

Getting Started with the Device GUI on VPN Routers

Introduction

Allied Telesis Virtual Private Network (VPN) Routers are the ideal secure gateway for modern businesses. Powerful firewall and VPN functionality is combined with routing and switching, to provide an innovative high performance solution.

What information will you find in this document?

The Device GUI provides graphical management and monitoring for switches, UTM firewalls, and VPN routers running the AlliedWare Plus™ operating system.

This guide show how to configure a VPN Router using the Device GUI.

The Device GUI provides setup of the router, enabling the configuration of entities (zones, networks, and hosts) and then creating firewall, NAT, and traffic-control rules for managing traffic between these entities. Features such as the Intrusion Prevention System (IPS) and URL Filtering help protect the network, and manage website access.

The GUI also supports a number of other features such as interface, VLAN, file, log, and wireless network management, as well as a CLI window and a Dashboard for network monitoring. The Dashboard shows interface and firewall traffic, system and environmental information, and the security monitoring widget lets you view and manage rules and security features.

You can configure the complete AlliedWare Plus feature-set using the GUI's built-in industry standard Command Line Interface (CLI) window.



Contents

Introduction	1
What information will you find in this document?	1
Products and software version that apply to this guide	3
Related documents	3
The Device GUI	4
Connecting to the GUI	4
Updating the GUI	4
Using the Wizard to configure Internet and VPN connections	6
Setup an Internet connection	6
Configuring a VPN connection	16
What is a firewall?	19
What are entities?	19
Zones, networks, and hosts	20
Using rules	21
Configuring the router	22
Part 1: Configure a standard 3-zone network	22
Part 2: Configure the router for Update Manager	37
Part 3: Configure security features	39
Creating custom lists	43
The Dashboard	44
The network map	47
The network map features	47
Viewing node information	48
Configuring the topology view	48
Customizing network node icon images	49
Access to device GUI by clicking on device icon	50
Wireless management	51
Other features	52
File management	52
Logging management	54

Products and software version that apply to this guide

This guide applies to all AR-Series VPN Routers running AlliedWare Plus™ software version 5.4.7-x.x or 5.4.8-x.x. Supported models include the AR2050V, AR2010V. The AR1050V is supported from software version 5.5.0-2.1 onwards.

Feature support may change in later software versions. For the latest information, see the following documents:

- The [product's Datasheet](#)
- The [AlliedWare Plus Datasheet](#)
- The product's [Command Reference](#)

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

Related documents

You also may find the following AlliedWare Plus Feature Overviews useful:

- [URL Filtering](#)
- [Intrusion Prevention System](#)

To configure an Allied Telesis UTM firewall or switch using the Device GUI, see the following guides:

- [Getting Started with the Device GUI on UTM Firewalls](#)
- [Getting Started with the Device GUI on Switches](#)

For detailed documentation on wireless configuration, see:

- [User Guide: Wireless Management \(AWC\) with Vista Manager mini](#).

The Device GUI

This section describes how to connect your router to the Device GUI. Your router will have a GUI already loaded. If your router has an older GUI version, you can update it using the steps outlined below.

Your router must be running AlliedWare Plus software version **5.4.8-0.2** or later.

Supported web browsers for connecting to the Device GUI are:

- Google Chrome™
- Mozilla Firefox™
- Microsoft Edge or Internet Explorer 11™
- Apple Safari™

Connecting to the GUI

To connect to the GUI, use the following steps:

1. Connect to any of the LAN ports.
2. Open a web browser and browse to the default IP address for VLAN1.
 - The default IP address is 169.254.42.42
 - Alternatively, give VLAN1 an IP address of your choice and browse to that address.
3. Log in with the default username of **manager** and the default password of **friend**.

Updating the GUI

Perform the following steps if you have been running an earlier version of the GUI and need to update it.

1. Obtain the GUI file from our [Software Download](#) centre. The filename ends in .gui. The file is not device-specific; the same file works on all AlliedWare Plus devices.

2. Log into the GUI:

Start a browser and browse to the device's IP address, using HTTPS. You can access the GUI via any reachable IP address on any interface.

The GUI starts up and displays a login screen. Log in with your username and password.

The default username is **manager** and the default password is **friend**.

3. Go to **System > File Management**
4. Click **Upload**.

The screenshot shows the File Management interface for an AR2010V router. The main area displays a table of files in the /fs/flash directory:

Name	Modified	Size(bytes)	Actions
AR2010V-5.5.0-...	12/21/2020, 12:02:30 PM	58463543	Download Delete
AR2010V-5.5.1-...	5/3/2021, 11:12:55 AM	52924011	Download Delete
awplus-gui_551...	5/3/2021, 11:14:34 AM	2707456	Download Delete
default.cfg	9/8/2020, 3:01:23 PM	1926	Download Delete
docnet-base.cfg	12/7/2020, 4:47:54 PM	1873	Download Delete
gui-userdata	1/3/2019, 10:38:24 AM		

The right sidebar contains the following sections:

- Set Boot Release File:** Current: flash:/AR2010 V-5.5.1-0.2.rel; Backup: flash:/AR2010 V-5.5.0-2.3.rel
- Set Boot Config File:** Current: flash:/default.cfg; Backup: Not Set
- Flash Usage:** 3% (116.6M / 3.6G)

- Locate and select the GUI file you downloaded from our Software Download centre. The new GUI file is added to the **File Management** window.
- Use a Serial console connection, or Telnet, or SSH to access the CLI, then use the following commands to stop and restart the HTTP service:


```
awplus# configure terminal
awplus(config)# no service http
awplus(config)# service http
```
- In the Device GUI, go to **System > About** to check that the latest file has been successfully added to the device. Look for the GUI Version and GUI Build entries. The first part of the GUI Build entry is the GUI build date.

System Information	
Name:	AR2010V
Model:	AR2010V
MAC Address:	00-1a-eb-94-2a-39
Serial Number:	000190G154600008
Environment:	✔ Status: Good
Current Software:	AR2010V-5.5.1-0.2.rel
Software Version:	5.5.1-0.2
Bootloader:	5.0.5
GUI Version:	2.8.0
GUI Build:	20210423_1329

The device GUI service expects a GUI resource file with a .gui extension. If there is more than one .gui file then it will pick up the one with the highest number in its name.

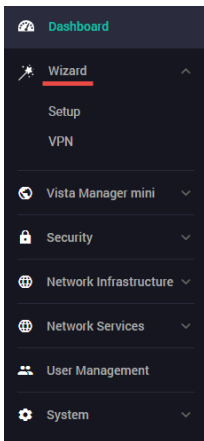
For example, if the following two files are present:

- awplus-gui_550_22.gui
- awplus-gui_551_23.gui

The GUI service will use the .gui file with the 23 in its name, as this is the highest number.

Using the Wizard to configure Internet and VPN connections

On AR2050V and AR10150V routers, a wizard makes it easy to set up Internet and VPN connections.



Setup an Internet connection

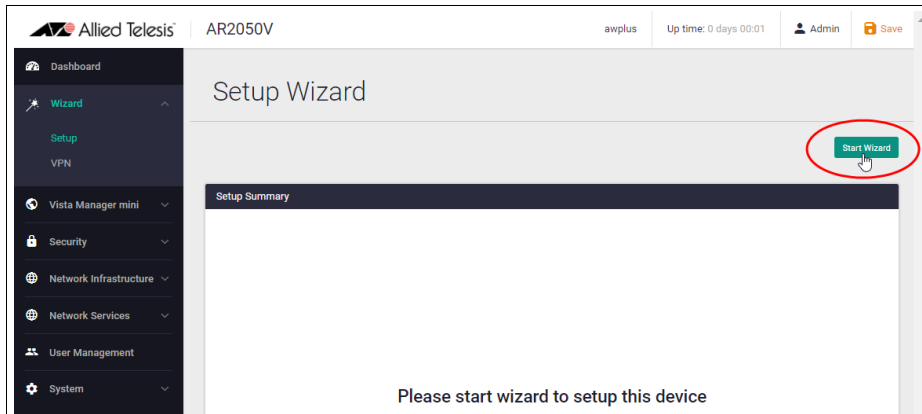
You can use the wizard to set up a router's WAN interface along with creating a basic configuration for a LAN. There are three IPv4 methods available: DHCP, Fixed IP, and PPPoE, and two IPv6 methods available: IPoE and V6 Transition (IPv4 over IPv6).

Once the wizard has run, the Setup Summary page displays the current configuration. You can change other things in the GUI after having run the setup wizard, however if you choose to go back and run the wizard again, all your previous configuration will be removed.

The configuration steps are:

Step 1: Start the Wizard.

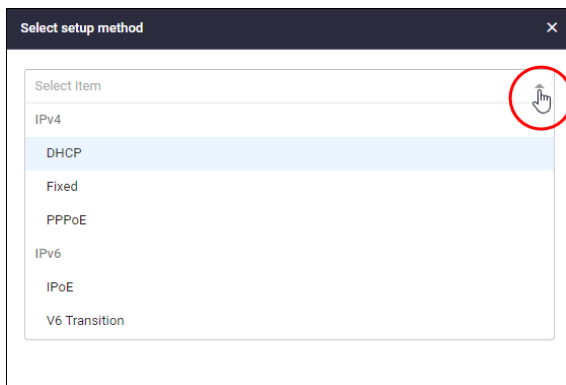
- Click the **Start Wizard** button.
- If you don't have an Internet connection setup, you'll see a blank **Setup Summary** screen:



- If you do have an Internet connection setup, then you'll see those details displayed in the **Setup Summary** screen. Click the **Start Wizard** button in that same screen to reconfigure your current Internet connection settings.

Step 2: Choose a connection method.

- Select a method to connect to the Internet.



Step 3: Configure the connection method.

This section describes the configuration settings for each connection method.

- Note:** If you turn on the DHCP server, it will assign clients addresses that are in the same subnet as the LAN interface's default address. This will not work if you have changed the LAN interface's address. In that case, select OFF for DHCP Server and manually configure the DHCP server from the Network Services menu after the Wizard is complete.

IPv4 - DHCP Connection

Configure the IPv4 DHCP connection:

Field	Description
WAN interface	The interface used to connect to the Internet, for example eth1.
DNS Servers	Specifies the DNS server to use for name resolution. <ul style="list-style-type: none"> ■ If you want DHCP to automatically obtain a DNS server address, use the default Auto. ■ If fixed settings are required, click the down arrow on the right, click + Add DNS Server, and enter the IP address of the DNS server.
DHCP Server	Select: <ul style="list-style-type: none"> ■ ON to operate the DHCP server function on the LAN-side interface of the device and provide IP addresses etc. to the LAN-side terminals. ■ OFF if you do not want to use the DHCP server function.

IPv4 - Fixed IP Connection

Configure the IPv4 fixed IP connection:

Field	Description
IP Address	Enter the IP address you want to configure for the WAN-side interface.
Default Gateway	Enter the IP address of the default gateway that you want to use to connect to the Internet.
WAN interface	Select the interface used to connect to the Internet.

Field	Description
DNS Servers	Specifies the DNS server to use for name resolution. Click the down arrow on the right, click + Add DNS Server , and enter the IP address of the DNS server.
DHCP Server	Select: <ul style="list-style-type: none"> ■ ON to operate the DHCP server function on the LAN-side interface of the device and provide IP addresses etc. to the LAN-side terminals. ■ OFF if you do not want to use the DHCP server function.

IPv4 - PPPoE Connection

Configure the IPv4 PPPoE connection:

PPPoE Connection
✕

Service Name (Optional)
Please enter your service name

Username
Please enter your username

Password
Please enter your password

WAN Interface eth1 ▾

DNS Servers (Optional) Auto ▾

DHCP Server
 OFF ON

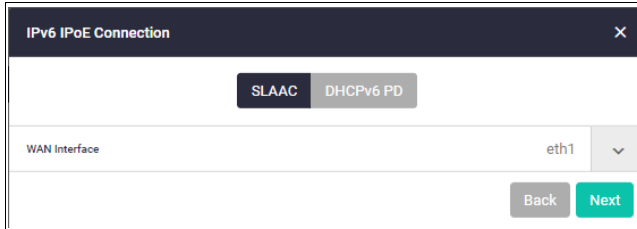
Back
Next

Field	Description
Service Name	This is the PPPoE service name. You can usually leave it blank. Enter the PPPoE service name only if your Internet service provider (ISP) has specified it.
Username	PPP user name. Enter the user name for the Internet connection notified by your ISP.
Password	PPP password. Enter the password for the Internet connection provided by your ISP.
WAN interface	This is the interface used to connect to the Internet.
DNS Servers	Specifies the DNS server to use for name resolution. <ul style="list-style-type: none"> ■ If you want IPCP to automatically obtain the DNS server address when connecting to PPPoE, you can leave it as the default. ■ If fixed settings are required, click the down arrow on the right, click + Add DNS Server, and enter the IP address of the DNS server.
DHCP Server	Select: <ul style="list-style-type: none"> ■ ON to operate the DHCP server function on the LAN-side interface of the device and provide IP addresses etc. to the LAN-side terminals. ■ OFF if you do not want to use the DHCP server function.

IPv6 - IPoE Connection

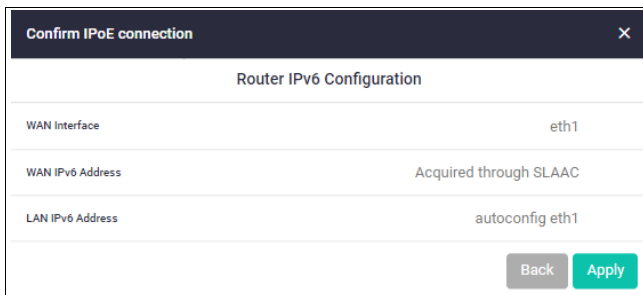
Configure the IPv6 IPoE connection. There are two tabs in this window, SLAAC (Stateless Address Auto-Configuration) and DHCPv6 PD (Prefix Delegation).

1. SLAAC number (RA method)



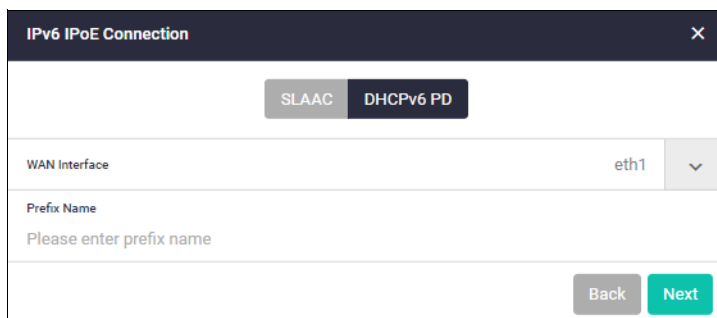
Field	Description
WAN interface	The interface used to connect to the Internet, for example eth1.

- Click the drop down arrow to select the WAN interface.
- Click **Next**. The following confirmation window appears:



- Click **Apply** to continue.

2. DHCPv6 PD (Prefix Delegation)



Field	Description
WAN interface	The interface used to connect to the Internet, for example eth1.
Prefix Name	Enter a name to refer to the retrieved prefix. This is the IPv6 prefix name advertised on the router advertisement message sent from the device. The IPv6 prefix name is delegated from the DHCPv6 Server configured for DHCPv6 Prefix-Delegation.

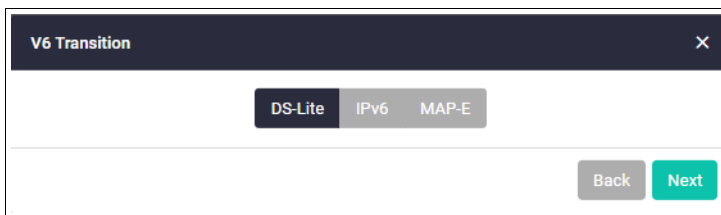
- Click the drop down arrow to select the WAN interface.
- Enter a **Prefix Name**.
- Click **Next**

V6 Transition (IPv4 over IPv6)

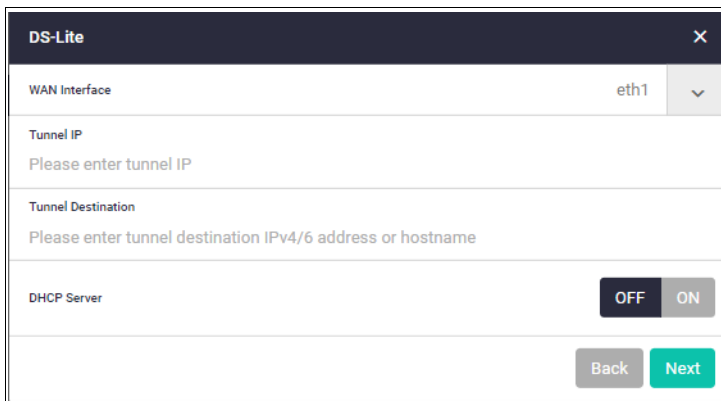
Configure the V6 transition options.

There are three tabs in this window:

1. DS-Lite
2. IPv6
3. MAP-E



1. DS-Lite



Field	Description
WAN Interface	This is the interface used to connect to the Internet.
Tunnel IP	Enter the IPv4 address that you want to configure for the tunnel interface.
Tunnel Destination	Enter the destination address for packets sent over the tunnel.
DHCP Server	Select: <ul style="list-style-type: none"> ■ ON to operate the DHCP server function on the LAN-side interface of the device and provide IP addresses etc. to the LAN-side terminals. ■ OFF if you do not want to use the DHCP server function.

2. IPv6

■ IPv6 - SLAAC

Configure the IPv4 connections with IPv6 IPoE connections (RA method) and IPv6 tunnels (fixed)

The screenshot shows a configuration window titled 'IPv6' with a close button (X). At the top, there are two tabs: 'SLAAC' (selected) and 'DHCPv6 PD'. Below the tabs, the configuration is organized into several sections:

- WAN Interface:** A dropdown menu showing 'eth1'.
- Tunnel IP:** A text input field with the placeholder text 'Please enter tunnel IP'.
- Tunnel Destination:** A text input field with the placeholder text 'Please enter tunnel destination IPv4/6 address or hostname'.
- Suffix:** A text input field containing '::1'.
- DDNS Server:** A toggle switch currently set to 'OFF'.
- DHCP Server:** A toggle switch currently set to 'OFF'.

At the bottom right of the form, there are two buttons: 'Back' and 'Next'.

Field	Description
WAN Interface	This is the interface used to connect to the Internet.
Tunnel IP	Enter the address you want to configure for the tunnel interface.
Tunnel Destination	Enter the destination address for packets traversing the tunnel.
Suffix	Enter the interface ID specified in advance by your ISP.
DDNS Server	Use the dynamic DNS client feature to notify the update server of the IPv6 address updates.
DHCP Server	Select: <ul style="list-style-type: none"> ■ ON to operate the DHCP server function on the LAN-side interface of the device and provide IP addresses etc. to the LAN-side terminals. ■ OFF if you do not want to use the DHCP server function

■ IPv6 - DHCPv6 PD

Configure IPv4 connections with IPv6 IPoE connections (DHCPv6 PD method) and IPv6 tunnels (fixed).

The screenshot shows a configuration window titled 'IPv6' with a close button. At the top, there are two tabs: 'SLAAC' and 'DHCPv6 PD', with 'DHCPv6 PD' being the active tab. The configuration fields are as follows:

- WAN Interface:** eth1 (with a dropdown arrow)
- Prefix Name:** Please enter prefix name
- Tunnel IP:** Please enter tunnel IP
- Tunnel Destination:** Please enter tunnel destination IPv4/6 address or hostname
- Suffix:** :::1
- DDNS Server:** OFF (with an ON button)
- DHCP Server:** OFF (with an ON button)

At the bottom right, there are 'Back' and 'Next' buttons.

Field	Description
WAN Interface	This is the interface used to connect to the Internet.
Prefix Name	Enter a name to refer to the retrieved prefix.
Tunnel IP	Enter the IPv4 address that you want to configure for the tunnel interface.
Tunnel Destination	Enter the end point (on-the-go device: operator router (BR)) address of the delivery packet sent from the tunnel interface.
Suffix	Enter the interface ID specified in advance by your ISP.
DDNS Server	Use the dynamic DNS client feature to notify the update server of IPv6 address updates. When enabled, the fields 'DDNS update URL', 'DDNS user name', and 'DDNS password' are displayed.
DHCP Server	Select: <ul style="list-style-type: none"> ■ ON to operate the DHCP server function on the LAN-side interface of the device and provide IP addresses etc. to the LAN-side terminals. ■ OFF if you do not want to use the DHCP server function.

3. MAP-E

Configure IPv6 IPoE and MAP-E IPv4 connections.

Field	Description
WAN Interface	Select the interface used to connect to the Internet, for example eth1.
Softwire Configuration Name	Enter a name to create a new soft wire configuration.
IP Phone	Select: <ul style="list-style-type: none"> ■ ON to use an IP phone. When enabled, the Prefix Name field is displayed. ■ OFF if you do not want to use the IP Phone function.
DHCP Server	Select: <ul style="list-style-type: none"> ■ ON to operate the DHCP server function on the LAN-side interface of the device and provide IP addresses etc. to the LAN-side terminals. ■ OFF if you do not want to use the DHCP server function.

Step 4: Check and Save the settings.

- Check your configuration is correct and click **Save** to continue.

Step 5: Save the settings to the startup configuration.

When the configuration save is complete, a summary of the connection status is displayed.

- The contents set in the simple setting are stored in the running configuration and reflected in the operation, but are not automatically saved in the **startup** configuration.
- After confirming that there are no problems with the settings, manually save the settings to the startup configuration using the **Save** button in the navigation bar.
- You can run the Wizard again to make changes to your connection method settings.

The screenshot displays the 'Setup Wizard' interface for an Allied Telesis AR2050V router. The top navigation bar includes the Allied Telesis logo, the device model 'AR2050V', the user 'awplus', the system 'Up time: 0 days 00:40', the user 'Admin', and a 'Save' button highlighted with a red arrow. The left sidebar contains a menu with options: Dashboard, Wizard (selected), Setup, VPN, Vista Manager mini, Security, Network Infrastructure, Network Services, User Management, and System. The main content area is titled 'Setup Wizard' and features a 'Start Wizard' button. Below this is a 'Setup Summary' section with two main parts: 'Router Basic Configuration' and 'DHCP Server Configuration'. The 'Router Basic Configuration' table lists WAN IP Address (eth1: 192.168.101.1), LAN IP Address (vlan1: 10.00.20.10), Default Gateway (10.00.20.1, 192.168.101.100), and DNS Server (10.00.16.00, 10.00.16.01, 10.00.16.02). The 'DHCP Server Configuration' table lists DHCP pool name, Lease time, Target Subnet, and IP Address range, all with dashes indicating they are not yet configured.

Router Basic Configuration			
WAN IP Address	eth1:	192.168.101.1	
LAN IP Address	vlan1:	10.00.20.10	
Default Gateway	10.00.20.1, 192.168.101.100		
DNS Server	10.00.16.00, 10.00.16.01, 10.00.16.02		

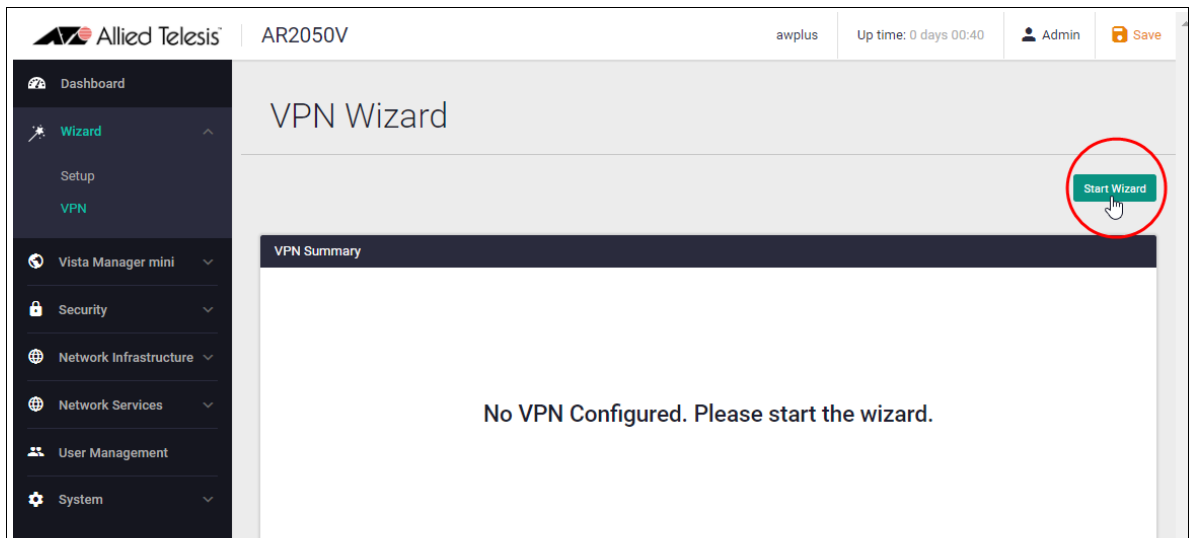
DHCP Server Configuration	
DHCP pool name	-
Lease time	-
Target Subnet	-
IP Address range	-

Configuring a VPN connection

To configure a secure VPN connection, first make sure you have an Internet connection, and then use the following steps:

Step 1: Start the Wizard.

- Click the **Start Wizard** button.
- If you don't have an existing VPN connection, you'll see a blank **VPN Summary** screen:



- If you do have an existing VPN connection, then you'll see those details displayed in the **VPN Summary** screen. Click the **Start Wizard** button on that same screen to reconfigure your current VPN connection settings.

Step 2: Enter the VPN connection information.

VPN Connection ✕

Tunnel IP
Please enter tunnel IP

Tunnel Source eth1 ▾

Tunnel Destination
Please enter tunnel destination IPv4/6 address or hostname

Tunnel Local Name (Optional)
Please enter tunnel local name

Tunnel Remote Name (Optional)
Please enter tunnel remote name

Crypto Preshared Key
Key

Destination LAN (Optional)
Please enter IP address and mask of the destination network.

Cancel Next

Field	Description
Tunnel IP	Enter the IPv4 address of the tunnel interface.
Tunnel Source	Select the interface for the VPN connection.

Field	Description
Tunnel Destination	Enter the end IP address or host name of the VPN destination.
Tunnel Local Name	Enter the ISAKMP IP (local ID) for the local router.
Tunnel Remote Name	Enter the ISAKMP IP (remote ID) for the remote router.
Crypto Preshared Key	Enter the password (ISAKMP pre-shared key) for the VPN connection.
Destination LAN	Enter the LAN-side IPv4 address of the destination network.

Step 3: Confirm VPN tunnel connection.

Confirm VPN connection
×

Tunnel Confirmation

Tunnel IP	192.168.101.100/24
Tunnel Source	eth1
Tunnel Destination	192.168.101.100
Tunnel Local Name	TestTunnel
Crypto Preshared Key	XXXXXXXX

Back
Apply

Step 4: Review and Save your settings.

- Check your configuration is correct and click **Apply** to continue.
- If you click **Save** with a VPN connection already set up, the existing settings on the running configuration will be erased and replaced with the newly configured content.

Step 5: Save the settings to the startup configuration.

When the configuration save is complete, a summary of the VPN connection status is displayed.

- The contents set in the simple setting are stored in the running configuration and reflected in the operation, but are not automatically saved in the **startup** configuration.
- After confirming that there are no problems with the settings, manually save the settings to the **startup** configuration using the **Save** button in the navigation bar.

- You can always run the Wizard again to make changes to your VPN connection settings.

The screenshot displays the Allied Telesis web interface for an AR2050V router. The top navigation bar includes the logo, device name, status (awplus), uptime (0 days 00:40), user (Admin), and a 'Save' button. A red arrow points to the 'Save' button. The main content area is titled 'VPN Wizard' and features a 'Start Wizard' button. Below this is a 'VPN Summary' section with a 'Tunnel Configuration' table.

VPN Summary	
Tunnel Configuration	
Tunnel State	Up
Tunnel Name	tunnel1
Tunnel Source	eth1
Tunnel Source IP	192.168.101.1
Tunnel Destination	192.168.101.100
Mode	IPsec IPv4
Protection Type	IPsec

What is a firewall?

The next sections describe the AlliedWare Plus firewall and how to configure it. The router's firewall at its simplest level, controls traffic flow between a trusted network (such as a corporate LAN) and an untrusted or public network (such as the Internet). Firewalls determine whether traffic is allowed or disallowed based on characteristics of the packets, including their destination and source IP addresses and TCP/ UDP port numbers.

Applications can be created using a combination of protocol and port numbers, and then be used by firewall, NAT, and traffic control rules to manage traffic.

What are entities?

Before we begin to configure the router, let's take a look at the building blocks that allow this advanced control of online network activity.

When the router is deciding how it should treat a traffic stream, among the questions it needs to ask are "*where is the stream coming from?*" and "*where is it going to?*"

To help answer those questions, the firewall needs to have a logical map of the network environment, so that it can categorize the sources and destinations of the flows that it is managing.

Allied Telesis firewalls and routers map out the network environment into regions, using three tiers of granularity. The divisions into which it cuts up its environment are referred to collectively as **entities**. The three levels of granularity in the dividing up of the environment are:

- zones
- networks
- hosts

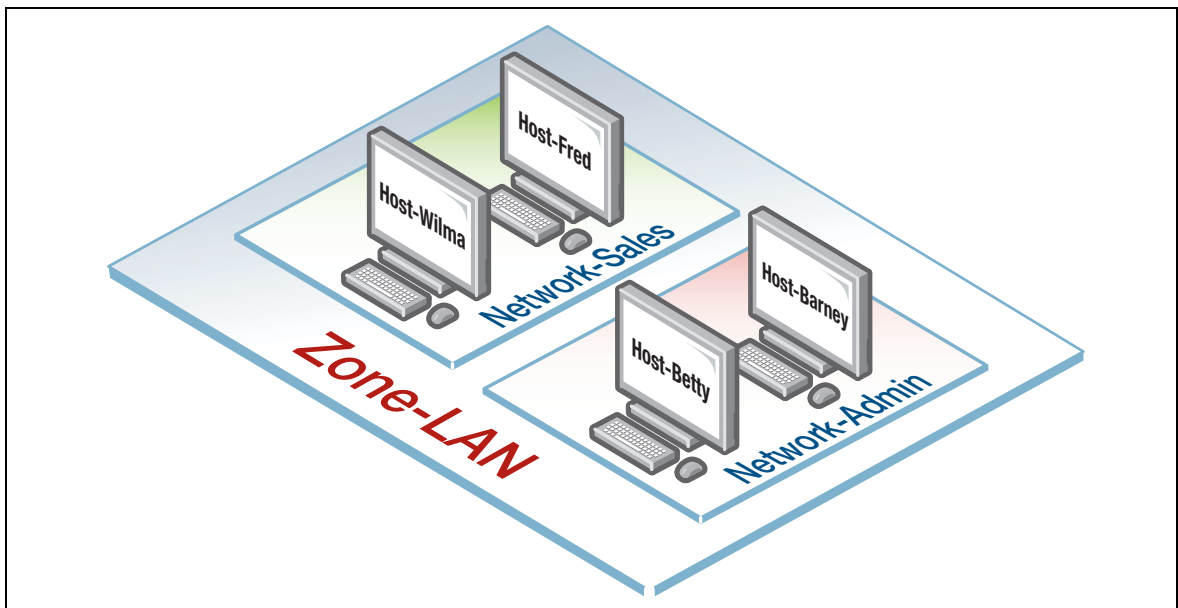
This hierarchy of entities empowers organizations to accurately apply security policies at company, department, or individual level.

Zones, networks, and hosts

A **zone** is the highest level of division within the network. It defines a boundary where traffic is subjected to policy restrictions as it crosses to another region of your network. A typical network environment might contain a public (WAN) zone representing the Internet, a private (LAN) zone behind the firewall, and a Demilitarized zone (DMZ) containing publicly accessible web servers. Zones are divided up into networks, which in turn contain hosts.

A **network** is a logical grouping of hosts within a zone, for example, the sales network within the LAN zone. Networks consist of the IP subnets and interfaces over which they are reachable. The allocating of networks to zones is the core activity in dividing the network up into logical regions to which different security policies apply. A zone has no real meaning in itself until it has one or more networks allocated to it. Once networks have been allocated to a zone, the zone is then the entity that collectively represents that set of networks. Then rules can be applied to the zone as a whole, or to individual networks within the zone.

A **host** is a single node in a network, for example, the PC of a specific employee. The diagram below shows PC Wilma is a host within the sales network within the LAN zone. Host entities are defined so that specific rules can be applied to those particular hosts - e.g. a server to which certain types of sessions may be initiated.



Using rules

Rules allow the advanced control of users, and the applications they use on the network.

Firewall rules: filter traffic, allowing or denying, between any two entities. This allows for granular control, as rules can be based on traffic sources that might be zones, networks, or hosts, and traffic destinations that might be zones, networks, or hosts.

For example, an organization may choose to block Skype™ company-wide (i.e. from ANY zone to ANY zone), or allow it only for the marketing department (i.e. allow Skype from the Marketing network to ANY zone, but block it from any other network, zone, or host).

Traffic control rules: control the bandwidth that applications use. For example, Spotify™ music streaming may be allowed, but limited in bandwidth due to an acceptable use policy ensuring company Internet connectivity is prioritized for business traffic.

Network Address Translation (NAT) rules: hide private network addresses for traffic bound for the Internet. All company traffic leaving the corporate office can share a public network address for routing through the Internet to its destination.

The firewall supports:

- NAT with IP masquerade, where private source addresses are mapped to a public source address with source port translation to identify the association. The single public IP address masquerades as the source IP on traffic from the private addresses as it goes out to the Internet.
- Port forwarding, to provide public access to internal servers. Port forwarding redirects traffic to a specific host, e.g. forwarding HTTP traffic to a web server in the DMZ.

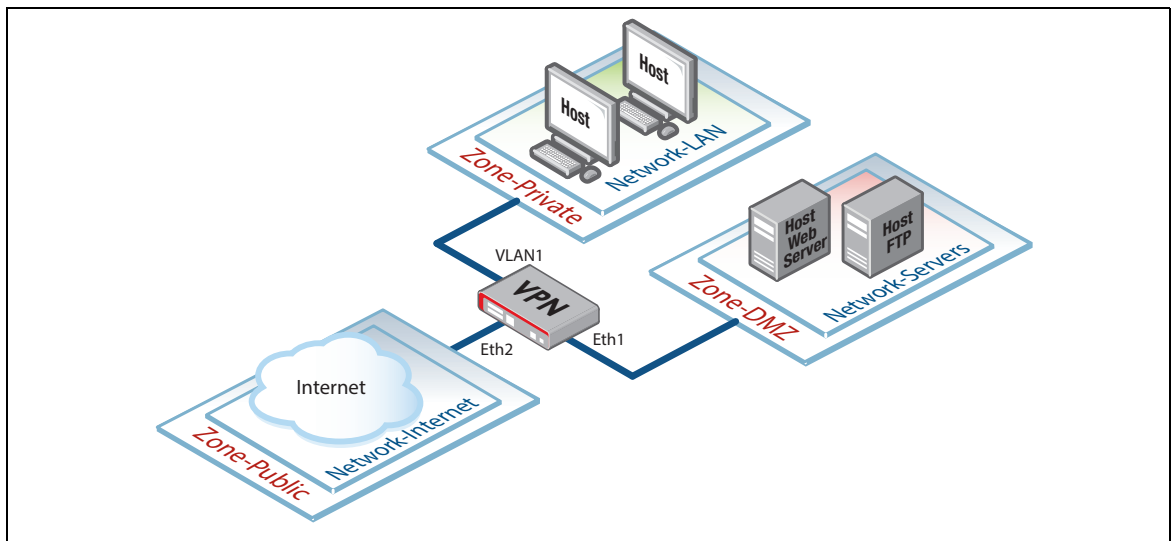
Configuring the router

This section comprises three parts, and describes how to configure:

1. A standard 3-zone network scenario, as shown below.
2. Rules to allow Update Manager to update the GUI, see [page 37](#)
3. Security features - IPS, and Custom URL Filtering, see [page 39](#)

Part 1: Configure a standard 3-zone network

The configuration section of this guide uses the AR2050V as the example device.



Note: If your router is new and unused, it will already have the Device GUI installed from the factory, with the IP address 192.168.1.1 on VLAN1 (AR2050V), or Eth1 (AR2010V, AR1050V), and the HTTP service enabled. Connect to any switch port (AR2050V) or Eth1 (AR2010V, AR1050V) and browse to 192.168.1.1 to begin.

Step 1: Configure router interfaces.

From the CLI, add the following interface addresses:

IP address for eth2

```
awplus(config)#interface eth2
awplus(config-if)#ip address 128.0.0.1/24
awplus(config-if)#exit
```

IP address for eth1

```
awplus(config-if)#interface eth1
awplus(config-if)#ip address 172.16.0.1/24
awplus(config-if)#exit
```

IP address for VLAN 1

```
awplus(config)#interface vlan1
awplus(config-if)#ip address 192.168.1.1/24
awplus(config-if)#exit
```

Step 2: Enable the Web server.

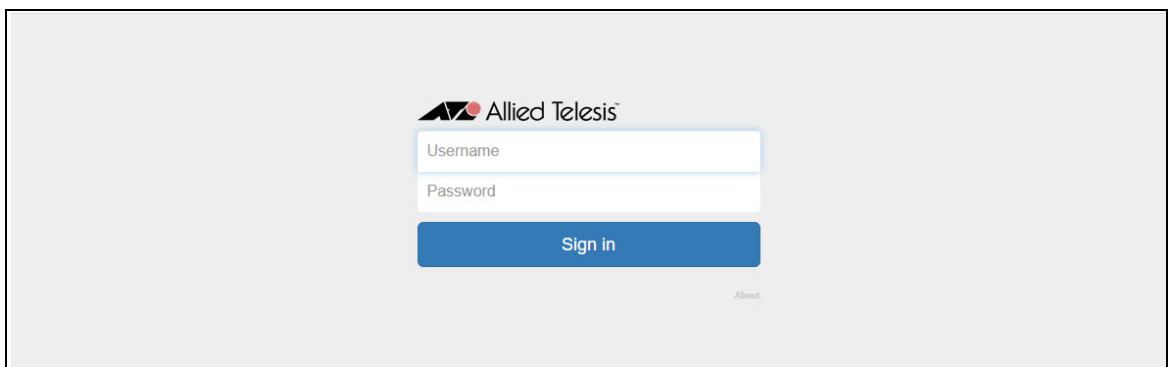
Enable HTTP so the router will serve the Device GUI pages:

```
awplus(config)#service http
```

Step 3: Login to the Device GUI.

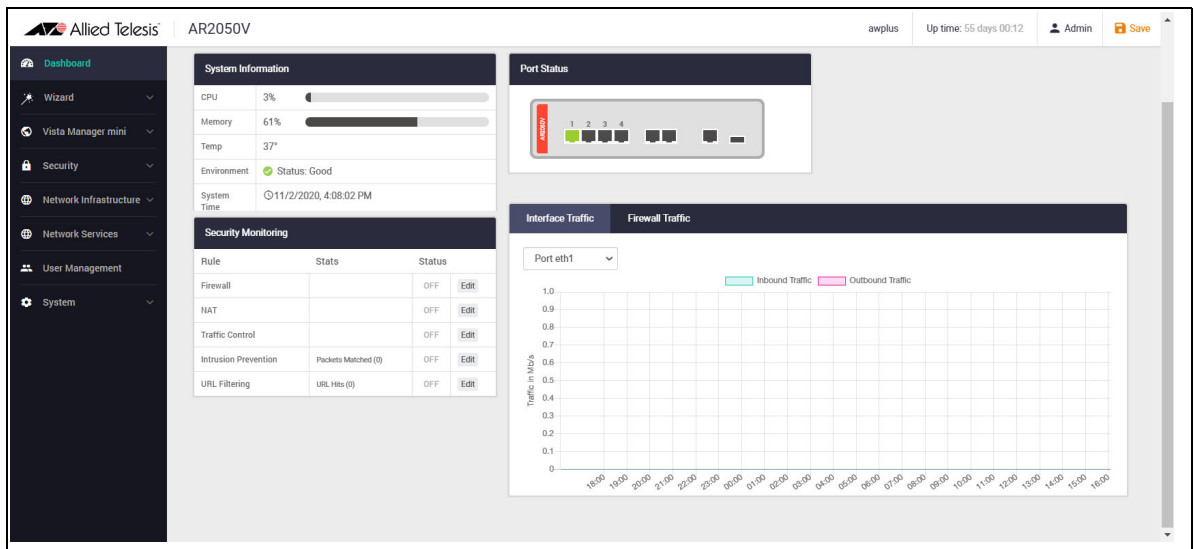
Browse to the IP address of the router on the interface you are connecting to - e.g. 192.168.1.1 for VLAN1.

The login page is displayed:



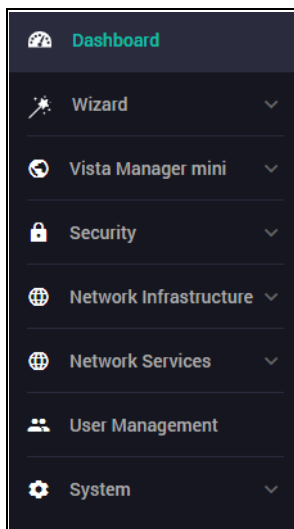
You can log in using any valid username/password combination that has been configured on the unit, or use the default username/password (**manager/friend**), if that has not been deleted.

The **Dashboard** is displayed.



The Dashboard has a number of useful widgets for monitoring the state of your router. We'll look closer at the various Dashboard widgets later, after we've configured the firewall.

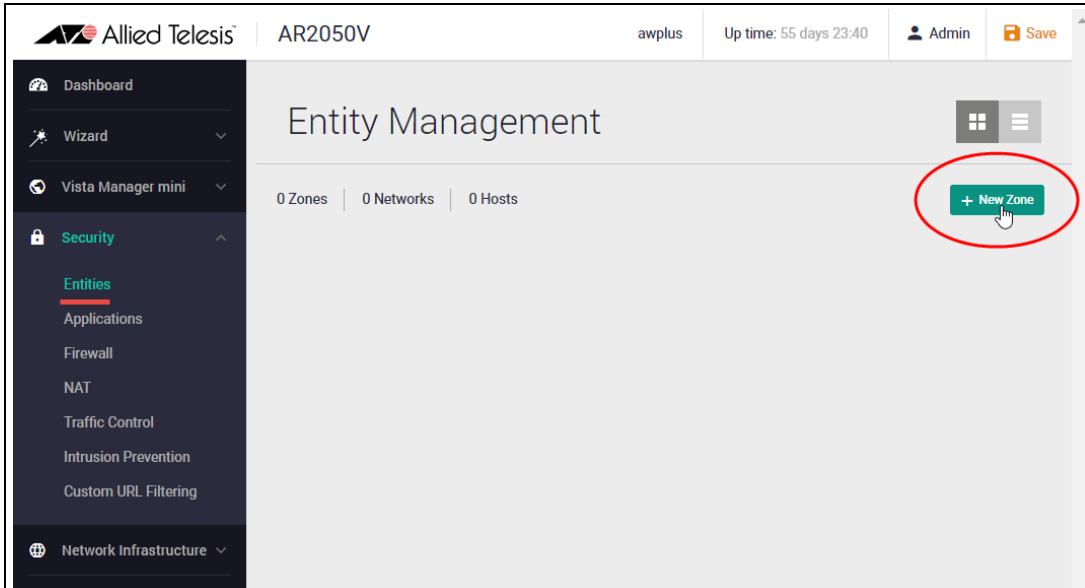
On the left-hand side of the Dashboard page is the main navigation bar. From here you can access the **Wizard**, **Vista Manager mini**, **Security**, **Network Infrastructure**, **Network Services**, **User Management** and **System** menus.



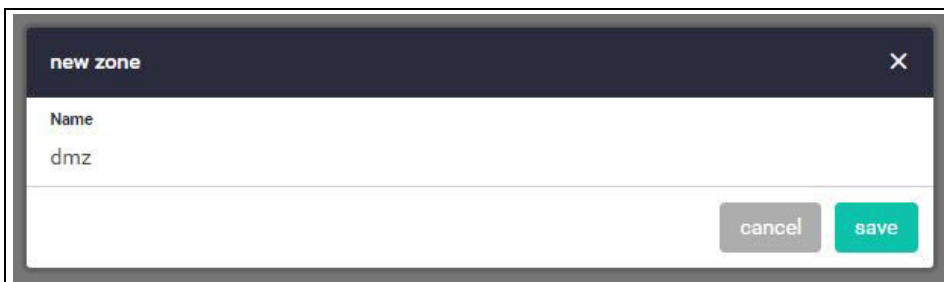
Step 4: Configure Entities.

To configure the router, we'll first create entities to which rules can be applied.

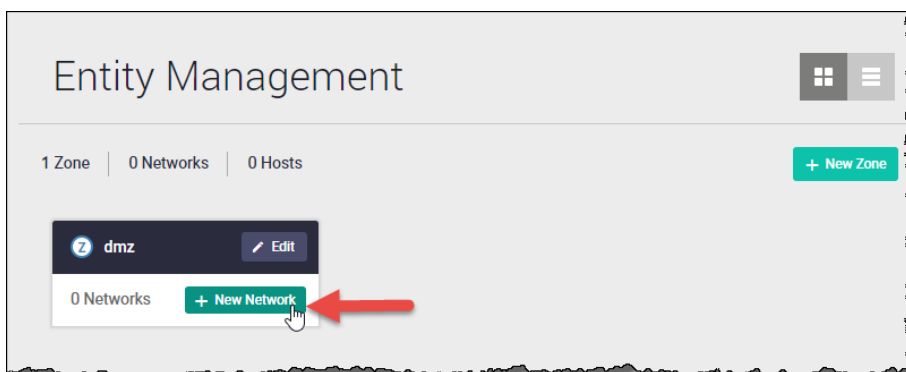
- Select **Entities** from the **Security** menu.



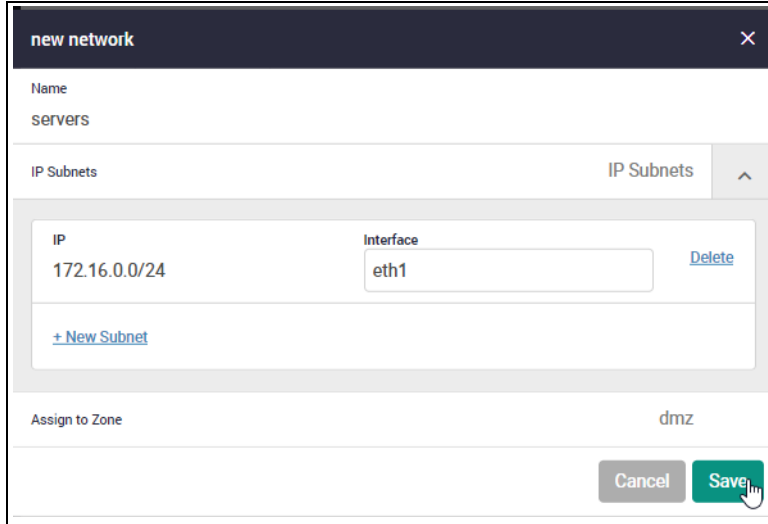
- As no entities have yet been created, click the green + **New Zone** button to add a zone.
- The first zone we will add is the **DMZ** zone to be used for company servers that we want to be accessible from the Internet.



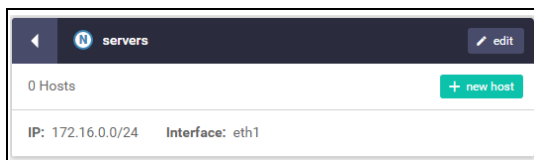
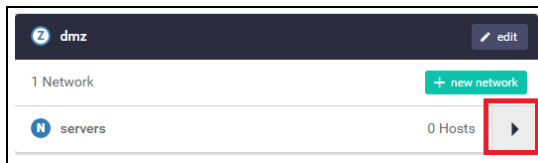
- Next click the green + **New Network** button in the DMZ zone to add our **servers** network.



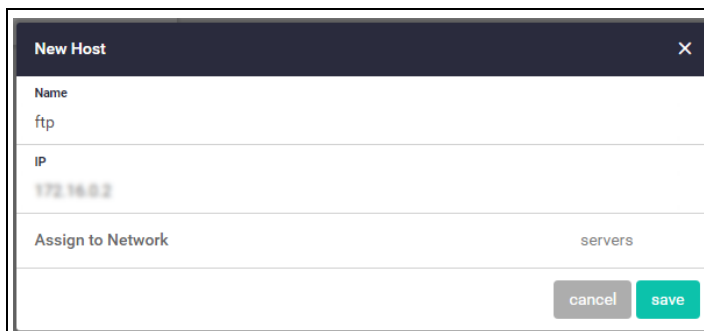
- Name the new network **servers**.
- Add the IP subnet 172.16.0.0/24 and **eth1** as the interface over which this network will be reachable.
- Click **Save**.



- We can now add specific hosts (servers in this case) to the DMZ network.
- Click on the slide arrow to see Ip and interface details of the servers network.



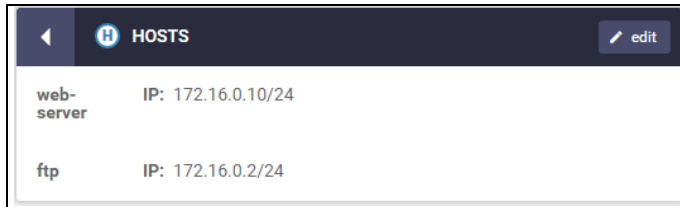
- Click the green **+New Host** button.
- In the New Host window, enter the host name **ftp**
- Enter IP address 172.16.0.2



- Add a second host named **web-server** with an IP address of 172.16.0.10

Our DMZ zone now contains a network named **servers** with two hosts:

- web-server
- ftp



Repeat the same steps to create private and public zones/networks with the following details:

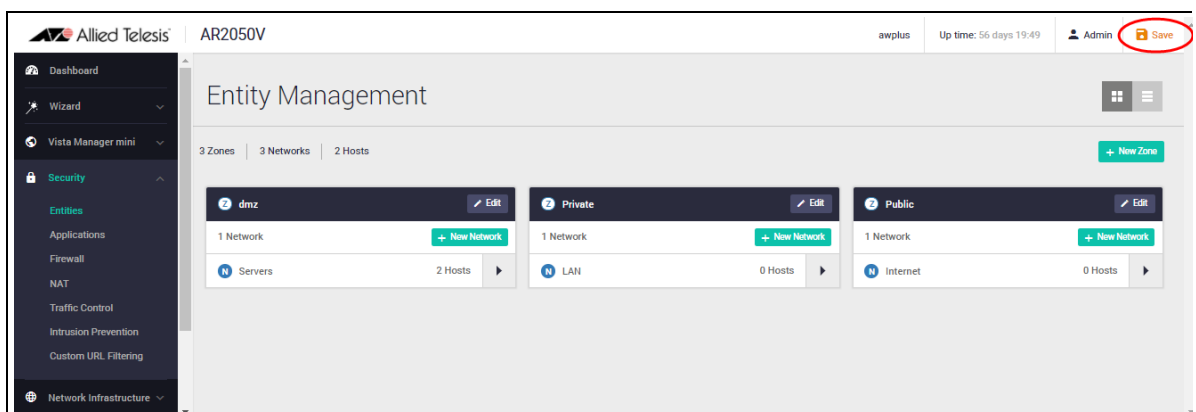
Private zone:

- Zone name = private
- Network name = lan
- Network subnet and interface = 192.168.1.0/24, VLAN1

Public zone:

- Zone name = public
- Network name = internet
- Network subnet and interface = 0.0.0.0/0, eth1

The Entities Management page now contains our 3-zone network.



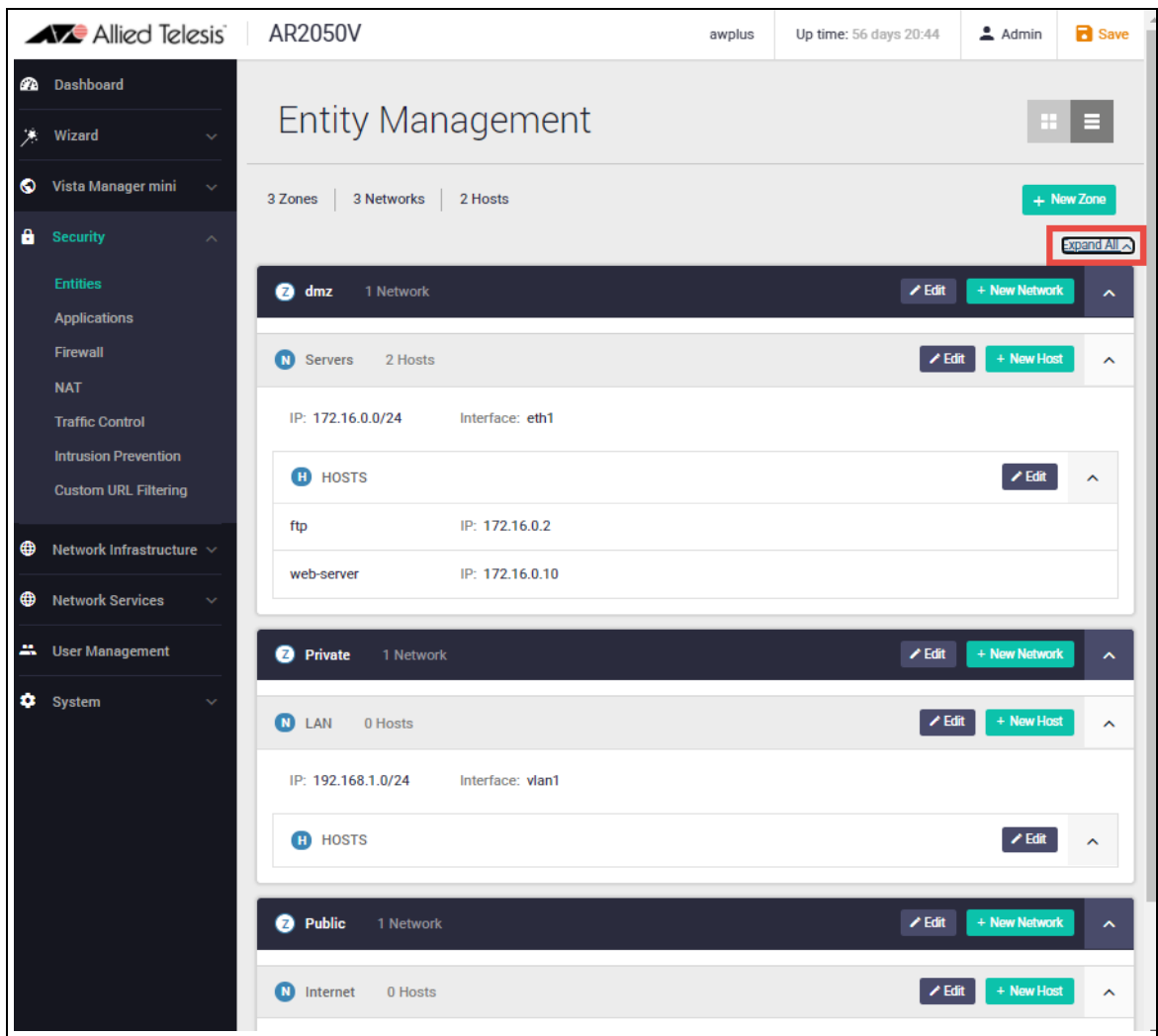
- Click the **Save** button at the top right of the window to continue.

Entity list view

An alternative view from the tiled view shown above, is the list view. To view and manage entities in a list view, click on the list icon on the right side of the page.



Clicking **expand all** (on the right side of the page) displays all entities and their interfaces, IP addresses, and so on. The list view is a good option for an overall entity view.



If you'd like to view these changes as added to the router configuration file:

- select **CLI** under the **System** menu, this opens a CLI tab.
- type **ena** to access Privileged Exec mode, then use the CLI commands:
show running-config entity and **show entity**.

```

AlliedWare Plus (TM) 5.5.0 09/02/20 21:20:39
awplus>ena
awplus#show running-config entity
zone dmz
  network Servers
  ip subnet 172.16.0.0/24 interface eth1
  host ftp
  ip address 172.16.0.2
  host web-server
  ip address 172.16.0.10
!
zone Private
  network LAN
  ip subnet 192.168.1.0/24 interface vlan1
!
zone Public
  network Internet
  ip subnet 0.0.0.0/0 interface eth1
!
awplus#show entity
Zone:      dmz
Network:   dmz.Servers
Subnet:    172.16.0.0/24 via eth1
Host:      dmz.Servers.ftp
Address:   172.16.0.2
Host:      dmz.Servers.web-server
Address:   172.16.0.10

Zone:      Private
Network:   Private.LAN
Subnet:    192.168.1.0/24 via vlan1

Zone:      Public
Network:   Public.Internet
Subnet:    0.0.0.0/0 via eth1

awplus#

```

Note the syntax that is used for identifying a network or host entity.

The syntax for naming a **network** entity is:

```
<parent zone name>.<network name>
```

- For example, `private.LAN`

The syntax for identifying a **host** entity is:

```
<parent zone name>.<parent network name>.<host name>
```

- For example, `dmz.servers.ftp`

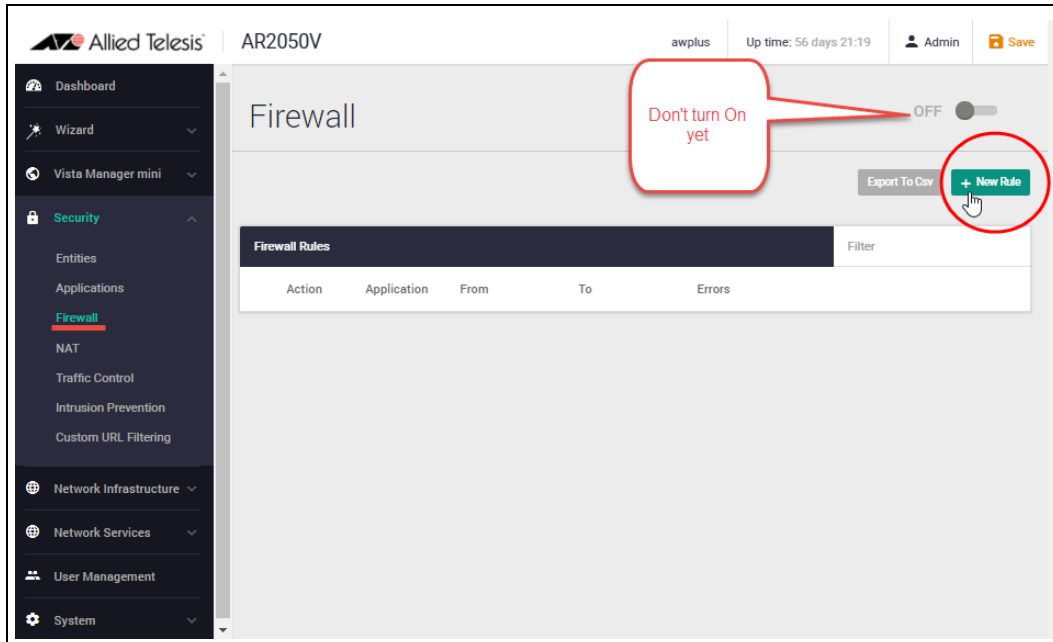
So, the hierarchy is included in the identifier of a second-tier or bottom-tier entity.

- For example, **dmz.servers.web-server** indicates that this host named **web-server** is part of the **servers** network within the **dmz** domain.

Step 5: Configure firewall rules.

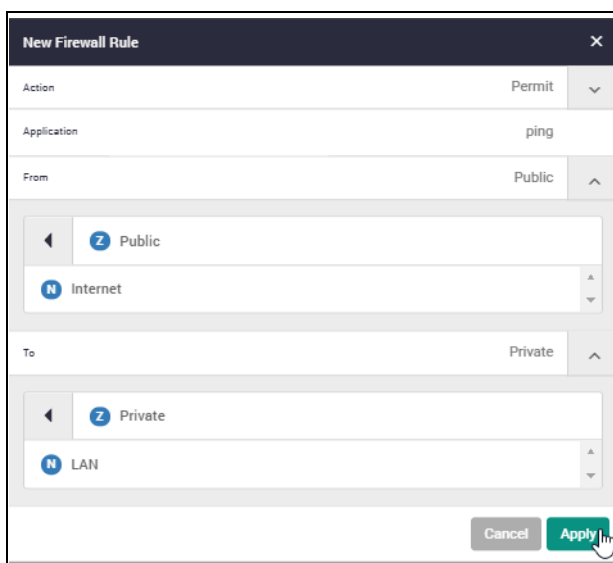
We now have a 3-zone network (Public, Private, and DMZ), so we can now configure the firewall rules to manage the traffic between these entities.

- Navigate to **Firewall** under the **Security** menu.



WARNING: Enabling the firewall with the **ON/OFF** switch will block all applications between all entities by default - No traffic will flow. It is therefore important to create firewall rules to allow application usage as desired prior to enabling the firewall.

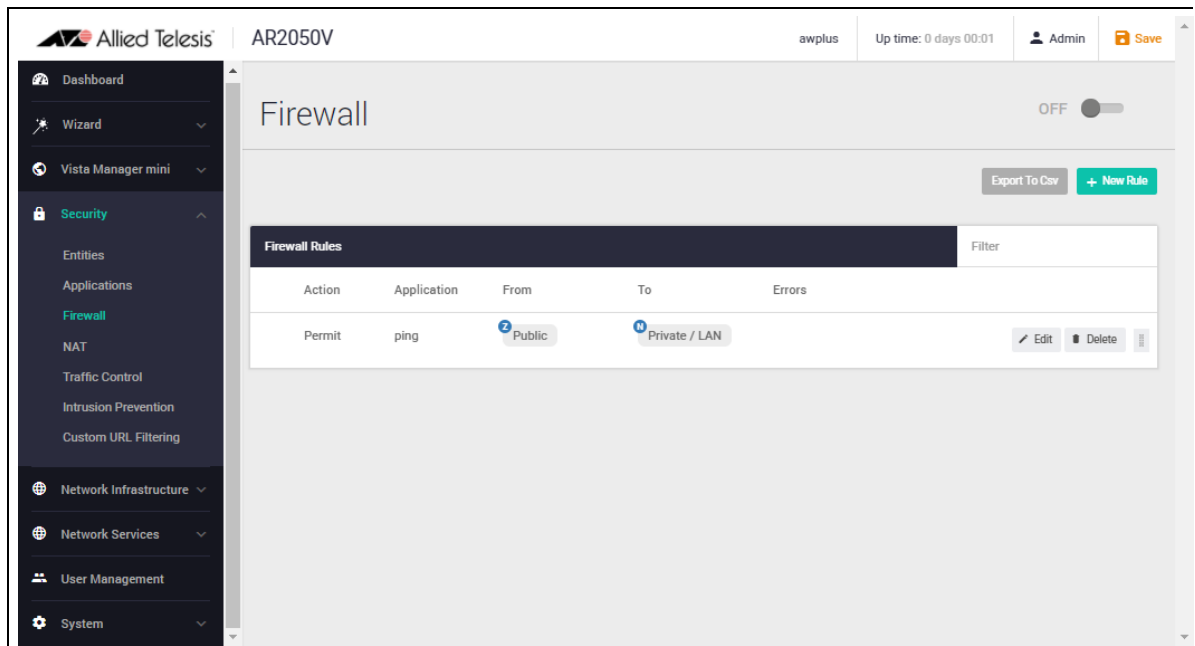
- Click **+ New Rule** and create a rule to allow **Ping** traffic from the Public zone to the Private zone. This will allow us to test connectivity through the firewall.
- Click **Apply**.



Tip: To select an application such as 'ping', simply start typing 'ping' in the application field.

Note: If you don't see any applications, turn on the built-in list of applications, or create your own custom applications from the **Applications** page, under the **Security** menu.

- You can see the new rule added to the firewall.



Repeat step 5 to create further new firewall rules:

Further Ping rules to allow connectivity checking:

- Permit Ping from Public to DMZ
- Permit Ping from Private to DMZ
- Permit Ping from DMZ to Private

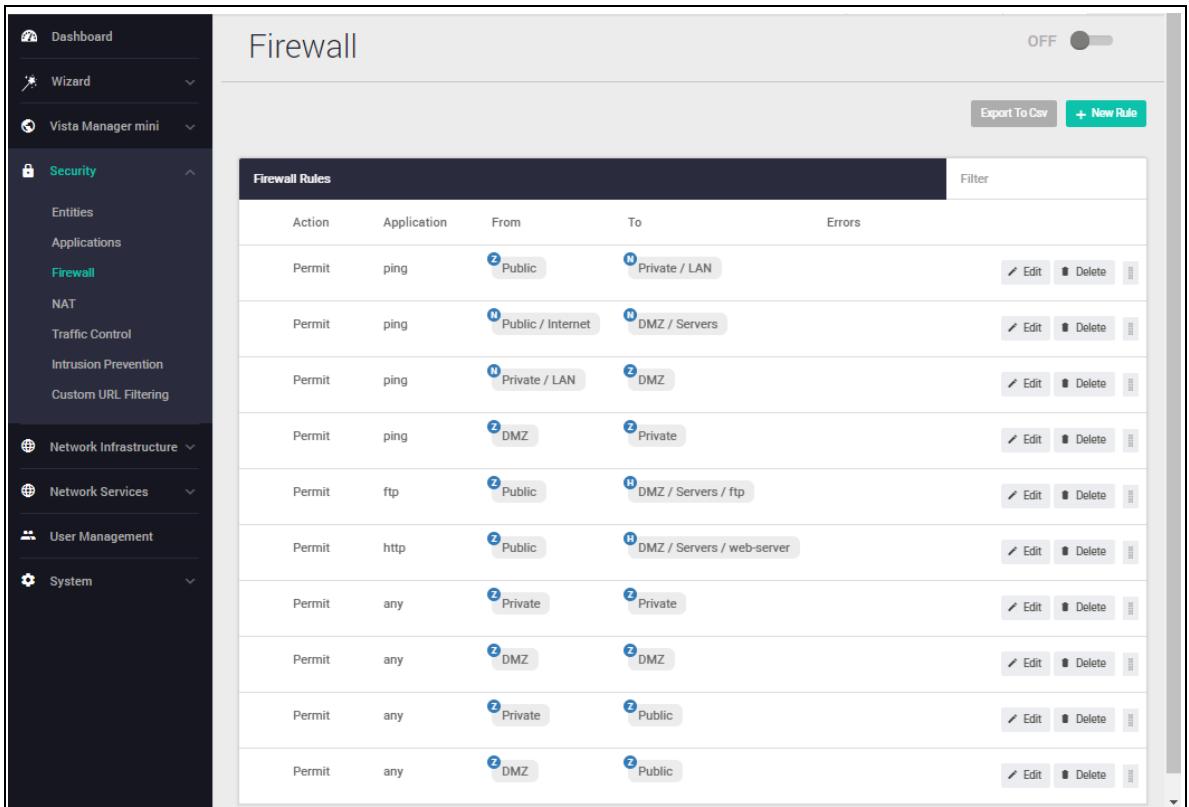
Allow Public traffic from the Internet to our DMZ servers:

- Permit ftp from Public to dmz.servers.ftp
- Permit http from Public to dmz.servers.web-server

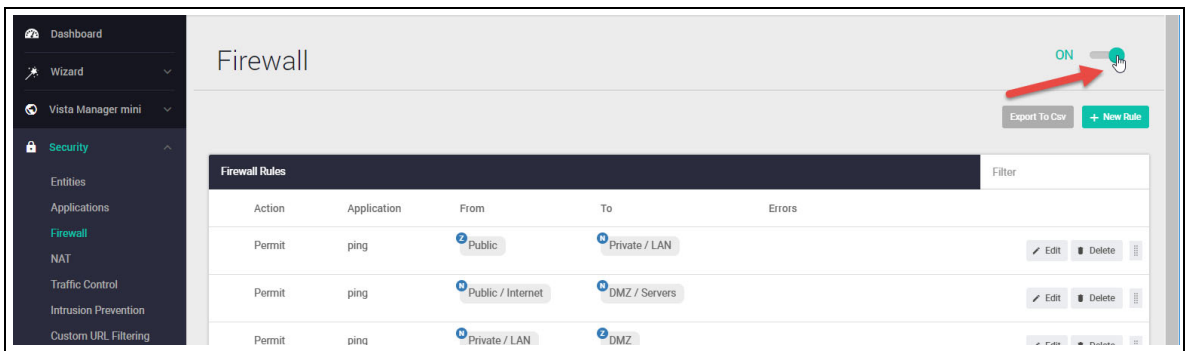
Allow private side firewall zones to initiate traffic flows with each other and out to the Internet:

- Permit Any from Private to Private
- Permit Any from DMZ to DMZ
- Permit Any from Private to Public
- Permit Any from DMZ to Public

We can now see all these firewall rules displayed:



- Now that the firewall rules are created, you can turn the firewall **on** using the **ON/OFF** button at the top right of the Dashboard page.

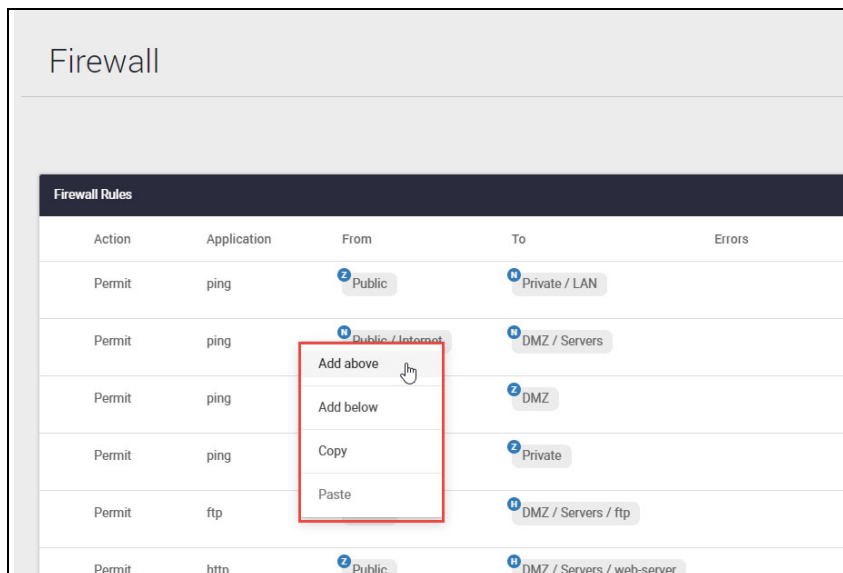


Firewall rule placement

The firewall rules are displayed in the order they were created, which is also the order in which they will be **actioned** by the firewall. If you need to change the order of any specific rule, it can be dragged to a different location in the list.

By default a new rule is added to the bottom of the list, and can then be dragged to a new location. There are two other options for placing new rules:

- **Right-click** on any firewall rule and the menu gives you the option to create a new rule above or below that rule. This allows new rules to be immediately placed in the desired location, and order of processing.
- The **right-click** menu also has a copy-and-paste function, so you can copy an existing rule that is similar to the new rule you wish to create, and paste it into a different location. It can then be edited to suit.



These right-click options are very useful when you have a large number of firewall rules. The same right-click options are also available when creating new NAT and Traffic Control rules.

If you'd like to use the CLI to view the updated firewall configuration, use the CLI window and the commands: **show firewall rule**, **show running-config firewall** and **show firewall**.

```

AlliedWare Plus (TM) 5.5.0 09/02/20 21:20:39
awplus>ena
awplus#show firewall rule

[* = Rule is not valid - see "show firewall rule config-check"]
  ID      Action  App      From          To             Hits
-----
  10      permit  ping     Public        Private.LAN    0
  20      permit  ping     Public.Internet DMZ.Servers   0
  30      permit  ping     Private.LAN   DMZ            0
  40      permit  ping     DMZ           Private        0
  50      permit  ftp      Public        DMZ.Servers.ftp 0
  60      permit  http     Public        DMZ.Servers.web-server
                                0
  70      permit  any      Private       Private        286
  80      permit  any      DMZ           DMZ            118
  90      permit  any      Private       Public         0
  100     permit  any      DMZ           Public         0
awplus#show running-config firewall
firewall
rule 10 permit ping from Public to Private.LAN
rule 20 permit ping from Public.Internet to DMZ.Servers
rule 30 permit ping from Private.LAN to DMZ
rule 40 permit ping from DMZ to Private
rule 50 permit ftp from Public to DMZ.Servers.ftp
rule 60 permit http from Public to DMZ.Servers.web-server
rule 70 permit any from Private to Private
rule 80 permit any from DMZ to DMZ
rule 90 permit any from Private to Public
rule 100 permit any from DMZ to Public
protect
!
awplus#show firewall
Firewall protection is enabled
Active connections: 10
awplus#

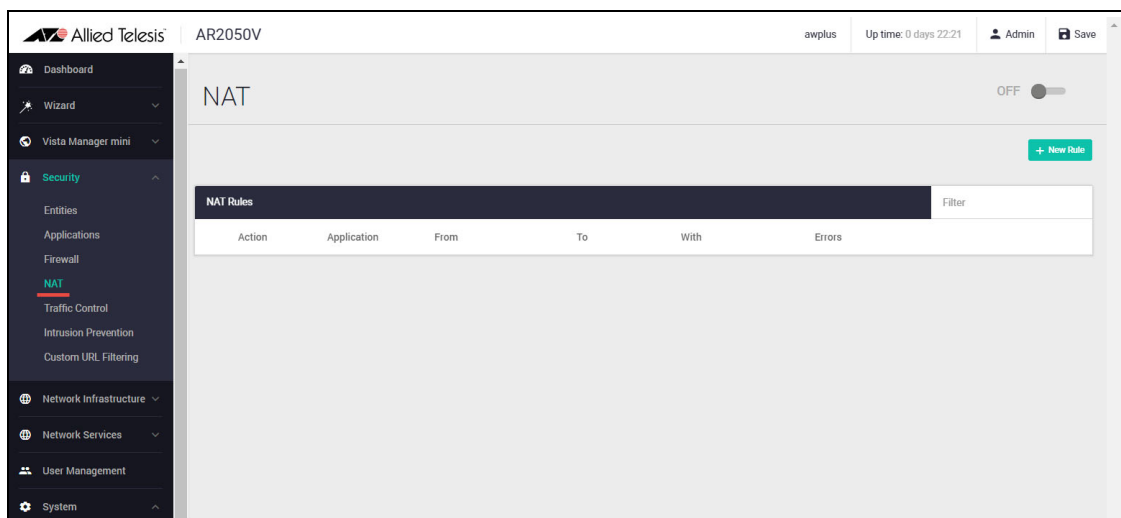
```

Note that the firewall rules are numbered in the order in which they will be actioned (e.g. 10, 20, 30 and so on). If a rule is dragged to a different location in the list displayed by the GUI, the rules will be renumbered to reflect the change in order of operation.

Step 6: Configure NAT rules.

Now let's configure NAT rules to manage IP address translation between the Internet and our internal networks.

Navigate to **NAT** under the **Security** menu.



We need two NAT masquerade rules for private to public address translation, which are:

1. Any traffic going from the Private zone out to the Public zone will have NAT applied, so that it appears to have come from the IP address of the eth2 interface
2. Any traffic going from the DMZ zone out to the Public zone will have NAT applied, so that it appears to have come from the IP address of the eth2 interface.

Click + **new rule** to create the first rule for Private to Public traffic:

- Action = Masquerade, Application = any, From = Private, To = Public

New NAT Rule		✕
Action	Masquerade	▼
Application	any	
From	Private	▼
To	Public	▼
With (Optional)		▼
		Cancel Save

Click + **new rule** again and create the second NAT masquerade rule in the same way for DMZ to Public traffic with these details:

- Action = Masquerade, Application = any, From = DMZ, To = Public

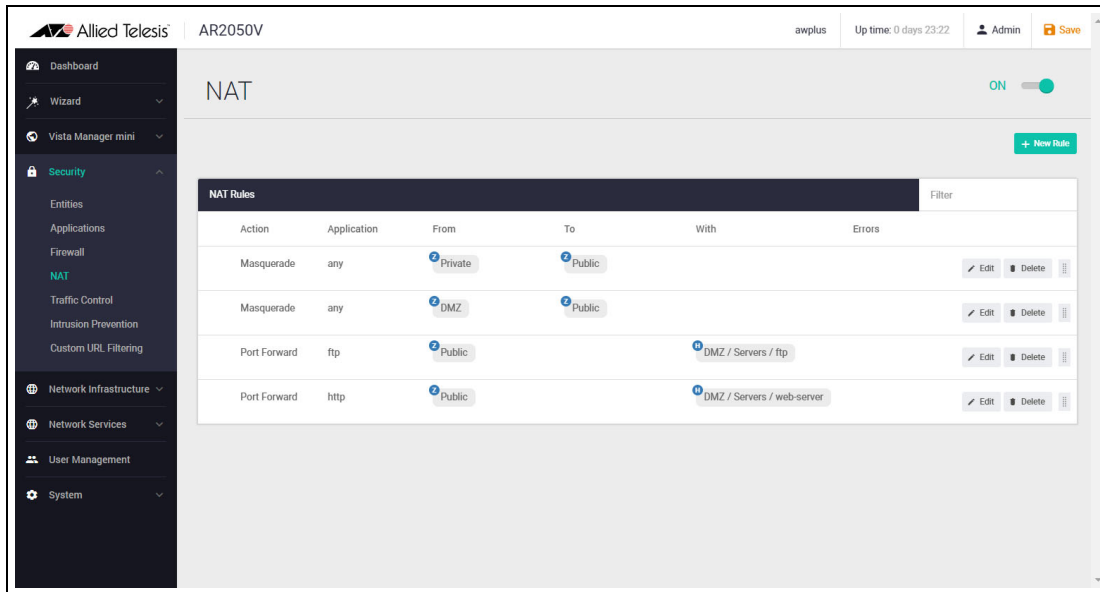
We now need to create two NAT port-forwarding rules to enable access to the FTP and Web servers to be delivered to the right destinations. To users in the Public zone, both servers will appear to have the IP address that is on the eth2 interface, so sessions towards those servers will be initiated to that address. The firewall must then forward those sessions to the actual addresses of the servers.

Click + **new rule** and create the two NAT port-forward rules with the following details:

- Action = Port Forward, Application = ftp, From = public, With = dmz.servers.ftp
- Action = Port Forward, Application = http, From = public, With = dmz.servers.web-server

Now click the **ON/OFF** button at the top right of the Dashboard page to activate NAT.

You can see the four new NAT rules:



You can also see these new NAT rules with the command **show nat rule**.

```

AlliedWare Plus (TM) 5.5.0 09/02/20 21:20:39
awplus>ena
awplus#show nat rule

[* = Rule is not valid - see "show nat rule config-check"]
-----
ID      Action  From      To      With (dst/src) Entity  Hits
      App    To
-----
10      masq    Private   Public  -                -      0
      any    Public
20      masq    DMZ       Public  -                -      0
      any    Public
30      portfwd Public    -        DMZ.Servers.ftp  -      0
      ftp
40      portfwd Public    -        DMZ.Servers.web-server -      0
      http
awplus#
    
```

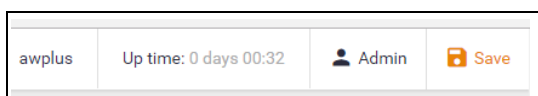
Step 7: Save configuration changes.

The configuration we have made so far is part of the running-configuration on the firewall.

Save these configuration changes to make them part of the boot configuration, so they can be backed up and will survive a reboot of the firewall.

- Click the **Save** button at the top right of the GUI screen.

Tip: The **Save** button will be orange anytime there is unsaved configuration.



Part 2: Configure the router for Update Manager

Updating the GUI

As new versions of the Device GUI become available with additional functionality, they are made available on the update server to be downloaded and installed on the firewall.

To check if there is a new version of the Device GUI, and install it on your router, firstly ensure that the firewall can contact the update server using the steps below, and then simply enter the following command from the CLI window:

```
awplus# update webgui now
```

Configuration of entities and rules is required to allow connectivity between Update Manager and the Update Server.

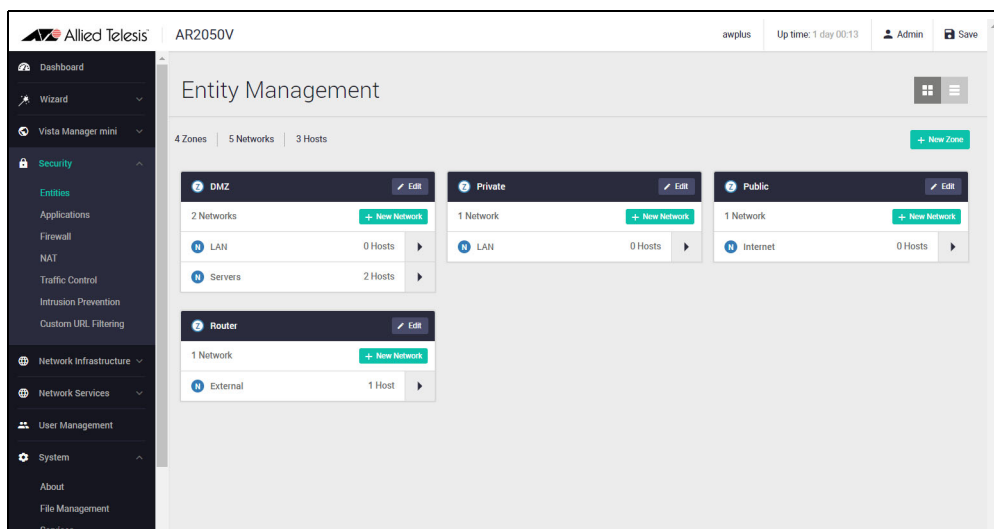
Step 1: Create appropriate entities.

Updating the Device GUI involves sessions that are initiated from the firewall unit itself. This means that firewall rules are required that permit these sessions. Create a zone that represents the firewall itself, with a public interface that exists as a host within this zone.

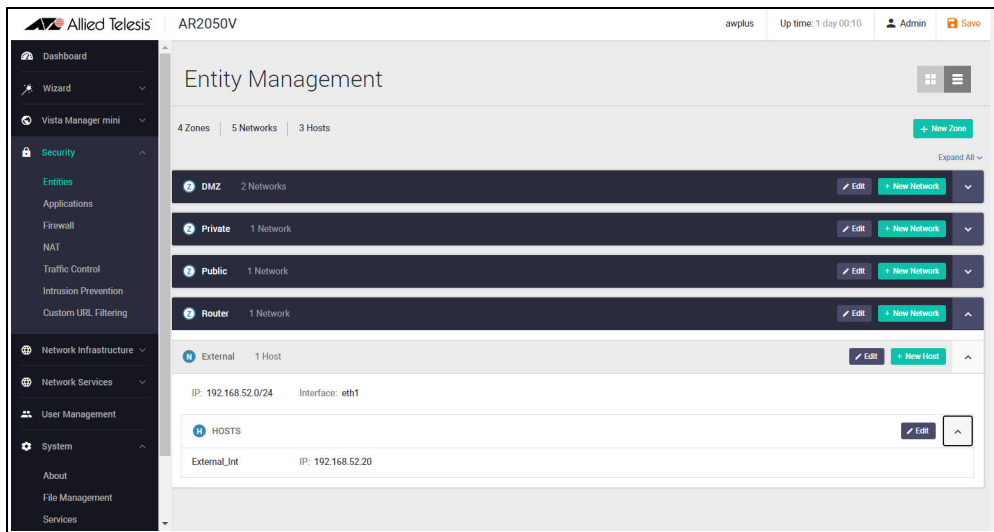
From the **Entities** menu, create zone/network/host entities for the Update Manager source traffic with the following details:

- Zone name = Router
- Network name = External
- Network subnet and interface = 192.168.52.0/24, Eth1
- Host name = External_Int
- Host IP address = 192.168.52.20

The updated **Entity Management** page will look like this:



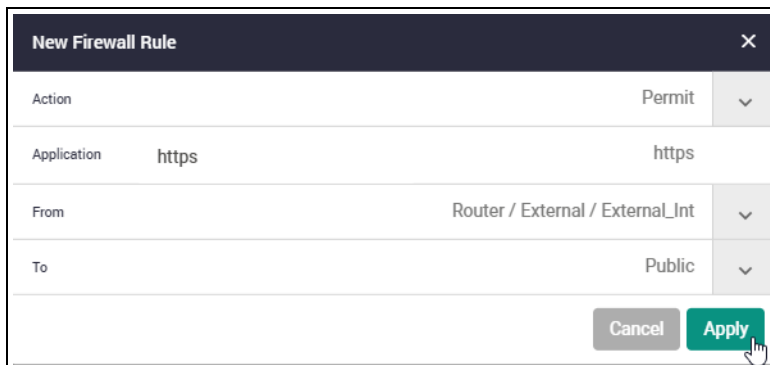
Or this - in list view (with just the new zone expanded):



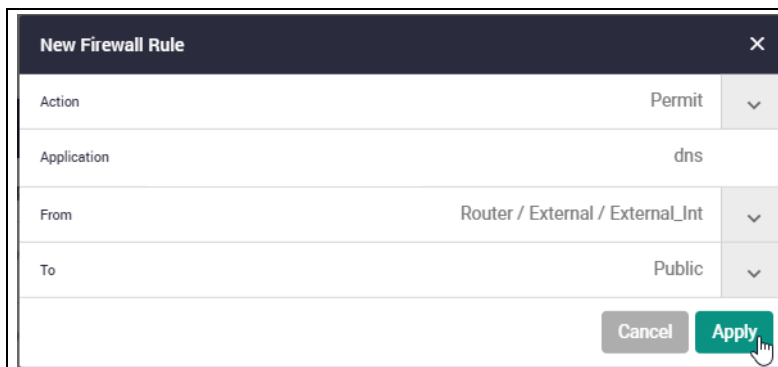
Step 2: Create firewall rules for the Update Manager traffic.

The Update Manager uses HTTPS for secure connectivity.

From the **Firewall** menu, create a firewall rule with the following details to allow HTTPS traffic out to the update server.



Also create a rule to allow DNS resolution of the update server's URL.

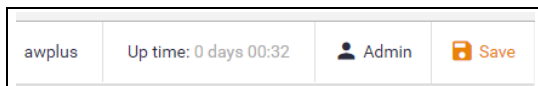


These new rules can be seen added to the firewall rule set.

Permit	https	Router / External / External_Int	public
Permit	dns	Router / External / External_Int	public

Step 3: Save configuration changes.

Once again, click the **Save** button on the GUI top bar to save the Update Manager configuration to the boot configuration file.



Part 3: Configure security features

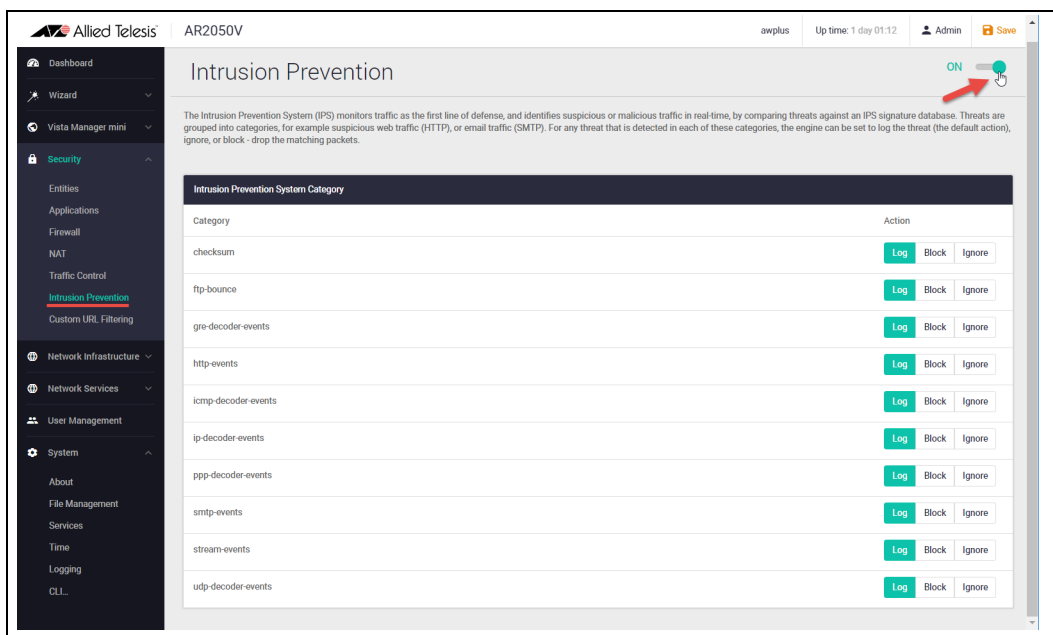
The VPN routers allow you to configure the Intrusion Prevention System (IPS) for network protection, and URL filtering to manage website access.

Intrusion Prevention System

IPS monitors inbound and outbound traffic as the first line of defense, and identifies suspicious or malicious traffic in real-time by comparing threats against an IPS known signature database.

Step 1: Enable IPS.

- Navigate to the **Intrusion Prevention** configuration page under **Security**.
- Click the **ON/OFF** switch on the top right of the page to enable IPS.



Step 2: Configure IPS actions.

Threats are grouped into categories, for example suspicious web traffic (HTTP), or email traffic (SMTP). For any threat that is detected in each of these categories, the engine can be set to **log** the threat (which is the default action), **ignore**, or **block** - drop the matching packets.

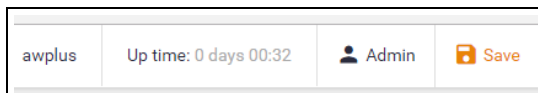
- To drop suspicious SMTP traffic, set the action to **block**.

Intrusion Prevention System Category	
Category	Action
checksum	<input type="button" value="Log"/> <input type="button" value="Block"/> <input type="button" value="Ignore"/>
ftp-bounce	<input type="button" value="Log"/> <input type="button" value="Block"/> <input type="button" value="Ignore"/>
gre-decoder-events	<input type="button" value="Log"/> <input type="button" value="Block"/> <input type="button" value="Ignore"/>
http-events	<input type="button" value="Log"/> <input type="button" value="Block"/> <input type="button" value="Ignore"/>
icmp-decoder-events	<input type="button" value="Log"/> <input type="button" value="Block"/> <input type="button" value="Ignore"/>
ip-decoder-events	<input type="button" value="Log"/> <input type="button" value="Block"/> <input type="button" value="Ignore"/>
ppp-decoder-events	<input type="button" value="Log"/> <input type="button" value="Block"/> <input type="button" value="Ignore"/>
smtp-events	<input type="button" value="Log"/> <input checked="" type="button" value="Block"/> <input type="button" value="Ignore"/>
stream-events	<input type="button" value="Log"/> <input type="button" value="Block"/> <input type="button" value="Ignore"/>
udp-decoder-events	<input type="button" value="Log"/> <input type="button" value="Block"/> <input type="button" value="Ignore"/>

You can monitor IPS matches on the Dashboard security monitoring widget.

Step 3: Save configuration changes.

- **Save** the IPS configuration changes to make them part of the boot configuration file.

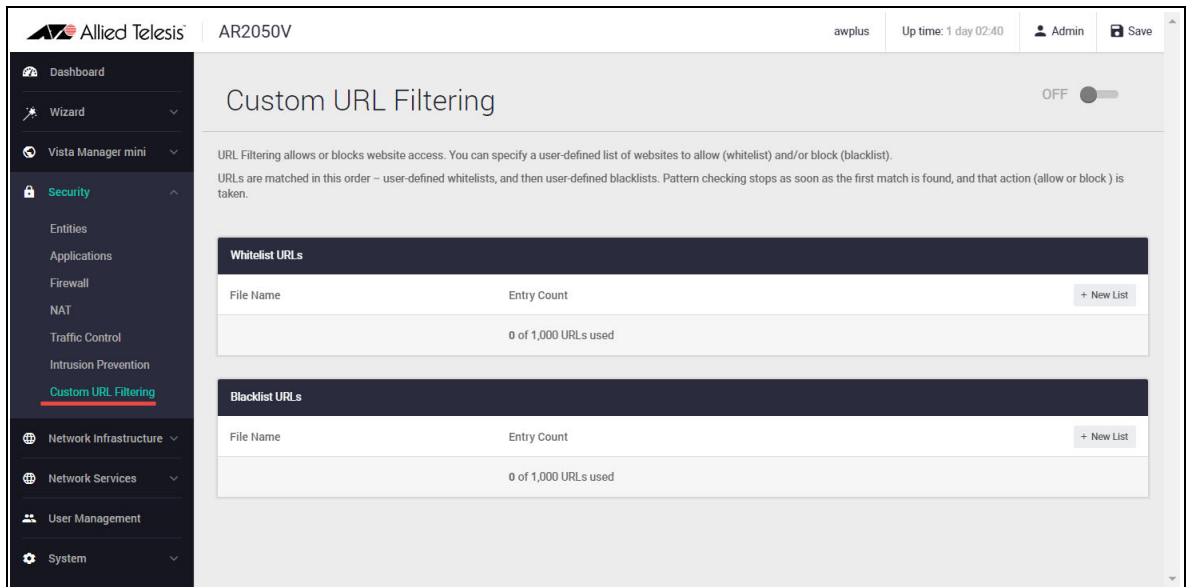
**Custom URL Filtering**

URL Filtering is a fast efficient (stream-based) method to allow or block employee's website access. You can specify a user-defined list of websites to allow (whitelist) and/or block (blacklist).

URLs are matched in this order: user-defined whitelists and then user-defined backlists. Pattern checking stops as soon as the first match is found, and that action (allow or block) is taken. If no match is found, website access will be allowed.

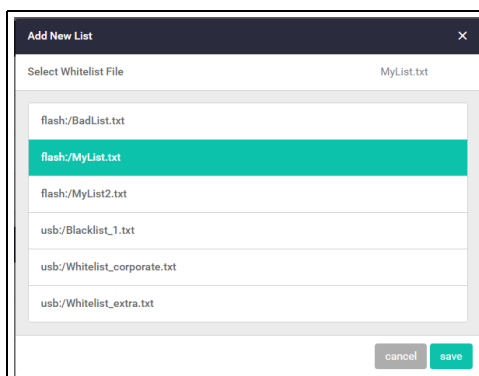
Step 1: Configure custom URL filtering.

- Navigate to the **Custom URL Filtering** page under **Security**.

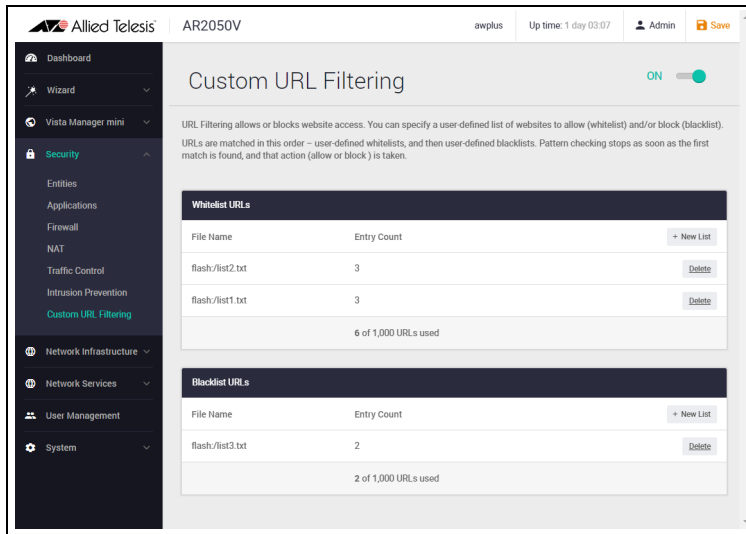


You can now add user-defined whitelists of URLs to allow, and/or blacklists of URLs to block. You can add multiple lists, and these can have a total maximum of 1000 whitelist URLs and 1000 blacklist URLs. The GUI page lets you know how many URLs are in each list and the total URLs used.

- Click on the **+New list** button to add new whitelist or blacklist URLs.
- Select the file(s).
- Click **Save**.



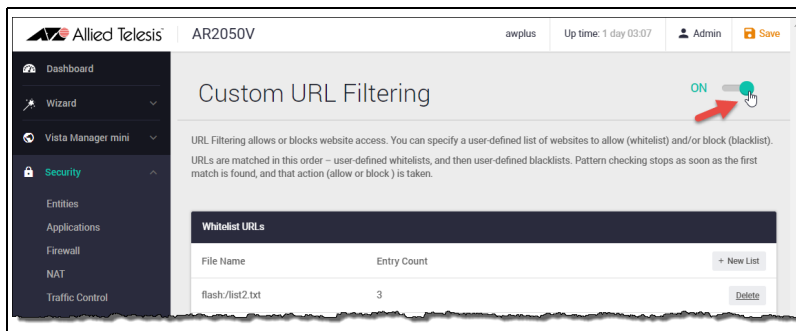
Currently active whitelists and blacklists are shown on the page. The Entry Count shows the number of URLs used:



For information on creating custom lists, see ["Creating custom lists"](#) on page 43.

Step 2: Enable URL Filtering.

Enable URL Filtering with the **ON/OFF** switch at the top of the page:

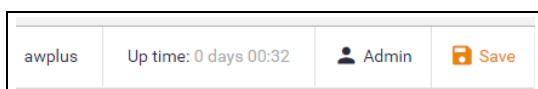


The router will now match any website URLs that users try to browse to against the whitelist/s, then the blacklist/s. Pattern checking stops as soon as the first match is found, and that action (allow or block) is taken. If no match is found, website access will be allowed.

Tip: You can monitor URL Filtering hits on the Dashboard security monitoring widget.

Step 3: Save configuration changes.

Save your Custom URL Filtering changes to make them part of the boot configuration.



Creating custom lists

A custom list is an ASCII formatted text file containing zero or more single-line pattern matches.

For example, the content of a text file named *blacklist-example.txt*, consisting of three patterns to match, (listed line-by-line) could look like this:

```
example.net/viruses/*
*/viruses/*
bad_url.com
```

URL pattern matches listed within the text file may take two forms:

- either a base domain, which will match all content of that domain, and all content of sub-domains:

```
example.com
```

- or a wild-card match, where an asterisk will match zero or more characters in a URL:

```
example.net/viruses/*
*/viruses/*
```

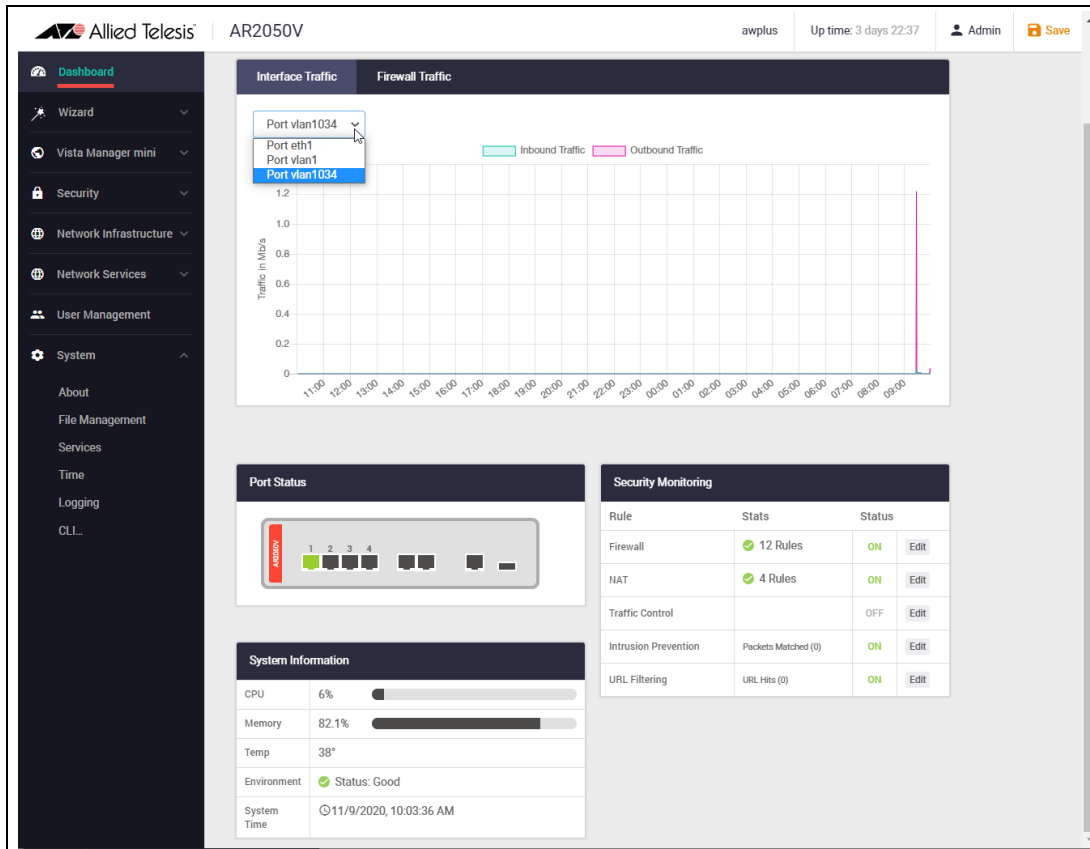
Once this list is available to the system (stored in Flash, USB, or on an SD card), the configuration to enable URL filtering is straight forward.

Tip: You can use the CLI in the Device GUI to create new or edit an existing custom list.

See the [URL Filtering Feature Overview Guide](#) for more information about creating user-defined URL Filtering lists.

The Dashboard

Now that we have configured the router, let's take a look at the Dashboard of the GUI and the information provided in the various widgets.

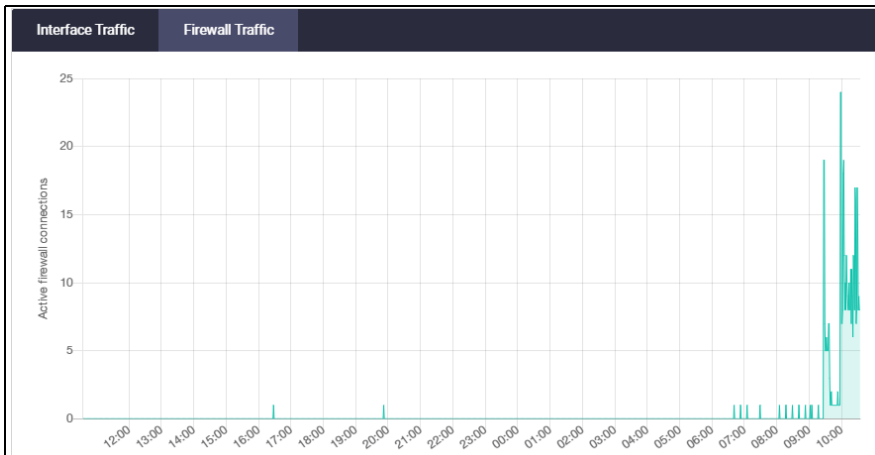


Currently there are **Interface/Firewall Traffic**, **Port Status**, **Security Monitoring**, and **System Information** widgets.

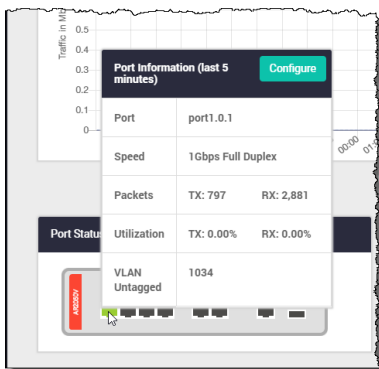
Interface Traffic - shows traffic passing through the selected interface in both directions over a 24 hour period.



Firewall Traffic Firewall Traffic shows traffic passing through the firewall over a 24 hour period.



Port Status The **Port Status** widget shows port information: port number, speed, packet TX and RX, utilization, and interface.





Security Monitoring The **Security Monitoring** widget shows the traffic rules and security features in one handy location. You can see which are currently enabled and which are not. You can select **edit** to go to that features dedicated page to configure it further.

Security Monitoring			
Rule	Stats	Status	
Firewall	✔ 12 Rules	ON	Edit
NAT	✔ 4 Rules	ON	Edit
Traffic Control		OFF	Edit
Intrusion Prevention	Packets Matched (0)	ON	Edit
URL Filtering	URL Hits (0)	ON	Edit

You can also see how many rules are configured for the various features, as well as IPS matches, and URL Filtering rule hit statistics.

System Information

The **System Information** widget shows CPU and memory use, as well as device health and system time.

System Information	
CPU	5% 
Memory	82.1% 
Temp	38°
Environment	✔ Status: Good
System Time	🕒 11/9/2020, 10:07:36 AM

System Page

Further system information is available on the **About** page, under the **System** menu. You can see the device model name, MAC address, serial number, environment status, GUI version and build, and so on here.

System Information	
Name:	awplus
Model:	AR2050V
MAC Address:	00-1a-eb-94-27-e7
Serial Number:	A05236G154300028
Environment:	✔ Status: Good <input type="button" value="v"/>
Current Software:	AR2050V-5.5.0-1.3.rel
Software Version:	5.5.0-1.3
Bootloader:	5.0.5
GUI Version:	2.6.1
GUI Build:	20200904_1632

The network map

Under the Vista Manager mini menu, there is a network topology map. This map shows details of the devices connected to the switch or firewall. You can use it to see your:

- wired devices
- APs
- wireless deployment and coverage.

This section begins with a brief description of the network map window and the tasks you can perform there. The section ends with a look at configuring the network topology view and customizing node icon images.

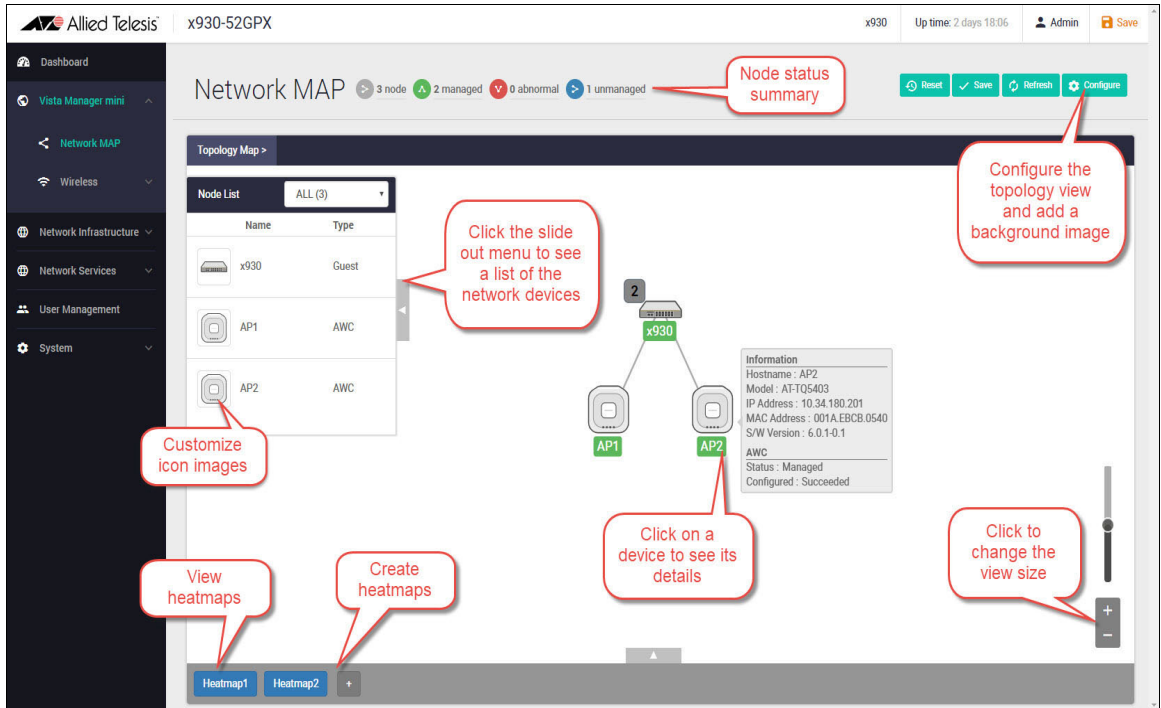
Note that the screenshots in this section show an x930 Series switch, but the functionality is the same for all models that include Vista Manager mini.

The network map features

The network map displays details of a network configuration. Double click on an area to see all the nodes in that area. Use the network map to check the status of a node at a glance. Node status is indicated by the node title background color. Abnormal is red, managed is green, and blue indicates an unmanaged node.

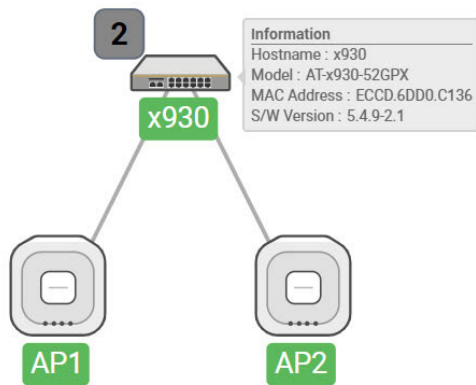
From the **network MAP** page, you can:

- customize network icon images
- view individual node details
- see a list of network nodes
- configure the topology view
- create a heat map
- view stored heat maps



Viewing node information

In the network topology map view, click on a device to see information about the Hostname, Model, MAC address, and software version.



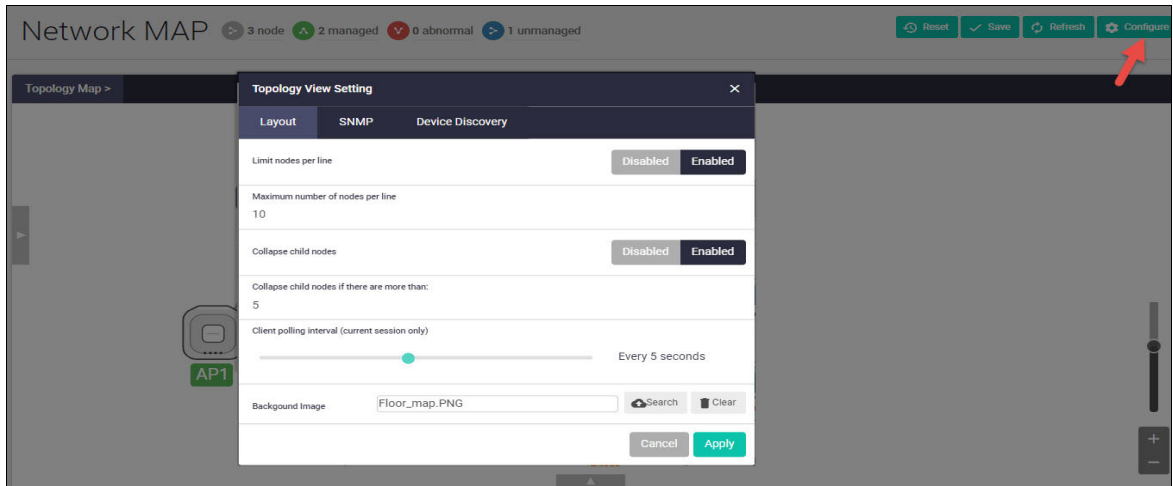
Configuring the topology view

Vista Manager mini automatically creates a complete topology map from an AMF network of switches, firewalls, and wireless access points (APs), showing areas and multiple levels of connected nodes and devices.

To change the topology view settings:

- In the Topology Map view, select **Configure** - the menu is located at top right corner.

- In the **Topology View Settings** window, you can choose to:
 - limit nodes per line
 - collapse child nodes
 - select a background image
- **Save** your changes.



Customizing network node icon images

You can customize the look of your network nodes with icon images. For example, you can add access point, switch, and router images to make the network map easier to understand at a glance.

You can create an icon library to help store, organize, and find images.

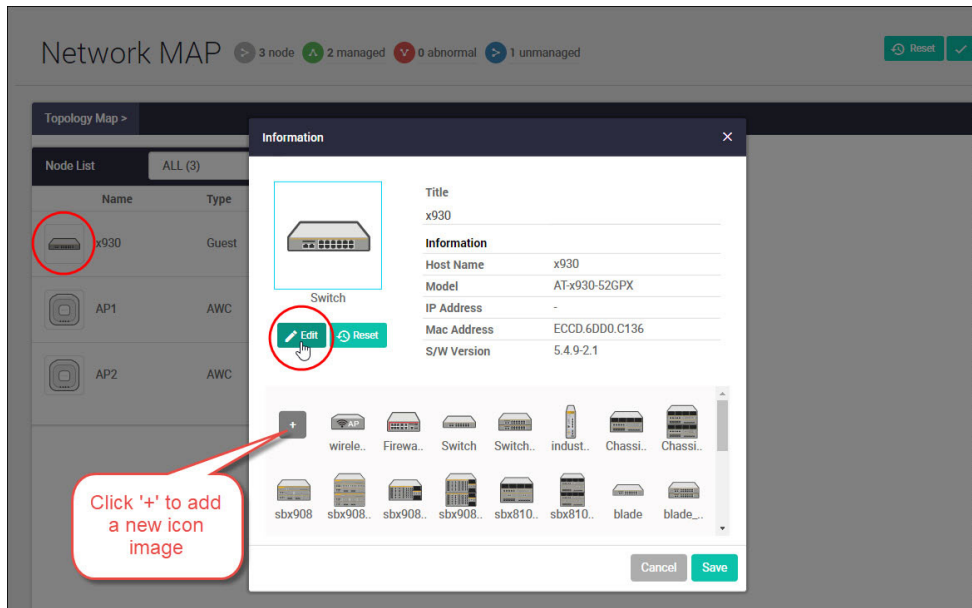
To customize a network node icon:

1. In the Topology Map view, open the **Node List** (slide-out menu)



2. Click on a node's icon image.
3. Click **Edit**.

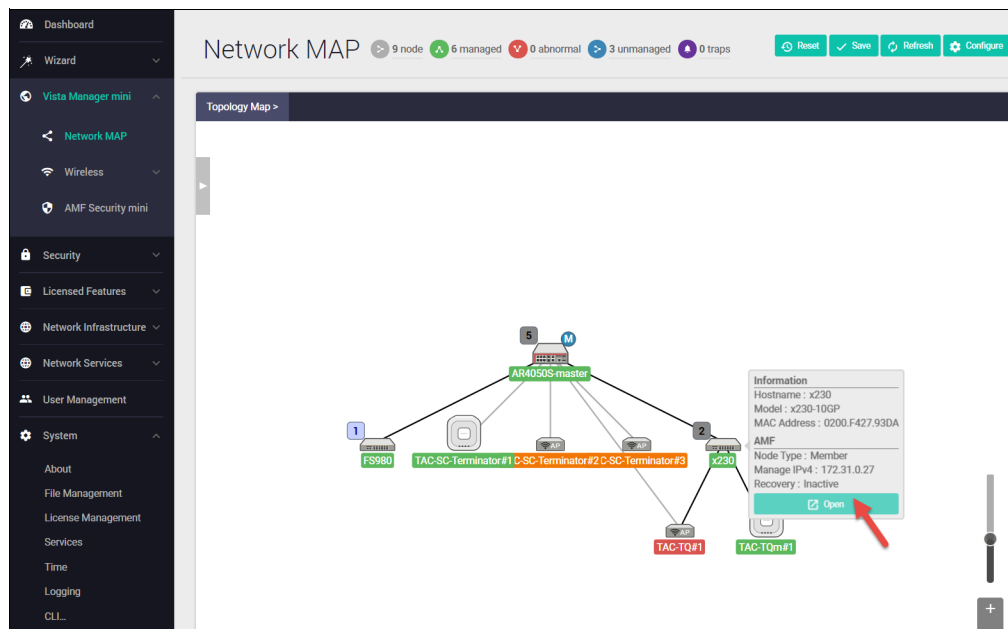
4. Select an image from the library or click the '+' sign to add a new one.
5. Click **Save**.



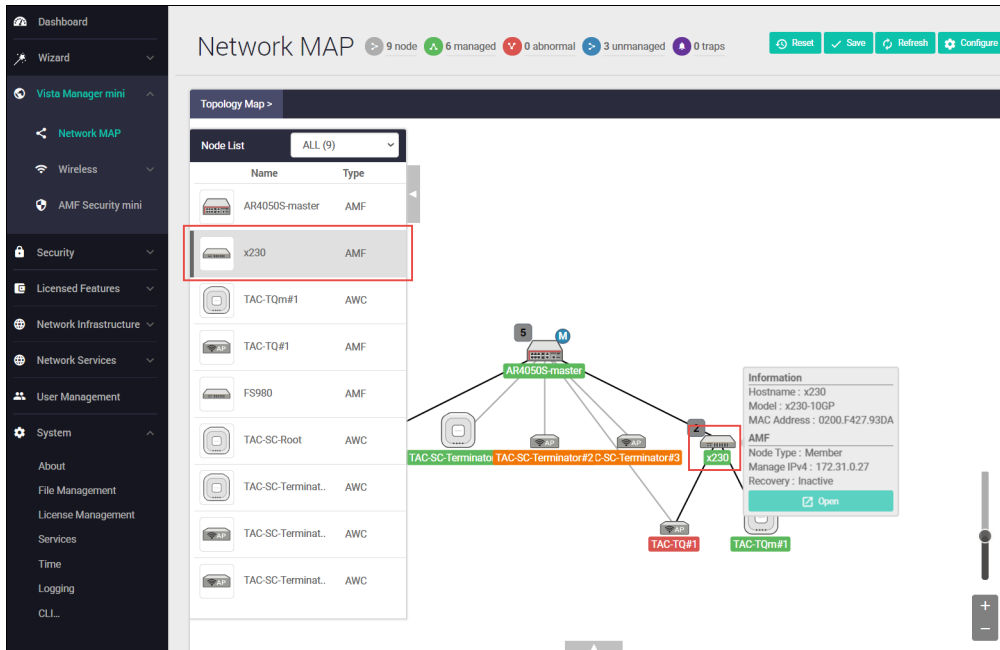
Access to device GUI by clicking on device icon

From version 2.5.2 onwards, you can open the GUI for a device in your network (e.g. an x230) from the network map in the GUI of another device in your network (e.g. an AR4050S).

When you click a node icon on the Network Map, the node information is displayed. In the node information window, click on the **Open** button to access the device's GUI.



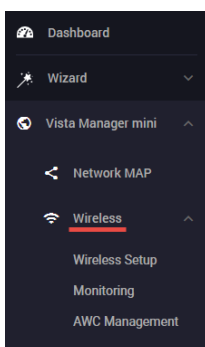
You can use the **Node List** to help you locate a device in the network map. Simply click the device in the Node List to see its **Information** details.



Wireless management

Most Allied Telesis VPN Routers incorporate Autonomous Wave Control (AWC) wireless management, allowing your wireless access points (APs) to be setup and managed from the Device GUI on your security appliance. AWC uses wireless intelligence to constantly model AP location and signal strength information. It then automatically optimizes wireless output and channel selection for optimum performance.

The device GUI includes a Wireless Management menu, which enables you to set up your wireless network, monitor and configure the network, and manage AWC:



The device GUI also displays heat maps for managed APs on the network map.

For more information about heat maps, AWC and how to manage wireless devices, see the [User Guide: Wireless Management \(AWC\) with Vista Manager mini](#).

Other features

The Device GUI has a number of other great features. The **Network Infrastructure** menu includes interface management, VLAN management, tools. The **Network Services** menu allows you to configure the firewall as a DHCP server for the network. There are configuration options for SMTP, RADIUS, Tools, and AAA here too. These will not be detailed here, but are easy and intuitive to use.

File management

Use the **File Management** page to view all files stored on the device, as well as any USB device or SD card that is plugged in. The upload and download functions provide an easy way to add new files such as firmware, configurations, scripts, or URL lists to the device, as well as save configurations for backup.

You can use this page to set the software release and configuration files, and reboot the device for easy firmware upgrade.

The **File Management** page can be found under the **System** menu:

The screenshot shows the File Management interface for an AR2050V device. The breadcrumb navigation path is **/fs/flash**, which is circled in red. Below it is a table of files:

Name	Modified	Size(bytes)	Actions
AR2050V-5.5.0-1.1.rel	7/23/2020, 12:09:07 PM	57725431	Download Delete
AR2050V-5.5.0-1.3.rel	9/8/2020, 2:50:21 PM	57753951	Download Delete
awplus-gui_550_20.gui	9/8/2020, 10:39:41 AM	2646016	Download Delete
default.cfg	11/6/2020, 2:42:52 PM	2817	Download Delete
dpi-arc-5.5.0-1.3-1-16044490...	11/4/2020, 1:18:13 PM	949467	Download Delete
dpi-arc-5.5.0-1.3-1-16044490...	11/4/2020, 1:18:53 PM	4646280	Download Delete
dpi-arc-5.5.0-1.3-1-16044491...	11/4/2020, 1:19:29 PM	4680038	Download Delete

On the right side, there are two configuration sections:

- Set Boot Release File:** Current: flash/AR2050V-5.5.0-1.3.rel (Browse); Backup: flash/AR2050V-5.5.0-1.1.rel (Browse)
- Set Boot Config File:** Current: flash/default.cfg (Browse); Backup: Not Set (Browse)

At the bottom right, the **Flash Usage** section shows a progress bar at 4% and '139.5M / 3.6G'.

By default, the flash system files are shown as above. To view files on a USB device, navigate back to the main file system (**fs**), and choose **usb**:

The screenshot shows the File Management interface for the main file system (**fs**). The breadcrumb navigation path is **/fs**. Below it is a table of file systems:

Name	Modified
flash	Sun Apr 09 17:09:21 2017 UTC
usb	Thu Jan 01 00:00:00 1970 UTC

Use the **Upload** button to browse and locate the file you wish to add to the firewall. From here you can easily add more files and change the release and configuration files.

For example, for an easy 3-click firmware upgrade, simply:

1. Browse to the new firmware file using the **upload** option
2. Set the new firmware file to be the boot release
3. Re-boot the device.

The screenshot shows the File Management interface for an AR2050V router. The main area displays a table of files in the /fs/flash directory:

Name	Modified	Size(bytes)	Actions
AR2050V-5.5.0-1.1.rel	7/23/2020, 12:09:07 PM	57725431	Download Delete
AR2050V-5.5.0-1.3.rel	9/8/2020, 2:50:21 PM	57753951	Download Delete
awplus-gui_550_20.gui	9/8/2020, 10:39:41 AM	2646016	Download Delete
default.cfg	11/6/2020, 2:42:52 PM	2817	Download Delete
dpi-arc-5.5.0-1.3-1-16044490...	11/4/2020, 1:18:13 PM	949467	Download Delete
dpi-arc-5.5.0-1.3-1-16044490...	11/4/2020, 1:18:53 PM	4646280	Download Delete
dpi-arc-5.5.0-1.3-1-16044491...	11/4/2020, 1:19:29 PM	4680038	Download Delete
dpi-arc-5.5.0-1.3-1-16044491...	11/4/2020, 1:20:01 PM	4725720	Download Delete
dpi-arc-5.5.0-1.3-1-16044491...	11/4/2020, 1:20:35 PM	4752130	Download Delete

On the right side, there are panels for 'Set Boot Release File' and 'Set Boot Config File'. The 'Set Boot Release File' panel shows 'Current: flash/AR2050V-5.5.0-1.3.rel' and 'Backup: flash/AR2050V-5.5.0-1.1.rel', with a 'Browse' button highlighted by a red box labeled '2'. The 'Set Boot Config File' panel shows 'Current: flash/default.cfg' and 'Backup: Not Set', with a 'Browse' button. At the bottom right, the 'Flash Usage' panel shows a progress bar at 4% and '139.5M / 3.6G'.

Tip Use the **Flash Usage** panel to see the currently used flash and available storage size.

The Flash Usage panel shows a progress bar at 10% and the text '346.1M / 3.6G'.

Logging management

The **Logging** page shows buffered and permanent log messages stored on the device.

- By default the buffered logs tab is displayed.

Date ^	Facility ^	Level ^	Program ^	Message ^
2018-04-23 18:25:14	user	notice	ATMF	Last message 'Incarnation is not p' repeated 9 times, suppressed by syslog-ng on 3
2018-04-23 18:25:14	user	debug	VCS	STK TRACE: Stack member-1 changed status from Syncing to Ready
2018-04-23 18:25:16	user	notice	ATMF	Incarnation is not possible with the data received port1.0.9 (ifindex 5009)
2018-04-23 18:25:45	user	notice	ATMF	Last message 'Incarnation is not p' repeated 14 times, suppressed by syslog-ng on 3
2018-04-23 18:25:45	syslog	notice	syslog-ng	Syslog connection established; fd='61', server='AF_INET(10.37.95.65:514)', local='AF_INET(0.0.0.0:0.0.0.0:514)'
2018-04-23 18:25:45	syslog	err	syslog-ng	I/O error occurred while writing; fd='61', error='Connection refused (146)'
2018-04-23 18:25:45	syslog	notice	syslog-ng	Syslog connection broken; fd='61', server='AF_INET(10.37.95.65:514)', time_reopen='60'
2018-04-23 18:25:46	user	notice	ATMF	Incarnation is not possible with the data received port1.0.9 (ifindex 5009)
2018-04-23 18:26:45	user	notice	ATMF	Last message 'Incarnation is not p' repeated 29 times, suppressed by syslog-ng on 3
2018-04-23 18:26:45	syslog	notice	syslog-ng	Syslog connection established; fd='29', server='AF_INET(10.37.95.65:514)', local='AF_INET(0.0.0.0:0.0.0.0:514)'

You can filter the logs in three ways to focus your view and support easy analysis:

1. any information column in ascending or descending order

Date ^	Facility ^	Level ^	Program ^	Message ^
2018-04-23 18:46:21	local6	crit	ATMF	AR4050 has left. 4 members in total.
2018-04-23 18:58:20	local6	crit	ATMF	AR4050 has joined. 5 members in total.
2018-04-23 18:34:14	local6	crit	ATMF	AR4050 has joined. 5 members in total.
2018-04-23 18:36:38	local6	crit	ATMF	AR4050 has left. 4 members in total.
2018-04-23 18:36:47	local6	crit	ATMF	AR4050 has joined. 5 members in total.
2018-04-23 18:33:58	local6	crit	ATMF	AR4050 has left. 4 members in total.
2018-04-23 18:46:24	local6	crit	ATMF	AR4050 has joined. 5 members in total.
2018-04-23 18:48:40	user	crit	IMISH	Virtual Terminal connection #0 has timed out.

2. selecting the level of logs to display: Critical, Warning, Error etc.

Date ^	Facility ^	Level ^	Program ^	Message ^
2018-04-23 18:33:58	local6	crit	ATMF	AR4050 has left. 4 members in total.
2018-04-23 18:34:14	local6	crit	ATMF	AR4050 has joined. 5 members in total.
2018-04-23 18:36:38	local6	crit	ATMF	AR4050 has left. 4 members in total.
2018-04-23 18:36:47	local6	crit	ATMF	AR4050 has joined. 5 members in total.

3. searching for any text string found in the logs.

The screenshot shows the 'Logging' page with a search filter set to 'received'. The table below shows log entries with the word 'received' highlighted in red in the message column.

Date	Facility	Level	Program	Message
2018-04-23 18:31:36	user	notice	ATMF	Incarnation is not possible with the data received port1.0.9
2018-04-23 18:31:40	user	notice	ATMF	Incarnation is not possible with the data received port1.0.9
2018-04-23 18:31:46	user	notice	ATMF	Incarnation is not possible with the data received port1.0.9

Click the **Configure Logging** button to access the Logging Configuration page. This page allows you to create filters to manage which logs are stored on the device and also set up a Syslog server(s) for remote log storage.

The screenshot shows the 'Logging' page with the 'Configure Logging' button highlighted in red. The table below shows log entries related to AR4050.

Date	Facility	Level	Program	Message
2018-04-23 18:33:58	local6	crit	ATMF	AR4050 has left. 4 members in total.
2018-04-23 18:34:14	local6	crit	ATMF	AR4050 has joined. 5 members in total.
2018-04-23 18:36:38	local6	crit	ATMF	AR4050 has left. 4 members in total.
2018-04-23 18:36:47	local6	crit	ATMF	AR4050 has joined. 5 members in total.

The **Logging Configuration** page has tabs for local and remote (syslog server) settings.

The screenshot shows the 'Logging Configuration' page with the 'Local' tab selected. It displays two sections: 'Buffered' and 'Permanent' logs, each with a table of filters and a 'Clear Logs' button.

Level	Facility	Program	Message
Notice	cron	all	*
Alert	daemon	iml	*
Notice	authpriv	dhcpcd	*
Debug	all	all	*

Level	Facility	Program	Message
Debug	all	all	*
Warning	all	all	*

Use the **Local** tab (default) to create filters to manage the level of logs that are stored in the buffered and permanent logs on the device. You can also delete the buffered or permanent logs using the **Clear Logs** button.

Use the **View Logs** button to return to the Logging page.

When you create a new logging filter you can specify any/all of level, facility, program, and message to be included or excluded in the log storage. This means you can configure log storage exactly as you want it.

The screenshot shows a dialog box titled "Add Filter For Buffered Log". It contains the following fields and controls:

- Level:** A dropdown menu currently set to "Critical".
- Facility:** A text input field containing "daemon".
- Program:** A text input field with the placeholder "Enter program here" and a dropdown menu set to "all".
- Message:** A text input field containing an asterisk (*).
- Radio Buttons:** Two buttons labeled "Included" and "Excluded".
- Save Button:** A green button labeled "save".

Use the **Remote** tab and the **+New Host** button to set up a syslog server to send log messages to for storage and analysis. Use the **+New Filter** button to configure filters that specify the type of logs (include or exclude) to be sent to the syslog server.

The screenshot shows the "Logging Configuration" interface with the "Remote" tab selected. It features a table of filters and several action buttons:

Level	Facility	Program	Message
Emergency	all	all	*
Notice	all	all	*

Buttons visible in the interface include: "+ New Host", "Delete Hosts", "+ new filter", and "delete".

C613-22094-00 REV L



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

© 2022 Allied Telesis, Inc. All rights reserved. Information in this document is subject to change without notice. All company names, logos, and product designs that are trademarks or registered trademarks are the property of their respective owners.