### **Technical Guide**

# Getting Started with the Device GUI on VPN Routers

Feature Overview and Configuration Guide

## 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.

00000100000010101000001010100101

Allied Telesis

### 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<sup>™</sup> 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
What is a Firewall?	4
What are Entities?	4
Zones, networks, and hosts	5
Using Rules	6
Configuring the Router	7
Part 1: Configure a standard 3-zone network	7
Part 2: Configure the router for Update Manager2	1
Part 3: Configure security features	4
The Dashboard	8
Other Features	0
File Management	0
Logging Management33	3
Wireless management	5

## Products and software version that apply to this guide

This guide applies to all AR-Series VPN Routers running AlliedWare Plus<sup>™</sup> software version 5.4.7x.x or 5.4.8-x.x. Supported models include the AR2050V and AR2010V.

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

To configure Autonomous Wave Control using the Device GUI, see AWC Wireless Control on AR-Series Devices.

## What is a Firewall?

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.

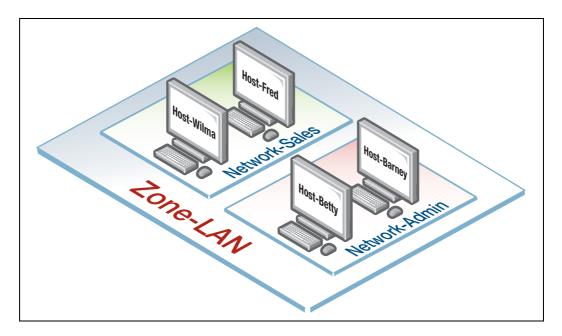
Allied Telesis firewalls and routers map out the network environment into regions, using three tiers of granularity. The divisions into which it cuts up its environment are referred to collectively as **Entities**. The three levels of granularity in the dividing up of the environment are zones, networks,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

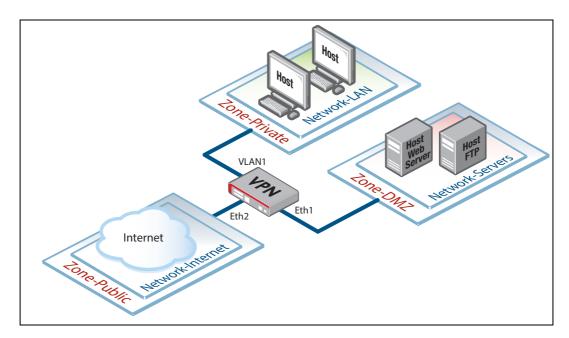
## Configuring the Router

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 21
- 3. Security features IPS, and Custom URL Filtering, see page 24

### Part 1: Configure a standard 3-zone network

The rest of this guide will use the AR2050V as the example device. The compact AR2010V offers the same functionality, but has only two Ethernet ports and no switch ports.



#### Step 1. Configure router interfaces.

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), and the HTTP service enabled. Connect to any switch port (AR2050V) or Eth1 (AR2010V) and browse to 192.168.1.1 to begin.

To use the Device GUI, we need to add an IP address to an interface over which we will connect with our browser, once the GUI resource file has been loaded onto the firewall.

We will also add IP addresses to the other interfaces that will be used in our network.

Alternatively, you can just add an IP address to the interface over which you will connect with your browser, and then add the other two IP addresses using the Device GUI Interface Management page.

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.
```

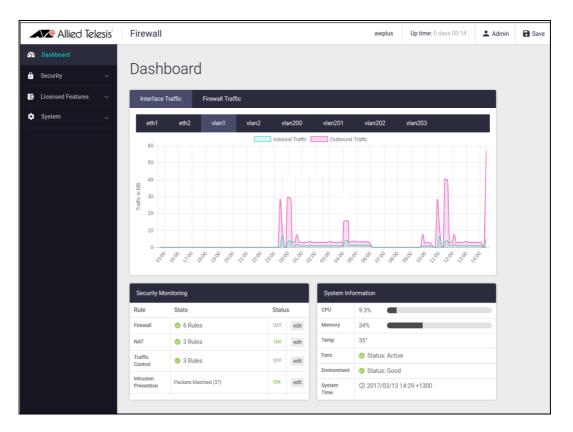
Browse to the IP address of the router on the interface you are connecting to - e.g. 192.168.1.1 for VLAN1.

Note: The Device GUI currently supports the Firefox<sup>™</sup>, Microsoft Edge<sup>™</sup> and Internet Explorer 11, Apple Safari<sup>™</sup> and Chrome<sup>™</sup> web browsers.

The following login page is displayed:

e https://19216811/public/login.html	⇒ C <sup>i</sup> Q, Search	☆自	0	+	<b>f</b>	9
	Allied Telesis					
	Username					
	Password					
	Sign in					
	About the application 😒					

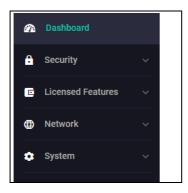
You can log in using any valid username/password combination that has been configured on the unit, or use the default username/password (**manager/friend**), if that has not been deleted.



Once logged in you will be on the Dashboard of the Device GUI.

The Dashboard shows 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 navigation bar, with options to view the **Dashboard** or the **Security**, **Network**, **System**, and **Wireless Management** menus for configuration.



### Step 4. Configure Entities.

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

Select **Entities** under the **Security** menu.

Allied Telesis	Firewall	awplut	Up time: 0 days 03:43	1 Admin 🔂 🗤
Dashboard				
Security -	Entity Management			
Entities				
Applications	© Zones   0 Networks   0 Hosts			+
Fernal				
NAT				
Traffic Control				
Intrusion Prevention				
Contern URL Filtering				
Licensed Features				
Network ~				
System				

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.

new zone	×
Name	
dmz	
	cancel save

Next click the green + new network button in the DMZ zone to add our servers network.

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

new network		×
Name servers		
IP 172.16.0.0/24	Interface eth1	<u>delete</u>
<u>+ new subnet</u>		
Assign to Zone		dmz
		cancel save

- We can now add specific hosts (servers in this case).
- Click on the slide arrow to open details of the servers network.

🖌 edit
+ new network
0 Hosts

•	🕦 servers	🖌 edit
0 Ho	osts	+ new host
IP: 1	172.16.0.0/24 Interface: eth1	

Click the green +new host button to add the ftp server with an IP address of 172.16.0.2

New Host	×
Name ftp	
<b>IP</b> 172.16.0.2	
Assign to Network	servers
	cancel save

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

•	H HOSTS	🖌 edit
web- serve		
ftp	<b>IP:</b> 172.16.0.2/24	

Use 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, eth2

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

Allied Telesis	Firewall			avplus	Up time: O days 03:43 🔒 Admin 🔒 🏣
Dashboard					
Security -	Entity Management				* =
Entities Applications	3 Zones   3 Networks   2 Hosts				
Fermult	( O HOSTS	V mili	V mit	😑 public	✓ eff.
Traffic Control	ftp IP: 172.16.0.2	1-Network	+ ten start	1 Network	· new tellsort
Intrusion Prevention	web- IP: 172.16.0.10	O ten	D Hosts	C internati	0 Hosta
Network ~					
titer onen					
titer onen					
tika dan					

#### 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.

s	Firewall				awplus	Up time: 0 days 03.42	🛓 Admin 🔒 San	
	Entity Management							
	3 Zones   3 Networks   2 Hosts						+ ten tord	
	HOSTS	∕ elt	e) private	✓ eit	9 public		✓ edt	
	ftp IP: 172.16.0.2		1 Network	+ new network	1 Network		+ new network	
	web- server IP: 172.16.0.10		O lan	0 Hosts	internet		0 Hosts	

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

Allied Telesis	Firewall	avplus	Up time: If days US-62	🛓 Admin	Bire
Dashboard     Security ~	Entity Management				
Entition Applications Firmul	3 Zones   3 Helevolta   2 Hores				expend of a
NAT Traffic Control	💿 dez - 13steat		× +10	+ text advant	
Intrusion Prevention	O servers 2 Hosts		2		•
Caston URL Filtering	IP: 172.16.0.0/24 Interface: eth1				
Licensed Practices	NOSTS			≠ elt	^
O System ~	Pp IP 1721602				
					_
	private     1 National		Zell	+ investments	•
	O lan O Huntz		20	a na ha	•
	IP: 192.168.1.0/24 Interface: vlan1				
	MOSTS			<b>≠</b> eff	^
	puble I Network		2.00	+ see labor	

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) 5.4.6 11/10/16 03:51:21
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
Ĩ
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 Eth2
I
awplus#
awplus#show entity
Zone:
              dmz
Zone: um_
Network: dmz.servers
Subnet: 172.16.0.0/24 via Eth1
   Host: dmz.servers.ftp
Address: 172.16.0.2
 Host:
 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
0.0.0.0/0 via Eth2
  Subnet:
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.

									7
Allied Telesis	Firewall				amplus	Up time: 0 days 0103	1 Admin	B Save	
Deshboard	Electrical II.								
a Security -	Firewall							-	
Entline						10			
Applications Freesal	Firmed Dates								
NANT	TRANSFORMER .					Titur			
Traffic Gentral	Action	Application	Fram	Ta	Errora				
Intrusion Prevention									
E Licensed Features ~									
Network -									
¢ System									

- 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.

New Firewall Rule		×
Action	Permit	~
Application	ping	
From	public	~
То	private	~

Note: To select an application, simply start typing in the application field. Available options will be filtered down until you select the desired one.

As well as using the built-in list of applications, you can also create your own custom applications on the **Applications** page, under the **Security** menu.

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

Allied Telesis	Firewall				amplue Up 5	ener D dages 102/01 🕹 Aufreim 🔒 Save
Dashboard						
Security 2.4	Firewall					OFF 🖝
Eritlee Applications	1 Rule					
Frend	Fernal Rules					the .
NAT Traffic Control	Action	Application	Trom	To	Errors	
Intrusion Presention	Fernit	ping	Opublic	Oprivate		≠ all X Done 1

#### Create further new firewall rules with these details:

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 these firewall rules displayed:

Allied Telesis	Firewall				awpłus	Up time: 0 days 00:00	🛓 Admin	B Save
Dashboard								
B Security A	Firewall						OFF	<del>0</del> -
Entities	10 Rules					1		+ new talk
Applications Firewall	Firewall Rules					The		
NAT Traffic Control	Action	Application	From	To	Errora			
Intrusion Prevention	Permit	ping	O public	Oprivate			/ ell X De	1
🖨 Licensed Features 🛛 😒	Pent	ang.	O public	Odma			/ est X de	1
• Network	Parnt	ping	Pphysite	Odra			/ +dt X Dr	1 (100
O System	Pernit	ping	Odna	Oprivate			/ ell X De	. [100
	Pernt:	hp	Public	Odrog / servers / hp			/ ell X Or	1
	Pernt	hetp.	Opublic	Oding / servers / web server			/ elt × De	1
	Pernt	any.	Ophysia	Oprivate			/ est X.De	ine 1
	Parriet	any	Odma	O druz.			/ edit X De	
	Pernit	any	O provata	Opublic			/ edi X De	1
	Pernt	any	O dena	Opublic			Feat X De	. 1999

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

Allied Telesis	Firewall				avplus Up	Some: Dulaye 00.01 1 Admin 1 Sav
Deshboard						
a Security ~	Firewall					ON
Entries	10 Rules					agenthease 4 and 1.0
Applications	Firewall Rules					The .
NAT Traffic Control	Action	Application	From	To	Errons	
Intrusion Prevention	Perrat.	ping	Oputitie	Oprivata		🖌 att 🗙 Dente 📲
Doensed Peatures	Pernit	ping	Opublic	O drue		≠ stil X Datale
🖨 Network 🚽	Permit	prog	Oprivate	Qdna		≠ ett. X.leins 1
<ul> <li>System</li> </ul>	Permit:	ping	Quint	O privata		≠ efs X Dense
	Permit	tu.	Opublic	Odraz / servers		≠ ont X Dente
	Pernit	hete	Opublic	Odmz / servers		≠ selt × Delate
	Permit	ary	Oprivate	Optionte		≠ sitt X Delate I
	Permit	ey.	O <sub>dm2</sub>	Odma		× an X lease 1
	Parmit .	any	Opercente	Opublic		≠ sett X Dente
	Parrut	#79	O drat	Opublic		≠ sett X faister [

#### 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.

	Allied Telesis	Firewall				
	Dashboard Security ^	Firewall				
	Entities Applications Firewall	12 Rules				
	Firewall NAT Traffic Control	Firewall Rules Action	Application	From	То	Errors
	Intrusion Prevention Custom URL Filtering	Permit	http youtube	e public	tervers / web-se	rver
•	Network ~ System	Permit	any	Add above Add below ste	• private	
		Permit	any	Copy Paste	e dmz	
		Permit	ping	<b>Public</b>	<ol> <li>private</li> </ol>	

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**.

* = Ru	le is not	valid -	see "show firewall	rule config-check"]	
ID	Action	Арр	From	То	Hits
* 10	permit	ping	public	private	0
			public	dmz	0
	permit		private	dmz	0
* 40	permit		dmz	private	0
* 50	permit		public	dmz.servers.ftp	0
* 60	permit		public	dmz.servers.web-	server
	10				0
* 70	permit	anv	private	private	0
* 80	permit		dmz	dmz	0
	permit		private	public	0
* 100	permit		dmz	public	0
rule 2 rule 3 rule 4 rule 5 rule 6 rule 7 rule 8 rule 9	10 permit 20 permit 30 permit 40 permit 50 permit 50 permit 30 permit 30 permit	ping from ping from ping from ftp from http from any from any from any from	private to private dmz to dmz log private to public	g g ers.ftp log vers.web-server log log log	
! awplus# awplus# Firewal	•	wall ion is di	n dmz to public log isabled		

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.

Allied Telesis	Firewall				avabian	Up time: 3 days 02:00	🛓 Admin	C Save
Dashboard								
Becurity	NAT						OFF	•
Entition								
Applications	-							
Firewall	NAT Bules					Fiber		
NAT Traffic Control	Action	Application	From	Les	9.).			
Intrasion Prevention								
Unersed Perform								
Network -								
Interface Management								
VLAN								
DHCP Server								
Toole								
CH B								
System								

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

- 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
- 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:

New NAT Rule		×
Action	Masquerade	~
Application	any	
From	private	~
То	public	~
	cancel	/e

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:

Allied Telesis	Firewall					avplus	Up time; 0 days 05:50	1 Admin	B Save
Duebboard     Security	NAT							<b>OF</b>	0
Entres Applications	4 Rules							weet lite een	+ nee sale
Firewall	NAT Rules						The		
Traffic Cortrol	Action	Application	From	To	with	Errors			
Intrivion Prevention	Masquerade	any	Ogrivate	Opublic				× sit X	Delete 1
Network	Masquerade	ary.	Odra	Opublic				/ elt X	Deinte 1
<ul> <li>System</li> </ul>	Port Forward	fupetid	Opdate		O daru / servers / hp			/ =11 X	Delete 1
	Port Forward	http	Opublic		Octraz / servers / web-server			× edit X	Delote ]

To use the CLI window to see these new NAT rules, use the command show nat rule.

	#show nat ru			
T = K	Action	alid - see "show nat r  From	1	Hits
ID	App	То	With dport	nits
10	masq	private	-	0
	any	public	976	
20	masq	dmz	0=0	0
	any	public	1 <u>1</u> 1	
30	portfwd	public	dmz.servers.web-server	0
	ftp	-	-	
40	portfwd	public	dmz.servers.web-server	0
	http	•		

#### 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. The Save button will be orange anytime there is unsaved configuration.

awplus Up time: 0 days 00:32 🚨 Admin	in 🔒 Save
--------------------------------------	-----------

### Part 2: Configure the router for Update Manager

#### Updating the GUI

As new versions of the Device GUI become available with additional functionality, they will be 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:

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.

The retrieval of a new Device GUI file using Update Manager involves sessions that are initiated from the firewall unit itself. This means that firewall rules are required that permit these sessions. So, a zone needs to be created that represents the firewall itself, and the public interface of the firewall has to exist as a host within this zone.

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, Eth2
- Host name = External\_Int
- Host IP address = 192.168.52.20

The updated Entity Management page will look like this:

Allied Telesis	Firewall				anplus	Up time 3 days 30-02	🛓 Admin	8
<ul> <li>Dathboard</li> <li>Security ~</li> </ul>	Entity Management							D.
Entities Applications	4 Zones   4 Networks   3 Heats							
Firmed NAT	← ● HOSTS     ftp = #9:172.15.0.2	and the other designs of the local division of the local divisiono	private     Thetesete	2.00	public     Network			-
Traffic Control Intrusion Prevention Doctory URL Fibering	Np IP: 172.16.0.3 web- server IP: 172.16.0.10		O lan	0 Hosts	Antariset		0 Hosts	-
Licensed Peakies	Router     Network							
betrock -	• external	1Host.						

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

Allied Telesis	Firewall	awplus	Up time: 0 days 03:42	1 Admin	🗃 Save
<ul> <li>Dashboard</li> <li>Security ^</li> </ul>	Entity Management				
Entities Applications Firewall	4Zones   4Networks   3Hosts				expand all $\wedge$
NAT Traffic Control	😧 ánz 🛛 Network		≠ edit	+ new network	• ·
Intrusion Prevention Custom URI, Filtering	🔮 privite - 1. Network		✓ edt	+ new related	•
E Licensed Features	Duble Hetwork		∕ edt	+ new network	× .
Network ~	Boday 1 Natwork		≠ edt	+ new network	^
💠 System 🗸 🗸	external 1 Host		1	62 + new hoel	•
	IP: 192.168.32.0/24 Interface: e82				
	O HOSTS			≠ edit	^
	edemaLint IP: 192.166.52.20				

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

The Update Manager uses HTTPS for secure connectivity, so we'll create a firewall rule with the following details to allow HTTPS traffic out to the update server.

New Firewall Rule		×
Action	Permit	~
Application	https	
From	Router / External / External_Int	Y
tion Permit plication https	~	

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

New Firewall Rule		×
Action	Permit	~
Application	dns	
From	Router / External / External_Int	~
Action Permit Application dns From Router / External / External_Int	~	
	cancel	ve

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	<sup>2</sup> 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.

awplus	<b>Up time:</b> 0 days 00:32	💄 Admin	🗟 Save

### 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.

Allied Telesis	Firewall	awplus	Up time: 1 may 12.48	1 4	fesin	B Save
Dashboard						
Security of	Intrusion Prevention				ON	•
Entities Applications	The Intrusion Prevention System (PE) monitors traffic as the first here of defense, and identifies asspectave or malicious buffic in real-time, by conversing threat agreest an PE aspectave distalance traffic (HTTP); or wald buffic (SMTP). For any threat that is detected in each of these categories, the engine can be set to log the threat (bit default action), sprove, or block-drop the matching para	Threats are kets.	grouped into categories, fo	example	suspicio	nae werb
Finwall	Instruction Provention System Calegory					
Traffic Control	Category		Action			
Statusion Prevention	absats events		Trip.	Block.	liptore	
Doensed Features	iong-decoder-eventa		Tog	Block	ignore	
Noberk	hy-louine		Log	Black	lgtore	
System	ge-decader-overta		tog	Block	lgnore	
	ppp-decoder-events		tog	Block.	lgnore	
	tp-decoder events		1.00	Block	Ignore	
	Mpevents		3.mg	Block	liptore	
	udp decoder events		it.eg	Block	lgnore	
	thedisan		tog	Block	lgtore	
	unda everta			Block.	lations.	

#### 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**.

AM Allied Telesis	Firewall	amphas Up time: 0 days 02.40	1	dmin	B Save
Dashboard					-
Security ~	Intrusion Prevention			ON	•
Entries Applications	The Intrustion Prevention System (IPO) montres traffic as the first line of defense, and silentifies suspicious or malicious traffic in real-time, by companing threats against an IPO signature database. Itselfic (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 (the databat sector), grow, or block-drog the matching pack	hveats are grouped into categories, etc.	for example	suspicio	ut web
Firewall NAT	Intrusion Prevention System Category				
Traffic Control	Category	Actor			
Intrusion Prevention	abrast-events	Log	Block	ignore	
Ucensed Features	komp-decoder-events	1.03	Block	lgiore	
🕽 Network. 🧹	fip bource .	tig	Block	lgsore	
🗘 System	gre-decoder-events	Lig	Block	lgtore	
	ppp-diccoder events	Log	Block	Ignore	
	tp-decoder-events	Log	Block	lgtore	
	http-events	leg	Block	lgson	
	utp-decoder-eventa	tog	Block	liptore	
	checksum	Log	Block	lgtore	
	antip events	Log	Book	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.

Allied Telesis	Firewall		amplas	Up time: 0 days 00.02	🛓 Admin	Bien
Dashboard     Security -	Custom URL Filter	ng			OFF	•
Entrus Applications Firmus	Kaspersky URL filtering	is can specify a user-defined list of websites to allow (wheshe) and/or block (blackles). You can also tellen, user-defined backless, Kaspenity Mackles. Pattern checking stops as soon as the first match		he UNL filtering license insta	Red. Click here t	o enable
NAT Traffic Control	Whitefait URLa					
Intrusion Prevention	File Narw	Entry Count			•	nesi lat
Custom URL Filtering		0 of 1,000 URLs used				
Licensed Peatures	Backlet URLs					
Network	File Norte	Entry Count			+	raine fait
C System		0 of 1,000 URLs used				

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 green **+New list** button to add a new whitelist or blacklist. The custom URL list must be a text file (.txt). Any .txt files in Flash, USB, or SD card are shown and able to be selected and saved for use by the custom URL Filtering feature. See the URL Filtering Feature Overview Guide for more information about creating user-defined URL Filtering lists.

Add New List	×
Select Whitelist File MyList.txt	
flash:/BadList.txt	
flash:/MyList.txt	
flash:/MyList2.txt	
usb:/Blacklist_1.txt	
usb:/Whitelist_corporate.txt	
usb:/Whitelist_extra.txt	
cancel	save

Any whitelists and blacklists that have been selected are now shown on the page, with the entry count showing the number of URLs used:

@ #	Dashboard Security	^	Custom URL Filtering	
	Entities Applications Firewall NAT		Kaspersky URL filtering.	ify a user-defined list of websites to allow (whitelist) and/or block (blar r-defined backlists, Kaspersky blacklist. Pattern checking stops as soc
	Traffic Control Intrusion Prevention Custom URL Filtering		Whitelist URLs File Name MyList.txt	Entry Count 29
6	Licensed Features	~	MyList2.txt	37
0	Network	~		66 of 1,000 URLs used
٠	System		Blackhot URL a File Name BadList tot	Entry Count 48 48 of 1,000 URLs used

#### Step 2. Enable URL Filtering

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

Allied Telesis	Firewall		awplus	Up time: 0 days 00:22	🛓 Admin	E Lore
Desbloard Security -	Custom URL Filte	ring			OFF.	•
Entities Applications Forwall	Kaspersky URL filtering	. You care specify a user-defined list of websites to allow (abitelist) and/or block (blockled). You care adultates, user-defined Sachlets, Ragarsky Mackled, Patters shocking stops are soon as the first r		er URL filtering Scenae insta	Red. Citch have to	enable
NAT Traffic Control	Whitefast URLs					
Intrusion Prevention	Fde Name	Entry Count			(4)	en let

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.

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

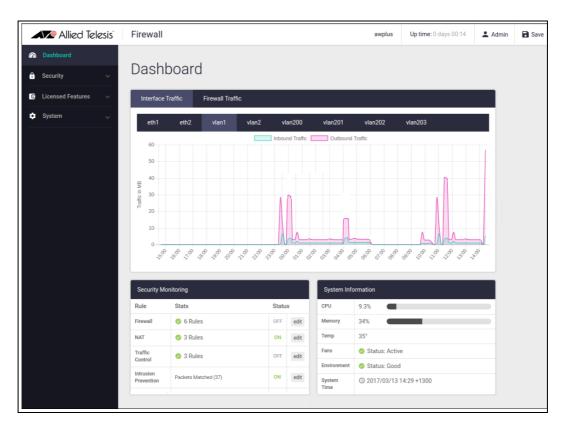
01 0	<b>•</b>		
Step 3.	Save	configuration	changes

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

awplus	Up time: 0 days 00:32	💄 Admin	🗟 Save

## The Dashboard

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



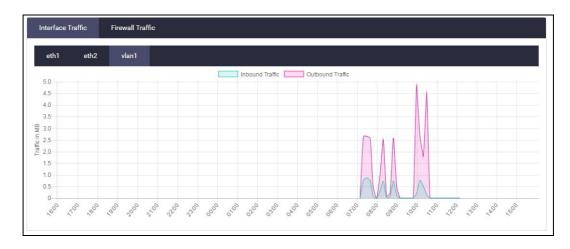
Currently there is a **System Information** widget that displays details about the firewalls status. The **Traffic** widget show traffic through the firewall, or per interface. The **Security Monitoring** widget shows the various traffic rules and security features.

System Information

**m** Shows CPU and memory use, as well as device health.

System Information					
CPU	3.8%				
Memory	65%				
Temp	30°				
Fans	🤣 Status: Active				
Environment	🥏 Status: Good				
System Time	O Nov 23 21:34:23 2016				

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



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



#### Security Monitoring

y The Security Monitoring widget shows the traffic rules and security features in one handy location.
9 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	🤣 2 Rules	OFF edit				
NAT	🥏 2 Rules	ON edit				
Traffic Control	🤣 2 Rules	ON edit				
Intrusion Prevention	Packets Matched (65)	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 Further system information is available on the About page, under the System menu, such as model,Page serial number, firmware and GUI versions, and so on.

Allied Telesis	Firewall	
Image: Dashboard       Image: Dashboard       Image: Dashboard       Image: Dashboard       Image: Dashboard       Image: Dashboard	About	
Hetwork	System Information	
🔹 System 🔷 🔨		
About	System Information	
	Host Name:	awplus
	Model:	AR2050V
	MAC Address:	00-1a-eb-94-27-a5
	Serial Number:	A05236G154300080
	Environment:	Status: Good
	System Time:	Dec 21 03:27:31 2016
	Firmware Version:	AR2050V-5.4.6_2-latest.rel
	GUI Version:	2.20161220.4
	Bootloader:	5.0.5

## **Other Features**

The Device GUI has a number of other great features. The Network menu includes interface management, VLAN management, tools, and the ability to configure the firewall as a DHCP server for the network. These will not be detailed here, but are easy and intuitive to use.

Let's look at File Management and Logging from the System menu, and the Wireless Management menu.

## File Management

The **File Management** page on the GUI allows users 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.

The page also lets you set the software release and configuration files to be used, and reboot the device, providing easy firmware upgrade.

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

Allied Telesis	AR3050S				emplus Up time. Onlarys 03:17	🛓 Admin 🔒 Tieve
Deshboard	File Management					3 ferrent
a Security ~	i lie Management					
Licensed Features ~	/fs/flash			A Uptood	Set Boot Release File	
Network	Name	Modified	Size (bytes)	Actions	Current: flash/A030505-5.4.8-0.2.rel	D Browne
• 5000 ·	In two	20/04/2018, 10:46:00			Backup: Bash:/ar30505-5.4.7-2.5.rel	D Broote
About: The Management	an ag	14/11/2016, 21 39:01			Set Boot Config File	
License Management	AR30505-5-4.8-0 2.94	20/04/2018, 10:44:13	43742531	<b>&amp;</b> townat X anne	Current: flash/default.clg	D downs
CU B	B Ballath	27/02/2017, 06:55:58	553	<b>O</b> Diverged × genera	Backup: Bash:/default.clg	D Bowte
🕈 Wireless Management 🖂	в мусиси	13/12/2016, 12:07:50	281	<b>&amp;</b> prevent × porter	Flash Usage	
	S MILINEEM	13/12/2016, 12:07:56	41D	<b>O</b> Downard X contra	105	346.1M/3.6G
	app.zp	12/07/2017, 15:39:21	7068944	& boundary × onto		
	ar30505-5.4.7-2.5.rel	06/03/2018, 15:55:10	42175271	<b>O</b> (newspace) × meters		
	ar3050s.bm	14/07/2016, 07:57:14	2439	<b>O</b> Devenued 1 × points		
	📓 amplus gul., 548, 52. tat gz	20/04/2018, 10:40:13	1113330	<b>O</b> Download X strafe		
	i orbatisty	22/03/2018, 09:16:41	3319	<b>O</b> powned X seems		
	Secretion log	17/08/2017, 14:16:59	157	<b>O</b> Download X datales		
pm//182.168.1.1/#/dechtoard		11/10/2016, 12:35:58	1859	Contract X seleter		

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:

File Management	
ifs	
Name	Modified
M flash	Sun Apr 09 17:09:21 2017 UTC
deu 📾	Thu Jan 01 00:00:00 1970 UTC

Allied Telesis	Firewall			
<ul> <li>Dashboard</li> <li>Security ~</li> </ul>	File Management			
Licensed Features	/fa/uob			
System ^	Name	Modified	Size	Ac
About	CV	Fri Oct 28 16:49:52 2016 UTC		
File Management License Management	Study	Fri Mar 17 22:03:02 2017 UTC		
CLI 🛛	System Volume Information	Fri Mar 17 22:02:28 2017 UTC		
	AR2050V-5.4.6-2.3.rel	Thu Dec 22 09:30:04 2016 UTC	40709551	•
	AR3050S-5.4.6-0.3.rel	Fri Aug 05 15:59:40 2016 UTC	42624803	•

The **upload** option allows you to browse and locate the file you wish to add to the firewall. From here it is easy to add more files and change the release and configuration files to be used.

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

AT Allied Telesis	AR3050S						awplus	Op time: 0.44ys 03:17	🛓 Admin 🔒 🖬
Deshboerd	File Management								3 0 minut
Security ~	File Management								
Licensed Pestures ~	ifaifash			1	Ca Liptour	Set Boot	leieuse File		
Network	Name	Modified	Size (bytes)	Actions		Current	flash/AR30505	5.4.9-0.2 <i>m</i> l	2 Direct
Dystem -	Taos	20/04/2018, 10:46:00				Backup	flash/w30505	547-2.5 ml	D Brinte
About The Management	ing ing	14/11/2016, 21:59:01				Set Boot	Config File		
Litense Management	AR30505-5.4.8-0.2.HI	20/04/2018, 10:4413	43742531	O tremat ×	C preter	Current	Rash:/default.cf	0	D trave
cu 8	B BadLister	, 27/02/2017, 06:55:58	553	<b>O</b> (revenue) ×	< orien	Backup	flashc/default.cf	ų	D Broote
Wreless Management	MyLinthi -	13/12/2016, 12:07:50	291	<b>O</b> tremet	Costen	Flash Usa			
	MyList2.bit	13/12/2016, 12:07:56	410	<b>O</b> townat X	comm.	105	~		346.1M / 3.6G
	B 100.00	12/07/2017, 15:39:21	706894	O Doetlaat X	Contre .				
	B #30505-5.4.7-2.5.H	06/03/2016, 15:53:10	42175271	Δ tremat X	< orde				
	adotostes	14/07/2016; 07:57:14	2438	O premiet ×	C contra				
	avplan-gul, 548, 02.1ar.gz	20/04/2018, 10:40:13	1113236	O trent X	< oren				
	B default.cfg	22/03/2018, 09:16:41	3319	O Downad X	C anes				
	scoption.log	17/08/2017, 14:16:59	157	<b>G</b> tremat	< one				
PTR2.158.1.1.4V/dashboard		11/10/2016.12:35:58	1859	O Deermant X					

Tip Currently used and total Flash Usage information is available.

Flash Usage	
10%	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.

Allied Telesis	AR2050V				3	Up time: 0 days 00:20	🛓 Admin	8
a Dashboard								
D Network ~	Logging							
Interface Management	Buffered Permane	wat _					/ Contigors	Logging
DHOP Server VLAN			All Severity			Total Mess	inges 409 📀	
Tools	Date A	Facility ~	Level o	Program 🔿	Messape ~			
a System -	2018-04-23 18:25:14	user.	hotice	ATMP	Last message Incarnation is not p' repeated 9 times, suppressed by systog og on 3			
About	2018-04-23 18:25:14	user	debug	VCS	STK TRACE Stack member-1 changed status from Syrcing to Ready			
File Management	2018-04-23 18:25:16	uter	notice	ATMF	Incarnation is not possible with the data received port1.0.9 (findex 5009)			
License Management	2018-04-23 18:25:45	uter	notice	ATME	Last message 'incarnation is not p' repeated 14 times, suppressed by sysloging on 3			
Libaying	2018-04-23 18:25:45	eyslog	notice	syslog-ng	Syslog connection established, fd=%1, server=XF_INET(10.37.95.65.514), local=XF_INET(0.0.0.00)			
CU B	2018-04-23 18:25:45	eyslog	er	skeyoð-uð	1/0 error occurred while writing, 30×161', error×"Connection refused (146)'			
	2018-04-23 18:25:45	nyslog	notice	eyslog-ng	Syslog connection broker; fd='61', server='AF_INET(10.37.95.65.514)', time_teopen='60'			
	2018-04-23 18:25:46	user	notice	ATMP	Incarnation is hot possible with the data received port1.0.9 ((findex 5009)			
	2018-04-23 18:25:45	user	notice	ATME	Last message 'incarnation is not p' repeated 29 times, suppressed by sysloging on 3			
	2018-04-23 18:26:45	syslog	notice	syslog og	Syslog connection established, M='29', server='AF_JNET(10.37.95.65.514)', local='AF_JNET(0.0.0.02)'			
	2018-04-23 18:26:45	syslog	etr	syslog-ng	(/O error occurred while writing; 10+29, enor+Connection refused (146)/			
	2018-04-23 18:25:45	syslog	notice	syslog-ng	Syslog connection broker; 50=29', server-'AF_INET(10.37.95.65:514)', time_reopen='60'			
	2018-04-23 18:26:46	user	notice	ATM/	Incaination is not possible with the data received port1.0.9 (ifedex 5009)			
	2018-04-23 18:27:41	user	notice	ATMF	Last message 'incarnation is not p' repeated 37 times, suppressed by sysloging on 3			
	2018-04-23 18:27:41	authority	warning	bries	pam,Jastlog(remote-login.session): file /var/log/tastlog created			
	2018-04-23 18:27.42	user	notice	ATMF	Incarnation is not possible with the data received port1.0.9 (dividex 5009)			
	2018-04-23 18:27:45	user.	notice	ATMF	Last message 'moarnation is not p' repeated 1 times, suppressed by sysloging on 3			

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

Filter logs by:

1. any information column in ascending or descending order

	All Severity	Ŧ	
Facility ^	Level ^	Program A	Message ^
localó	crit	ATMF	AR4050 has left. 4 members in total.
localó	crit	ATMF	AR4050 has joined. 5 members in total.
local6	crit	ATME	AR4050 has joined. 5 members in total.
local6	crit	ATME	AR4050 has left. 4 members in total.
local6	crit	ATMF	AR4050 has joined. 5 members in total.
local6	crit	ATMF	AR4050 has left. 4 members in total.
local6	crit	ATMF	AR4050 has joined. 5 members in total.
	Facility ^ local6 local6 local6 local6 local6 local6	localó crit localó crit localó crit localó crit localó crit localó crit	Facility         Level         Program           local6         crit         ATMF           local6         crit         ATMF

Buffered Permane	nt			
		Critical	•	
Date ~	Facility ^	All Severity Emergency Alert		Message ^
2018-04-23 18:33:58	local6	Critical Error		AR4050 has left. 4 members in total.
2018-04-23 18:34:14	local6	Warning Notice		AR4050 has joined. 5 members in total
2018-04-23 18:36:38	local6	Info Debug		AR4050 has left. 4 members in total.
2018-04-23 18:36:47	local6	crit	ATME	AR4050 has joined. 5 members in total

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

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

Logging				
Buffered Permane	nt			
received		All Severity	٣	
Date ^	Facility ^	Level 🛩	Program A	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	ATME	Incarnation is not possible with the data received port1.0.

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 switch and also set up a Syslog server(s) for remote log storage.

Logging					
Buffered Permane	nt				Configure Logging
		Critical	•		Total Messages 11 🧔 Retries
Date 🛩	Facility 🔿	Level ~	Program 🔺	Message A	
2018-04-23 18:33:58	local6	crit.	ATME	AR4050 has left, 4 members in total.	
2018-04-23 18:34:14	local6	crit	ATME	AR4050 has joined. 5 members in total.	
2018-04-23 18:36:38	localó	crit	ATME	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.

Logging Configuration						
Local Rem	note			VewLogs		
Buffered				✓ CearLogs		
Level	Facility	Program	Message	+ new filter		
Notice	cron	all	•	g soute		
Alert	daemon	imi	•	g costs		
Notice	authpriv	dhcpsn		I costs		
Debug	all	all	•	g coste		
Permanent				✓ Chertopi		
Level	Facility	Program	Message	+ new filter		
Debug	all	all	•	S deste		
Warning	all	all	•	g costs		

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 switch. 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 creating 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 enables log storage on the device to be configured exactly as desired.

Add Filter F	For Buffered Log		×
Level		Critical	~
Facility		daemon	
Program	Enter program here	all	
Message *			
		Included Exclu	uded
			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.

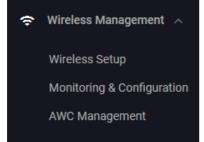
Logging	Configura	tion		
Local Remo	te			View Logs
				+ New Hod
10.37.95.65				Delete Hosts
Level	Facility	Program	Message	+ new filter
Emergency	all	all	•	E caleta
Notice	all	all	•	E sere

### Wireless management

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:



Form more information about AWC and how to configure it, see AWC Wireless Control on AR-Series Devices Feature Overview and Configuration Guide.

C613-22094-00 REV G

#### 🔨 🖉 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

© 2018 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.