop,timestamp 239187903 5203
48>
   7: 07:04:04.439827       49.37.41.50.50479 > 20.157.64.169.80: . ack 2880872723 win 2052 <nop,nop,timestamp 239187903 520348>
   8: 07:04:04.440055       49.37.41.50.50479 > 20.157.64.169.80: P 2274994640:2274995193(553) ack 2880872723 win 2052 <nop,nop,timestamp 239187903 520
348>
```

Troubleshooting Tips

- If you see no traffic, check
  - GWLB configuration
  - Interface configuration on the firewall
- If you see the packet only once
  - check your access policy



Edit VNI Interface

Name: vni1

☑ Enabled

Description:

Security Zone: VNIZone

Priority: 0 (0 - 65535)

VNI ID*: 1 (1 - 10000)

Proxy Paired: ☑

Internal Port*: 10800 (1024 - 65535)

External Port*: 10801 (1024 - 65535)

Internal Segment ID*: 800 (1 - 16777215)

External Segment ID*: 801 (1 - 16777215)

NVE Mapped to VTEP Interface: ☑

NVE Number: 1

Agenda

- Introduction
- Azure Load Balancers
- Load Balancer Challenges
- Traffic Flow in Azure
- Gateway Load Balancer Components
- Configuration
- Demo
- Automation and Auto scale Solution Overview
- Key Takeaway

FMC REST API Support

FTD Configuration Automation

REST API Support the following operations enabling FTD Configuration Automation

- Onboard FTD devices to FMC
- Configure Interfaces
- Create VTEP
- Create VNI Interface

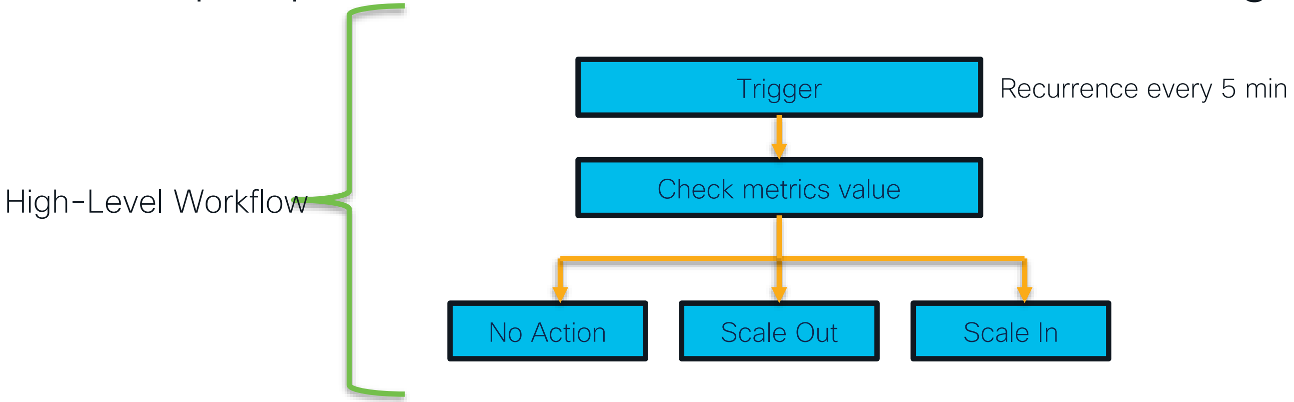
Autoscale Solution with Azure GWLB - Overview

- A serverless solution to scale-out or scale-in firewall instances based on usage
- Helps saving up on resources
- Deploy Resources in Azure using ARM Template
- Uses Function App and Logic App to automate firewall instance scaling
- The Threat defence instances will be part of a **virtual machine scale set**
  - Enable Scaling and managing of the firewall instances
  - Provides high availability of instances
  - collects CPU metrics from the instances

Autoscale Solution with Azure GWLB

Logic App

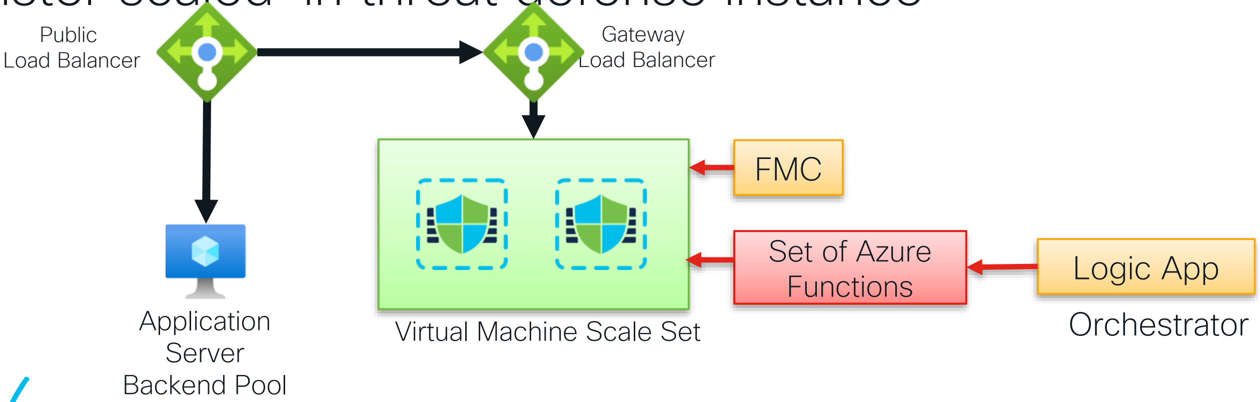
- Create and run automated workflows
- Sequences execution of functions and exchange information between them
- Each step represents an Azure function or built-in logic



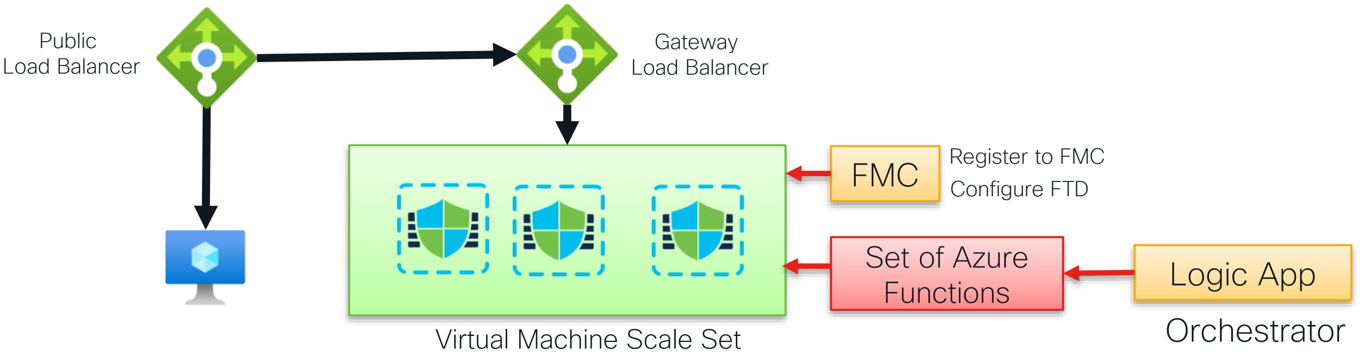
Autoscale Solution with Azure GWLB

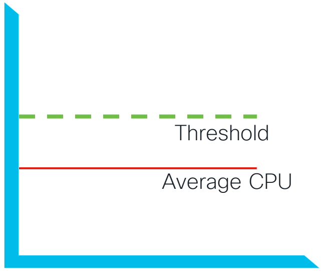
Function App

- Source code written using C++ is compiled and uploaded to the function app
- Probe metrics periodically and trigger scale-in/scale-out operations
- Register and Configure the new threat defense instance
- Unregister scaled-in threat defense instance



Autoscale Solution with Azure GWLB





Function App assigned the role of Contributor

Wrap Up

Complete your Session Survey

- Please complete your session survey after each session. Your feedback is important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (open from Thursday) to receive your Cisco Live t-shirt.

- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Session Catalog and clicking the "Attendee Dashboard” at https://www.ciscolive.com/emea/learn/sessions/session-catalog.html

Please Fill Out The Survey!

Key Takeaways

- Transparent insertion of firewalls allows a simpler design and minimizes the need for an architectural change.
- This solution simplifies the deployment, management and scaling of the firewall in the Azure environment.
- This solution enables traffic visibility at the endpoint with the original source IP address, which is a requirement for many use cases.

Continue Your Education

- Visit the Cisco Showcase for related demos.
- Book your one-on-one Meet the Engineer meeting.
- Attend any of the related sessions at the DevNet, Capture the Flag, and Walk-in Labs zones.
- Visit the On-Demand Library for more sessions at ciscolive.com/on-demand.

Security Technologies

Next Generation Firewall

Learn how Cisco Secure Firewall keeps businesses moving while keeping it secure. They offer deep visibility using built-in advanced security features like Cisco Secure IPS and Cisco Secure Endpoint to detect and stop advanced threats.

START

Feb 5 | 16:45
LABSEC-2030
Firepower Threat Defense: identity based firewall for VPN remote users - configuration and troubleshooting

Feb 5 | 16:45
LABSEC-2334
Deploying Cisco NGFW in Public Cloud (AWS).

Feb 5 | 18:15
LABSEC-1671
Adaptive Network Control with ISE and FTD

Feb 5 | 19:00
LABSEC-3449
Implementing and troubleshooting SAML authentication for AnyConnect VPN users terminated on Firepower Threat Defense

Feb 6 | 08:45
TECSEC-3782
Troubleshooting Firepower Threat Defense like a TAC Engineer

Feb 7 | 08:30
BRKSEC-1018
Introduction to cloud-delivered Firewall Management Center

Feb 7 | 3:30
BRKSEC-2109
Traffic Inspection in Azure Cloud Environment using Cisco Secure Firewall and Gateway Load Balancer

Feb 7 | 14:45
BRKSEC-1138
Security Management from Anywhere: Cisco Defense Orchestrator & Security Analytics and Logging

Feb 8 | 08:30
BRKSEC-2236
Keeping Up on Network Security with Cisco Secure Firewall

Feb 8 | 08:30
LTRSEC-3391
Secure Firewalls in ACI Deep Dive Lab

If you are unable to attend a live session, you can watch it On Demand after the event

CISCO Live!

Feb 8 | 09:00

PSOSEC-1211

Cisco Secure Firewall: Driving Security Resilience Across a Hybrid and Multicloud World

Feb 8 | 13:30

BRKSEC-2484

Snort 3 with the Cisco Secure Firewall

Feb 8 | 16:45

BRKSEC-2201

SecureX and Secure Firewall Better Together

Feb 8 | 17:00

BRKSEC-2123

Solving the Segmentation Puzzle! Secure Workload and Secure Firewall Integration

Feb 9 | 08:30

BRKSEC-3320

Demystifying TLS Decryption and Encrypted Visibility Engine on Cisco Secure Firewall Threat Defense

Feb 9 | 14:00

LTRSEC-2735

Deploying Cisco Firewalls in the Azure Public Cloud

Feb 9 | 15:45

BRKSEC-3058

Route based VPNs with Cisco Secure Firewall

Feb 10 | 11:15

FINISH **BRKSEC-3533**

Think Like a TAC Engineer:
A guide to Cisco Secure Firewall most common pain points

If you are unable to attend a live session, you can watch it On Demand after the event

Q & A

The bridge to possible

Thank you

cisco Live!