01001011001 01001011001 01001011001

Technical Guide

000101101

Getting Started with the Device GUI on UTM Firewalls

Feature Overview and Configuration Guide

Introduction

Allied Telesis Unified Threat Management (UTM) Firewalls are the ideal integrated security platform for modern businesses. Powerful firewall and threat protection is combined with routing and switching, to provide an innovative high performance solution.

Allied Telesis

Our UTM Firewalls have an integrated architecture built on the AlliedWare Plus[™] OS, bringing its verified and superior operation to the security needs of today's networks. As well as Allied Telesis' advanced feature set, and powerful VPN connectivity options for remote network access, the firewalls utilize best of breed security providers, for up-to-the-minute protection from all known threats.

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 UTM Firewall using the Device GUI.

The Device GUI provides setup of the firewall, enabling the configuration of entities (zones, networks and hosts) and then creating firewall, NAT and traffic-control rules for managing traffic between these entities. Advanced firewall features such as Application control and Web control, as well as threat management features such as Intrusion Prevention, Malware protection, and Antivirus, can be enabled, configured and customized for a comprehensive security solution.

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 manage which security features are enabled, as well as providing statistics. The top 10 applications, and top 10 categories widgets show what is using the most firewall bandwidth, with rules able to be configured in response to this monitoring.

The complete AlliedWare Plus feature-set can be configured using the Device GUIs built-in industry standard Command Line Interface (CLI) window.

Allied Ware Plus' operating system

Contents

Introduction1
What information will you find in this document?1
Products and software version that apply to this guide3
Related documents3
What is a Firewall?
What are Entities? 4
Zones, networks, and hosts5
Using Rules 6
Configuring the Firewall7
Part 1: Configure a standard 3-zone network7
Part 2: Configure the firewall for Update Manager21
Part 3: Configure free security features
Part 4: Configure licensed firewall security features
Part 5: Configure licensed Advanced Threat Protection (ATP) security features 36
The Dashboard
Other Features
File Management
License management 47
Logging management 49
Wireless management

Products and software version that apply to this guide

This guide applies to all AR-Series UTM Firewalls running version **5.4.7-x.x** or **5.4.8-x.x**. Supported models include the AR3050S and AR4050S.

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:

- Application Control
- Web Control
- URL Filtering
- Intrusion Prevention System
- IP Reputation
- Malware Protection
- Antivirus

To configure an Allied Telesis VPN Router or Switch using the Device GUI see the following guides:

- Getting Started with the Device GUI for VPN Routers Guide
- 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?

A 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). Previous generations of firewalls were port-based or used packet filtering. These traditional firewalls determined whether traffic is allowed or disallowed based on characteristics of the packets, including their destination and source IP addresses and TCP/ UDP port numbers. However, traditional firewalls have failed to keep pace with the increased use of modern applications, and network security threats.

Allied Telesis firewalls use a **Deep Packet Inspection** (DPI) engine that provides real-time, Layer 7 classification of network traffic. Rather than being limited to filtering packets based on protocols and ports, the firewall can determine the **application** associated with the packet, for example social networking, instant messaging, file sharing, or streaming. This allows Enterprises to accurately differentiate business-critical from non-critical applications, and enforce security and acceptable-use policies for applications in ways that make sense for the business.

This comprehensive application, content, and user identification provides full visibility into network activity, to allow intelligent control of network traffic. Visibility and control, partnered with advanced threat protection, together provide comprehensive online security.

What are Entities?

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

When the firewall 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 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 Firewall

This section comprises five 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 firewalls components, see page 21
- 3. Free security features IPS, and Custom URL Filtering, see page 24
- 4. Advanced firewall features App Control, Web control, and URL Filtering, see page 29
- Advanced threat protection features IP Reputation, Malware Protection, and Antivirus, see page 36



Part 1: Configure a standard 3-zone network

Step 1. Configure firewall interfaces.

Note: If your firewall is new and unused, it will already have the GUI installed from the factory, and the IP address 192.168.1.1 on VLAN1, and the HTTP service enabled. Connect to any switch port 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 Device 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 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 firewall will serve the Device GUI pages:

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

```
Step 3. Login to the firewall GUI.
```

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

Note: The Device GUI currently supports the Firefox[™], Chrome[™], Microsoft Edge[™], Internet Explorer 11[™], and Apple Safari[™] web browsers.

The following login page is displayed:

Allied Telesis Next-Generat × +	and the second second						x
https://192.168.1.1/public/login.html	⊤ C Q Search	☆ 自	D	÷	A	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 firewall. 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**, and the **Security**, **Licensed Features**, **Network**, **System**, **and AWC Wireless Management** menus for configuration.



Step 4. Configure Entities.

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

Select Entities under 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.

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	delete
+ new subnet		
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.

2 dmz	🖌 edit
1 Network	+ new network
N servers	0 Hosts
▲ (N) servers	🖍 edit
0 Hosts	+ new host
IP: 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	
IP 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

	(1) HOSTS	🖍 edit
web- serve	IP: 172.16.0.10/24	
ftp	IP: 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

 Parked
 Beddy
 Freval
 Beddy
 Ettity Management

 Parked
 Beddy
 Image
 Image
 Image

 Parked
 Image
 Image
 Image
 Image

 Image
 Image
 Image
 Image
 Image

 Image

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

Entity list view

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

Firewall				awplus	Up time: 0 days 03:42	🛓 Admin	B San
Entity Management						:	
IZones 3 Networks 2 Hosts						++	en 1070.
(🕘 HOSTS	∕ edt	9 private	✓ edt.	2 public		P	P +61
ftp IP: 172.16.0.2		1 Network	+ new network	1 Network		+ new ne	deals
web- IP: 172.16.0.10		() 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		anglas	Up time: 2-54ys 13-62	± Admin	Blase
Deshboard Security	Entity Mar	agement			E	
Entition Applications Freewall	3 Zones 3 Networks	2 Made				ere turne
NAT Traffic Control	3 dmg - 1 Network			/ =1	a sea setas	
Intrusion Prevention Contorn URL Fibering	P 172.16.0.0/24	Interface. eth1		×1	er en ho	•
E Licensed Features v	HOSTS				≠ att	^
🗘 System 🖂	fg websener	IP: 172.16.0.2				
	• private - 1 factors			Velt	a text tables	•
	O lan O Hosts			7		•
	P 192.168.1.0/24	inerface, vlavl			≠ all	
	3 public Thetwo			7 -8	A tex set-of	

If you'd like to view these changes as added to the firewall 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 P	lus (TM) 5.4.6 11/10/16 03:51:21
awplus≻ena awplus#show zone dmz network ser ip subnet host ftp ip addres host web-s	running-config entity vers 172.16.0.0/24 interface Eth1 s 172.16.0.2 erver - 172.16.0.10
ip addres	\$ 172.16.0.10
1	
zone private	
ip subnet	192.168.1.0/24 interface VLAN1
zone public	
network Int	ernet
ip subnet	0.0.0.0/0 interface Eth2
1	
awplus#	
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 Eth2
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 firewalls 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.

Allied Telesis	Firewall				amplus	Up time: 0 days 00.01	🛓 Admin	B Sere
Dashboard Security	Firewall						OFF	e
Critics						5	orthane 🛛	-
Freedo	Firewall Pulses					Film		
Traffic Control	Action	Application	Fram	5	Errors			
Licensed Features								
• Neberk ~								
 Bystem 								

- 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	~
	cancel	ave

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

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

Allied Telesis	Firewall				aveplus	Up time: 0 days 00.01	1 Admin	B Save -
Dashbaard	Firewall						OFF	
Entities Applications	1 Rule						-	
Treval	Firewall Rules					Film		
NAT Traffic Control	Action	Application	Fram	Tu	Errors			
Intrusion Prevention	Parent	parg	Opublic	Ogevente			ent Xb	ne 1
Dicensed Features								
🔹 Network 👘 🐳								
• System								

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				auplus	Up time: II days 00:00	Idmin 🗑	Bave Save
Dashboard								
E Security A	Firewall						OLL .	
Entities Applications	10 Rules					and the second sec		- 14
Firmal	Firewall Rules					. Film		
NAT Traffic Control	Action	Application	From	To	Errors			
Intrusion Prevention	Print.	ping	Opublic	Oprivate		1 +01)C Deista	1
G Licensed Features	Fernit.	ping	Opublic	O _{dme}		× 100	X Debte	11
D Network	Perrot	ping	Oprivate	Odenz		× 100	X Debts	11
3 System	Pernt.	ping	Odma	• private		2 mil	× Detete	11
	Farrit	tp .	Opuble	Odrag / servers / fgs		/ eds	X Deute	11
	Farrat	http	Opublic	Odrog / servers / web-server		/ 101	× Dente	1
	Permit	any	Oprivate	Oprivatia		/ all	X Deinte	11
	Farmit	any	Odre	Oding		/ edi	X Delate	1
	Peret	any	Oprivate	Oputhic		× +01	X Deate	11
	Perrit	any	O dena	Opublic		1 +00	3C Delate	i.

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				avplue	Up time: 0 days 00.01	1 Admin	Bilav
Dashboard Security	Firewall						ON	
Entities Applications	10 Rules						anthana 💽	t sale tub
Freedal	Firewall Rules					Film.		
Traffic Control	Action	Application	From	To	Errora			
Intrasian Prevention	Perrat	ping	Opublic	Oprivata			≠ att X De	ini 1
Licensed Peatures	Permit.	ping	O _{public}	Odne			/ +01 X Del	ini 1
Network 🗠	Permit	prog	Oproate	Odna			≠ +01 × 04	ane) 1
System	Permit	prog.	O deta	Oprivata			≠ ett X De	-
	Permit	ftpi	Opublic	O _{dm2 / servers}			r ent X De	-
	Pernat	keta	Opublic	O druz / servers			/ with [X Dec	in i
	Perret	arty.	Ogervate	Optimite			z ein X be	nne i
	Permit	897	• deaz	O drue			z en X be	ani) 1
	Parmit .	any	Ogwivate	Opublic			≠ eft X De	ini) i
	Parriet	100 C	O	Onder			Arrest Market	

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					
A	Dashboard	F :					
ô	Security ^	Firewall					
	Entities Applications	12 Rules					
	Firewall	Firewall Rules					
	NAT Traffic Control	Action	Application	From	n	То	Errors
	Intrusion Prevention	Permit	http	3 pu	blic	dmz / servers / web-server	
G	Licensed Features	Permit	youtube	Add above	ic	9 private	
•	Network v	Permit	any	Add below	ate	9 private	
٠	System	Permit	any	Сору	0	3 dmz	
		Permit	any	Paste	ate	³ public	
		Permit	ping	⊘ pu	blic	Oprivate 0	

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**.

* = RL	le is not	valid -	see "show firewall	rule config-check"]	
ID	Action	Арр	From	То	Hits
* 10	permit	ping	public	private	0
* 20	permit	ping	public	dmz	0
* 30	permit	ping	private	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	0
* 80	permit	any	dmz	dmz	0
* 90	permit	any	private	public	0
* 100	permit	any	dmz	public	0
rule 1 rule 2 rule 3 rule 4 rule 5 rule 6 rule 7 rule 8 rule 8	0 permit 0 permit 10 permit 10 permit 10 permit 10 permit 10 permit 10 permit 10 permit	ping from ping from ping from ftp from http from any from any from any from	public to private public to dmz log private to dmz log dmz to private lo public to dmz.serv private to private dmz to dmz log private to public	log g gers.ftp log vers.web-server log log log	
rule 1 ! awplus# awplus#	.00 permit # #show fire	any from wall	ı dmz to public log sabled		

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				awphus	Up time: 0 days 00:00	🛓 Admin	B Save
Dashboard Security -	NAT						OFF	0-
Entities Applications								t new rafe
Finnerall NAT	NAT Bules	Application	From		Errors	The		
Traffic Control								
Literard Features								
Interface Management								
VLAN DHCP Server								
CLJ (8								
O 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	ve

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					soplas	Up time: 0 days (05.50	🛓 Admin	B Save
Dashboard Security ~	NAT							OFF	-
Entritions Applications	4 Rules							erthered C	and the
Frend	NAT Rules						The		
NAT Turffic Control	Action	Application	From	Te	With	Emin			
Intrusion Prevention	Masquerade	ary	Opticate	Ppulle				≠ adt × De	1 100
Unersed Features ~	Masquerade	ary	Odne	Opublic				/ +01 X De	1 144
Application Control Web Control	Port Forward	fiquetel	Opublic		O danie / servers / hp			/ =01 X De	1 10
IP Reputation	Part Forward	http	Opublic		odiviz / servers / web-server			≠ edt × De	1
Antheiran									
O Nelseyk									
• System									

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

awplus awplus [* = R	≻ena #show nat ru ule is not v	le alid - see "show nat rul	e config-check"]	
ID	Action App	From To	With (dst/src) Entity With dport	Hits
* 10	masq	private	-	0
* 20	any masq	dmz		0
* 30	portfwd	public	- dmz.servers.web-server	0
* 10	portfwd	public	dmz.servers.web-server	0

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 🔂 Sar	awplus Up time: 0 days 00	:32 💄	Admin	🔒 Save
--	---------------------------	-------	-------	--------

Part 2: Configure the firewall for Update Manager

Modern security devices require regular updates to keep rule-sets and threat signature databases up to date, ensuring effective protection for business networks. Features such as IP Reputation, Malware Protection, and Antivirus (which we'll configure in parts 5 and 6), monitor network traffic and detect malicious activity in real-time by comparing the threats' characteristics and patterns against known lists and databases.

The leading security providers employed by the firewall, such as **Kaspersky** and **Emerging Threats**, keep their databases regularly updated with the very latest **threat signatures**, so security scanning of firewall traffic catches the latest malicious threats. The firewall utilizes **Update Manager** to contact the Allied Telesis update server and download the latest components at pre-defined intervals, or at specific user request.

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 files 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 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						emplue	Up time 2 days \$3.42	± Admin	Blace
 Deshboard Becurity - 	Entity Management								E	
Entries Applications	4 Zonee A Networks 3 Hosts									-
Formall NAS	O HOSTS B: 17218.02	V #8	private 1 Notwork	2	-	g public Unitstoch				e add
Traffic Control Intrusion Prevention Coaton URL Fibering	web- server IP: 17216.510		0 -	6 Hosta	•	O internet			2 Hoets	•
Licensed Features	Router INstructure	Z alt.								
Network ··· System ···	• esternal	3 Host 🕨								

Or in List View (with just the new zone expanded) like this:

Allied Telesis	Firewall	awplus	Up time: 0 days 03:42	🛓 Admin	Save 1
🔊 Dashboard	Entity Management				
Entities Applications Firewall	A Zeres A Networks SHarks			+	expand all A
NAT Traffic Control	😗 des 1 Network		≠ edit	+ new networ	•
Intrusion Prevention Custom URL Filtering	🔮 pehvala – 1 Histoch		✓ edit	t new networ	1 ×
Licensed Features ~	public 1 Nichmark		✓ edit	+ new networ	3 ×
🔹 Network. 🗠	Router 1 Network		≠ edit	+ new networ	•
🗘 System 🗸 🗸	external 1 Host		1 0	St • new her	•
	19: 192.168.52.0/24 Interface: +th2				
	O HOSTS			≠ edit	^
	external_int IP: 192.168.52.20				

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

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
То	public	~

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

Permit	~
dns	
Router / External / External_Int	~
public	~
	Permit dns Router / External_Int public

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

Permit	https	• Router / External / External_Int	Opublic
Permit	dns	Router / External / External_Int	☑ public
Permit	dns	Router / External / External_Int	

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	Up time: 0 days 00:32	💄 Admin	B Save

Updating the GUI

As new versions of the Device GUI become available with additional functionality, they will also 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 firewall, firstly ensure that the firewall can contact the update server using the steps above, and then simply enter the following command from the CLI window:

update webgui now

Part 3: Configure free security features

Allied Telesis firewalls have a number of security features that can be configured to manage application and website usage, as well as provide comprehensive threat protection.

This section will configure the Intrusion Prevention System (IPS) and Custom URL Filtering, which are both free to use on the firewall. Parts 4 and 5 of the guide will configure licensed firewall and threat protection features.

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.

Prevention sten (90) moher halfs as the feat law of defense, a c (2007), For any threat that is detected in each of the an Category	and sheetifies exaptroves of maleston terms of the art to a set to the provide set to the set to th	a buffic in real-time, by comparing diverted to big the thread (the default action), yes	a against au IPS signature distabans. This one, or block - drop the matching packets.	ata ani grouped into catagories, fo Action	r example Block	ON =	- • •
Prevention stee (91) mother build: as the first loss of defense, as (2017). For any thread that is detected in each of thee am Category	and similar exercises of indicates ere categories, the engine can be set to	t haffer in real-time, by comparing the alter to begine these time default action), gins	a against an IPS signature databasis. Thire one, or block - drop the matching packets.	ats are grouped into categories, fo Action	r example Block	ON =	r web
nten (PD) monitors builds as the first loss of defense, as c (DMTP). For any thread that is detected in such of the em Calegory	and identifies exaptions or malicous rese categories, the engine can be set to	a haffe in real-time, by comparing threads	a against an IPS signature detables. This ion, or block - drop the matching packets.	ata are grouped into catagories, fo Action	or example Block	suspicióu Ignore	
um Calegory				Action	Block.	ligitore	
				Action 1/mg	Block	lignore	
				Top	Block.	liptone	
				teg	Block	Ignore	
				Ling	Black	liptone	
				ting	Block	lgnore	
				tog	Block.	lignore	
				Ing	Block	Ignore	
				log.	Block	lgtore	
				Log	Block	Ignore	
				ting	Block	lgnore	
				100	Block	ligtore	
					می ای ای ای ای ای ای ای ای ای ای ای ای ای	ini	Import Import Import Import

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.

Allied Telesis	Firewall	anplus	- Up time: 0 days 02.46	1 Admin	B Save
A Dashboard					
🛔 Security 🗠	Intrusion Prevention			ON	-
Entries Applications	The Intrustee Prevention System (PD) montres traffic as the first lives of defense, and identifies suspicious or malicious traffic in read-time, by comparing threats against an IPS signature data traffic (HTTP), or email traffic (IMTP), for any threat that is detected in each of these categories, the angine can be set to log the threat (the default action), agrees, or block-deep the match	tabase. Threats are ing packata.	i gituped into categories, fo	r example sus	picious web
Firewall NAT	Instruction Prevention System Category				
Traffic Control	Category		Action		
Intrusion Prevention	abrain-events		Log	Block Ign	ure
Licensed Features ~	konp discoder events		Log	Block Ign	pre .
Network ~	Ap-bounce -		Trep	Block Ign	one
System	gre-facoder events		Log	Block Ign	Drw
	ppp-decoder-events		log	Block Ign	pre
	ip-decoder-events		Log	Block Ign	one
	http-peerta		Log	Block Ign	110
	udpidecodinieventa		Log	Block Ign	Drie
	checksum		trig	Block Ign	bre
	antp-owning		Log	Block Ign	pre

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) on the free-to-use Custom URL Filtering page. You can also subscribe to the Kaspersky blacklist service if you have the URL Filtering license installed, which is shown in "Part 4: Configure licensed firewall security features" on page 29.

URLs are matched in this order – user-defined whitelists, user-defined backlists, Kaspersky blacklist. 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		avplus	Up time, 0 days 00.10	1. Admin	8 100
Dashboard	Custom URL Filter	ng			OFF	-
Erettes Applications Firmual	URL Filtering allows or blocks website access. Y Kaspersky URL Ritering. URLs are matched in this order - user defined w	e can specify a user-defined lat of websites to allow (whitelist) and/or block (blacklet). Yo telets, user-defined backlets, Kaspenity blacklet, Patters thecking stops as soon as the	u can also subscribe to the Kaspersky blackflat service if you have t feat match is found, and that action (allow or block) is taken.	he URL filtering license insta	fed. Click here	to enable
NAT Traffic Control	Whitelist URLs					
Intrusion Prevention	File Name	Entry Count			E	tere fait
Custom URL Fillering		© of 1,000 URLs used				
E Usensed Peatures	Blackbat URLa					
• Network ~	File Name	Erity Count			E	Test Int
 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:

a	Dashboard	
ô	Security ^	Custom URL Filtering
	Entities Applications Firewall NAT	URL Filtering allows or blocks website access. You can specify a user-defined list of websites to allow (whitelist) and/or block (bla Kaspersky URL filtering. URLs are matched in this order – user-defined whitelists, user-defined backlists, Kaspersky blacklist. Pattern checking stops as so Whitelist URLs
	Intrusion Prevention	File Name Entry Count
_		MyList.bd 29
	Licensed Features V	MyLiat2.txt 37
0	Network ~	66 of 1,000 URLs used
٠	System	Blackist URLs
		File Name Entry Count
		BadList.txt 48
		48 of 1,000 URLs used

Step 2. Enable URL Filtering

Enable	URL Filterir	ig with the C	N/OFF switcl	h at the top	of the page:

Allied Telesis	Firewall		amplus	Up time: 9 days 00:32	🛓 Admin	B Save
Deshboard						
Security A	Custom URL Filtering				OFF	0
Emilian	UPIL Filtering allows or blocks website access. You can specify a user-defined its Kaspenity URI, filtering.	t of websites to allow (whitehat) and/or block (blackint). You can also subscribe to the Kaspersity blackint service t	you have I	he URL Ethering license instal	led. Click here t	o enable
Frewall	UBLs are matched in this order - user-defined whitekiss, user-defined backlists.	Kaspensity blacklist. Pattern checking stops as soon as the first match is found, and that action (allow or block) is t	Aen.			
NAT Traffic Control	Whitelist URLs					
Intrusion Provention	File Name	Entry Count			+	tes list
Custom URL Filtering		0 of 1,000 LFLs used				

The firewall will now match any website URLs that users try to browse to against the whitelist/s, then the blacklist/s, and then the Kaspersky blacklist (if you are using the Kaspersky licensed URL Filtering). 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.

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	B Save
------------------------------	---------	--------

Part 4: Configure licensed firewall security features

Online business activity is now based around applications that enable people to interact with services such as collaborative document creation, social networking, video conferencing, cloud-based storage, and much more. Organizations need to be able to control the applications that their people use, and how they use them, as well as managing website traffic.

Allied Telesis firewalls are application aware, and so provide the visibility and control necessary to safely navigate the increase in online applications and web traffic that are used for effective business today.

The Advanced Firewall feature license includes **Application Control**, **Web Control** and **URL Filtering**. The Advanced Firewall feature license is available in 1, 3, and 5 year subscriptions. You can view current license status by navigating to the **License** page under the **System** menu.

	Allied Tele	zsis	AR4050S							
<i>a</i>	Dashboard									
e	Security	~	License M	ana	gem	nent				
C	Licensed Features	~								
۲	Network	~	Feature Licenses							
٠	System	^					2018			
	About			Apr	May	Jun	Jul	Aug	Sep	C
	File Management		Base License							
	License Management						Base Licen	se		
	Logging		Advanced Firewall							
	CLI 🗹						Advanced	Firewall		
÷	Wireless Management	t ~								

Application Control

The Deep Packet Inspection (DPI) firewall engine allows fine-grained application control. Reliable identification of the individual applications means that rules can be established to govern application use, and to enforce security and acceptable use policies. For example, Skype chat may be allowed company wide, while Skype video calls can only be made by the sales department.

Step 1. Configure application control.

Navigate to the Application Control configuration page under Security.

Click the ON/OFF switch to enable Application Control, and select the Update interval.

Allied Telesis	Firewall	avplus	Up time: 0 days 00.52	1 Admin	B Save
A Dashboard					
a Security	Application Control			ON	-•
Entries Applications	Orders business activity is now based around applications that enable people to interact with services such as collaborative docume their people use, and how they use them.	rf creation, social networking, video conferencing, and much more. Drganisa	tions need to be able to con	eol (se applica	ions that
Firmal	With the purchase of a subscription learner, the ferevall can utilize the Process Networks application visibility Morary to identify aroun accurate and annexistable understable and annexistable annexistabl	d 1400 individual applications. Firewall and TiteRic Control rules can be estat	blahed to povers application	runii, aeul to ari	loter -
NAT Terffer Control	For more information or to parchase a subscription, contact your local Alled Talesis sales representative. Find your local Alled Tales	in office at www.allectulesis.com/contact			
Intrusion Prevention	Provider: Procera				
	License Duration: N/A				
Upersed Pestures A	Check for updates: 24 hours +				
Application Control					
Web Control					
IP Reputation					
Malware Protection					
Arthreas					
Asterna					
O System					
13275667					

Application Control uses the Procera Networks application visibility library to identify around 1400 individual applications. The firewall will update the library from the Allied Telesis update server (as configured in Part 2) at the specified interval to ensure the latest applications are known.

Custom Applications

Note: As well as the application library from Procera Networks, you can create your own custom application on the Applications page, under the Security menu. You can specify the protocol and source/destination port numbers and so on. Any custom application you create will be available, along with the Procera list, when creating rules to manage traffic.

Step 2. Add rules to manage applications.

You can now create firewall or traffic shaping rules to manage how applications are allowed to be used on the network.

For example, to block the use of Spotify[™] (a music streaming service) company-wide, create a firewall rule denying the Spotify application from the Public (Internet) zone to the Private (LAN) zone.

New Firewall Rule	
Action	Deny
Application	spotify
From	public
То	private
	cancel sav

Step 3. Add rules to manage application bandwidth.

As well as using the Firewall to block undesired traffic, you can also use the **Traffic Control** page to manage the bandwidth that certain applications are able to use on the firewall.

For example, to limit Youtube traffic through the firewall to 10Mbps, go to the **Traffic Control** page and add a new rule from the Public (Internet) zone to the Private (LAN) zone.

New Traffic-Control Rule		×
Application	youtube	
From	public	~
То	private	~
Bandwidth 10 Mbps		
10000		
	cancel	ave

You can see the new Traffic Control rule applied with a bandwidth limit of 10Mbps for the application **youtube**.

Allied Telesis	Firewall					
n Dashboard	Traffic Cont	rol				
Entities Applications	1 Rule					
Firewall	Traffic Control Rules					
Traffic Control	Application	From	То	Bandwidth		
Intrusion Prevention	youtube	Opublic	• private	10.00 Mbps		
🖸 Licensed Features 🔗						
Application Control						
Web Control						
IP Reputation						
Malware Protection						
Antivirua						

Step 4. Save configuration changes.

Save the Application Control configuration changes to make them part of the boot configuration.

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

Web Control

Web Control provides Enterprises with an easy means to monitor and control their employees' web traffic for productivity, legal, and security purposes. The proxy-based Web Control uses Digitals Arts' active rating system for comprehensive and dynamic URL coverage, websites are accurately assigned into around 90 categories, which can be allowed or blocked.

When a user tries to browse to a website, the http request is intercepted and sent to the classifier engine, which queries Digital Arts constantly updated URL database for the category that the website belongs to.

One a particular URL has been categorized, the result is cached in the firewall so that any subsequent requests with the same URL can be immediately processed.

Step 1. Configure Web control.

- Navigate to the Web Control configuration page under Security.
- Click on the **ON/OFF** switch to enable **Web Control**.
- Select the **Default Action** (for web pages that do not match any specific rules, but match a Web Control category).

Allied Telesis	Firewall		avpl	s Up time: 0 days (0.04)	🛓 Admin	B Save
 Dashboard B Security ~ 	Web Control				ON	-•
Application Control Application Web Control IP Reputation Melevani Protection Antieleas	Web Control provides businesses with an easy means to months and control em- comprehenses and quence (URL coverage which accusately organises wholes accusately and a set of the set of the set of the set of the set of the Provider: Digital Anta License Duration: 01/01/2017+01/01/2018	ployees" web traffic for productivity, legal, and securi into around 100 high-level categories (i.e. gambling esis ashe representative, Find your local Allied Teles	ty purposes. With the purphase of a subactytion liones, the fewall contentaneout, etc.). These can then be easily densed or permitted from a office at were allochdosis conviccentext.	n utilise Digital Arts active ratio the nationals by orienting Web C	g system for ontrol rules. Cus	Rem
Network · · · · · · · · · · · · · · · · · · ·	Default Category Action: After considering any Nish Control Fulse created below, the set default action of Web Control Rules Coation Categories	will permit or damy any remaining web traffic that main	chec a Web Control sategory	riter		Permit
	Artisr : Categories	loor	Ener			

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

Step 2. Add rules to manage website categories.

The Web Control feature has its own set of rules, which are separate to the Firewall rules. The Web Control rules are created here on the Web Control configuration page.

To block gambling websites, for example, create a rule applied to the Internet network.

		×
Action	Deny	
Categories		^
Select all	gamb	
✓ Gambling		
Source	public / Internet	t v

You can see the new rule applied to the Internet network in the Public zone.

-	Allied Telesis	Firewall			
22a 8	Dashboard Security V	Web Co	ontrol		
	Licensed Features Application Control Web Control IP Reputation	Web Control provid comprehensive and categories can be o For more information Provider: Dic	as businesses with an easy me dynamic URL coverage which a reated as well. In or to purchase a subscription it al Arts	ans to monitor and control empl accurately organises websites in n, contact your local Allied Telesi	yees' web traffic for productivity, legal, and security purposes to around 100 high-level categories (i.e. gambling, entertainm s sales representative. Find your local Allied Telesis office at v
	Malware Protection Antivirus	License Expiry	т: N/А		
⊕	Network 🗸	Default Category After considering	Action: any Web Control rules created	below, the set default action wil	permit or deny any remaining web traffic that matches a Web
•	System	Web Control Ru 1 Rule Action Deny	les Custom Categories Categories Gambling		Source

Step 3. Create custom categories.

As well as using the predefined website categories, you can also create your own custom categories which match text strings you enter against website URLs. These custom categories can then have rules applied (as we did for gambling websites above).

For example, to create a movie category containing the IMDB and Rotten Tomatoes websites, go to the **Custom Categories** tab and click the **+ New category** button. Create the new movie category, and add text string matches for any website addresses containing IMDB or Rotten Tomatoes.

	×
Name	
Movie	
Text strings	
IMDB, Rotten Tomatoes	
	delete
	uciete dave

You can see the new category and its website matches.

-	Allied Telesi	is Firewall
<i>₽</i> 2	Dashboard Security	Web Control
	Licensed Features Application Control Web Control IP Reputation Malware Protection Antivirus	Web Control provides businesses with an easy means to monitor and control employees' web traffic for productivity, legal, and comprehensive and dynamic URL coverage which accurately organises websites into around 100 high-level categories (i.e. gar categories can be created as well. For more information or to purchase a subscription, contact your local Allied Telesis sales representative. Find your local Allied Provider: Digital Arts License Expiry: N/A
۲	Network	Default Category Action: After considering any Web Control rules created below, the set default action will permit or deny any remaining web traffic the
٠	System	Web Control Rules Custom Categories Name URL Text Matching Movie IMDB, Rotten Tomatoes

You can now use the web control rules tab to add rules for this category as desired.

Step 4. Save configuration changes.

Save the Web Control configuration changes to make them part of the boot configuration file.

Up time: 0 days 00:32	💄 Admin	B Save
-----------------------	---------	--------

Note: You can monitor category and rule hits etc. from the Security Monitoring widget on the Dashboard.

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) on the freeto-use Custom URL Filtering page, as described in Part 3 of this guide.

This page allows you to subscribe to the Kaspersky blacklist service if you have the URL Filtering license installed. This blacklist of approximately 64,000 URLs is updated regularly to ensure protection from harmful websites.

Step 1. Configure URL Filtering.

- Navigate to the URL Filtering page under Licensed Features
- Click the ON/OFF switch to enable URL Filtering
- Set an Update interval to contact the Update Server for updates to the Kaspersky URL Filtering blacklist.

Allied Telesis	Firewall	us Up time: 0 days 19:28	1 Admin	Bier
Dashboard	URL Filtering		ON	-•
Entitien Applications Farwall NAT Traffic Control Intrastan Faventican Castern LER, Fillering	IBI: Finger glanes in thirds periods across. With the produces of a subordprint formation for formal ten statistic to regardly blackfor service, which is regulately and advances and point of ten induces the formal ten statistic tensors. The formal tensors are defined advances and point of tensors are defined advances and point of tensors are defined advances. The provide of tensors are defined advances and point of tensors are advanced advances and point of tensors. The provide of tensors are defined advances are defined to tensors are defined to tensors are defined to tensors. The provide of tensors are advances are defined to tensors are defined to tensors are defined to tensors. The provide of tensors are advances are advanced to tensors are advanced to tensors. The provide of tensors are advanced to tensors are advanced to tensors. The provide of tensors are advanced to tensors are advanced to tensors. The provide of tensors are advanced to tensors are advanced to tensors. The provide of tensors are advanced to tensors are advanced to tensors. The provide of tensors are advanced to tensors and tensors are advanced to tensors. The provide of tensors are advanced to tensors and tensors are advanced to tensors. The provide of tensors are advanced to tensors are advanced to tensors and tensors are advanced to tensors. The provide of tensors are advanced to tensors are advanced to tensors. The provide of tensors are advanced to tensors are advanced to tensors. The provide of tensors are advanced to tensors are advanced to tensors. The provide of tensors are advanced to tensors are advanced to tensors. The provide of tensors are advanced to tensors are advanced to tensors. The provide of tensors are advanced to tensors are advanced to tensors. The provide of tensors are advanced to tensors are advanced to tensors. The provide of tensors are advanced to tensors are advanced to tensors. The provide of tensors are advanced to tensors are advanced to tensors are advanced to tensors are advanced to tensors are advanc	o specify a unser-defined but of se	dailan ti allow	(ahtalipt)
Lisensel features Application Control Web Control URL Filtering Playdation Molever Protection				
Network System				

URLs are matched in this order – user-defined whitelists, user-defined backlists, Kaspersky blacklist. 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.

Step 2. Save configuration changes.

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



Part 5: Configure licensed Advanced Threat Protection (ATP) security features

The fundamental shift to sophisticated application use has provided businesses with increased efficiency, and improved collaboration, along with new ways to manage customer interaction. However, this has also opened the door for greater security concerns. Business data is potentially vulnerable, and the rapid development of new services has introduced new types of cyber threats.

Allied Telesis firewalls provide comprehensive threat protection, utilizing security engines, and threat signature databases from the industry's leading vendors, with regular updates to ensure up-to-the-minute protection against cyber attacks.

The Advanced Threat Protection (ATP) license enables IP Reputation, Malware Protection, and Antivirus (note that Antivirus is only available on the AR4050S).

The ATP license (like the Advanced Firewall license) is available in 1, 3, and 5 year subscriptions. You can view current license status by navigating to the License page under the **System** menu.

	Allied Telesis AR4050S									
æ	Dashboard									
ß	Security	~	License Management							
C	Licensed Features	~								
۲	Network	~	Feature Licenses							
٠	System	^					2018			
	About			Apr	May	Jun	Jul	Aug	Sep	(
	File Management		Base License							
							Base Licer	ise		
	Logging		ATP							
							AT prote	ction		
¢	Wireless Managemen	t ~								

IP Reputation

IP Reputation provides comprehensive IP reputation lists through Emerging Threats ET Intelligence[™] (provided by Proofpoint[™]), which identifies and categorizes IP addresses that are sources of Spam, viruses and other malicious activity. With real-time threat analysis, and regular updates to reputation lists, IP Reputation keeps network protection against hazardous websites right up to date.

Step 1. Enable IP reputation.

Navigate to the IP Reputation page under Licensed Features.

- Click the **ON/OFF** switch to enable IP Reputation.
- Set an **Update interval** to contact the Update Server for IP Reputation list updates.

Allied Telesis	Firewall	auplus	Up time: 1 day 01.00	± Admin	B terr
Deshboard					
â Secutly -	IP Reputation			ON	-
El Licensed Pratures 6	P Reputedon privates comprehensive IP Reputation last through Dranging Threads' (T Stelligence, which identifies and tategorizes IP addresses that are sources of span, visues and other a optime to repute to repute to repute to induction last, IP reputation last, in repute to magnetic based on a sparse based on a sparse based on the spanse of the span	alicious activity	. With real-time threat analy	sis, and autom	**
Application Control Web Control	For more information or to purchase a subscription, contact your local Alled Talease sales representative. Find your local Alled Talease office at www.alleshalesis.com/contact.				
LIRE, Filturing	Provider: Emerging Threats				
IP Reputation	License Expiry: N/A				
Malware Protection	Check for updates: 48 hours +				
Network					
System	IP Reputation Cetegory				
Ender Strategy	Calegory		Action		

Step 2. Configure IP reputation categories.

IP Reputation uses categories to classify the nature of a host's bad reputation. For example, IP addresses known to be sources of Spam will be added to the **Spam** category.

For any category, IP Reputation can be set to log the threat (which is the default action), ignore, or block/drop the matching packets.

To drop traffic from websites known as sources of Spam, set the Spam category to Block.

Allied Telesis	Firewall	awplus	Up time: 0 days 01:37	🚨 Admin	Save
Dashboard Security	IP Reputation			ON	-•
Licensed Features Application Control Web Control IP Reputation Malware Protection Antivirus	IP Reputation provides comprehensive IP Reputation lasts through Emerging Threats' ET Intelligence, which identifies and catego threat analysis, and automatic updates to reputation lasts. IP reputation keeps network protection against hazardous websites rip For more information or to purchase a subscription, contact your local Alled Telesis sales representative. Find your local Alled T Provider: License Expiry:	rtizes IP addresses that are sources of sg pht up to date. Relesis office at www.alliedtelesis.com/or	am, viruses and other malici	ous activity. Wit	h real-time
Network -	IP Reputation Category		44		
System	Scamer		10	Block	
	Mobile_Spyware_CoC		la Ig	Block nore	
	DC_Source		10	Block	
	Spam		19	nore	
	Bot		10	Block nore	
In a shared of the local states	at			Block	

You can monitor IP Reputation blocked packets on the Dashboard security monitoring widget.

Step 3. Save configuration changes.

Save the IP Reputation configuration changes to be part of the boot configuration file.



Malware Protection

Malware Protection is a stream-based high performance technology to protect against the most dangerous cyber threats. By considering threat characteristics and patterns with heuristics analysis, unknown zero-day attacks can be prevented, along with server-side Malware, web-borne Malware, and other attack types. Detection covers all types of traffic passing through the firewall, including web, email and instant messaging - any Malware is blocked. The Kaspersky anti-Malware signature database is updated regularly to keep on top of the latest attack mechanisms.

Step 1. Configure Malware protection.

- Navigate to the Malware Protection configuration page under Licensed Features.
- Click the ON/OFF switch to enable Malware Protection.
- Set an Update Interval to contact the Update Server for updates to the Malware signature database.



You can monitor Malware packets dropped on the Dashboard security monitoring widget.

Step 2. Save configuration changes.

Save the Malware Protection configuration changes so they become part of the boot configuration file.



Antivirus

The firewalls proxy-based Antivirus guards against threats such as viruses, Trojans, worms, spyware, and adware. In addition to protecting the local network by blocking threats embedded in inbound traffic, it also prevents compromised hosts or malicious users from launching attacks. This is essential for protecting business reputation, and minimizing business disruption.

Using the Kaspersky Antivirus engine, the signature database containing known threat patterns is regularly updated.

Step 1. Configure Antivirus.

- Navigate to the **Antivirus** configuration page under **Licensed Features**.
- Click the **ON/OFF** switch to enable Antivirus,
- Set an Update Interval to contact the Update Server for updates to the Antivirus signature database.



Step 2. Save configuration changes.

Save the Antivirus configuration changes to make them part of the boot configuration file.



Note: You can monitor how many files have been scanned, viruses found, etc. using the security monitoring widget on the Dashboard.'

The Dashboard

Now that we have configured the firewall, application control, web control, and threat protection features, 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 security features, statistics, and allows you to go and configure them further.

The **Top 10 Applications** and **Top 10 Categories** widgets show applications and website categories using the most bandwidth through the firewall. Choose to configure new firewall or traffic control rules to manage these.

CRU	2.00
CPU	3.8%
Memory	65%
Temp	30°
Fans	Status: Active
Environment	🤣 Status: Good
System Time	() Nov 23 21:34:23 2016

System Shows CPU and memory use, as well as device health.

System Information

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



SecurityThe Security Monitoring widget shows the main security and threat protection features of the
firewall 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.

Rule	Stats	Statu	S
Firewall	🥝 2 Rules	OFF	ed
NAT	🤣 2 Rules	ON	edi
Traffic Control	2 Rules	ON	edi
Intrusion Prevention	Packets Matched (65)	ON	edi
Application Control		ON	edi
Web Control	Category Hits (0), Rule Hits (0), Cached URLs (0), Cache Hits (0)	OFF	edi
URL Filtering	URL Hits (0)	ON	edi
IP Reputation	Packets Blocked (43)	OFF	edi
Malware Protection	Packets Dropped (109)	ON	edi
Antivirus	Files Scanned (0), Files Skipped (0), Viruses Found (0),	ON	edi

You can also see how many rules are configured for the various features, and statistics for each of the security features, for example, URL rules hit, packets blocked, and viruses found.

Top 10 Application s

The Top 10 Applications widget shows the top applications using firewall bandwidth. You have the ability to take action based on this reporting, by adding a new Firewall, or Traffic Control rule from the widget, by clicking on the F or T add rule buttons.

Top 10 Applications		reset
Application	MB	Add Rule
ssl	117.3	FT
іструб	96.76	FT
udp	83.44	FT
eth	16.41	FT
dhcp	12.6	FT
wsdscvry	8.3	FT
arp	3.69	FT
ntbiosns	3.28	FT
pim	1.03	FT
ssdp	0.49	FT

The Top 10 Applications table shows cumulative totals, and is live, so the **MB** used will change and applications will move position in the table. Clicking the **reset** button will zero all totals and start to display the top used applications from that time onwards.

Top 10Similar to the Top 10 Applications widget, the Top 10 Categories widget shows the top Web controlCategorieswebsite categories that are using firewall bandwidth. You can create a new Web control rule from the
widget in response to this reporting.

Top 10 Categories		
Category	Hits	
News	57	w
Sports	7	w
Travel	2	w
Social Networking	1	w
Celebrities, Entertainment	1	W

SystemFurther system information is available on the About page, under the System menu, such as model,
serial number, firmware and GUI versions, and so on.

	Allied Telesis	Firewall	
æ	Dashboard		
e	Security ~	About	
C	Licensed Features \checkmark	System Information	
(†)	Network ~		
٠	System ^	System Information	
	About	Host Name:	awplus
	License Management	Model:	AR3050S
		MAC Address:	00-00-cd-38-02-27
		Serial Number:	A05049G151700023
		Environment:	Status: Good
		System Time:	Dec 14 18:53:30 2016
		Firmware Version:	ar3050s-5.4.6-2.1.rel
		GUI Version:	2.20161215.1
		Bootloader:	4.1.2-devel

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, License Management, and Logging from the System menu, and the Wireless Management menu.

File Management

The **File Management** page on the Device 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				amplus	Optime. 0 doys 03:17	🛓 Admin	a terr
A Dashboard	File Management							Factor
Licensed Features	/huflash			▲ Upload	Set Boot Release File			
Network	Name	Modified	Size (byles)	Actions	Current: flash:/AR30503	55.4.8-0.2.MI		droves -
System About	Tech	25/54/2018, 10:46:00			Backup: Resh:/ar30505	5.4.7-2.5ml		Droeve
File Management	🖬 log	14/11/2016, 21:59:01			Set Boot Config File			
License Management	R30505-5.4.9-0.2.ml	20/04/2018, 10:44:12	43742531	O powersel × centre	Current: Restu/default.c	itg		Direct.
eu el	BadListat	27/02/2017, 06:55:58	555	O Dowmad X mete	Backup: flashudefault.c	ifg	-	Drovene
🗢 Wireless Management 🖂	MyListet	13/12/2016, 12:07:50	281	A coverant X overs	Flash Usage			
	MyList2.txt	13/12/2016, 12:07:56	410	O Deveload X develo			346.1M/	/3.65
	B 100.00	12/07/2017, 15:39:21	706894	O Downad X overs				
	a30509-5.4.7-2.5.rel	08/03/2018, 15:55:10	42175271	O Doversal) × develo				
	🗎 #3050s.bin	14/07/2016, 07:57:14	2438	& Download X develo				
	📓 amplus-gui, 548, 02 tar.gz	20/04/2018, 10:40:13	1112336	O Downsat X center				
	📓 default.cfg	22/03/2018, 09:16-41	3319	O Develoant X develo				
	E exception log	17/08/2017, 14 16:59	157	O bowned × center				
		11/10/2014 10:00 40	1010	Contraction in the second				

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 Managemen	t
<i>th</i> a	
Name	Modified
Banh Sanh	Sun Apr 09 17:09:21 2017 UTC
i an	Thu Jan 01 00:00 00 1970 UTC

	🕼 Allied Telesi	s	Firewall			
<i>₽</i> ₽	Dashboard Security ~	,	File Management			
C	Licensed Features 🛛 🗸		/fa/usb			
0	Network ~		Name	Modified	Size	Ae
٠	System ^		CV CV	Fri Oct 28 16:49:52 2016 UTC		
	About File Management		Study	Fri Mar 17 22:03:02 2017 UTC		
	License Management		System Volume Information	Tue Jun 14 18:48:00 2016 UTC		
			Conf	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	0

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

Allied Telesis	AR3050S						explus	Up time: 0 days (03.17	🛓 Admin 🔒 Saye
n Deshboard									
a security ~	File Management								3 5 5 5 5
Licensed Features	Auflesh				1 Allerer	Set Boot F	Release File		1
Network	Name	Modified	Size (bytes)	Actions		Current	Resh/AR0050	5480.2.H	2 D Browne
• System	In fach	20/04/2016,10:46:00				Backup	flesh/er30505	54.7-2.5.ml	D Street
About File Management	in up	14/11/2016, 21:59:01				Set Boot 0	Config File		
License Management	AR30505-5.4.8-0.2.ml	20/04/2018,10:44:13	43742533	O Downad	× _{statete}	Current	Rest./default.c	dg	D Broose
сцв	Bart.ist.tet	27/02/2017, 06:55:58	553	C Covernad	× deteta	Backup;	Rash/default.c	fg	D Broom
🜩 Wireless Management 🖂	B MyListor	13/12/2016, 12:07:50	201	O Devented	× deteta	Darkting			
	MyList2.txt	13/12/2010, 12:07:56	410	O Devenued	× datata	100	*		345.1M/3.4G
	B 400.70	12/07/2017, 15:39:21	706894		× orier	-			
	B #30505-5.4.7-2.5.rd	08/03/2018, 15:55:10	42175271	O Downland	× salata				
	B arithdestee	14/07/2016, 07:57:14	2439	O Download	× celata				
	B amplus-gut_548_02.tar.gz	20/04/2018, 10:40:13	1113336		× ones				
	Contaut.ctg	22/03/2018.0916:41	2219		× delete				
	E exception.log	17/08/2017, 14:16:59	157	O Deventual	× _{chieles}				
thys.//192.568.1.1/4/dashboard		11/10/2016, 12:35:58	1809	O Downood	× cente				

Tip Currently used and total Flash Usage is available

Flash Usage	
10%	346.1M / 3.6G

License management

Feature licenses are available for the UTM firewalls to unlock advanced functionality.

Licenses such as advanced firewall, and advanced threat protection, enable additional security features as described in parts 4 and 5 of this guide. An AMF Master and AWC wireless license are available to enable management of wired and wireless network devices. All of the licenses are available in 1 or 5-year subscriptions.

The license management page shows the licenses you currently have on your device, and their expiry date. It also allows you to add new licenses.

Allied Telesis	AR40505 #00000	Up time: 1-Days 00110	🕹 Admin 🛛 🗃	Save
Dushband Security	License Management			
 Licensed Features Network 	Feature Licenses	C. street	orne i e ente ha	-
System About File Management Logging CU E3	App Many fam Mad Ang Top Col Base License Base License			
Workes Management ~				

Hover over a license to show details, including duration and included features.

	🔎 Allied Telesis	A	AR4050S								
æ	Dashboard										
ĉ	Security ~		Licens	se Ma	ana	gei	ment				
C	Licensed Features V										
۲	Network ~		Feature Licenses	s							
٥	System ^	Ľ						2010			
	About				Apr	May	/ Jun	Jul Au	ig Sep	Oct	
	File Management		Base License								
							E	ase License			
	Logging						Base License				
	CLI 🖸										
÷	Wireless Management 🗸						Duration 19/04/2018 -	Permanent			
							Features				
							BGP-FULL	BGP4+	CPU-L3-Route	IPv6Basic	L3-FORWARDING
							L3-MC-ROUT	E LAG-FULI	MLDSnoop	No-License-Lock	OSPF-FULL
							OSPFv3-FUL	L PIM	PIM-100	PIM6	RADIUS-FULL
							RIP	RIPNG	VRF-LITE	VRF-LITE-63	VRRP

Adding a new subscription feature license

Once you have purchased your new subscription license (for example a 1 year 'Advanced Threat Protection license'), to add it to your firewall:

1. Click the upload license button

enter license

2. Browse and select the .bin file you will have received. Once selected, the .bin file will be uploaded and the license added to your device.

Add License Result	×
Licenses added successfully	
	ок

The newly added Advanced Threat Protection license can now be seen.

	🗶 Allied Tele	esis	AF	R4050S								
æ	Dashboard											
ß	Security	~	L	licens	e Ma	nag	gem	nent				
C	Licensed Features	~										
۲	Network	~	Fea	ature Licenses								
٠	System	^										
	About					Apr	May	lup	2018	Aug	Sep	0
	File Management		В	ase License		Api	iviay	Juli	Jui	Aug	зер	
	License Management								Base Licen	se		
	Logging		A	TP								
	CLI 🗹								AT protec	tion		
÷	Wireless Management	~										

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	AR3050S				3	Up time: 0 days 00:30	🛓 Admin	8 50
A Dashboard								
O Network ~	Logging							
Interface Management DHCP Server	Buffered Perman	ent 🗟					/ Contigues	Logging
VLAN			All Severity			Total Mes	inges 409 🧔	Refrects
Tools	Date ~	Facility ~	Level o	Program ~	Messape ~			
O System -	2018-04-23 18:25-14	user:	hotice	ATMP	Last message Incarnation is not p' repeated 9 times, suppressed by syslog-rig on 3			
14404	2018-04-23 18:25:14	user	debug	VCS	STK TRACE Stack member 1 changed status from Syncing to Ready			
File Management	2018-04-23 18:25:16	uter	notice	ATME	Incarnation is not possible with the data received port1.0.9 (findex 5009)			
Lizense Management	2018-04-23 18:25:45	uter	notice	ATME	Last message 'incarnation is not p' repeated 14 times, suppressed by syslog-og on 3			
Looper	2018-04-23 18:25:45	eyslog	notice	syslog ng	Syslog connection established; fd='h1'; server=XF_INET(10.37.95.65.514); local=XF_INET(0.0.0.00)			
CU ES	2018-04-23 18:25:45	syslog	er	syslog-ng	1/0 error occurred while writing, 30+161', error+Connection refused (146)'			
	2018-04-23 18:25:45	nyslog	notice	syslog-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	ATME	Incarnation is not possible with the data received port1.0.9 (Ifindex 5009)			
	2018-04-23 18:26:45	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 ng	Syslog connection established, M='29', server='AF_INET(10.37.95.65.514)', local='AF_INET(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 broken; Mr-29, server-AF_INET(10.37.95.65.514), time_reopen=60			
	2018-04-23 18:26:46	user	notice	ATMF	Incarnation is not possible with the data received port1.0.9 (ifedex 5009)			
	2018-04-23 18:27:41	user	notice	ATMP	Last message 'incumation is not p' repeated 37 times, suppressed by sysloging on 3			
	2018-04-23 18:27:41	authority	warning	solid	pam_lastlog(remote-login session): file /var/log/lastlog 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	ATMP	Last message 'moarnation is not p' repeated 1 times, suppressed by sysloging on 3			

You can filter the logs in 3 ways to focus your view and support easy analysis.

Filter logs by:

1. any information column in ascending or descending order

Logging				
Buffered Permane	ent	All Severity	T	
Date A	Facility ^	Level ^	Program 🔨	Message ^
2018-04-23 18:46:21	localó	crit	ATME	AR4050 has left. 4 members in total.
2018-04-23 18:58:20	localó	crit	ATME	AR4050 has joined. 5 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	local6	crit	ATME	AR4050 has left. 4 members in total.
2018-04-23 18:36:47	local6	crit	ATME	AR4050 has joined. 5 members in total.
2018-04-23 18:33:58	local6	crit	ATME	AR4050 has left. 4 members in total.
2018-04-23 18:46:24	local6	crit	ATME	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, e.g Critical, Warning, Error etc.

Logging				
Buffered Permar	ent			
Date ~	Facility ^	Critical All Severity Emergency Alert		Message ^
2018-04-23 18:33:58	local6	Critical		AR4050 has left. 4 members in total
2018-04-23 18:34:14	local6	Warning		AR4050 has joined. 5 members in to
2018-04-23 18:36:38	local6	Info Debug		AR4050 has left. 4 members in total
2018-04-23 18:36:47	local6	crit	ATMF	AR4050 has joined. 5 members in to

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

Logging				
Buffered Perm	nanent			
received		All Severity	٣	
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 switch and also set up a Syslog server(s) for remote log storage.

Logging					
Buffered Permane	ent				Configure Logging
		Critical	٠		Total Messages 11 🧔 Antron
Date 🛩	Facility A	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.

Logg	Logging Configuration							
Local	Remote			VewLogs				
Buffere	4	j		✓ Deer Logs				
Level	Facility	Program	Message	+ new filter				
Notice	cron	all	•	E conte				
Alert	daemon	imi		I see				
Notice	authpriv	dhcpsn		E sets				
Debug	all	all		E conte				
Perman	lent			✓ Geir Logs				
Level	Facility	Program	Message	4 res file:				
Debug	all	all		E conte				
Warning	j all	all	*	E state				

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.

Logg	Logging Configuration							
Local	Remote				View Logs			
					+ New Hold			
10.37.9	5.65				Celete Hosts			
Level		Facility	Program	Message	+ new film			
Emerge	ncy	all	all		I cente			
Notice		all	all		Colete			

Wireless management

Allied Telesis UTM Firewalls 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.

C613-22078-00 REV M

🔨 🖉 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.