# Isolating Traffic with the 10GbE UTM Firewall

Feature Overview and Configuration Guide

## Introduction

This guide describes creating multiple firewalls and configuring them separately inside the 10GbE UTM Firewall application on the VST-APL appliance. Inside the 10GbE UTM firewall, separate firewall instances can be internally configured for a variety of network traffic solutions. This document shows an example of using this to separate traffic within a multi-tenant building.

Configuring this example involves two separate aspects:

- Configuring the VST-APL appliance, including creating the firewall instances
- Configuring each individual firewall instance that you create.

This guide describes both these aspects.

## Contents

## Products and software version that apply to this guide

This guide applies to the 10GbE UTM Firewall product, running version **5.5.3-0.1** or later.

For more information, see the following documents:

- VST-APL User Guide
- The 10GbE UTM Firewall Datasheet
- Getting Started with the Device GUI on UTM Firewalls Feature Overview Guide
- The product’s Command Reference

These documents are available from the above links on our website at alliedtelesis.com.

# Prerequisites

Before you start, make sure that you have installed the firewall application onto your VST-APL appliance and done other configuration of that appliance, such as creating users and specifying network settings. See the VST-APL User Guide for details about this.

You need a license (AT-FL-VFW-BASE) to run the firewall and VPN on the virtual firewall. Contact your Allied Telesis distributor or reseller to obtain a license.

# Ways to configure the appliance and firewall instances

This document refers to two GUIs:

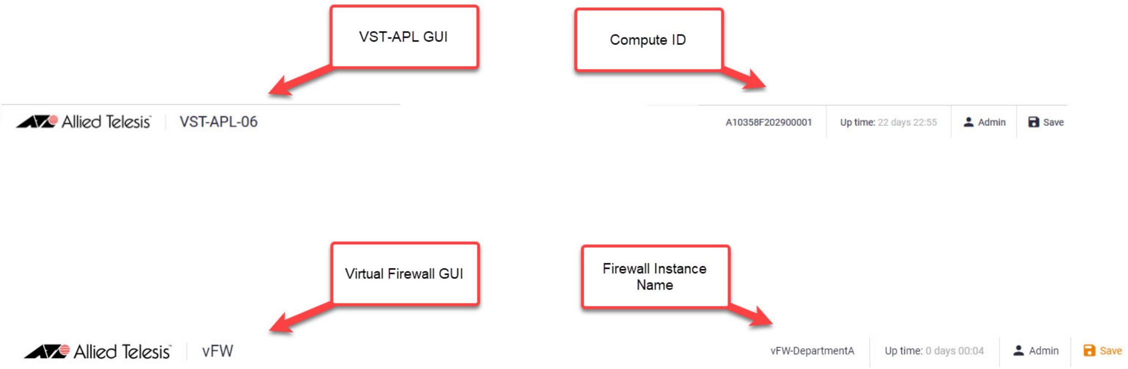
- the VST-APL GUI, which lets you configure the VST-APL appliance and create each firewall instance, and
- the Device GUI for each firewall instance, which lets you configure and monitor each firewall instance.

To create the scenario described in this Guide, you need to first configure the VST-APL appliance, and then each firewall instance.

To configure the VST-APL appliance, use its web-based GUI. In this document, we call this the VST-APL GUI. To access this, browse to the VST-APL IP address, using the web browser of your choice.

To configure the firewall instances, use either their web-based GUI or their CLI. To access a firewall instance's GUI, either browse to the instance’s IP address or click Open on the instance you wish to open on the Container Services page. To access the CLI, either use the System menu on the firewall instance’s Device GUI, or use an SSH client of your choice.

If you are using the GUIs to configure the appliance and the instances, make sure you know which GUI you are using. The easiest way to distinguish them is by checking the product name in the GUI:

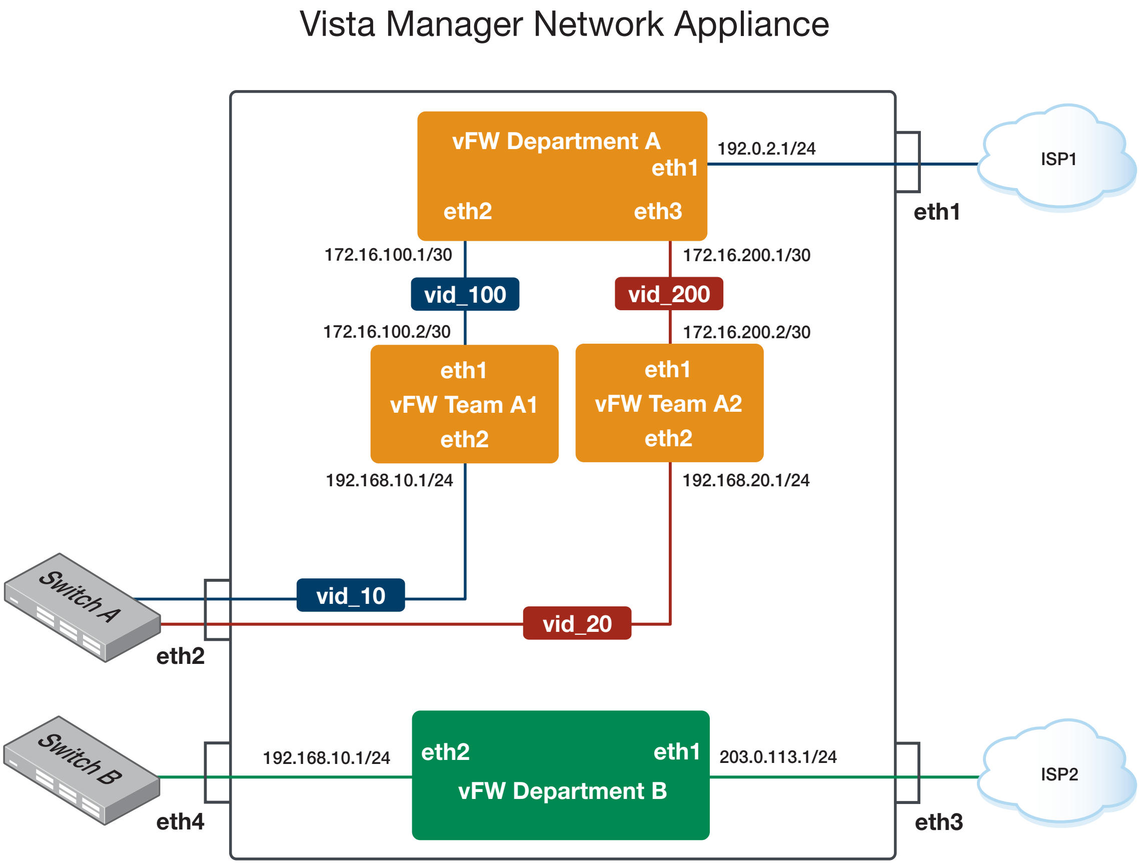


# Creating the firewall instances

You can create and configure multiple virtual firewall instances on a single VST-APL. This means you can create multiple independent routing domains with overlapping addressing. Multiple virtual router instances provide the functionality of VRF without the limitations of VRF-lite.

This example shows how to use multiple vFWs to manage different parts of a network independently. Department A's firewall is with ISP1, and TeamA1 and TeamA2 are isolated from each other with their own routers. Communication between the teams and Department A is achieved with virtual Ethernet interfaces. These interfaces are configured as part of the VST-APL appliance configuration. Another department, Department B, is also managed independently from Department A. Its firewall is with ISP2.

Figure 1: Multiple virtual firewalls with separated departments and teams



## Configure the bridging

To create the example above, you will need to configure the physical Ethernet connections via network bridging. This section describes how to do this. This means creating a bridge to connect Team A2 and Team A1's virtual interfaces to the physical Ethernet interface (eth2). We also need to remove some ports from br0, because this configuration uses them physically.

Step 1: **Open the VST-APL GUI.**

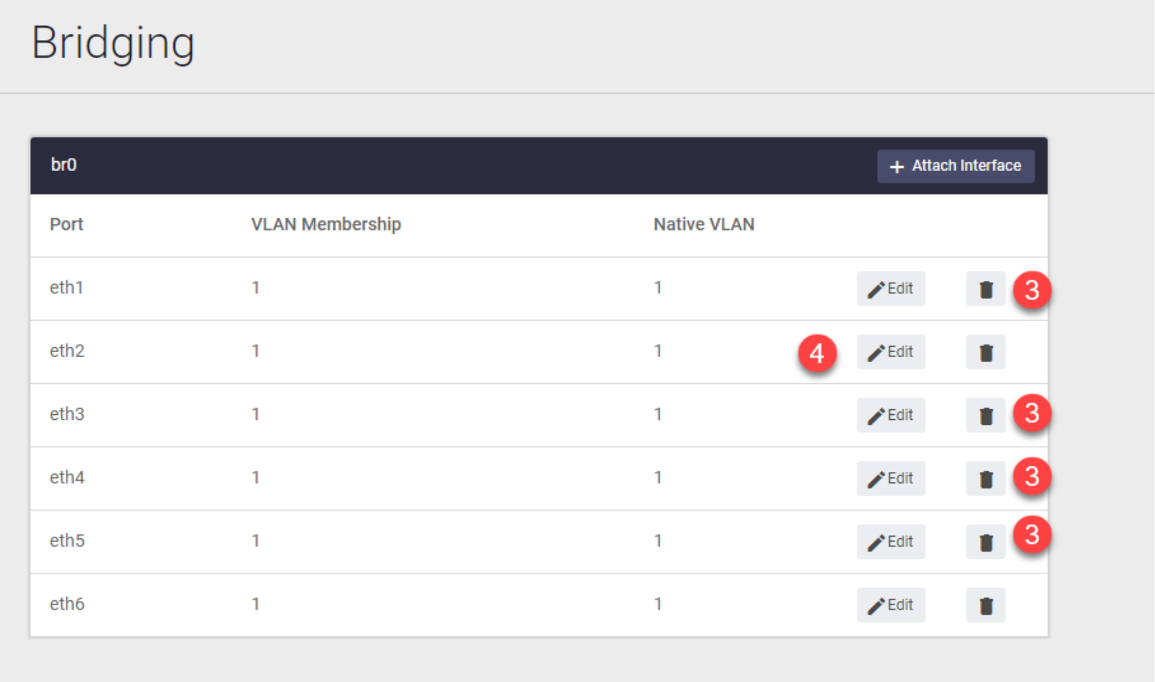
Step 2: **From the Network Infrastructure menu, click Bridging.**

Step 3: **Delete eth1, eth3, eth4, and eth5, from br0.**

In this example, VLAN1 is used for the management of the VST-APL appliance and all virtual routers. Eth6 is reserved for management traffic. You can choose any Ethernet ports to fit your desired network, however one Ethernet port must remain so you do not lose access to the VST-APL.

The physical port eth1 is assigned to Department A, so we need to remove it from br0. The physical ports eth3 and eth4 are assigned to Department B, so we need to remove them from br0.

Step 4: **Edit eth2.**



Bridging

br0

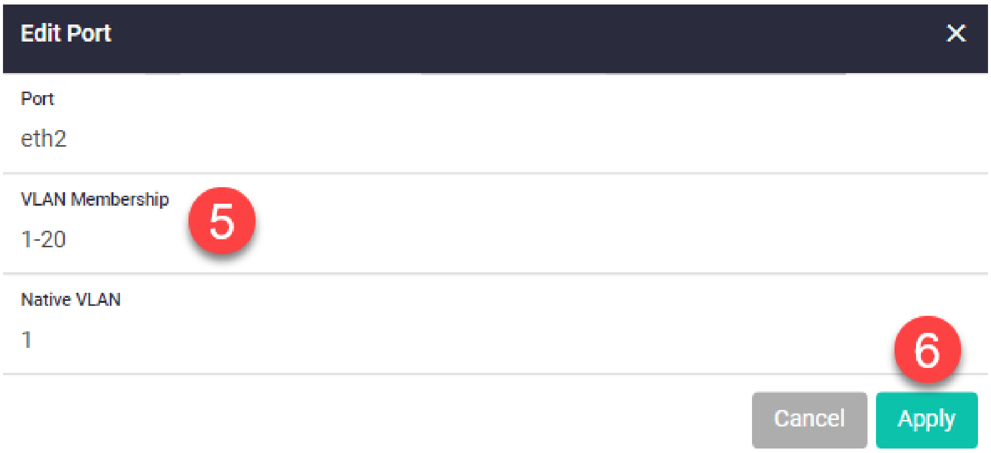
| Port | VLAN Membership | Native VLAN |
|---|---|---|
| eth1 | 1 | 1 |
| eth2 | 1 | 1 |
| eth3 | 1 | 1 |
| eth4 | 1 | 1 |
| eth5 | 1 | 1 |
| eth6 | 1 | 1 |

Step 5: **Set the VLAN membership to 1-20.**

Traffic from Team A1 (VLAN10) and Team A2 (VLAN 20) goes through eth2. Therefore, we need to include 10 and 20 in eth2's VLAN membership in the bridge.

In this example the VLAN membership ID is set to the range from 1-20. Our physical to virtual connections are using VLAN 10 and VLAN 20, however you can select any VLAN between 2 and 20 in this case.

Step 6: **Click Apply.**



Edit Port

Port: eth2

VLAN Membership: 1-20

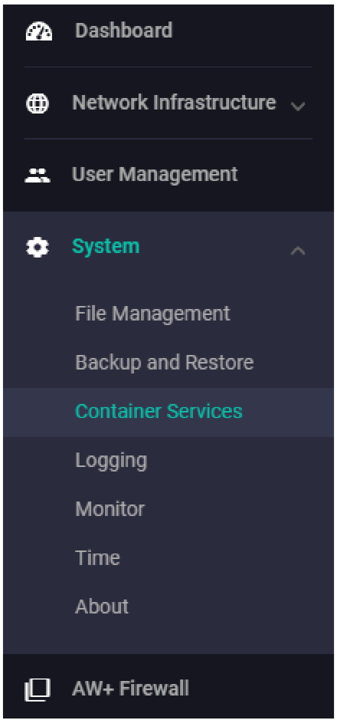
Native VLAN: 1

## Create the virtual firewall instances

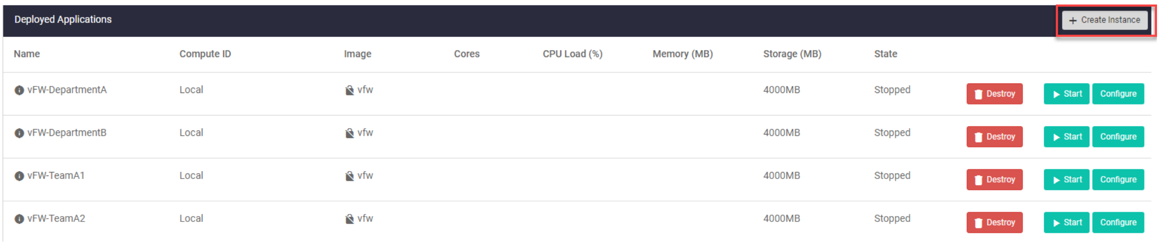
To begin to isolate traffic, we must first create the firewall instances we would like for our network. First we will create the different firewall instances:

Step 1: **Open the VST-APL GUI.**

Step 2: **From the System menu, click Container Services.**



### Step 3: In the Deployed Applications tab, click +Create Instance.



Deployed Applications

+ Create Instance

| Name | Compute ID | Image | Cores | CPU Load (%) | Memory (MB) | Storage (MB) | State | | |
|---|---|---|---|---|---|---|---|---|---|
| vFW-DepartmentA | Local | vfw | | | | 4000MB | Stopped | Destroy | ▶ Start Configure |
| vFW-DepartmentB | Local | vfw | | | | 4000MB | Stopped | Destroy | ▶ Start Configure |
| vFW-TeamA1 | Local | vfw | | | | 4000MB | Stopped | Destroy | ▶ Start Configure |
| vFW-TeamA2 | Local | vfw | | | | 4000MB | Stopped | Destroy | ▶ Start Configure |

### Step 1: Create an instance for Department A.

a. Enter the instance’s name.

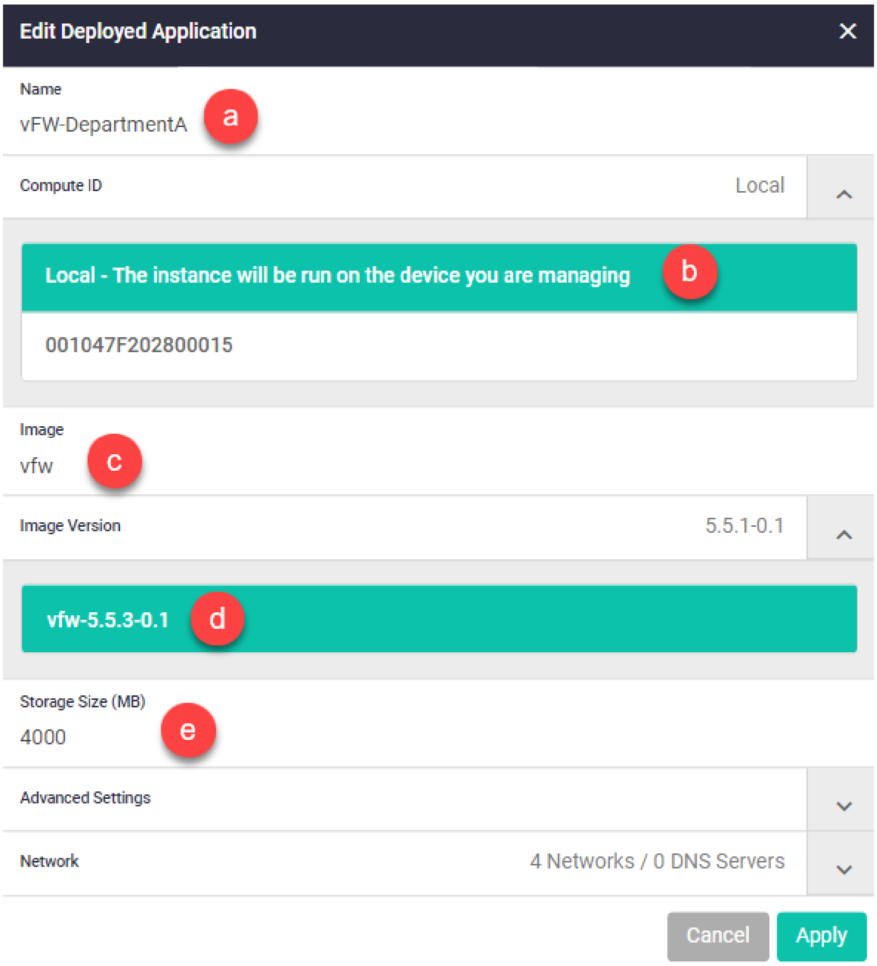
b. Select Local Compute ID.

c. Select Image.

d. Select the Image Version.

e. Input a storage size.

We recommend using a storage of at least 4000MB.



Edit Deployed Application

Name: vFW-DepartmentA

Compute ID: Local

Local - The instance will be run on the device you are managing

001047F202800015

Image: vfw

Image Version: 5.5.1-0.1

vfw-5.5.3-0.1

Storage Size (MB): 4000

Advanced Settings

Network: 4 Networks / 0 DNS Servers

Then, we create the rest of the instances.

Step 2: **Create an instance for Department B.**

Give this instance a unique name, such as vFW-DepartmentB. Fill out the rest of its settings, with the same values as Department A's instance. Repeat this for all instances.

Step 3: **Create an instance for Team A1.**

Step 4: **Create an instance for Team A2.**

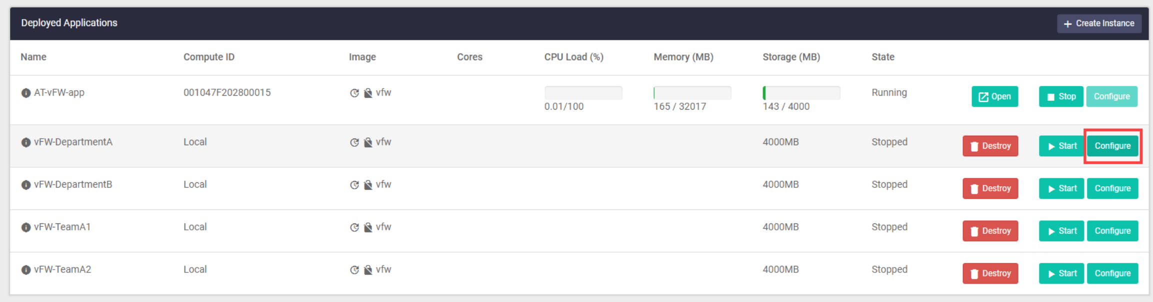
## Configure the virtual and physical interfaces

We will now configure the virtual and physical interfaces which connect the VST-APL to the VLANs, and the VLANs to their separated teams.

VLAN1 is used for management of the instances. This has to be configured before configuring the other interfaces.

### Configure the interfaces for Department A

Step 1: **On the Deployed Applications screen, click Configure next to the Department A instance. This opens the Edit Deployed Application screen.**



Deployed Applications

| Name | Compute ID | Image | Cores | CPU Load (%) | Memory (MB) | Storage (MB) | State | | |
|---|---|---|---|---|---|---|---|---|---|
| AT-vFW-app | 001047F202800015 | vfw | | 0.01/100 | 165 / 32017 | 143 / 4000 | Running | Open | Stop Configure |
| vFW-DepartmentA | Local | vfw | | | | 4000MB | Stopped | Destroy | ▶ Start Configure |
| vFW-DepartmentB | Local | vfw | | | | 4000MB | Stopped | Destroy | ▶ Start Configure |
| vFW-TeamA1 | Local | vfw | | | | 4000MB | Stopped | Destroy | ▶ Start Configure |
| vFW-TeamA2 | Local | vfw | | | | 4000MB | Stopped | Destroy | ▶ Start Configure |

Step 2: **Click on the Network drop-down.**

Step 3: **Configure the virtual interface for VLAN1.**

This is eth0 and is used for management. Make sure it has a VLAN ID of 1, and give it a management IP address and default gateway address if necessary.

Step 4: **Click +Add network.**

Step 5: **Configure the second interface as a physical interface with host interface eth1.**

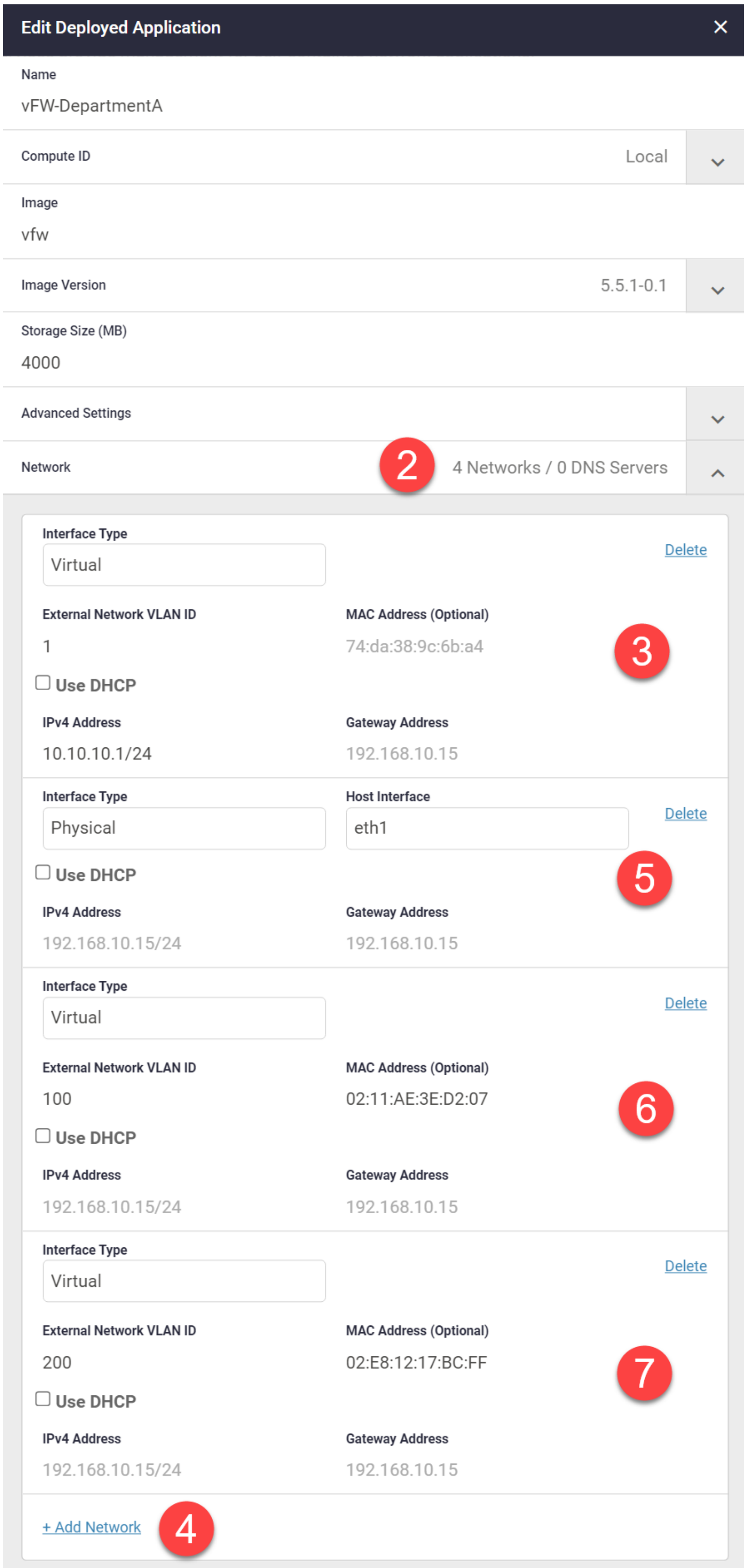
Step 6: **Click +Add Network again and configure the third interface as a virtual interface for VLAN100.**

This is eth2, which connects Department A to Team A1.

Step 7: **Click +Add Network again and configure the fourth interface as a virtual interface for VLAN200.**

This is eth3, which connects Department A to Team A2.

Figure 2: Settings for the virtual firewall instance for Department A



Edit Deployed Application

Name
vFW-DepartmentA

Compute ID: Local

Image
vfw

Image Version: 5.5.1-0.1

Storage Size (MB)
4000

Advanced Settings

Network: 4 Networks / 0 DNS Servers

Interface Type: Virtual
External Network VLAN ID: 1
MAC Address (Optional): 74:da:38:9c:6b:a4
□ Use DHCP
IPv4 Address: 10.10.10.1/24
Gateway Address: 192.168.10.15

Interface Type: Physical
Host Interface: eth1
□ Use DHCP
IPv4 Address: 192.168.10.15/24
Gateway Address: 192.168.10.15

Interface Type: Virtual
External Network VLAN ID: 100
MAC Address (Optional): 02:11:AE:3E:D2:07
□ Use DHCP
IPv4 Address: 192.168.10.15/24
Gateway Address: 192.168.10.15

Interface Type: Virtual
External Network VLAN ID: 200
MAC Address (Optional): 02:E8:12:17:BC:FF
□ Use DHCP
IPv4 Address: 192.168.10.15/24
Gateway Address: 192.168.10.15

### Configure the interfaces for Department B

Step 1: **On the Deployed Applications screen, click Configure next to the Department B instance. This opens the Edit Deployed Application screen.**

Step 2: **Click on the Network drop-down.**

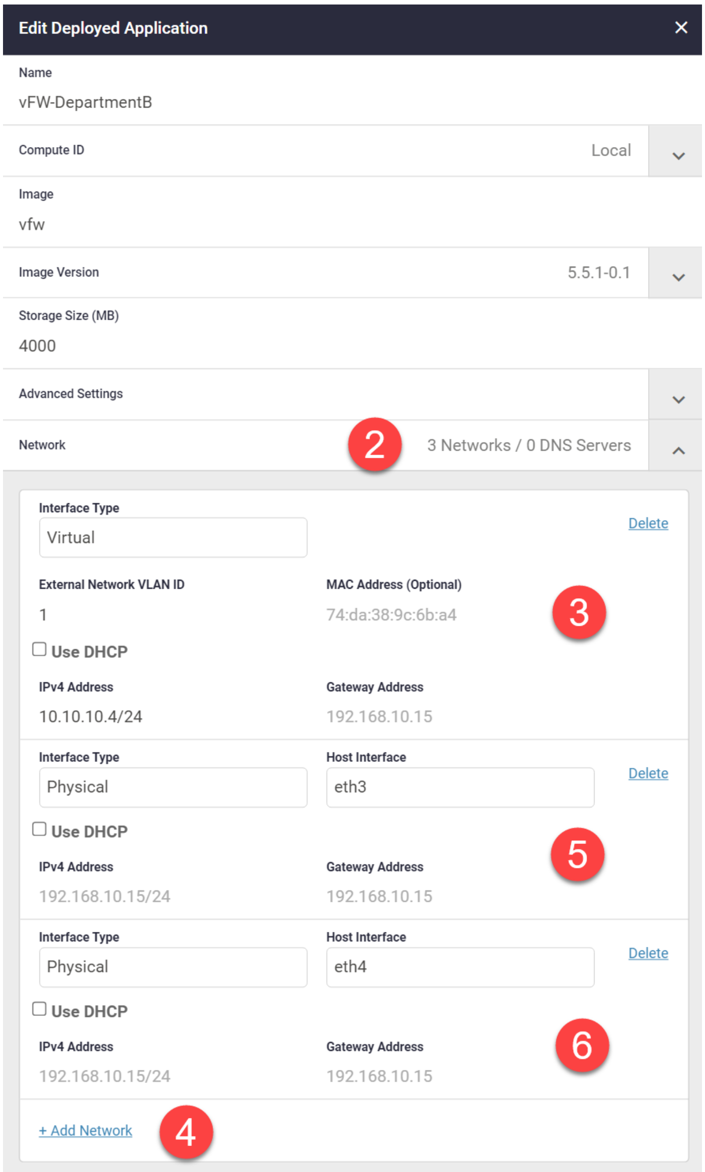
Step 3: **Click +Add network.**

Step 4: **Configure the virtual interface for VLAN1.**

Step 5: **Click +Add Network again and configure the physical host interface on eth3.**

Step 6: **Click +Add Network again and configure the physical host interface on eth4.**

Figure 3: Settings for the virtual firewall instance for Department B



Edit Deployed Application ✕

Name: vFW-DepartmentB

Compute ID: Local

Image: vfw

Image Version: 5.5.1-0.1

Storage Size (MB): 4000

Advanced Settings

Network: 3 Networks / 0 DNS Servers

Interface Type: Virtual — Delete

External Network VLAN ID: 1

MAC Address (Optional): 74:da:38:9c:6b:a4

□ Use DHCP

IPv4 Address: 10.10.10.4/24

Gateway Address: 192.168.10.15

Interface Type: Physical

Host Interface: eth3 — Delete

□ Use DHCP

IPv4 Address: 192.168.10.15/24

Gateway Address: 192.168.10.15

Interface Type: Physical

Host Interface: eth4 — Delete

□ Use DHCP

IPv4 Address: 192.168.10.15/24

Gateway Address: 192.168.10.15

+ Add Network

### Configure the interfaces for Team A1

Step 1: **On the Deployed Applications screen, click Configure next to the Team A1 instance. This opens the Edit Deployed Application screen.**

Step 2: **Click on the Network drop-down.**

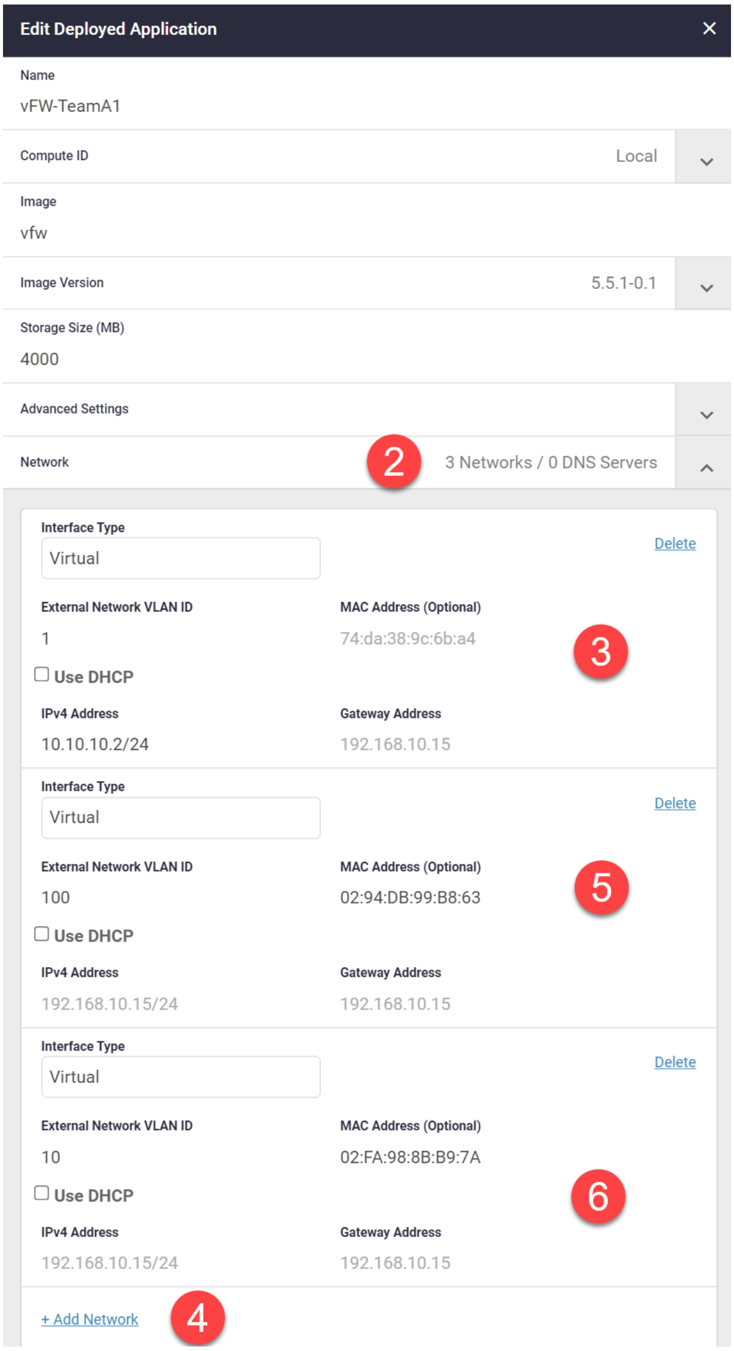
Step 3: **Click +Add network.**

Step 4: **Configure the virtual interface for VLAN1.**

Step 5: **Click +Add Network again and configure the virtual interface for VLAN100.**

Step 6: **Click +Add Network again and configure the virtual interface for VLAN10.**

Figure 4: Settings for the virtual firewall instance for Team A1



Edit Deployed Application ✕

Name
vFW-TeamA1

Compute ID: Local

Image
vfw

Image Version: 5.5.1-0.1

Storage Size (MB)
4000

Advanced Settings

Network — 2 — 3 Networks / 0 DNS Servers

Interface Type: Virtual — Delete
External Network VLAN ID: 1 — MAC Address (Optional): 74:da:38:9c:6b:a4 — 3
□ Use DHCP
IPv4 Address: 10.10.10.2/24 — Gateway Address: 192.168.10.15

Interface Type: Virtual — Delete
External Network VLAN ID: 100 — MAC Address (Optional): 02:94:DB:99:B8:63 — 5
□ Use DHCP
IPv4 Address: 192.168.10.15/24 — Gateway Address: 192.168.10.15

Interface Type: Virtual — Delete
External Network VLAN ID: 10 — MAC Address (Optional): 02:FA:98:8B:B9:7A — 6
□ Use DHCP
IPv4 Address: 192.168.10.15/24 — Gateway Address: 192.168.10.15

+ Add Network — 4

### Configure the interfaces for Team A2

Step 1: **On the Deployed Applications screen, click Configure next to the Team A2 instance. This opens the Edit Deployed Application screen.**

Step 2: **Click on the Network drop-down.**

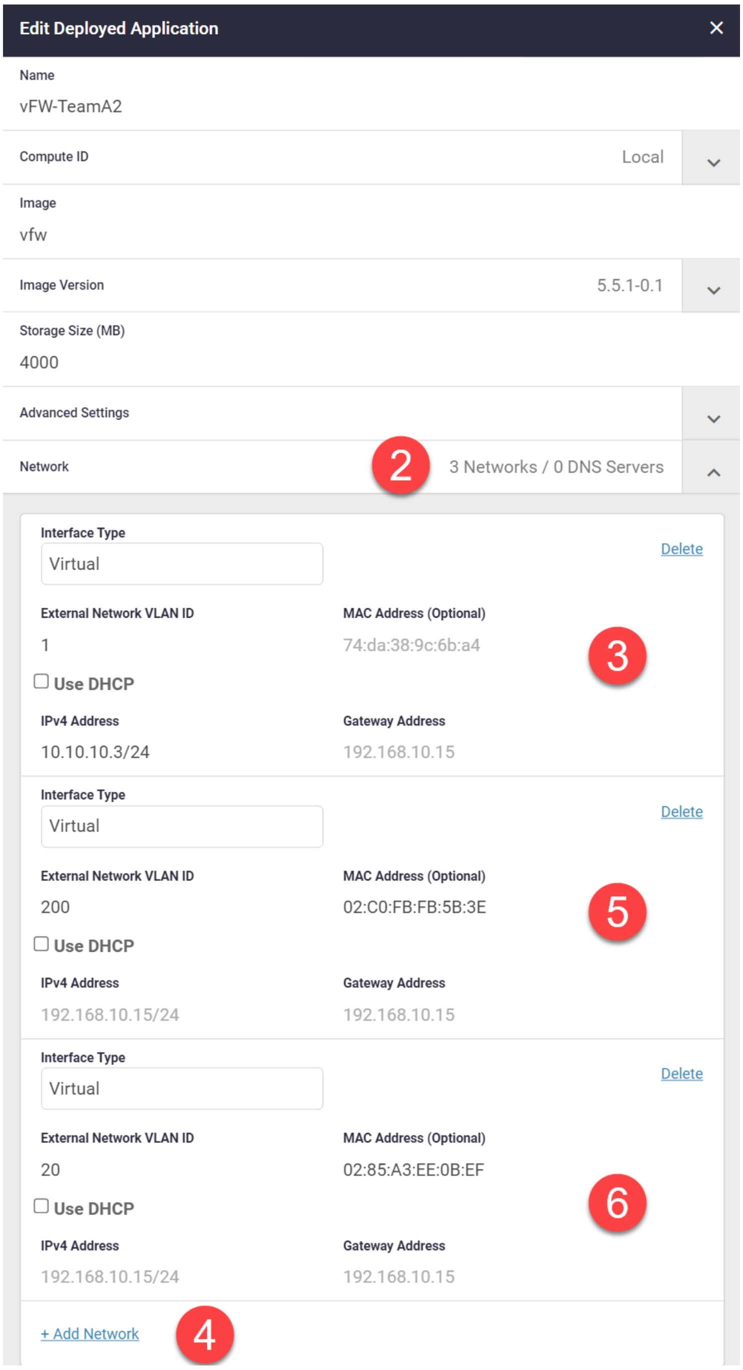
Step 3: **Click +Add network.**

Step 4: **Configure the virtual interface for VLAN1.**

Step 5: **Configure the virtual interface for VLAN 200.**

Step 6: **Configure the virtual interface for VLAN 20.**

Figure 5: Settings for the virtual firewall instance for Team A2



Edit Deployed Application

Name: vFW-TeamA2

Compute ID: Local

Image: vfw

Image Version: 5.5.1-0.1

Storage Size (MB): 4000

Advanced Settings

Network (2): 3 Networks / 0 DNS Servers

(3)
Interface Type: Virtual
External Network VLAN ID: 1
MAC Address (Optional): 74:da:38:9c:6b:a4
□ Use DHCP
IPv4 Address: 10.10.10.3/24
Gateway Address: 192.168.10.15

(5)
Interface Type: Virtual
External Network VLAN ID: 200
MAC Address (Optional): 02:C0:FB:FB:5B:3E
□ Use DHCP
IPv4 Address: 192.168.10.15/24
Gateway Address: 192.168.10.15

(6)
Interface Type: Virtual
External Network VLAN ID: 20
MAC Address (Optional): 02:85:A3:EE:0B:EF
□ Use DHCP
IPv4 Address: 192.168.10.15/24
Gateway Address: 192.168.10.15

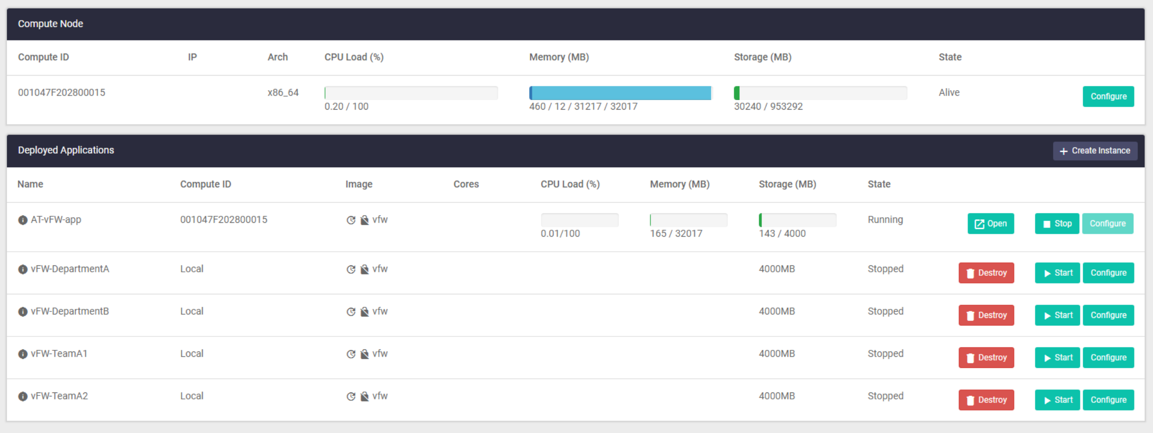
## Running each firewall instance

Now that you have created each of the firewall instances, the next step is to start them running. To do this:

Step 1: **Open the VST-APL GUI.**

Step 2: **From the System menu, click Container Services.**

Step 3: **On the Container Services page, click Start on each instance.**



Compute Node

| Compute ID | IP | Arch | CPU Load (%) | Memory (MB) | Storage (MB) | State | |
|---|---|---|---|---|---|---|---|
| 001047F202800015 | | x86_64 | 0.20 / 100 | 460 / 12 / 31217 / 32017 | 30240 / 953292 | Alive | Configure |

Deployed Applications

| Name | Compute ID | Image | Cores | CPU Load (%) | Memory (MB) | Storage (MB) | State | | |
|---|---|---|---|---|---|---|---|---|---|
| AT-vFW-app | 001047F202800015 | vfw | | 0.01/100 | 165 / 32017 | 143 / 4000 | Running | Open | Stop Configure |
| vFW-DepartmentA | Local | vfw | | | | 4000MB | Stopped | Destroy | ▶ Start Configure |
| vFW-DepartmentB | Local | vfw | | | | 4000MB | Stopped | Destroy | ▶ Start Configure |
| vFW-TeamA1 | Local | vfw | | | | 4000MB | Stopped | Destroy | ▶ Start Configure |
| vFW-TeamA2 | Local | vfw | | | | 4000MB | Stopped | Destroy | ▶ Start Configure |

Note that you cannot access multiple firewall instances from the AW+ Firewall menu in the VST-APL GUI. Instead, you need to access them from the Container Services page.

Step 4: **Back up the configuration.**

We recommend backing up the configuration in case you need to restore it later. See the VST-APL User Guide for details.

# Configuring the firewall instances

You can access each firewall instance through either its Device GUI or its CLI. The instances must be created first through the VST-APL GUI before they can be configured.

To access the virtual firewall GUI, either browse to the firewall instance's IP address or click Open on the instance you wish to open on the Container Services page. To access the CLI, either use the System menu on the firewall instance's Device GUI, or use an SSH client of your choice.

The following sections summarize the CLI commands for each firewall instance.

### Department A configuration

The configuration for Department A can be directly input through the firewall instance's command line interface. This section shows configurations for public and private zones, NAT rules and IP addresses.

```
zone private
 network management
  ip subnet 10.10.10.0/24
  host router
   ip address 10.10.10.1
 network teamA1
  ip subnet 172.16.100.0/30 interface eth2
 network teamA2
  ip subnet 172.16.200.0/30 interface eth3
!
zone public
 network all
  ip subnet 0.0.0.0/0
!
nat
 rule 10 masq any from private.teamA1 to public
 rule 20 masq any from private.teamA2 to public
 enable
!
interface eth0
 ip address 10.10.10.1/24
!
interface eth1
 ip address 192.0.2.1/24
!
interface eth2
 ip address 172.16.100.1/30
!
interface eth3
 ip address 172.16.200.1/30
!
ip route 0.0.0.0/0 192.0.2.2
```

### Team A1 configuration

```
zone private
 network local
  ip subnet 192.168.10.0/24 interface eth2
 network management
  ip subnet 10.10.10.0/24
  host router
   ip address 10.10.10.2
!
zone public
 network all
  ip subnet 0.0.0.0/0
!
nat
 rule 10 masq any from private.local to public
 enable
!
!
interface eth0
 ip address 10.10.10.2/24
!
interface eth1
 ip address 172.16.100.2/30
!
interface eth2
 ip address 192.168.10.1/24
!
ip route 0.0.0.0/0 172.16.100.1
```

### Team A2 configuration

```
zone private
 network local
  ip subnet 192.168.20.0/24 interface eth2
 network management
  ip subnet 10.10.10.0/24
  host router
   ip address 10.10.10.3
!
zone public
 network all
  ip subnet 0.0.0.0/0
!
nat
 rule 10 masq any from private.local to public
 enable
!
interface eth0
 ip address 10.10.10.3/24
!
interface eth1
 ip address 172.16.200.2/30
!
interface eth2
 ip address 192.168.20.1/24
!
ip route 0.0.0.0/0 172.16.200.1
```

## Department B configuration

```
zone private
 network local
  ip subnet 192.168.10.0/24 interface eth2
 network management
  ip subnet 10.10.10.0/24
  host router
   ip address 10.10.10.4
!
zone public
 network all
  ip subnet 0.0.0.0/0
!
nat
 rule 10 masq any from private.local to public
 enable
!
interface eth0
 ip address 10.10.10.4/24
!
interface eth1
 ip address 203.0.113.1/24
!
interface eth2
 ip address 192.168.10.1/24
!
ip route 0.0.0.0/0 203.0.113.2
```

Allied Telesis NETWORK SMARTER

**North America Headquarters** | 19800 North Creek Parkway | Suite 100 | Bothell | WA 98011 | USA | T: +1 800 424 4284 | F: +1 425 481 3895
**Asia-Pacific Headquarters** | 11 Tai Seng Link | Singapore | 534182 | T: +65 6383 3832 | F: +65 6383 3830
**EMEA & CSA Operations** | Incheonweg 7 | 1437 EK Rozenburg | The Netherlands | T: +31 20 7950020 | F: +31 20 7950021

**alliedtelesis**.com