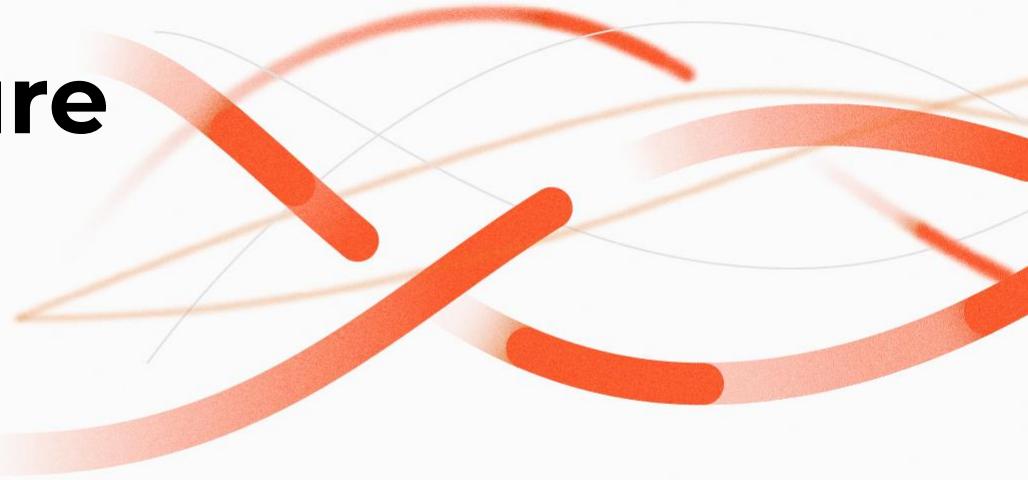




# VM-Series & Azure Virtual WAN

Template Build Guide



Matt McLimans, Public Cloud CE

January 2021

# Introduction

- This guide walks through several VM-Series deployment architectures for Azure Virtual WAN
- The build uses VM-Series scale sets deployed through Panorama Orchestration to secure:
  - Internet inbound traffic
  - Lateral Virtual WAN traffic traversing through a virtual hub
- The build is broken down into 5 steps
  1. Create Virtual WAN & Virtual Hub
  2. Connect Security Inbound VNET to the Virtual Hub
  3. Connect Security Outbound VNET to the Virtual Hub
  4. Peer Local VNET to Security Outbound VNET
  5. Connect Spoke VNET to Virtual Hub

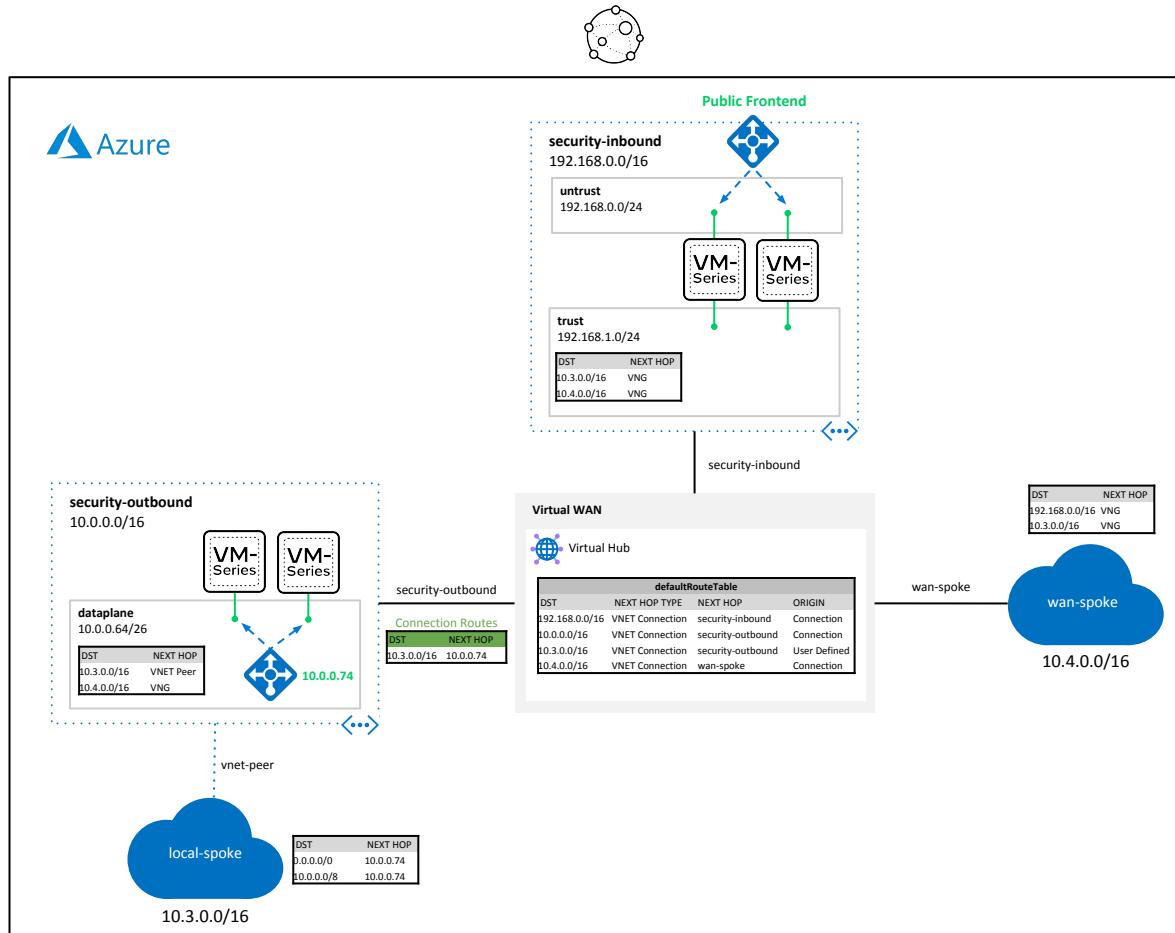
# Prerequisites

1. A active Azure subscription with appropriate permissions and resource allocation quota.
2. Panorama
  - a. PAN-OS 10.0.0 or greater
  - b. Panorama Azure Plugin 3.0 or greater
3. Access to this Github repo to automate the deployment of required Azure resources

<https://github.com/wwce/azure-arm-virtual-wan>

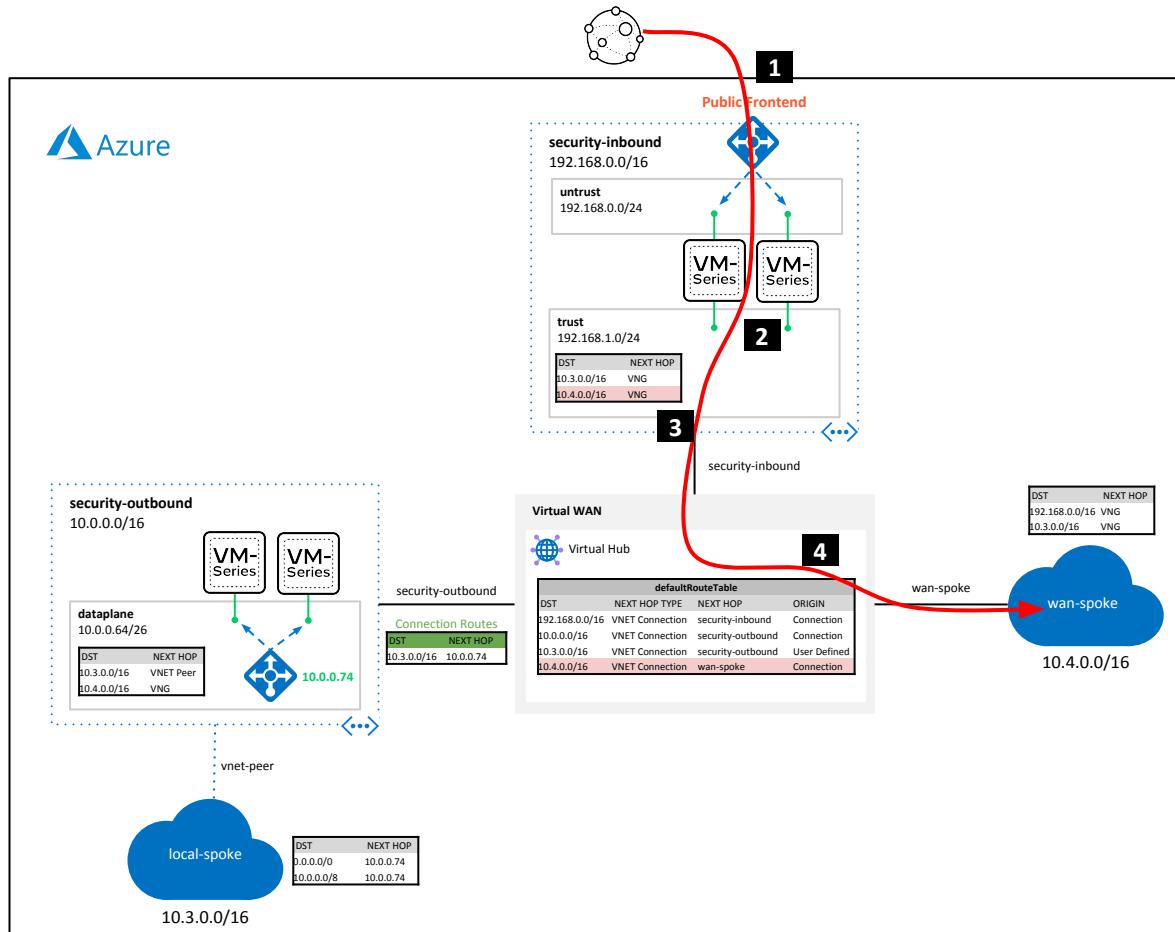
# Architecture Diagram

- Security Inbound
  - VM-Series scale set secures inbound traffic to wan-spoke
- Security Outbound
  - VM-Series scale set secures vWAN traffic to local-spoke



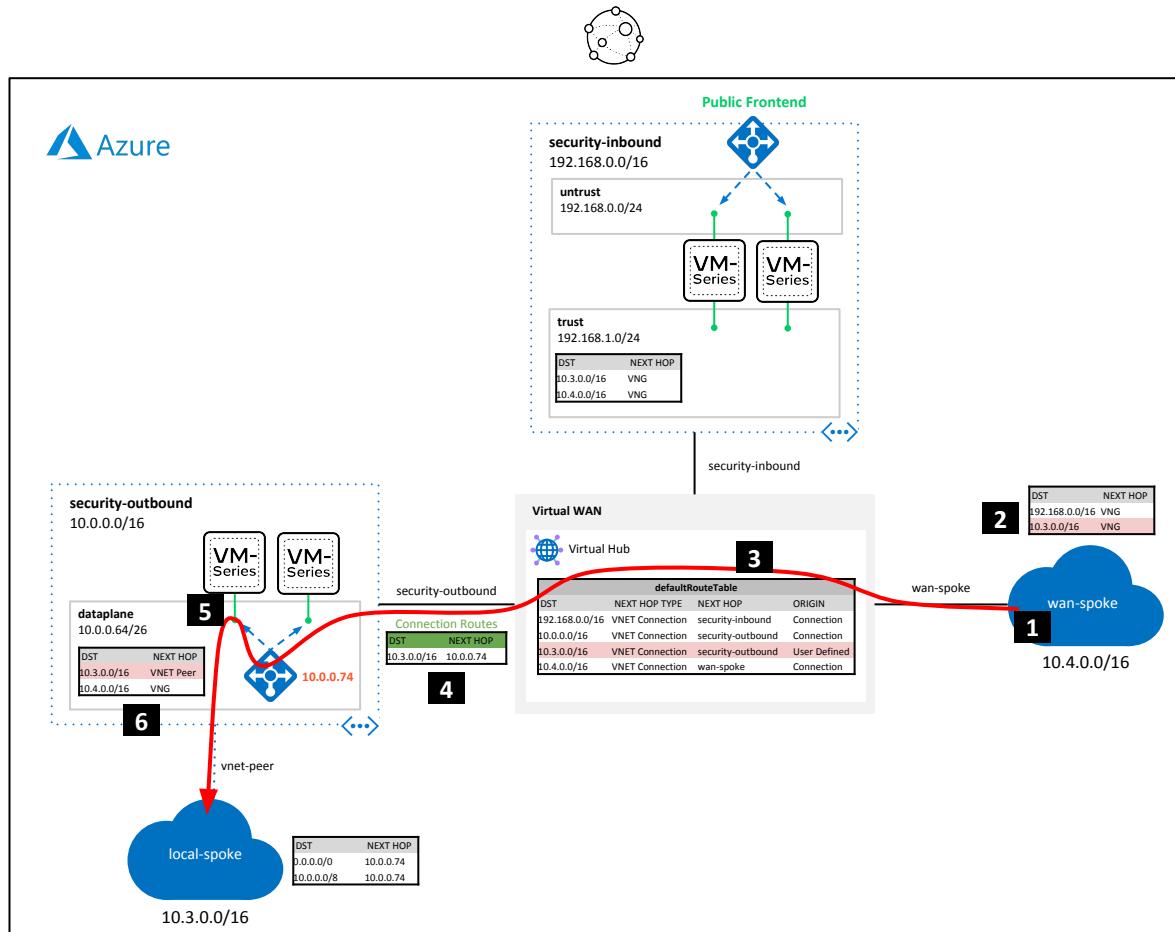
# Inbound Flow

1. Inbound request hits public load balancer frontend IP.
2. VM-Series SNAT to trust interface and DNAT to destination (10.4.0.x).
3. Trust subnet sends traffic to vWAN hub via propagated route.
4. vWAN hub route table sends request to wan-spoke VNET connection.



# Lateral Flow

1. wan-spoke VNET makes request to local-spoke (**10.3.0.x**)
2. Spoke subnet sends request to vWAN hub via propagated route.
3. vWAN hub route table has user defined route to direct request to the security-outbound VNET connection.
4. The security-outbound VNET connection has a “connection-route” to direct request to the internal load balancer of the VM-Series (**10.0.0.74**).
5. Internal load balancer forwards traffic to VM-Series
6. VM-Series dataplane subnet sends request to its local peer (**10.3.0.x**)



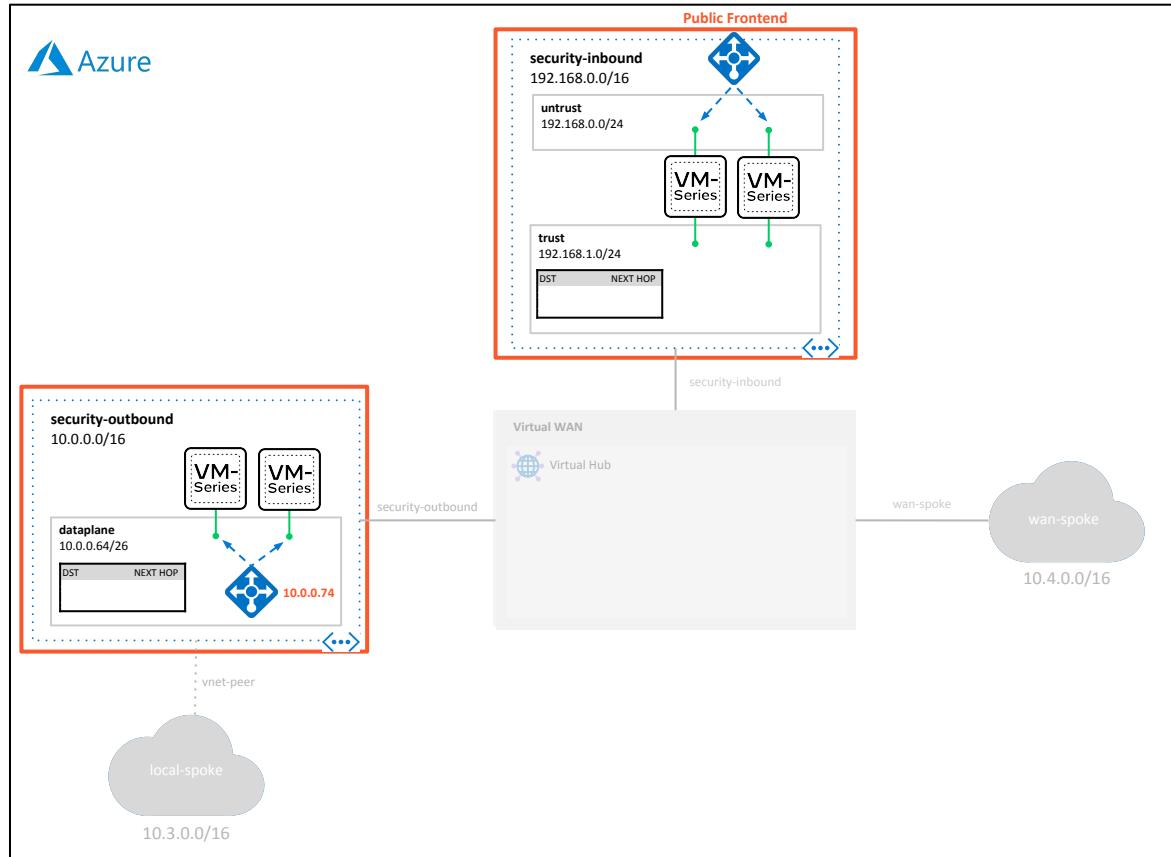
# Prerequisite Setup

# Create Inbound & Outbound Security VNETs



In this step, we will use Panorama Orchestrator to deploy an inbound and outbound VM-Series scale set.

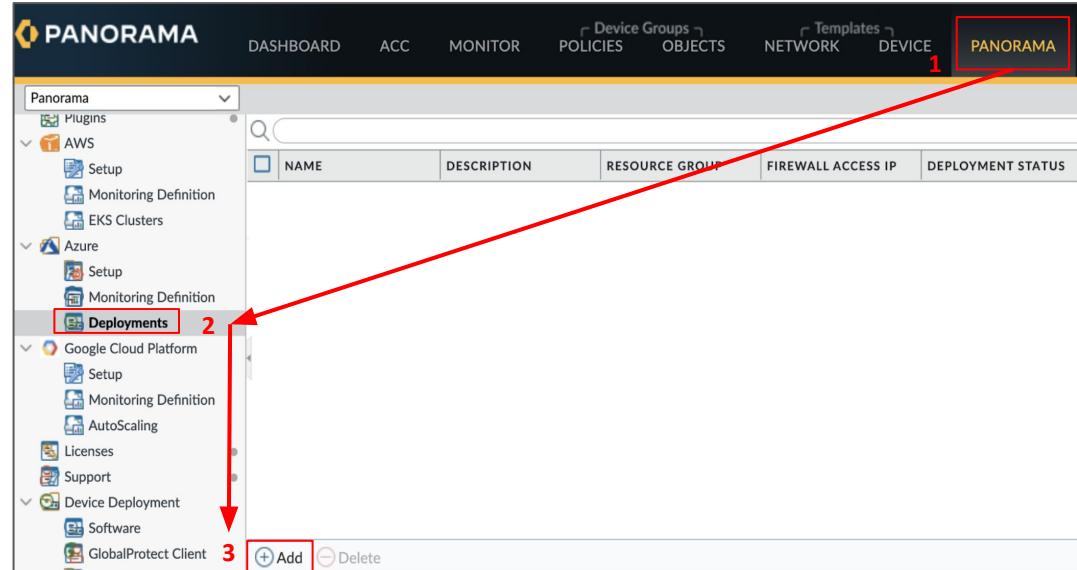
Each scale set will belong to its own VNET.



# Deploy VM-Series Scale Sets

## 1. Login to Panorama

Open Panorama tab  
→ Azure Plugin  
→ Deployments  
→ Add



# Create Inbound VM-Series Scale Set (1)

1. Enter a Name and select your Service Principal.

Configuration

Build | Protect

General | Azure | Firewall

Name: inbound-eastus

Description: Inbound VM-Series scale set for Virtual WAN environment.

Service Principal: service-principal-vs

Choose a service principal to enable other tabs. If service principal is not shown please make sure it is committed. It may take up to 1 min for newly committed service principals to be displayed.

OK Cancel

2. Select a region (must be same region as your Virtual Hub)
3. Enter a unique CIDR for the inbound VNET.

Configuration

Build | Protect

General | Azure | Firewall

Region: eastus

Existing VNET:  No  Yes

VNET CIDR: 192.168.0.0/22  
Prefix must be smaller than or equal to 22

Directory Domain: paloaltonetworks.onmicrosoft.com  
Please fill in this information to populate the URLs to your Appinsights and ARM deployments in deployment status page after launching deployment.

OK Cancel

# Create Inbound VM-Series Scale Set (2)

5. Virtual WAN best practices recommend separate VNETs for inbound and outbound security VNETs. Therefore, only select **Yes** to deploy the inbound VNET. Select **No** on the outbound/eastwest VNET.

**Configuration**

**Build** | Protect

General | Azure | **Firewall**

Stacks | Basic | Advanced

Protect Outbound/EastWest Application Traffic

Deploy  No  Yes

Protect Inbound Application Traffic

Deploy  No  Yes

License Type: Bundle2

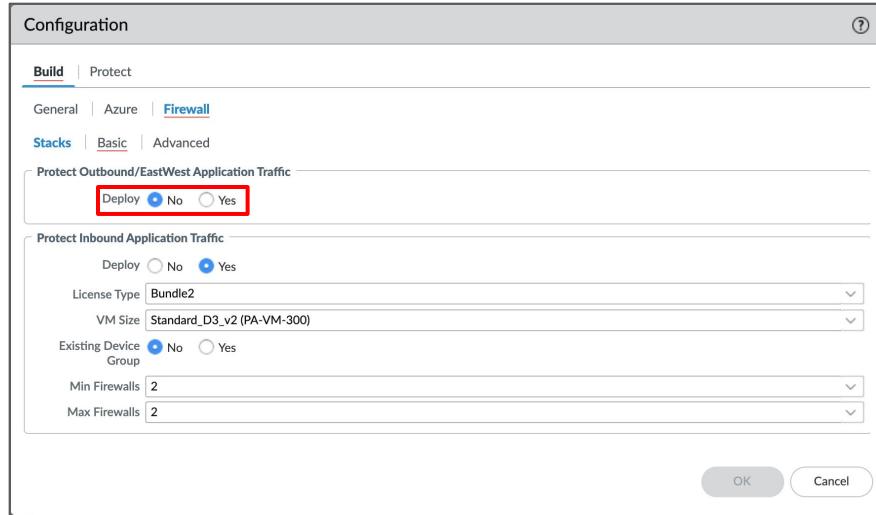
VM Size: Standard\_D3\_v2 (PA-VM-300)

Existing Device Group:  No  Yes

Min Firewalls: 2

Max Firewalls: 2

OK Cancel



6. Select Marketplace Image  
7. Select Software Version (must <= Panorama version).  
8. Enter a username and password.  
9. Enter your Panorama IP

**Configuration**

**Build** | Protect

General | Azure | **Firewall**

Stacks | **Basic** | Advanced

Image Type:  Marketplace Image  Custom Image

Software Version: 10.0.2

Username: paloalto

Password: \*\*\*\*\*

Confirm Password: \*\*\*\*\*

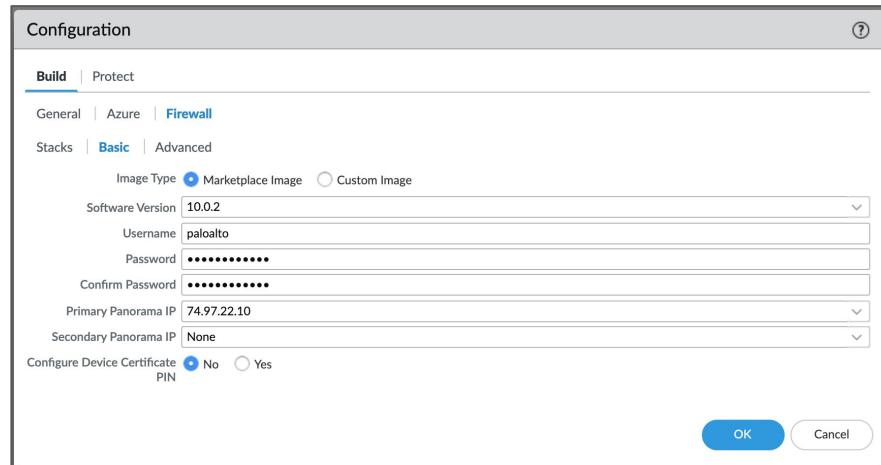
Primary Panorama IP: 74.97.22.10

Secondary Panorama IP: None

Configure Device Certificate:  No  Yes

PIN: \*\*\*\*\*

OK Cancel



# Create Outbound VM-Series Scale Set

# Create Outbound VM-Series Scale Set (1)

1. Enter a Name and select your Service Principal.

Configuration

Build | Protect

General | Azure | Firewall

Name: outbound-eastus

Description: Outbound VM-Series scale set for Virtual WAN environment.

Service Principal: service-principal-vs

Choose a service principal to enable other tabs. If service principal is not shown please make sure it is committed. It may take up to 1 min for newly committed service principals to be displayed.

OK Cancel

2. Select a region (must be same region as your Virtual Hub)
3. Enter a unique CIDR for the outbound VNET.

Configuration

Build | Protect

General | Azure | Firewall

Region: eastus

Existing VNET:  No  Yes

VNET CIDR: 10.0.0.0/16

Directory Domain: xyz.onmicrosoft.com

Please fill in this information to populate the URLs to your Appinsights and ARM deployments in deployment status page after launching deployment.

OK Cancel

# Create Outbound VM-Series Scale Set (2)

5. Virtual WAN best practices recommend separate VNETs for inbound and outbound security VNETs. Therefore, only select **No** to deploy the inbound VNET. Select **Yes** on the outbound/eastwest VNET.

**Configuration**

**Build** | Protect

General | Azure | **Firewall**

Stacks | Basic | Advanced

**Protect Outbound/EastWest Application Traffic**

- Deploy  No  Yes
- License Type: Bundle2
- VM Size: Standard\_D3\_v2 (PA-VM-300)
- Existing Device Group:  No  Yes
- Min Firewalls: 2
- Max Firewalls: 2

**Protect Inbound Application Traffic**

- Deploy  No  Yes

OK Cancel

6. Select Marketplace Image  
7. Select Software Version (must <= Panorama version).  
8. Enter a username and password.  
9. Enter your Panorama IP

**Configuration**

**Build** | Protect

General | Azure | **Firewall**

Stacks | **Basic** | Advanced

Image Type:  Marketplace Image  Custom Image

Software Version: 10.0.2

Username: pandemo

Password: \*\*\*\*\*

Confirm Password: \*\*\*\*\*

Primary Panorama IP: 74.97.22.10

Secondary Panorama IP: None

Configure Device Certificate:  No  Yes

PIN: \*\*\*\*\*

OK Cancel

# Commit to Panorama & Deploy

1. Commit the changes to Panorama.

The screenshot shows the Panorama interface with the 'Commit' button highlighted in red. A dropdown menu is open, showing three options: 'Commit to Panorama', 'Push to Devices', and 'Commit and Push'. The main table below lists two deployment entries: 'inbound-eastus' and 'outbound-eastus'.

NAME	DESCRIPTION	RESOURCE GROUP	FIREWALL ACCESS IP	DEPLOYMENT STATUS	ACTION
inbound-eastus	Inbound VM-Series scale set for Virtual WAN environment.			Commit Changes	
outbound-eastus	Outbound VM-Series scale set for Virtual WAN environment.			Commit Changes	

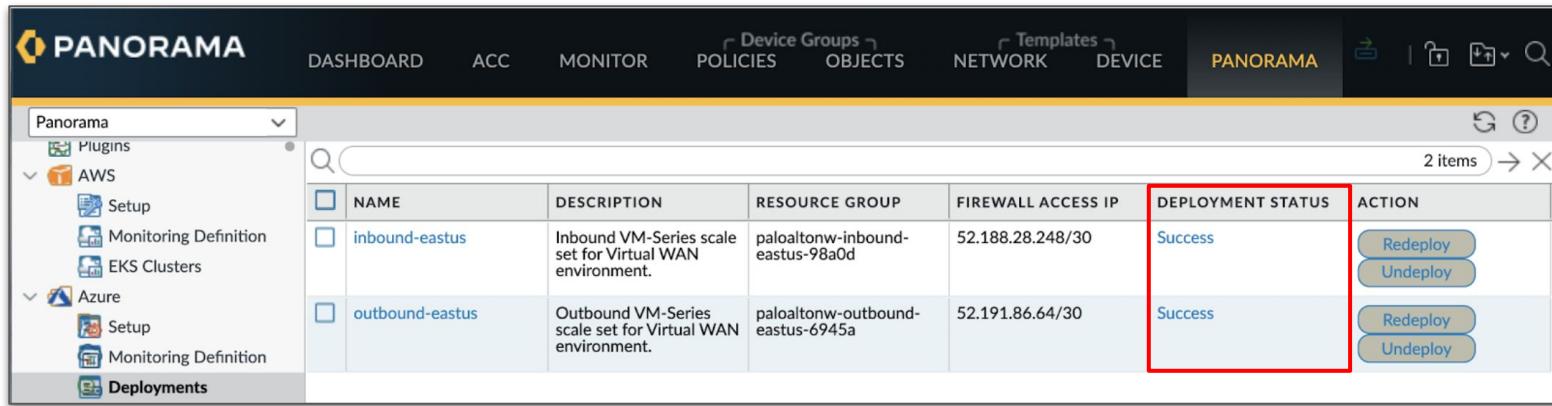
2. Click **Deploy** button for the inbound deployment
3. Click **Deploy** button for the outbound deployment

The screenshot shows the Panorama interface after deployment. The 'ACTION' column now contains 'Not Deployed' for both rows. Red boxes highlight the 'Deploy' buttons in the 'ACTION' column for both 'inbound-eastus' and 'outbound-eastus' entries.

NAME	DESCRIPTION	RESOURCE GROUP	FIREWALL ACCESS IP	DEPLOYMENT STATUS	ACTION
inbound-eastus	Inbound VM-Series scale set for Virtual WAN environment.			N/A	Not Deployed
outbound-eastus	Outbound VM-Series scale set for Virtual WAN environment.			N/A	Not Deployed

# Completion Verification

1. Continue to Part 1 once the deployment statuses' list as successful.



The screenshot shows the PANORAMA interface with the 'DEPLOYMENTS' tab selected. The left sidebar lists 'AWS' and 'Azure' sections, with 'Deployments' currently highlighted. The main pane displays a table with two rows of deployment information:

NAME	DESCRIPTION	RESOURCE GROUP	FIREWALL ACCESS IP	DEPLOYMENT STATUS	ACTION
inbound-eastus	Inbound VM-Series scale set for Virtual WAN environment.	paloaltonw-inbound-eastus-98a0d	52.188.28.248/30	Success	<button>Redeploy</button> <button>Undeploy</button>
outbound-eastus	Outbound VM-Series scale set for Virtual WAN environment.	paloaltonw-outbound-eastus-6945a	52.191.86.64/30	Success	<button>Redeploy</button> <button>Undeploy</button>

A red box highlights the 'DEPLOYMENT STATUS' column for both rows, which both show 'Success'. The 'ACTION' column contains two buttons each: 'Redeploy' and 'Undeploy'.

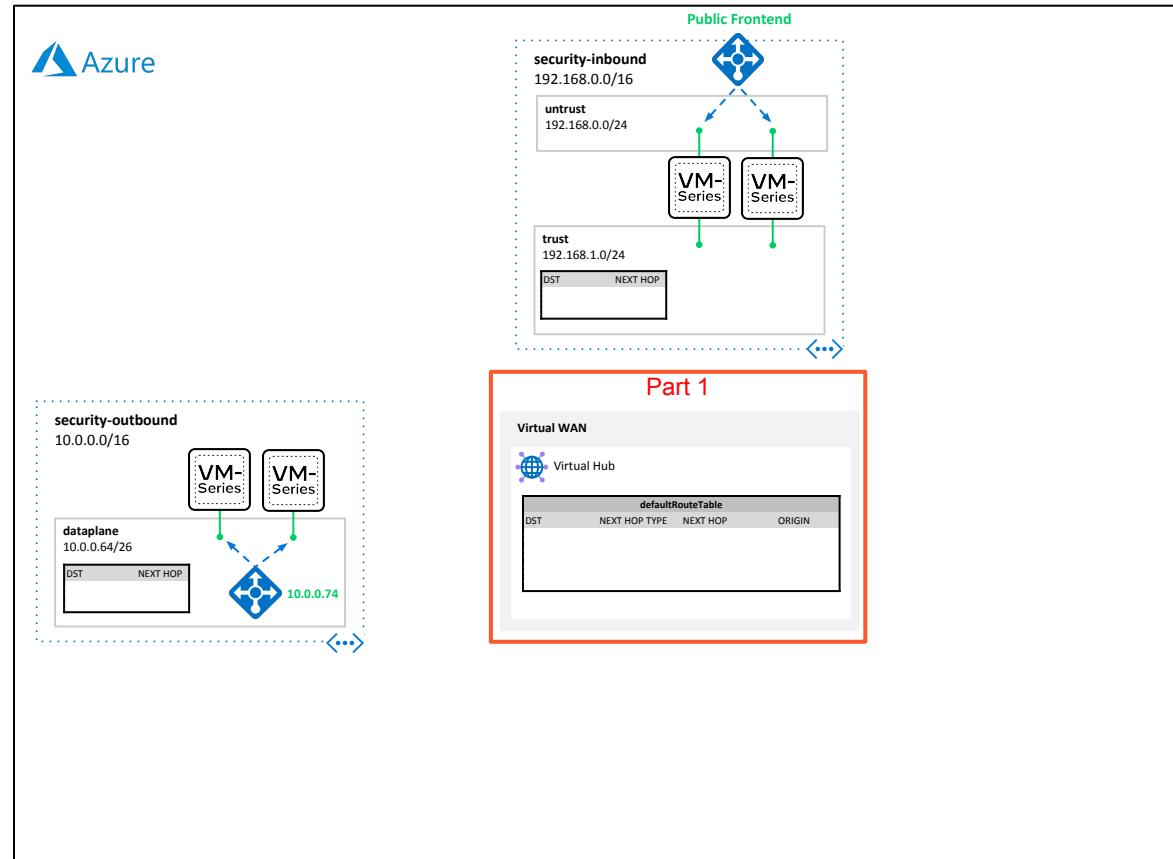
# Part 1

# Create Virtual WAN & Virtual Hub

# Part 1: Overview



- Part 1 creates a Virtual WAN and a Virtual Hub with a default route table.



# Part 1: Template Parameter Values

## Parameter Values

**Resource Group:** Create a new resource group

**Region:** Select a region

**WAN Name:** A name for the Virtual WAN

**Hub Name:** A name for the Virtual Hub

**Hub Address Prefix:** A unique CIDR range that does not overlap with other networks.

Click **Review + Create**

### Deployment scope

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription \* ⓘ

Visual Studio Professional

Resource group \* ⓘ

(New) virtual-wan-rg

[Create new](#)

### Parameters

Region \* ⓘ

East US

WAN Name ⓘ

virtual-wan

Hub Name ⓘ

hub1

Hub Address Prefix ⓘ

10.10.0.0/24

[Review + create](#)

< Previous

Next : [Review + create >](#)

# Part 1: Completion Verification (1)

- When the build completes, record the output values. These values will be used in later steps.

The screenshot shows two Azure portal pages. The left page displays deployment outputs: region (eastus), wan-name (virtual-wan), and hub-name (hub1). A red box highlights these three fields with the text "Record these values". An arrow points from the "Outputs" section of the left page to the "Outputs" section of the right page. The right page shows a deployment summary with a green checkmark and the message "Your deployment is complete". It includes deployment details like name, subscription, resource group, start time, and correlation ID. Below this is a table of resources with their types and statuses. At the bottom, there's a "Next steps" section with a "Go to resource group" button.

Search (Cmd+ /) <>

Overview

Inputs

**Outputs**

Template

Search (Cmd+ /) <>

Overview

Inputs

**Outputs**

Template

Record these values

region  
eastus

wan-name  
virtual-wan

hub-name  
hub1

Delete Cancel Redeploy Refresh

We'd love your feedback! →

**Your deployment is complete**

Deployment name: Microsoft.Template-20201229151258 Start time: 12/29/2020, 3:12:59 PM

Subscription: Visual Studio Professional Correlation ID: 9b5dadeb-5bee-47eb-a4c4-33

Resource Type Status

hub1/defaultRouteTable	Microsoft.Network/virtualHubs/hubRouteTables	OK
hub1/noneRouteTable	Microsoft.Network/virtualHubs/hubRouteTables	OK
hub1	Microsoft.Network/virtualHubs	OK
virtual-wan	Microsoft.Network/virtualWans	OK

Next steps

Go to resource group

# Part 1: Completion Verification (2)



Before proceeding, the Virtual Hub's router status must be in its “Succeeded” state.

This can take up to 30 minutes.

To check its status: Azure Portal → Virtual WANs → Hub → Overview



Home > Virtual WANs > virtual-wan >

**hub1** ✘  
Virtual HUB

Search (Cmd+/  
Delete Refresh Reset router Reset Hub

Overview

^ Essentials

Name : hub1
Hub status :  Succeeded
Routing status :  Provisioning <b>wait</b>

Connectivity

VPN (Site to site)



Home > Virtual WANs > virtual-wan >

**hub1** ✘  
Virtual HUB

Search (Cmd+/  
Delete Refresh Reset router Reset Hub

Overview

^ Essentials

Name : hub1
Hub status :  Succeeded
Routing status :  Provisioned <b>Go</b>

Connectivity

VPN (Site to site)

# Part 2

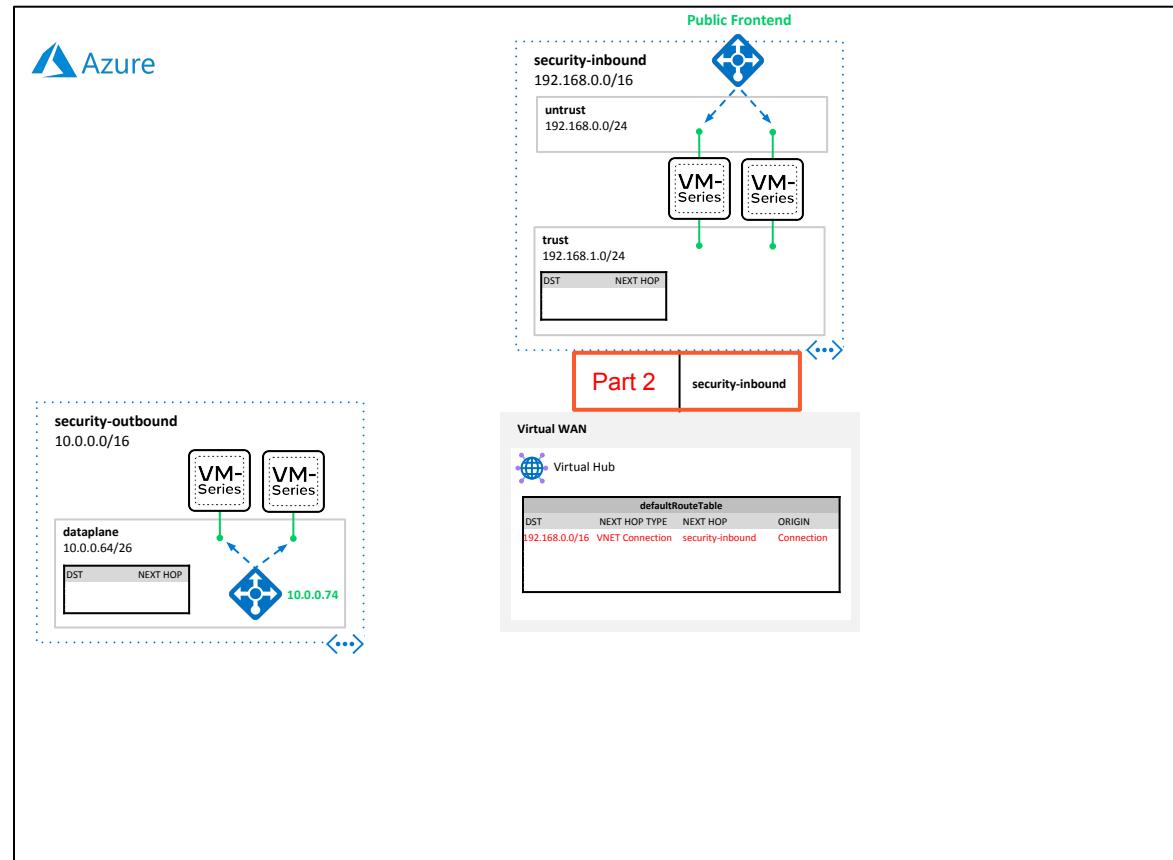
# Connect VM-Series Inbound Scale

# Set to the Virtual Hub

## Part 2: Overview



- In this section, we will connect the inbound VM-Series VNET to the virtual hub that was created in Part 1.



# Part 2: Template Parameter Values

## Parameter Values

**Resource Group:** Select inbound VNET resource group

**WAN Resource Group:** Deployment Resource Group from ([Part 1 wan-rg output](#))

**Security VNET Name:** Name of inbound VM-Series VNET

**Security VNET Resource Group:** Name of inbound VM-Series resource group

**Hub Name:** Virtual WAN hub name ([hub-name output from Part 1](#))

**Hub Associated Route Table:** Leave as `defaultRouteTable`

**Hub Propagated Route Table:** Leave as `defaultRouteTable`

Click [Review and Create](#)

**Deployment scope**

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription \* ⓘ Visual Studio Professional

Resource group \* ⓘ paloaltonw-inbound-eastus-98a0d

Create new

**Parameters**

Region ⓘ East US

WAN Resource Group ⓘ virtual-wan-rg

Security Vnet Name \* ⓘ paloaltonw-inbound-eastus-98a0d-vnet

Hub Name ⓘ hub1

Hub Associated Route Table ⓘ defaultRouteTable

Hub Propagated Route Table ⓘ defaultRouteTable

[Review + create](#) < Previous Next : Review + create >

## Part 2: Completion Verification

1. Proceed to Part 3 when the build completes.

The screenshot shows a deployment summary page in the Azure portal. At the top, there are buttons for Delete, Cancel, Redeploy, and Refresh. Below that is a feedback section with a link to provide feedback. The main message says "Your deployment is complete". It displays deployment details: name, subscription, and resource group. Deployment status information is shown, including start time, correlation ID, and resource type. A "Go to resource" button is at the bottom.

>Delete Cancel Redeploy Refresh

We'd love your feedback! →

✓ Your deployment is complete

Deployment name: Microsoft.Template-20201229153214  
Subscription: Visual Studio Professional  
Resource group: paloaltonw-inbound-eastus-98a0d

Start time: 12/29/2020, 3:32:15 PM  
Correlation ID: c6f8c9ce-801f-49f3-9e45-664e2a8ae69

Deployment details (Download)

Resource	Type	Status
✓ CREATE_HUB_CONNECTION	Microsoft.Resources/deployments	OK

Next steps

Go to resource

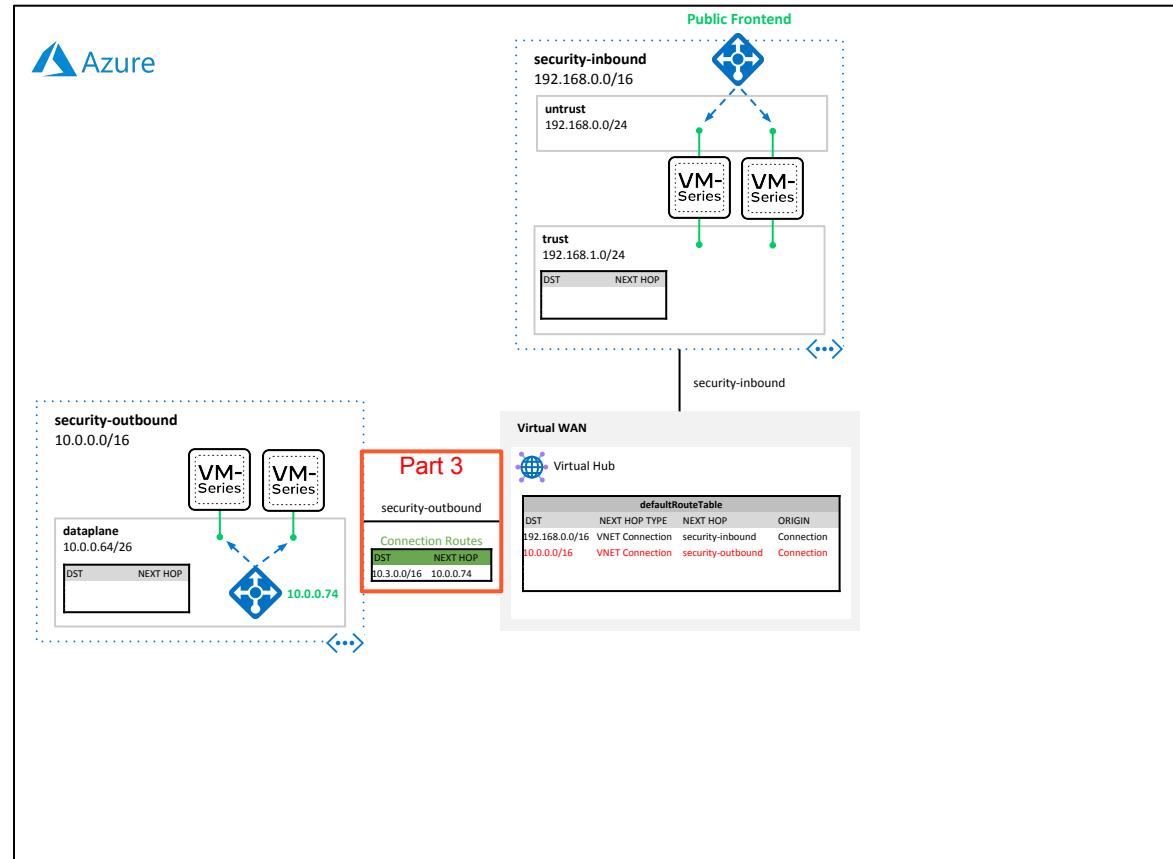
# **Part 3**

# **Connect VM-Series Outbound Scale Set to the Virtual Hub**

# Part 3: Overview



- In this section, we will connect the outbound VM-Series VNET to the virtual hub that was created in Part 1.



# Part 3: Record Outbound Deployment's Internal Load Balancer IP

## 1. Login to Panorama

Open Panorama tab

- Azure Plugin
- Deployments
- Open Outbound Deployment
- Copy **Egress Private IP** value

The screenshot shows the Palo Alto Networks Panorama web interface. At the top, there is a navigation bar with tabs: DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS, NETWORK, DEVICE, and PANORAMA. The PANORAMA tab is highlighted with a red box. Below the navigation bar is a sidebar with various configuration options like SAML, AWS, Azure, and Device Deployment, with the Deployments option highlighted by a red box. The main content area displays a table of deployments. One row for 'outbound-eastus' is selected, and its details are shown in a modal dialog box. The modal has a title 'Deployment Status - outbound-eastus' and tabs for 'Hub-Stack' and 'Inbound-Stack'. Under 'Hub-Stack', it shows the status as 'Success' (highlighted by a red box), the detail as '12/28/2020, 19:00:15', the device group as 'outbound-eastus-hub-dg-1.0', and the template stack as 'outbound-eastus-hub-ts-1.0'. It also lists the Egress Private IP as '10.0.0.74' (highlighted by a red box and labeled 'Record this value!'), the Egress Public IP as '20.72.136.216/30', the Deployment Link as 'GoToDeployments', and the AppInsights Link as 'GoToAppInsights'. A 'Close' button is at the bottom right of the modal.

NAME	DESCRIPTION	RESOURCE GROUP	FIREWALL ACCESS IP	DEPLOYMENT STATUS
inbound-eastus	Inbound VM-Series scale set for Virtual WAN environment.	paloaltonw-inbound-eastus-98a0d	40.88.250.28/30	Success
outbound-eastus	Outbound VM-Series scale set for Virtual WAN environment.	paloaltonw-outbound-eastus-6945a	20.72.136.216/30	Success

Deployment Status - outbound-eastus

Hub-Stack | Inbound-Stack

Status Success

Detail 12/28/2020, 19:00:15

Device Group outbound-eastus-hub-dg-1.0

Template Stack outbound-eastus-hub-ts-1.0

Egress Private IP 10.0.0.74 **Record this value!**

Egress Public IP 20.72.136.216/30

Deployment Link [GoToDeployments](#)

AppInsights Link [GoToAppInsights](#)

# Part 3: Template Parameter Values

## Parameter Values

**Resource Group:** Select outbound VM-Series resource group

**WAN Resource Group:** Deployment Resource Group from [Part 1](#)

**Security VNET Name:** Name of outbound VM-Series VNET

**Egress Private IP:** The IP Address of internal load balancer

**Hub Name:** Hub Name used in ([Part 1 hub-name output](#))

**Hub Associated Route Table:** Leave as `defaultRouteTable`

**Hub Propagated Route Table:** Leave as `defaultRouteTable`

Click [Review + Create](#)

**Deployment scope**  
Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription \* ⓘ Visual Studio Professional

Resource group \* ⓘ paloaltonw-outbound-eastus-6945a [Create new](#)

**Parameters**

Region ⓘ	East US
WAN Resource Group ⓘ	virtual-wan-rg
Security Vnet Name * ⓘ	paloaltonw-outbound-eastus-6945a-vnet
Egress Private IP * ⓘ	10.0.0.74
Hub Name ⓘ	hub1
Hub Associated Route Table ⓘ	defaultRouteTable
Hub Propagated Route Table ⓘ	defaultRouteTable

[Review + create](#) < Previous Next : Review + create >

## Part 3: Completion Verification (1)

- When the build completes, record the output values. These values will be used in the next step.

Microsoft.Template-20201229155032 | Outputs

Deployment

Search (Cmd+/)

Overview

Inputs

Outputs

Template

security-vnet-connection-name

paloaltonw-outbound-portus-69458-vnet-conn

Record this value

Microsoft.Template-20201229151258 | Overview

Deployment

Search (Cmd+/)

Overview

Inputs

Outputs

Template

We'd love your feedback! →

✓ Your deployment is complete

Deployment name: Microsoft.Template-20201229151258 Start time: 12/29/2020, 3:12:59 PM  
Subscription: Visual Studio Professional Correlation ID: 9b5dadeb-5bee-47eb-a4c4-33

Resource group: virtual-wan-rg

Deployment details (Download)

Resource	Type	Status	Operation details
hub1/defaultRouteTable	Microsoft.Network/virtu...	OK	<a href="#">Operation details</a>
hub1/noneRouteTable	Microsoft.Network/virtu...	OK	<a href="#">Operation details</a>
hub1	Microsoft.Network/virtu...	OK	<a href="#">Operation details</a>
virtual-wan	Microsoft.Network/virtu...	OK	<a href="#">Operation details</a>

Next steps

[Go to resource group](#)

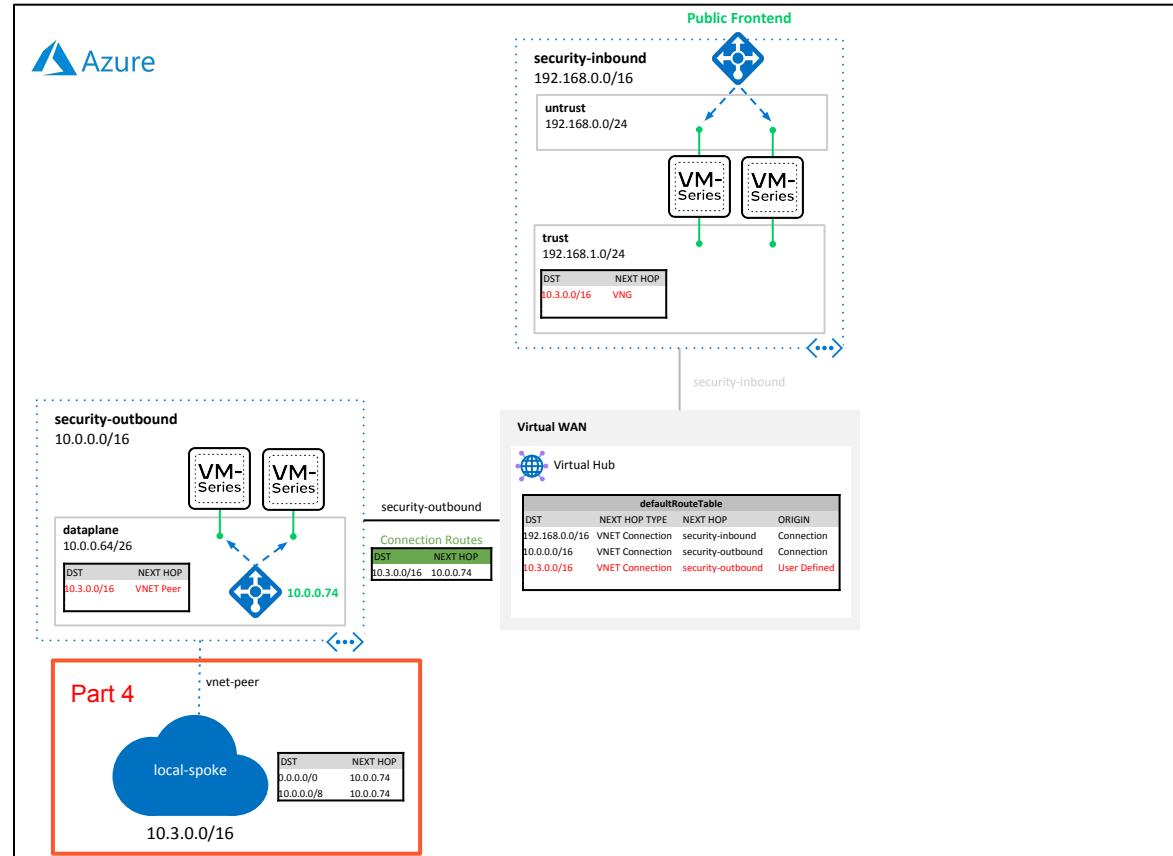
# Part 4

## Peer Local VNET to VM-Series Outbound VNET

# Part 4: Overview



- In this section, we will create a spoke VNET that will be connected to the outbound VNET via VNET peering.
- A route will then be added to the virtual hub route table. This will direct Virtual WAN traffic destined to the spoke VNET through the outbound firewalls.
- An Ubuntu VM is deployed in the VNET that we will use to test inbound and lateral flows.



# Part 4: Template Parameter Values

## Parameter Values

**Resource Group:** Create a new resource group

**Region:** Same region as previous deployments.

**Security VNET Resource Group:** Name of outbound VM-Series resource group

**Security VNET Name:** Name of outbound VM-Series VNET

**Security VNET Connection Name:** **Output value from Part 3**

**Egress Private IP:** The IP Address of internal load balancer

**WAN Resource Group:** Deployment Resource Group from **Part 1**

**Hub Name:** Hub Name used in **(Part 1 hub-name output)**

**Spoke Name Prefix:** Any name to append to created resources.

**Spoke VNET Prefix:** Unique CIDR Block for the spoke VNET.

**Spoke Subnet Prefix:** Unique subnet CIDR for the spoke subnet.

**Spoke Username/Password:** Credentials for Ubuntu VM.

Click **Review + Create**

### Deployment scope

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription \* ⓘ

Visual Studio Professional

Resource group \* ⓘ

(New) local-spoke-rg

Create new

### Parameters

Region \* ⓘ

East US

Security VNET Resource Group \* ⓘ

paloaltonw-outbound-eastus-6945a

Security VNET Name \* ⓘ

paloaltonw-outbound-eastus-6945a-vnet

Security VNET Connection Name \* ⓘ

paloaltonw-outbound-eastus-6945a-vnet-conn

Egress Private IP \* ⓘ

10.0.0.74

WAN Resource Group ⓘ

virtual-wan-rg

Hub Name ⓘ

hub1

Spoke Name Prefix ⓘ

spoke

Spoke VNET Prefix ⓘ

10.3.0.0/24

Spoke Subnet Prefix ⓘ

10.3.0.0/28

Spoke Username ⓘ

paloalto

Spoke Password ⓘ

\*\*\*\*\*

**Review + create**

< Previous

Next : **Review + create >**

# Part 4: Completion Verification

1. Proceed to Part 5 when the build completes.

The screenshot shows the Azure portal deployment summary page for a template named Microsoft.Template-20201229160105. The deployment was successful, starting at 12/29/2020, 4:01:06 PM with a Correlation ID of d40c393c-063e-43a9-b6b2-a4f3f5. It details the creation of various resources across a spoke-vnet and spoke-vm, including routes, network interfaces, and peer links. All resources are marked as OK. A 'Next steps' section includes a 'Go to resource group' button.

>Delete Cancel Redeploy Refresh

We'd love your feedback! →

✓ Your deployment is complete

Deployment name: Microsoft.Template-20201229160105 Start time: 12/29/2020, 4:01:06 PM  
Subscription: Visual Studio Professional Correlation ID: d40c393c-063e-43a9-b6b2-a4f3f5  
Resource group: local-spoke-rg

Deployment details (Download)

Resource	Type	Status	Operation details
CREATE_HUB_ROUTE	Microsoft.Resources/de...	OK	<a href="#">Operation details</a>
spoke-vnet/paloaltonw-01	Microsoft.Network/virtu...	OK	<a href="#">Operation details</a>
spoke-vm	Microsoft.Compute/virt...	OK	<a href="#">Operation details</a>
spoke-nic0	Microsoft.Network/netw...	Created	<a href="#">Operation details</a>
CREATE_PEER_LINK	Microsoft.Resources/de...	OK	<a href="#">Operation details</a>
spoke-vnet	Microsoft.Network/virtu...	OK	<a href="#">Operation details</a>
spoke-nsg	Microsoft.Network/netw...	OK	<a href="#">Operation details</a>
spoke-rtb	Microsoft.Network/rout...	OK	<a href="#">Operation details</a>

Next steps

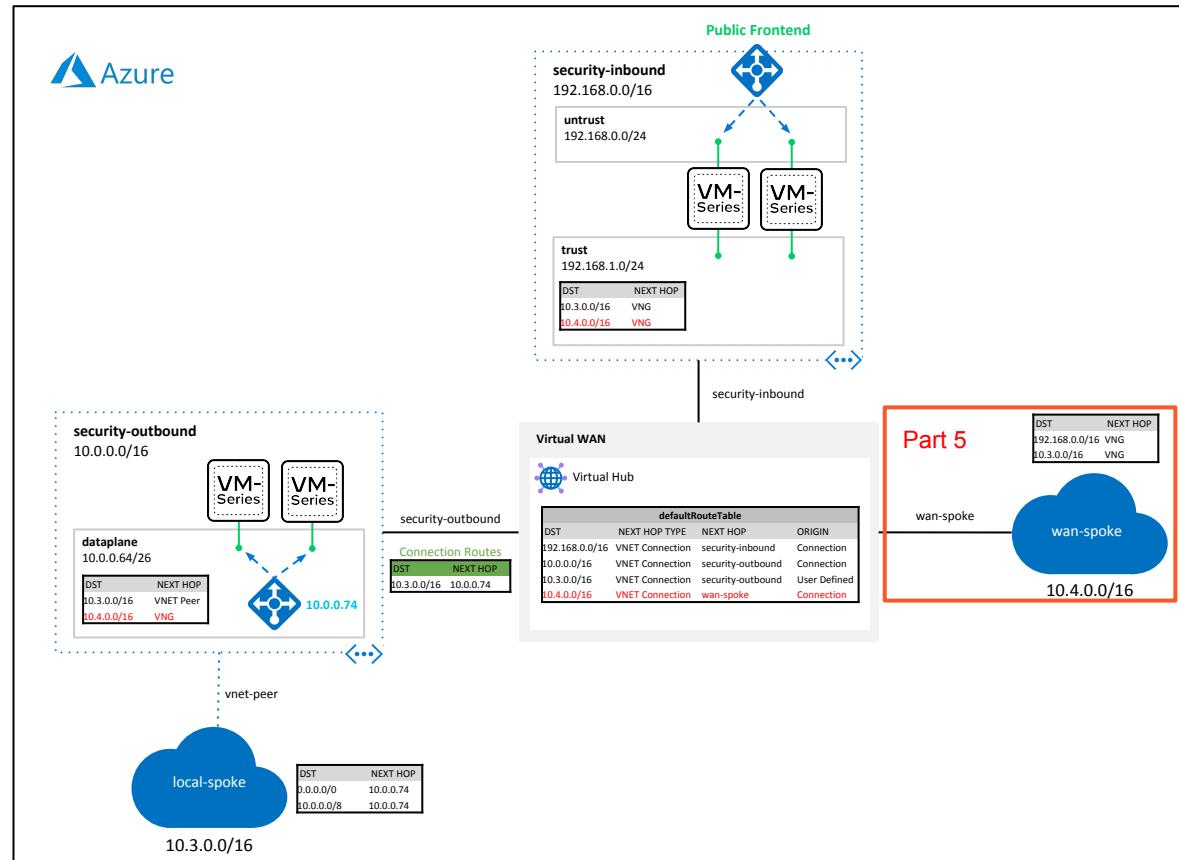
Go to resource group

# Part 5

# Connect WAN Spoke VNET to Virtual Hub

# Part 5: Overview

- Part 5 creates a Virtual Network and connects it to the Virtual Hub via a VNET Connection.
- An Ubuntu VM is deployed in the VNET that we will use to test inbound and lateral flows.



# Part 5: Template Parameter Values

## Parameter Values

**Resource Group:** Create a new resource group

**Region:** Same region as previous deployments.

**Spoke Name Prefix:** A unique name to prepend to the created resources

**Spoke VNET Prefix:** Unique CIDR Block for the VNET.

**Spoke Subnet Prefix:** Unique subnet CIDR for the test subnet.

**Spoke Username/Password:** Credentials for Ubuntu VM.

**WAN Resource Group:** Deployment Resource Group from [Part 1](#)

**Hub Name:** Hub Name used in ([Part 1 hub-name output](#))

**Hub Associated Route Table:** Leave as *defaultRouteTable*

**Hub Propagated Route Table:** Leave as *defaultRouteTable*

Click [Review + Create](#)

**Deployment scope**

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription \* ⓘ Visual Studio Professional

Resource group \* ⓘ (New) virtual-wan-spoke-rg

Create new

**Parameters**

Region * ⓘ	East US
Spoke Name Prefix ⓘ	wan-spoke
Spoke VNET Prefix ⓘ	10.4.0.0/24
Spoke Subnet Prefix ⓘ	10.4.0.0/28
Spoke Username ⓘ	paloalto
Spoke Password * ⓘ	*****
WAN Resource Group ⓘ	virtual-wan-rg
Hub Name ⓘ	hub1
Hub Associated Route Table ⓘ	defaultRouteTable
Hub Propagated Route Table ⓘ	defaultRouteTable

[Review + create](#) < Previous Next : Review + create >

# Part 5: Completion Verification

- When the build completes, you will see this from the portal.
- Click **Outputs** and record the spoke-address value. It will be used in Part 3 for testing the inbound flow.

Microsoft.Template-20201223125616 | Outputs

Deployment

Search (Cmd+ /)

Overview

Inputs

Outputs

Template

spoke-address

10.4.0.4 Record this value

Delete Cancel Redeploy Refresh

We'd love your feedback! →

Your deployment is complete

Deployment name: Microsoft.Template-20201229160730 Start time: 12/29/2020, 4:07:31 PM  
Subscription: Visual Studio Professional Correlation ID: e7af65b0-9bc3-4488-92a3-eaa72  
Resource group: virtual-wan-spoke-rg

Deployment details (Download)

Resource	Type	Status	Operation details
wan-spoke-vm/web-startup	Microsoft.Compute/virtu...	OK	Operation details
wan-spoke-vm	Microsoft.Compute/virtu...	OK	Operation details
wan-spoke-vm-nic0	Microsoft.Network/netw...	Created	Operation details
CREATE_HUB_CONNECTIO	Microsoft.Resources/dep...	OK	Operation details
wan-spoke-vnet	Microsoft.Network/virtu...	OK	Operation details
wan-spoke-vm-nsg	Microsoft.Network/netw...	OK	Operation details
wan-spoke-vm-pip	Microsoft.Network/publi...	OK	Operation details

Next steps

Go to resource group

# Part 6

# Test Flows

# Inbound Config - Add Route for vWAN Spoke VNET

Login to Panorama

Open Network tab

- Select your inbound template **stack**
- Click Virtual Routers
- Click **pan-inbound-asc-vr**
- Click Static Routes

1. Clone the **HV\_hub\_\*** route
2. Change route destination to your WAN Spoke VNET prefix from Part 5.
3. Click OK

The screenshot shows the Panorama interface with the 'NETWORK' tab selected. A red box highlights the 'Template' dropdown set to 'inbound-eastus-inbd-ts-1.0'. Another red box highlights the 'pan-inbound-asc-vr' virtual router entry in the list. A third red box highlights the 'Static Routes' tab in the configuration pane. A fourth red box highlights the 'Clone' button at the bottom of the static routes list. The right-hand panel displays the 'Virtual Router - Static Route - IPv4' configuration for a route named 'to-wan-spoke' with destination '10.4.0.0/16' via interface 'ethernet1/2' and next hop '192.168.1.1'. It also shows a cloned route 'HV\_hub1\_e...' with destination '10.10.0.0/24' via interface 'ethernet1/1'. The 'OK' button is visible at the bottom right of the dialog.

# Inbound Config - Add WAN Spoke Application

1. Open the *Panorama* Tab and go to Deployments within the Azure plugin
2. Open the inbound deployment and click to the *Protect* tab.
3. Create 2 protected applications.
  1. Inbound HTTP to the WAN Spoke VM.
  2. Inbound SSH to the WAN Spoke VM.

2. Use the spoke-address output from Part 5 output for the Backend IP value

The screenshot shows the Panorama interface with the 'Deployments' section selected. A table lists an inbound deployment named 'inbound-eastus' with a description: 'Inbound VM-Scale set for Virtual WAN environment.' The deployment status is 'Success'. Below the table, the 'Configuration' pane is open, showing the 'Protect' tab selected. Two protected applications are listed: 'wan-spoke-ssh' and 'wan-spoke-http'. The 'FrontEnd' table shows the configuration for each application.

NAME	NAT RULE NAME	FRONTEND IP	FRONTEND PORT	BACKEND IP	BACKEND PORT	PROTOCOL	FRONTEND STATUS
wan-spoke-ssh			80	10.4.0.4	80	TCP	Commit required
wan-spoke-http			22	10.4.0.4	22	TCP	Commit required

FrontEnd

Application	wan-spoke-ssh
Protocol	<input checked="" type="radio"/> TCP <input type="radio"/> UDP
Frontend IP Type	Existing Frontend
Frontend Name	default-frontend
Frontend Port	22
Backend IP	10.4.0.4
Backend Port	22

**OK** **Cancel**

FrontEnd

Application	wan-spoke-http
Protocol	<input checked="" type="radio"/> TCP <input type="radio"/> UDP
Frontend IP Type	Existing Frontend
Frontend Name	default-frontend
Frontend Port	80
Backend IP	10.4.0.4
Backend Port	80

**OK** **Cancel**

# Inbound Config - Add Security Policies

1. Go to Policies tab and select the inbound Device Group.
2. Within security pre-rules create 2 policies as seen below.
  - a. Health-probe allows the public load balancers health probes to traverse the firewalls.
  - b. Inbound-wan-spoke: allows inbound HTTP and SSH to the spoke network created in Part 5.

The screenshot shows the PANORAMA interface with the following details:

- Header:** PANORAMA, DASHBOARD, ACC, MONITOR, POLICIES (selected), OBJECTS, NETWORK, DEVICE, PANORAMA.
- Left Sidebar:** Panorama dropdown, Device Group dropdown set to "inbound-eastus-inbd-dg-1.0".
  - Security:** Pre Rules (selected), Post Rules, Default Rules.
  - NAT:** Pre Rules, Post Rules.
  - QoS:** Pre Rules.
- Table:** Displays two security policies in the "Pre Rules" section.

NAME	Source		Destination		APPLICATION	SERVICE	ACTION
	ZONE	ADDRESS	ZONE	ADDRESS			
1 health-probe	pan-untrust-zone	168.63.129.16	pan-untrust-zone	any	any	application-...	Allow
2 inbound-wan-spoke	pan-untrust-zone	any	pan-trust-zone	any	ssh	application-...	Allow

# Outbound Config - Add Security Policies

1. Go to Policies tab and select the outbound Device Group.
2. Within security pre-rules create a policy to allow traffic to flow.

The screenshot shows the PANORAMA interface with the following details:

- PANORAMA** logo and title bar.
- Navigation tabs: DASHBOARD, ACC, MONITOR, POLICIES (selected), Device Groups, OBJECTS, NETWORK, DEVICE, PANORAMA.
- Device Group dropdown: Panorama > Device Group > outbound-eastus-hub-dg-1.0.
- Left sidebar menu:
  - Security: Pre Rules (selected), Post Rules, Default Rules.
  - NAT: Pre Rules.
- Table view of security policies:

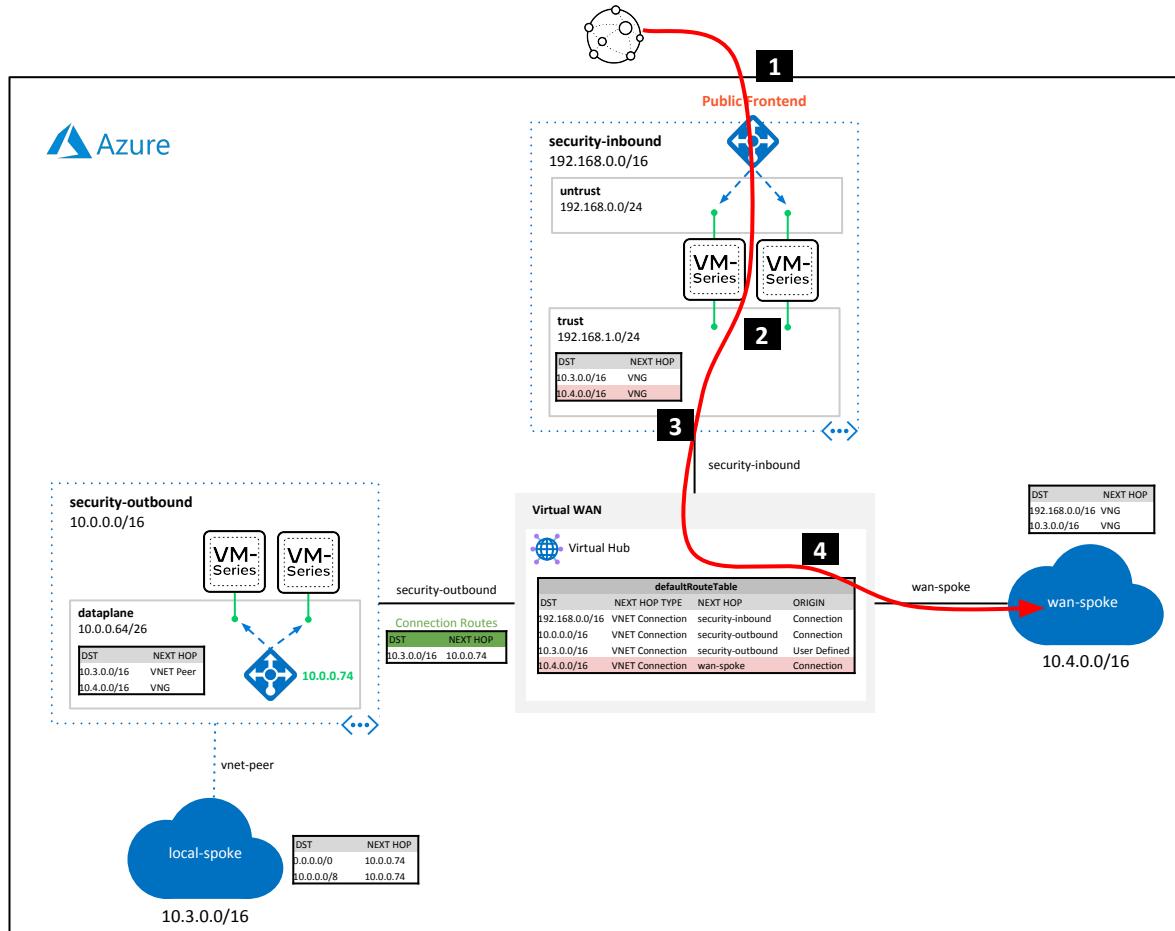
NAME	Source		Destination		APPLICATION	SERVICE	ACTION
	ZONE	ADDRESS	ZONE	ADDRESS			
lateral-flow	pan-data-zone	any	pan-data-zone	any	any	application-...	Allow

[Push & Commit Changes](#)

# Test Inbound Flow

# Inbound Flow

1. Inbound request hits public load balancer frontend IP.
2. VM-Series SNAT to trust interface and DNAT to destination (**10.4.0.4**).
3. Trust subnet sends traffic to vWAN hub via propagated route.
4. vWAN hub route table sends request to wan-spoke VNET connection.



# Add WAN Spoke Application

1. Go to back to the Protect tab within the inbound deployment.
2. Copy the Frontend IP address.
3. Paste `http://<frontend-ip>` into your web browser.

Configuration

Build | Protect

FrontEnd

	NAME	NAT RULE NAME	FRONTEND IP	FRONTEND PORT	BACKEND IP	BACKEND PORT	PROTOCOL	FRONTEND STATUS
<input type="checkbox"/>	wan-spoke-ssh	wan-spoke-ssh-inbound	52.142.39.213	22	10.4.0.4	22	TCP	Configured
<input type="checkbox"/>	wan-spoke-ssh	wan-spoke-ssh-inbound	52.142.39.213	22	10.4.0.4	22	TCP	Configured

(+) Add (-) Delete

OK Cancel

52.142.39.213

http://52.142.39.213

SOURCE & DESTINATION ADDRESSES

INTERVAL: 0.00018000602722168

SOURCE IP: 192.168.1.4

LOCAL IP: 10.4.0.4

VM NAME: wan-spoke-vm

HEADER INFORMATION

HTTP\_HOST: 52.142.39.213

HTTP\_USER\_AGENT: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:84.0) Gecko/20100101 Firefox/84.0

HTTP\_ACCEPT: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8

HTTP\_ACCEPT\_LANGUAGE: en-US,en;q=0.5

HTTP\_ACCEPT\_ENCODING: gzip, deflate

HTTP\_CONNECTION: keep-alive

HTTP\_UPGRADE\_INSECURE\_REQUESTS: 1

# Test Outbound Flow

# Add WAN Spoke Application

1. Use the same IP to SSH to the WAN spoke VM. Use the username/password from Part 5.

```
ssh <user>@<your-frontend-ip>
```

2. Ping to the locally peered spoke (created in Part 4).

```
~ $ ssh paloalto@52.142.39.213
paloalto@52.142.39.213's password:
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 5.4.0-1031-azure x86_64)
```

```
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/advantage

System information as of Wed Dec 30 01:11:25 UTC 2020

System load: 0.0          Processes:      118
Usage of /: 5.2% of 28.90GB  Users logged in: 0
Memory usage: 24%          IP address for eth0: 10.4.0.4
Swap usage: 0%             20 packages can be updated.
                           16 updates are security updates.
```

The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/\*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".  
See "man sudo\_root" for details.

```
paloalto@wan-spoke-vm:~$ ping 10.3.0.4
PING 10.3.0.4 (10.3.0.4) 56(84) bytes of data.
64 bytes from 10.3.0.4: icmp_seq=1 ttl=62 time=6.12 ms
64 bytes from 10.3.0.4: icmp_seq=2 ttl=62 time=4.17 ms
64 bytes from 10.3.0.4: icmp_seq=3 ttl=62 time=3.70 ms
64 bytes from 10.3.0.4: icmp_seq=4 ttl=62 time=6.34 ms
64 bytes from 10.3.0.4: icmp_seq=5 ttl=62 time=4.49 ms
64 bytes from 10.3.0.4: icmp_seq=6 ttl=62 time=4.13 ms
64 bytes from 10.3.0.4: icmp_seq=7 ttl=62 time=3.62 ms
64 bytes from 10.3.0.4: icmp_seq=8 ttl=62 time=3.71 ms
64 bytes from 10.3.0.4: icmp_seq=9 ttl=62 time=3.92 ms
^C
--- 10.3.0.4 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8012ms
rtt min/avg/max/mdev = 3.626/4.471/6.344/0.978 ms
paloalto@wan-spoke-vm:~$
```

# Add WAN Spoke Application

1. Go to the monitor tab
2. Filter for the HTTP & SSH logs within the inbound device group.

The screenshot shows the PANORAMA interface in monitor mode. The device group selected is "inbound-eastus-inbd-dg-1.0". The search bar contains the query "( app eq web-browsing ) or ( app eq ssh )". The results table displays two log entries:

	GENERATE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	DESTINATION	TO PORT	APPLICATION	ACTION	RULE	SESSION END REASON
	12/29 20:17:20	end	pan-untrust-zone	pan-trust-zone	74.97.22.10	52.142.39.213	22	ssh	allow	inbound-wan-spoke	tcp-fin
	12/29 20:16:50	end	pan-untrust-zone	pan-trust-zone	74.97.22.10	52.142.39.213	80	web-browsing	allow	inbound-wan-spoke	tcp-fin

3. Filter for the ping logs within the outbound device group.

The screenshot shows the PANORAMA interface in monitor mode. The device group selected is "outbound-eastus-hub-dg-1.0". The search bar contains the query "( app eq ping )". The results table displays three log entries:

	GENERATE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	DESTINATION	TO PORT	APPLICATION	ACTION	RULE	SESSION END REASON
	12/29 20:17:14	end	pan-data-zone	pan-data-zone	10.4.0.4	10.3.0.4	0	ping	allow	lateral-flow	aged-out
	12/29 20:11:54	end	pan-data-zone	pan-data-zone	10.4.0.4	10.3.0.4	0	ping	allow	lateral-flow	aged-out
	12/29 20:11:47	end	pan-data-zone	pan-data-zone	10.4.0.4	10.3.0.4	0	ping	allow	lateral-flow	aged-out



# Thank you

