Technical Guide

Getting Started with the UTM Firewall GUI

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.

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?

This guide shows how to configure a UTM Firewall using the Graphical User Interface (GUI).

The firewall 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 DHCP server, interface management, VLAN management, system tools, 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 firewalls built-in industry standard Command Line Interface (CLI). The firewall and its graphical management and monitoring functionality will increase with subsequent releases.

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 Firewall 7
Part 1: Configure a standard 3-zone network 7
Part 2: Configure the firewall for Update Manager 20
Part 3: Configure advanced firewall license security features 22
Part 4: Configure licensed Advanced Threat Protection (ATP) security features 28
The Dashboard 34

Products and software version that apply to this guide

This guide applies to all AR-Series UTM Firewalls running version **5.4.6-2.1** or later. 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

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.

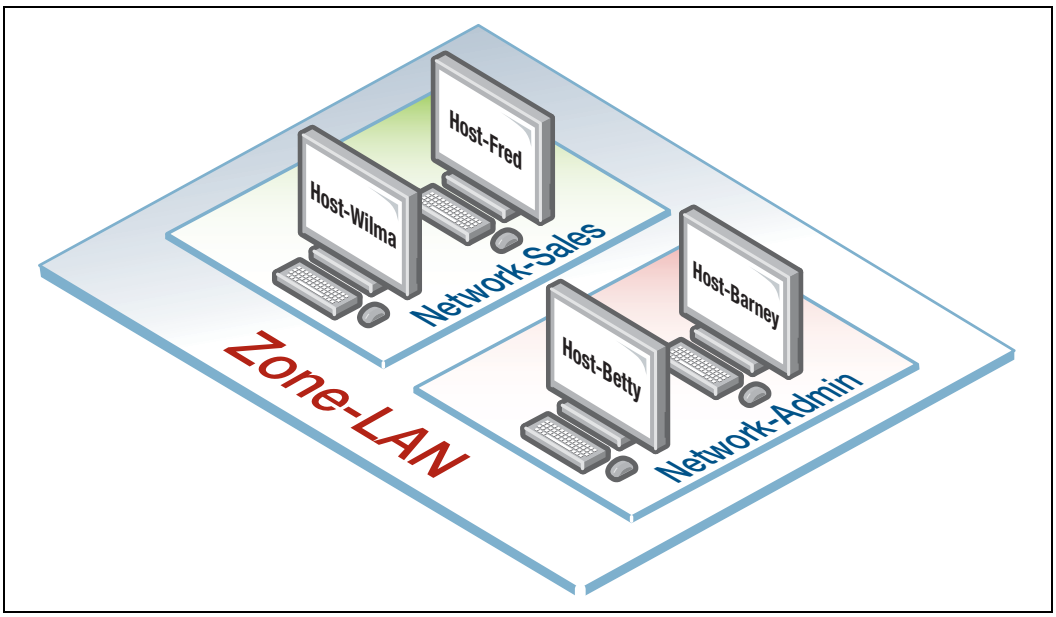
Allied Telesis firewalls map out the network environment into regions, using three tiers of granularity. The divisions into which it cuts up its environment are referred to collectively as **Entities**. The three levels of granularity in the dividing up of the environment are zones, networks, and hosts.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

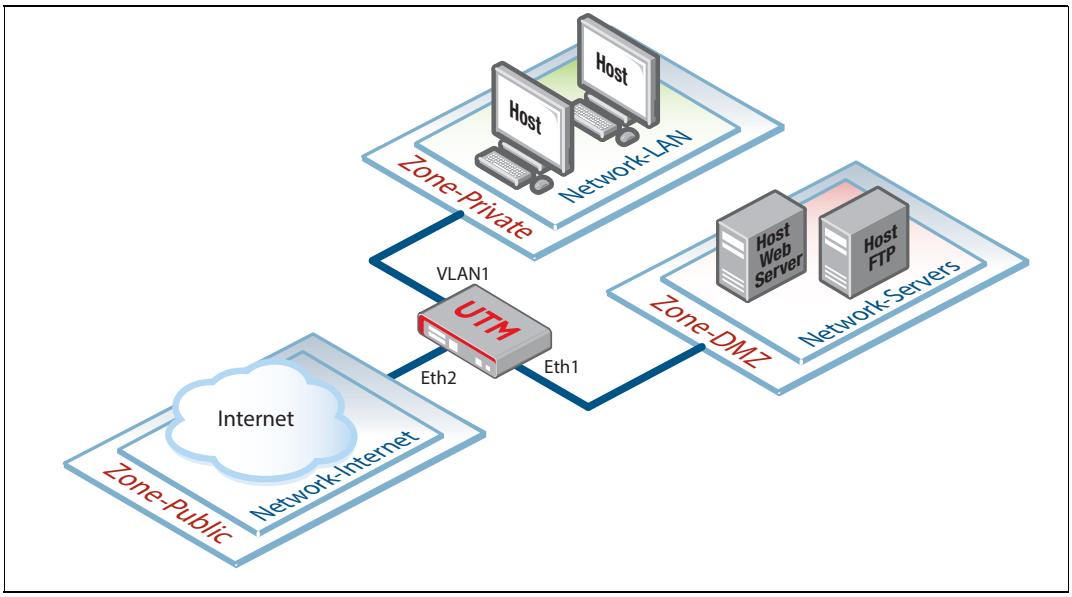
- NAT with IP Masquerade, where private source addresses are mapped to a public source address with source port translation to identify the association. The single public IP address masquerades as the source IP on traffic from the private addresses as it goes out to the Internet.
- Port Forwarding, to 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 four 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 20
3. Advanced firewall features - App Control and Web control, see page 22
4. Advanced threat protection features - IPS, IP Reputation, Malware Protection, and Antivirus, see page 28.

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 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 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 GUI pages:

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

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

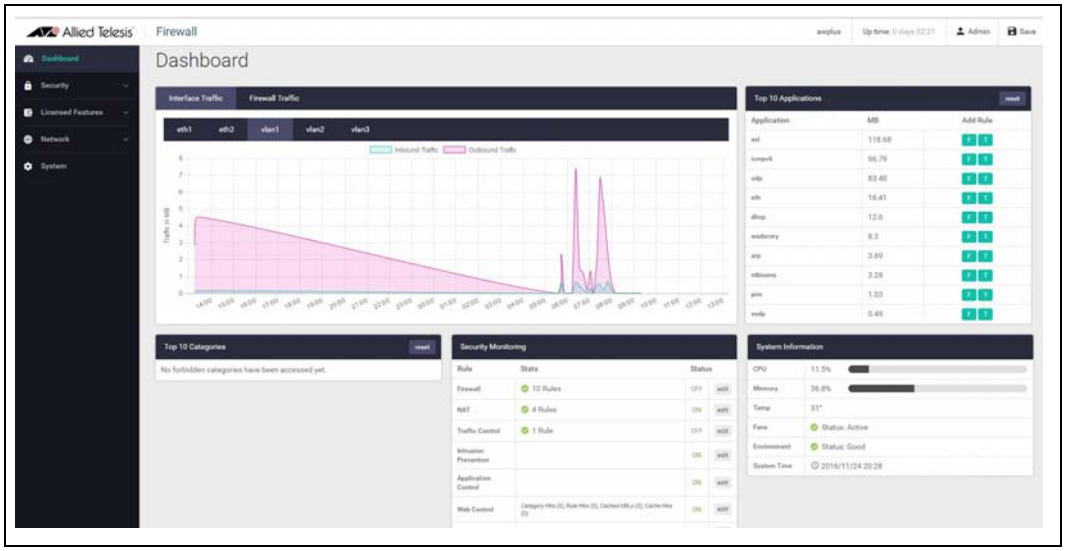
Browse to the IP address of the firewall on the interface you are connecting to - e.g. 192.168.1.1 for VLAN1.

Note: The firewall GUI currently supports the Firefox™ and Chrome™ web browsers.

The following login page is displayed:

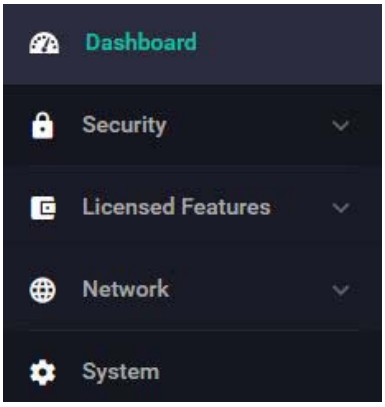
You can log in using any valid username/password combination that has been configured on the unit, or use the default username/password (**manager**/**friend**), if that has not been deleted.

Once logged in you will be on the dashboard of the firewall 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**, **Security**, **Licensed Features**, or **Network** menus for configuration, or select the **System** menu to view system information.



The **Network** menu includes, interface management, VLAN management, tools, access to the CLI, and the ability to configure the firewall as a DHCP server for the network. These will not be detailed in this document, as we'll concentrate on setting up the firewall and security.

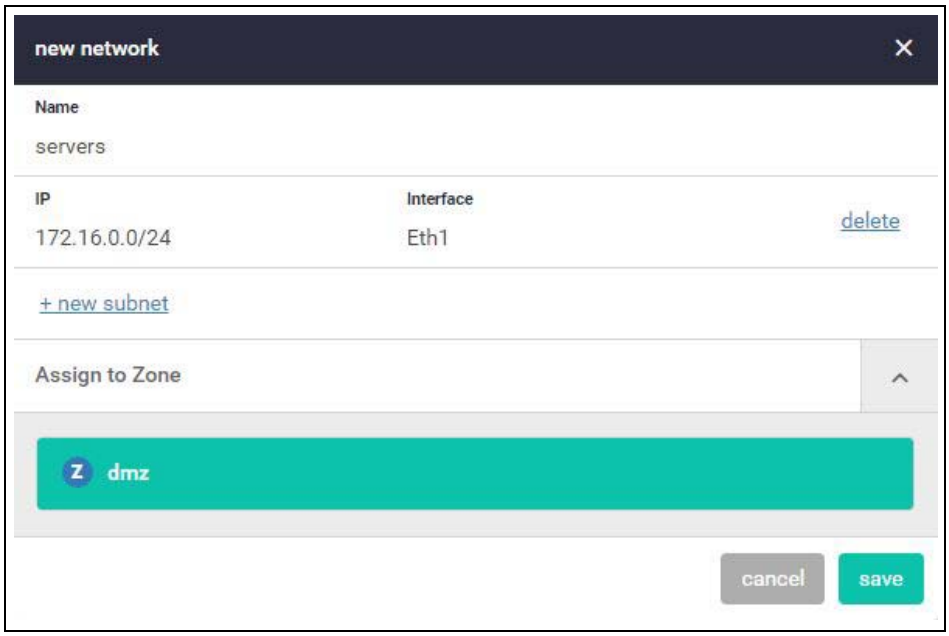
Step 4. **Configure Entities.**

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.

- Next click the green **+ new network** button to add our **servers** network to the DMZ zone.
- 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.
- Assign the network to the DMZ zone

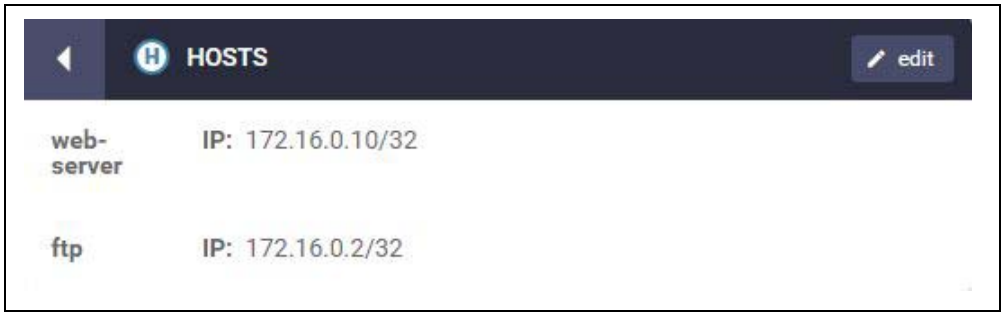


- We can now add specific hosts (servers in this case).
- Click the green **+new host** button to add the **ftp** server with an IP address of 172.16.0.2/32. Assign this host to the **servers** network.

- Add a second host named **web-server** with an IP address of 172.16.0.10/32

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

  - web-server
  - ftp



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

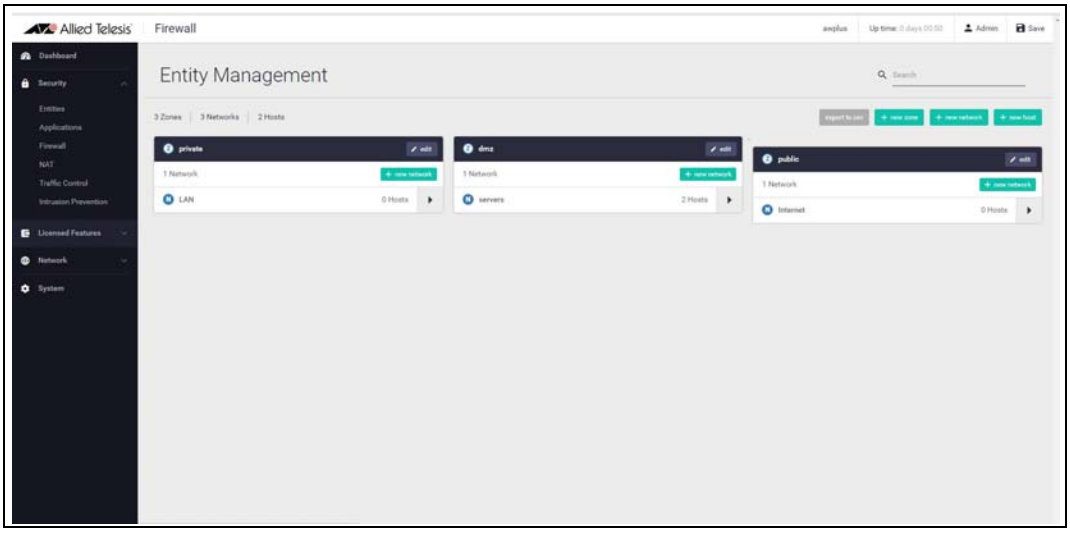
Private zone:

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

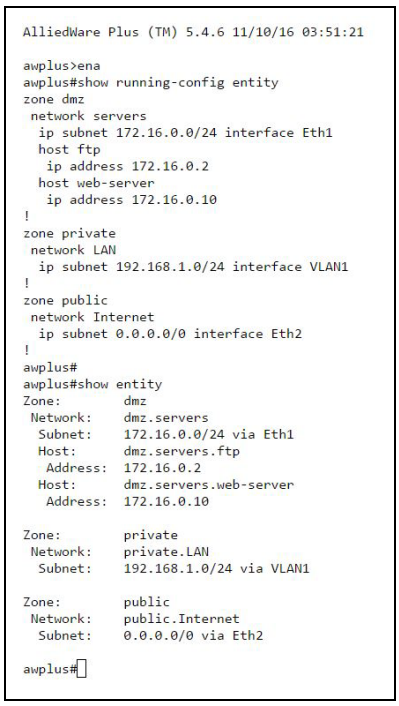
Public zone:

- 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.



If you'd like to view these changes as added to the firewall configuration file, select **CLI** under the **Network** menu. This opens a CLI tab. Type **ena** to access Priviledged Exec mode, then use the CLI commands **show running-config entity** and **show entity**.



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.

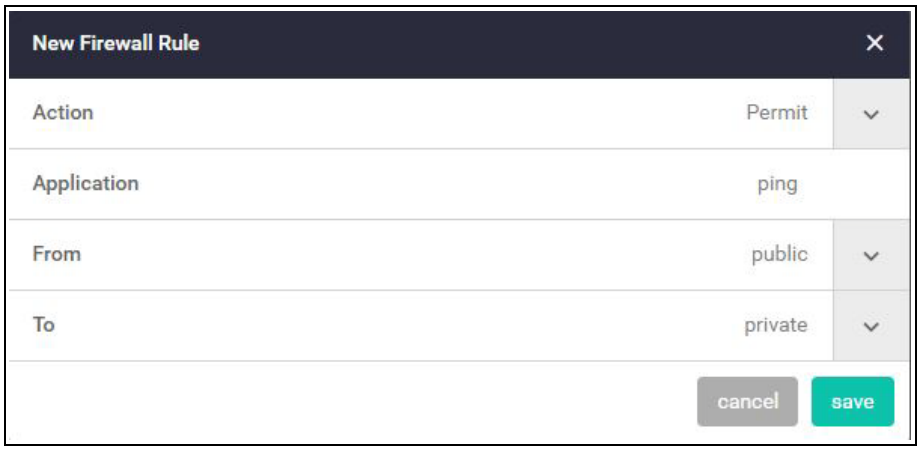
Step 5. **Configure firewalls rules.**

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.

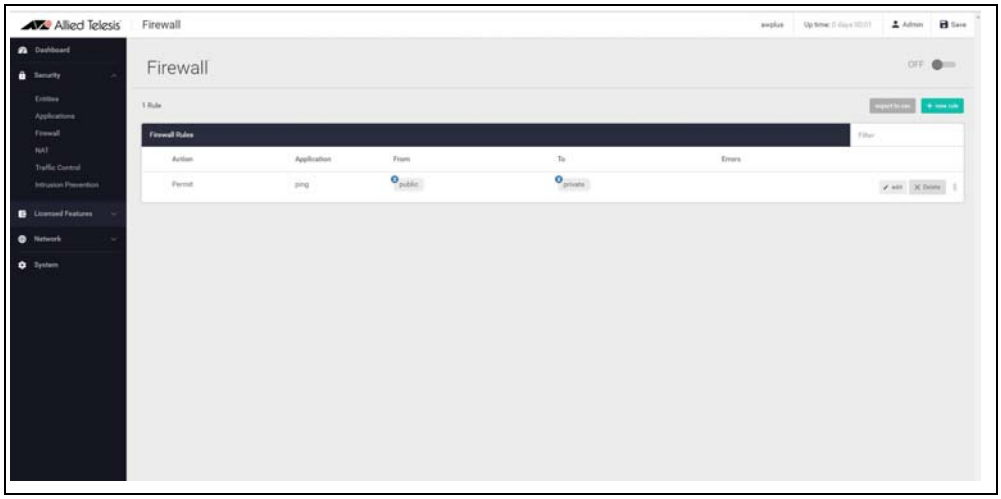
- Navigate to **Firewall** under the **Security** menu.

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.



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



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

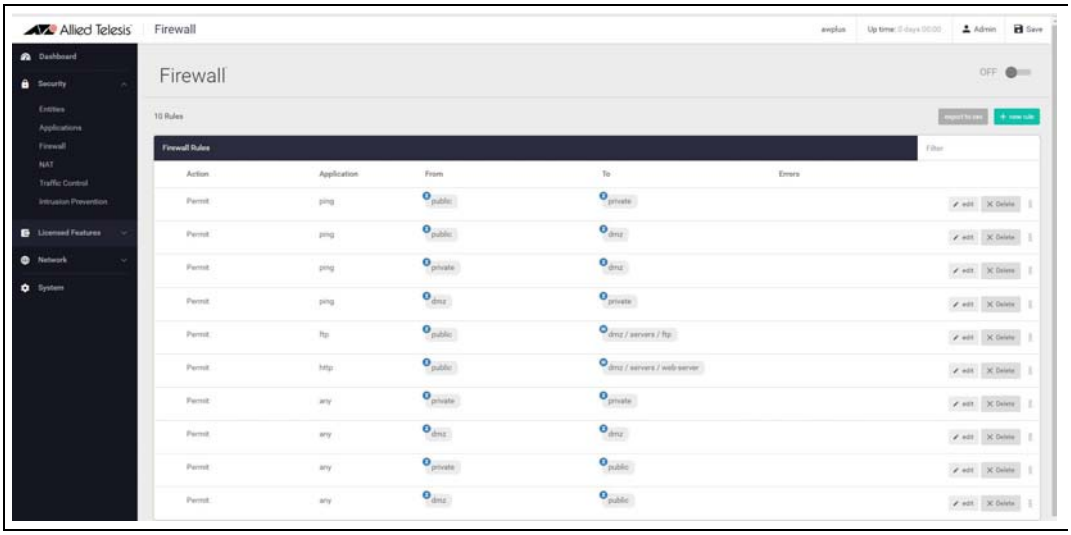
Allow Public traffic from the Internet to our DMZ servers:

- 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:

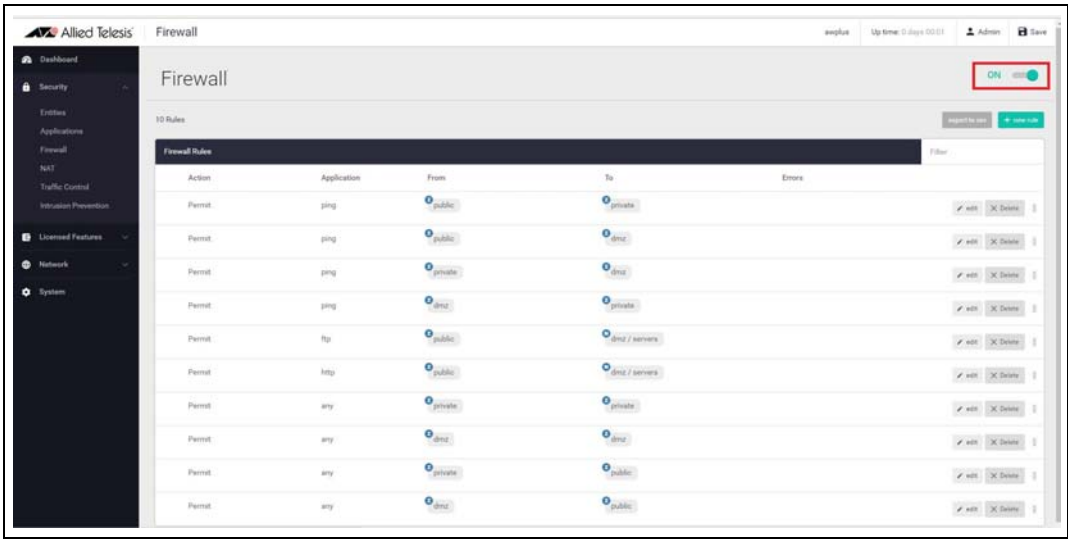
- Permit Any from Private to Private
- Permit Any from DMZ to DMZ
- Permit Any from Private to Public
- Permit Any from DMZ to Public

We can now see these firewall rules displayed:



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.

- 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.



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

```
AlliedWare Plus (TM) 5.4.6 11/10/16 03:51:21

awplus>ena
awplus#show firewall rule

[* = Rule is not valid - see "show firewall rule config-check"]
  ID     Action  App        From                To                  Hits
-------------------------------------------------------------------------------
* 10     permit  ping       public              private             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
awplus#
awplus#show running-config firewall
firewall
 rule 10 permit ping from public to private log
 rule 20 permit ping from public to dmz log
 rule 30 permit ping from private to dmz log
 rule 40 permit ping from dmz to private log
 rule 50 permit ftp from public to dmz.servers.ftp log
 rule 60 permit http from public to dmz.servers.web-server log
 rule 70 permit any from private to private log
 rule 80 permit any from dmz to dmz log
 rule 90 permit any from private to public log
 rule 100 permit any from dmz to public log
!
awplus#
awplus#show firewall
Firewall protection is disabled
Active connections: 13
awplus#
```

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

Step 6. **Configure NAT rules.**

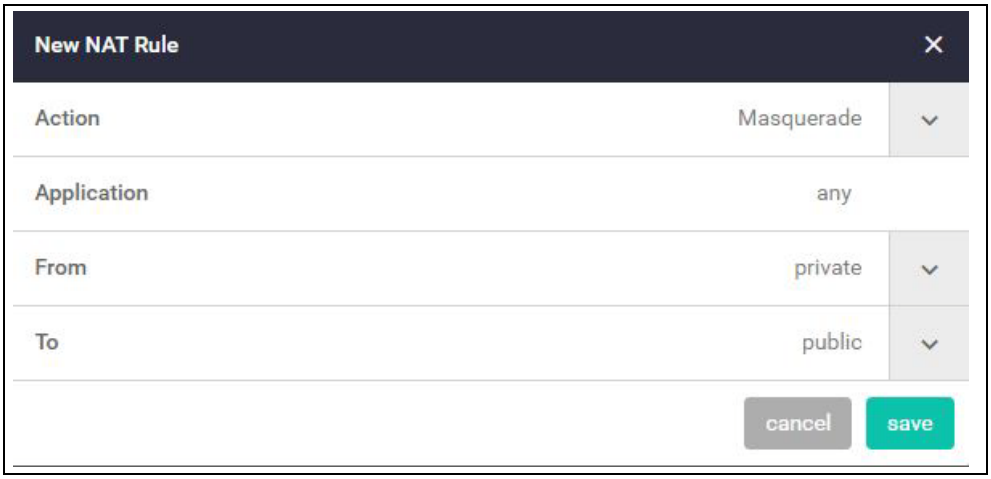
Now let's configure NAT rules to manage IP address translation between the Internet and our internal networks.

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

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

- 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:



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

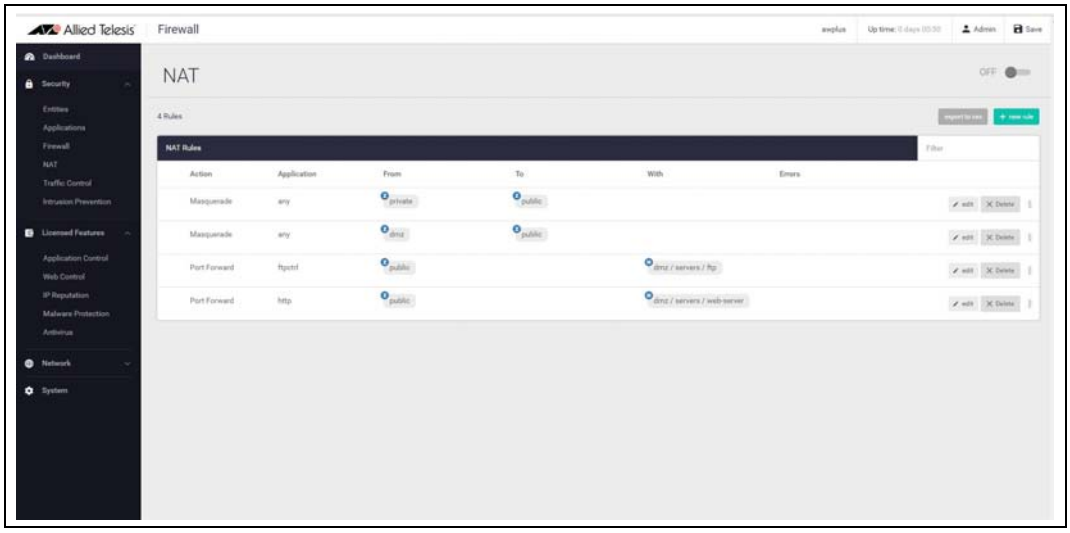
We now need to create two NAT port-forwarding rules to enable access to the FTP and Web servers to be delivered to the right destinations. To users in the Public zone, both servers will appear to have the IP address that is on the eth2 interface, so sessions towards those servers will be initiated to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



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

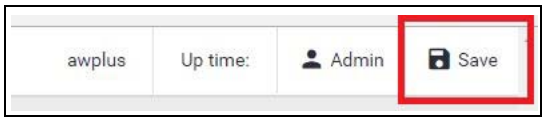
```
AlliedWare Plus (TM) 5.4.6 11/10/16 03:51:21

awplus>ena
awplus#show nat rule

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

Step 7. **Save configuration changes.**

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



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 3 and 4), 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.

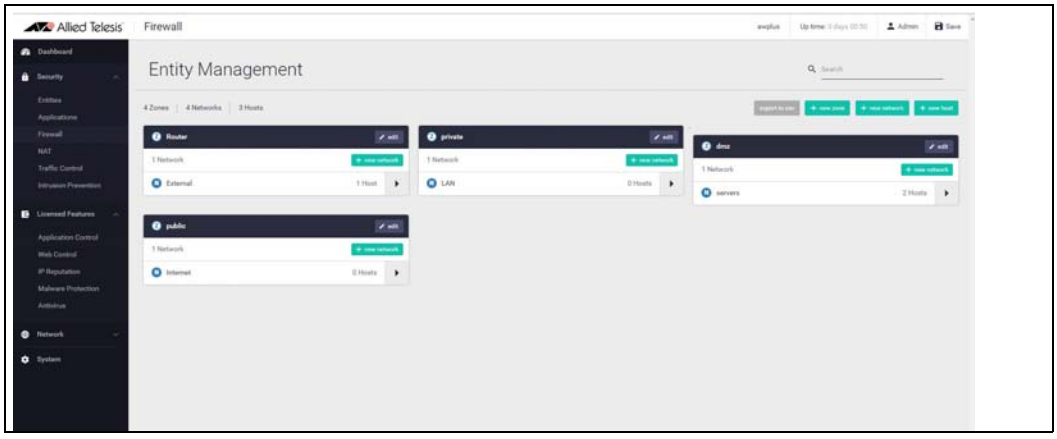
Step 1. **Create appropriate entities.**

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 = 192.168.52.20/24

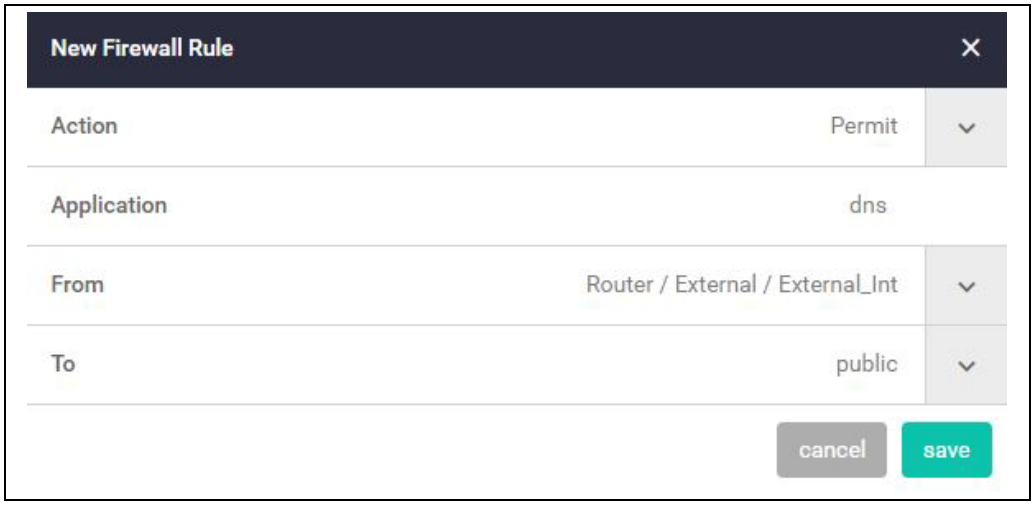
The updated **Entity Management** page will look like this:



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.

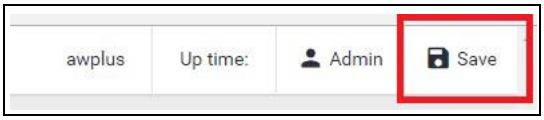
Also create a rule to allow DNS resolution of the update server's URL.



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

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.



Updating the GUI

As new versions of the firewall 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 GUI, and install it on your firewall, firstly ensure that the firewall GFW can contact the update server using the steps above, and then simply enter the following command from the CLI window:

```
update webgui now
```

Note: The updating mechanism will be added to the GUI itself in a subsequent release, so the GUI is able to be updated without using the CLI window.

Part 3: Configure advanced firewall license 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** [1]. The Advanced Firewall feature license is available in 1, 3, and 5 year subscriptions.

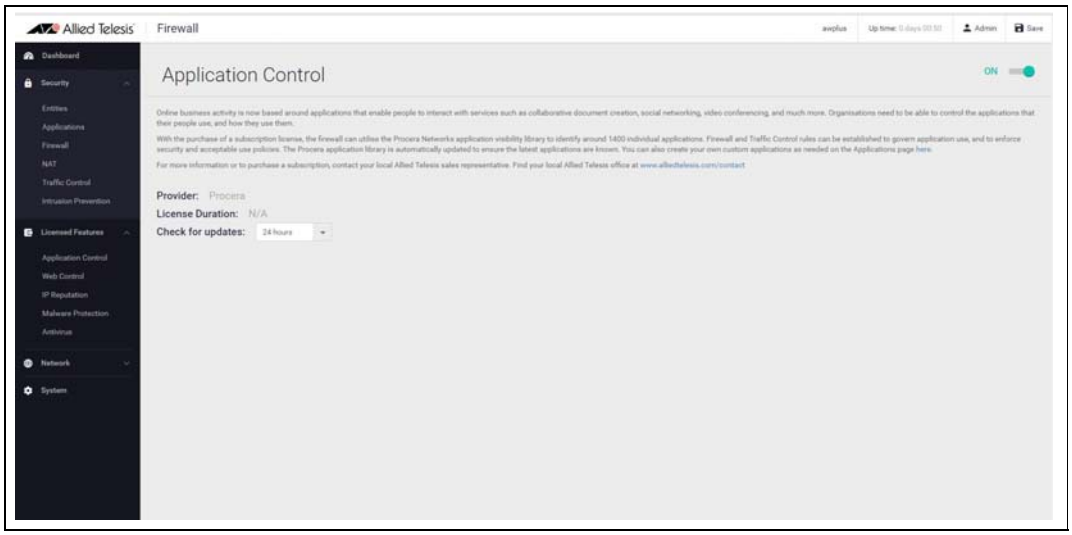
1. URL Filtering will be added to the GUI in the near future.

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 on the switch to enable Application Control, and select the provider and update interval.



Application Control uses the Procera Networks application visibility library to identify thousands of 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.

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.

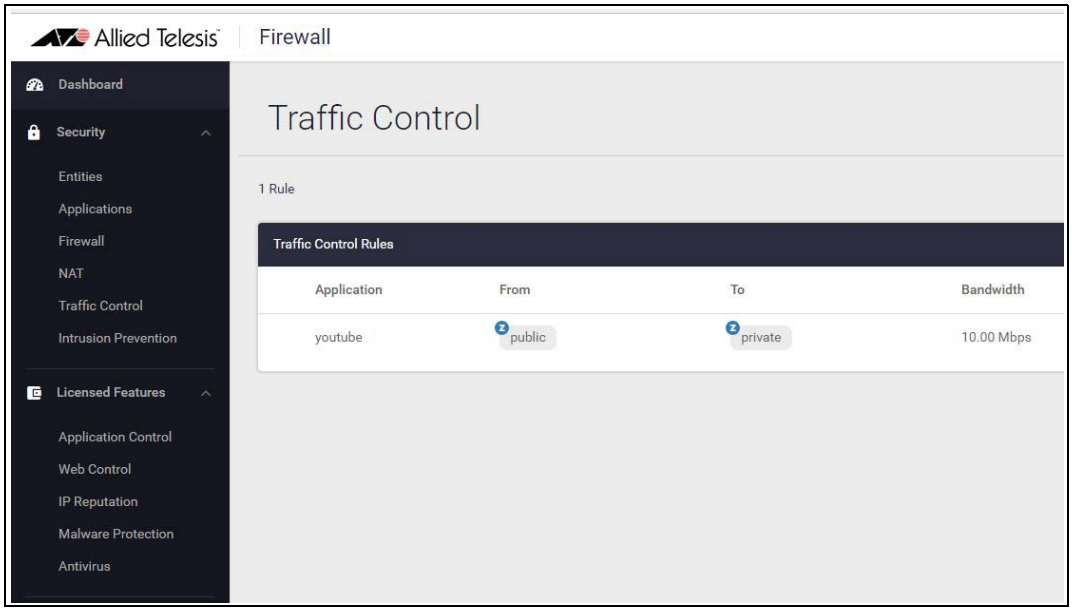
For example, to block the use of Spotify™ (a music streaming service) company-wide, create a firewall rule denying the Spotify application from the Public (Internet) zone to the Private (LAN) zone.

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.

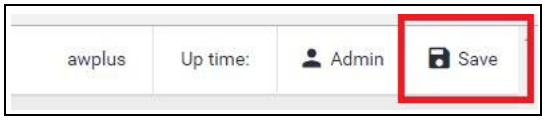
For example, to limit Youtube traffic through the firewall to 10Mbps, go to the **Traffic Control** page and add a new rule from the Public (Internet) zone to the Private (LAN) zone.

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



Step 4. **Save configuration changes.**

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



Web Control

Web Control provides Enterprises with an easy means to monitor and control their employees' web traffic for productivity, legal, and security purposes. Utilizing 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.

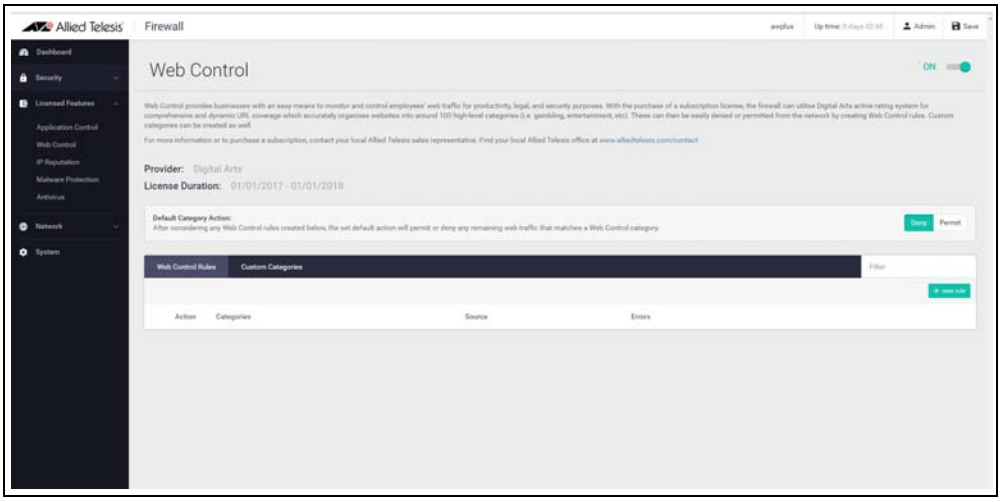
When a user tries to browse to a website, the http request is intercepted and sent to the classifier engine, which queries Digital Arts constantly updated URL database for the category that the website belongs to.

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 switch to enable **Web Control**.

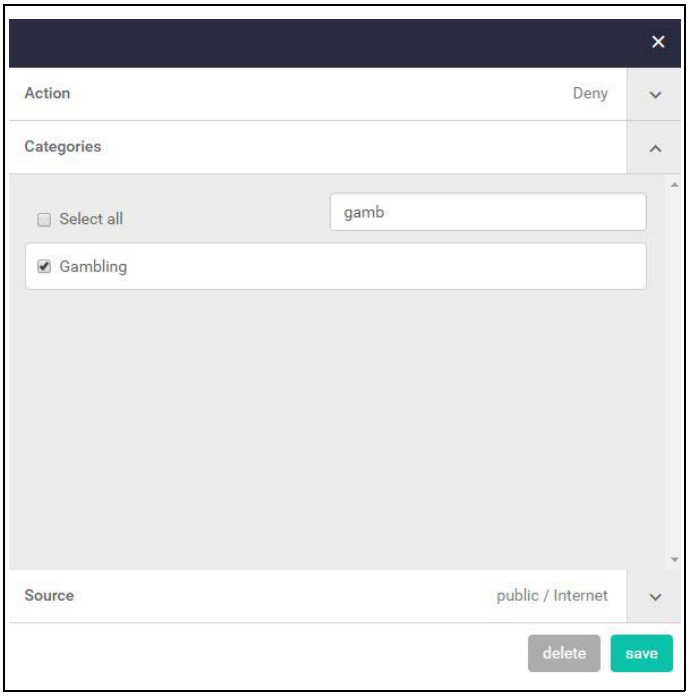
- Select the **Default Action** (for web pages that do not match any specific rules, but match a Web Control category).



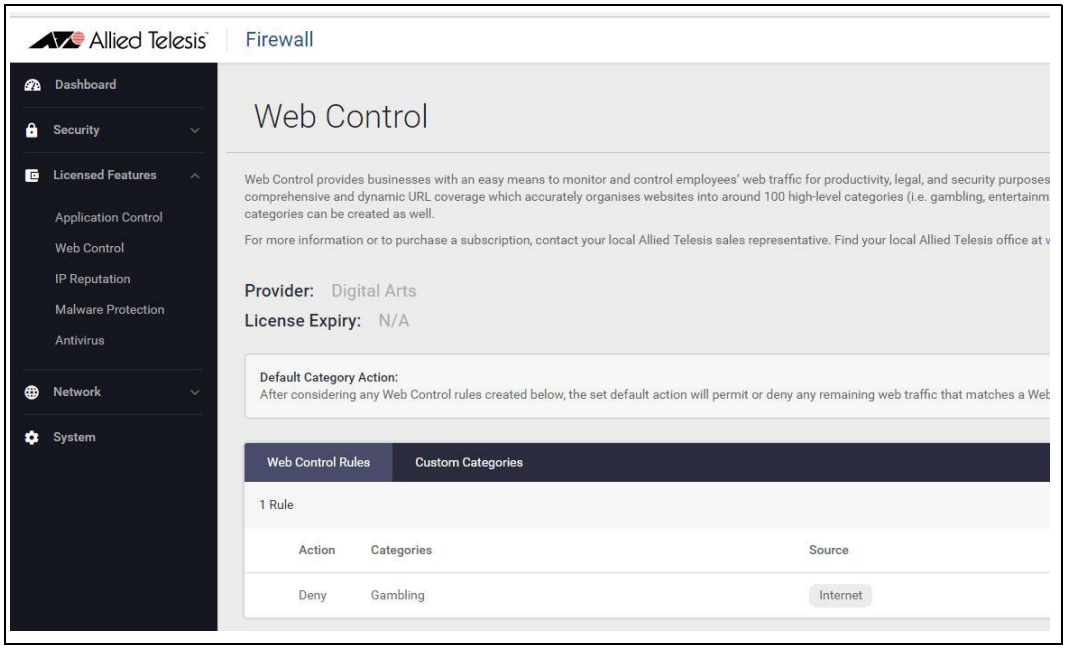
Step 2. **Add rules to manage website categories.**

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.



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

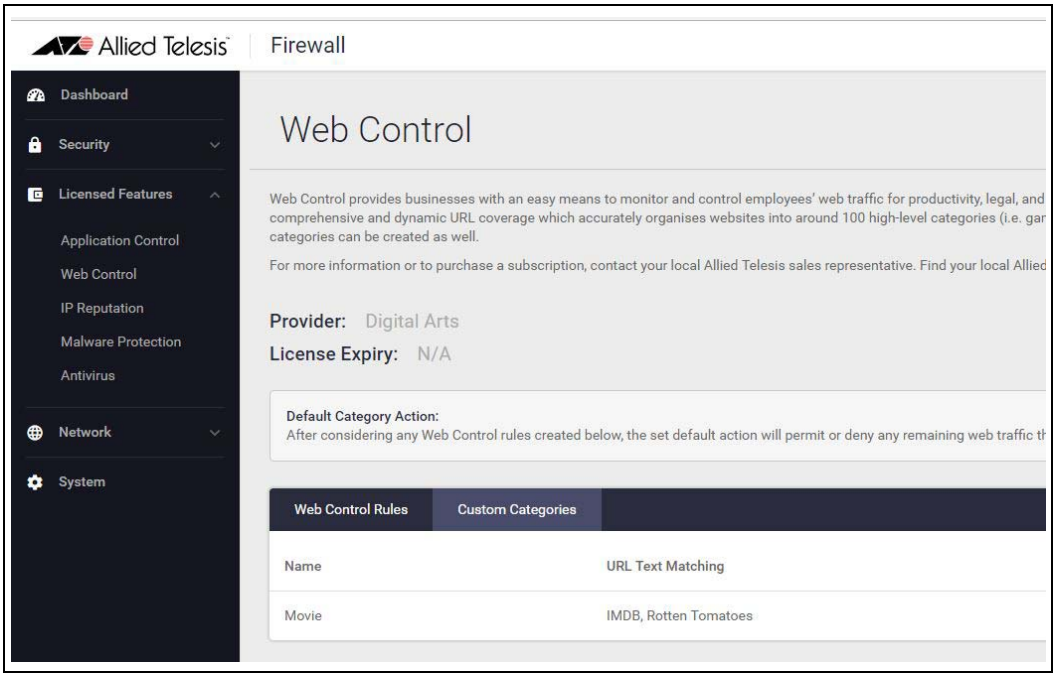


Step 3. **Create custom categories.**

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, Rotten Tomatoes

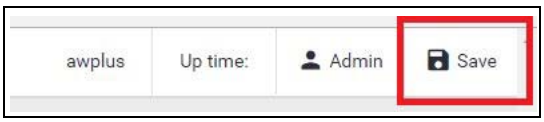
You can see the new category and its website matches.



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.



You can monitor category and rule hits etc. from the Security Monitoring widget on the dashboard.

Part 4: 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.

Intrusion Prevention System (IPS) is provided free on the firewalls, while the Advanced Threat Protection (ATP) license adds IP Reputation, Malware Protection, and Antivirus (note that currently Antivirus is only available on the AR4050).

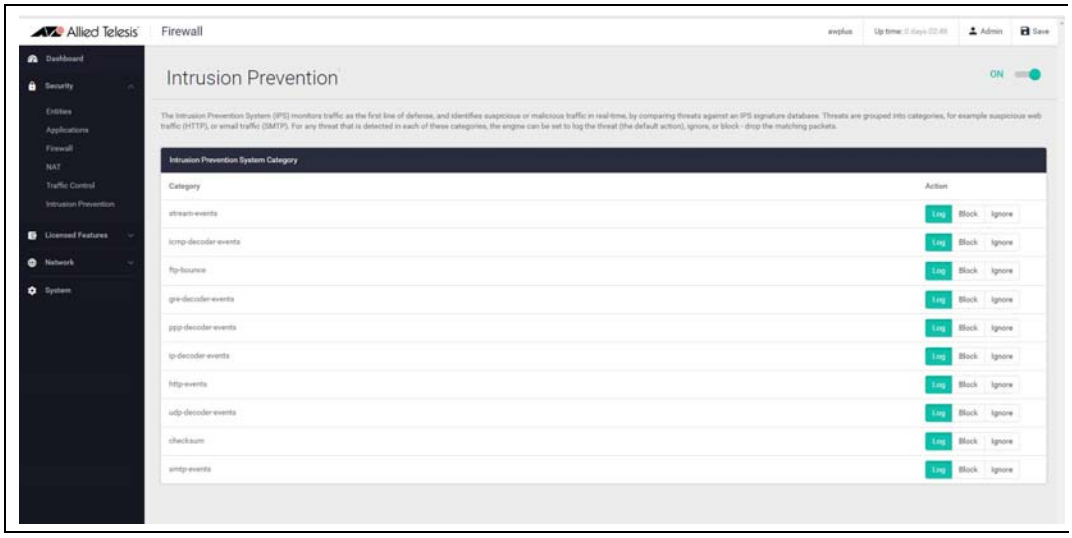
The ATP license (like the Advanced Firewall license) is available in 1, 3, and 5 year subscriptions.

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.**

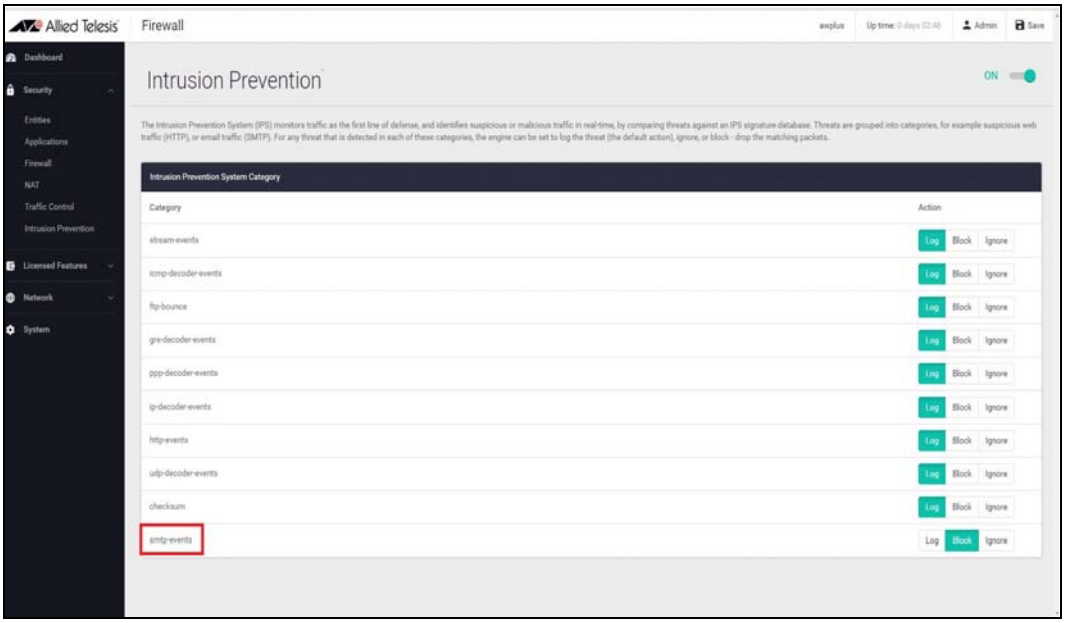
Navigate to the **Intrusion Prevention** configuration page under **Security**. Click the switch on the top right of the page to enable IPS.



Step 2. **Configure IPS actions.**

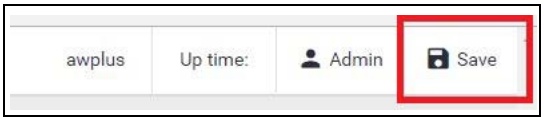
Threats are grouped into categories, for example suspicious web traffic (HTTP), or email traffic (SMTP). For any threat that is detected in each of these categories, the engine can be set to log the threat (which is the default action), ignore, or block - drop the matching packets.

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



Step 3. **Save configuration changes.**

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



IP Reputation

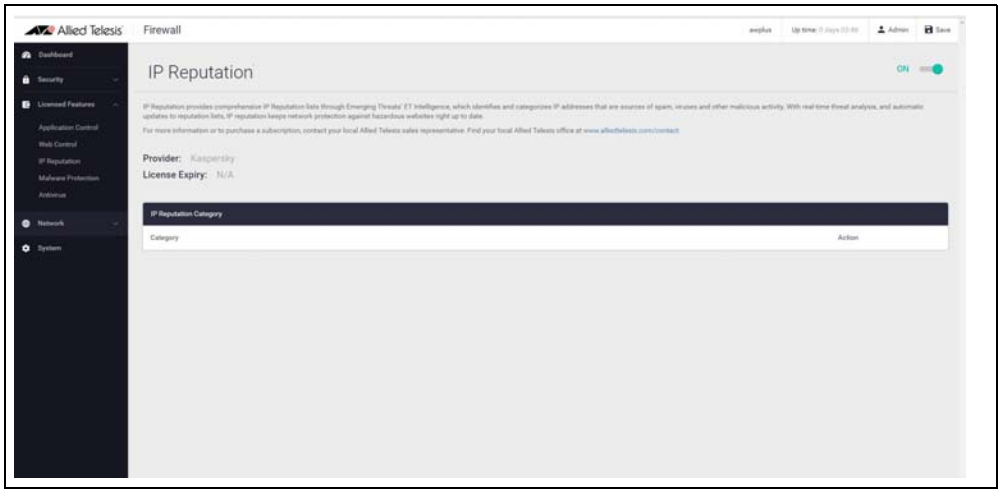
IP Reputation provides comprehensive IP reputation lists through Emerging Threats ET Intelligence™ (provided by Proofpoint™), which identifies and categorizes IP addresses that are sources of Spam, viruses and other malicious activity. With real-time threat analysis, and regular updates to reputation 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 switch to enable IP Reputation (**Protect**)

- Set an **Update interval** to contact the Update Server for IP Reputation list updates.

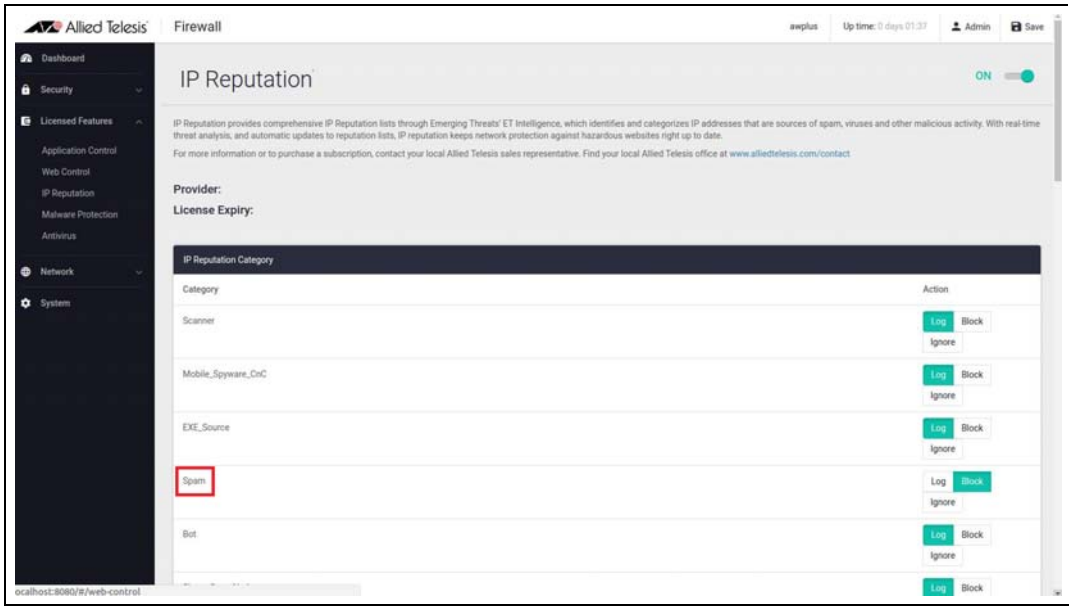


Step 2. **Configure IP reputation categories.**

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.

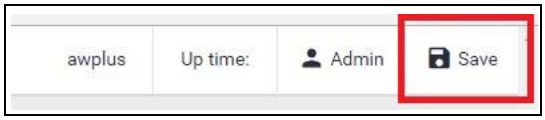
For any category, IP Reputation can be set to log the threat (which is the default action), ignore, or block/drop the matching packets.

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



Step 3. **Save configuration changes.**

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



Malware Protection

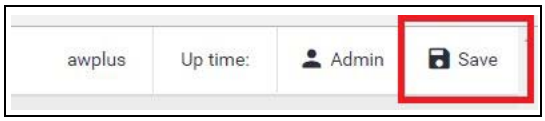
Malware Protection is a stream-based high performance technology to protect against the most dangerous cyber threats. By considering threat characteristics and patterns with heuristics analysis, unknown zero-day attacks can be prevented, along with server-side Malware, web-borne Malware, and other attack 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 switch to enable Malware Protection.
- Set an **Update Interval** to contact the Update Server for updates to the Malware signature database.

Step 2. **Save configuration changes.**

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



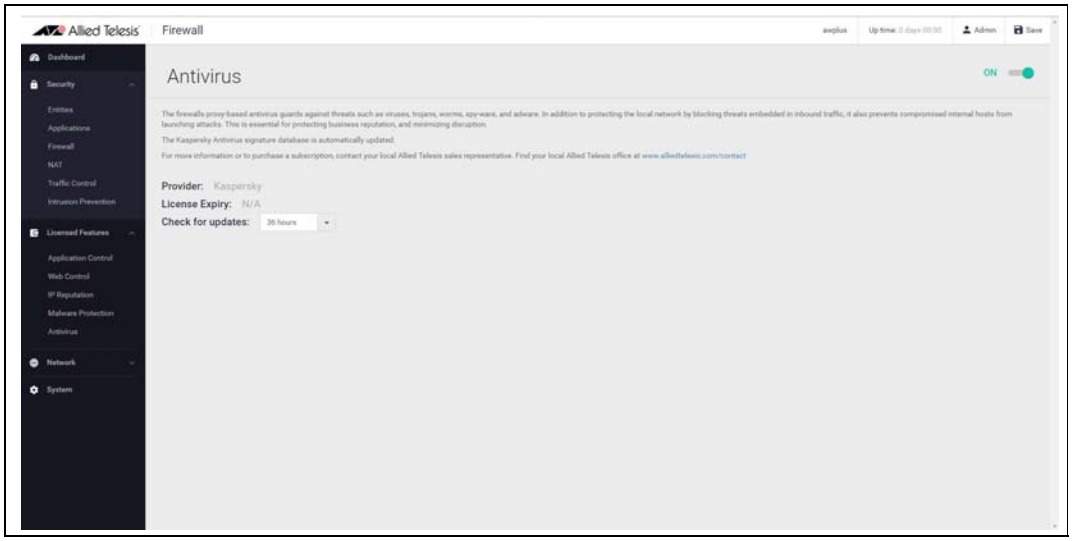
Antivirus

The firewalls proxy-based Antivirus guards against threats such as viruses, Trojans, worms, spy-ware, 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.

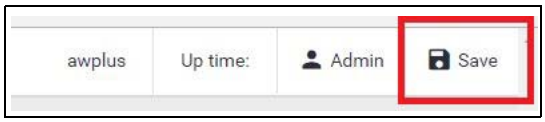
Step 1. **Configure antivirus.**

- Navigate to the **Antivirus** configuration page under **Licensed Features**.
- Click the **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.**

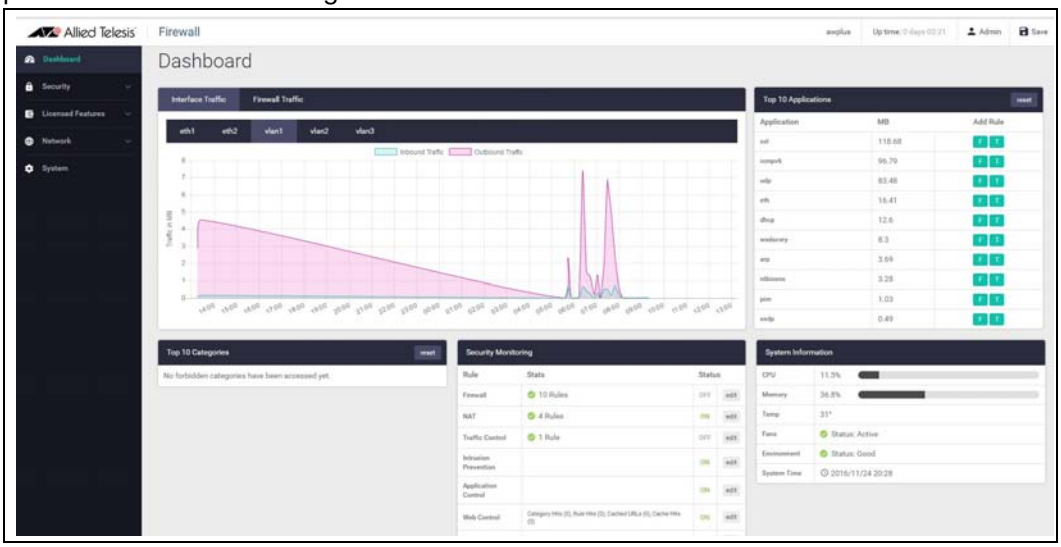
Save the Antivirus configuration changes to make them part of the boot configuration file.



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

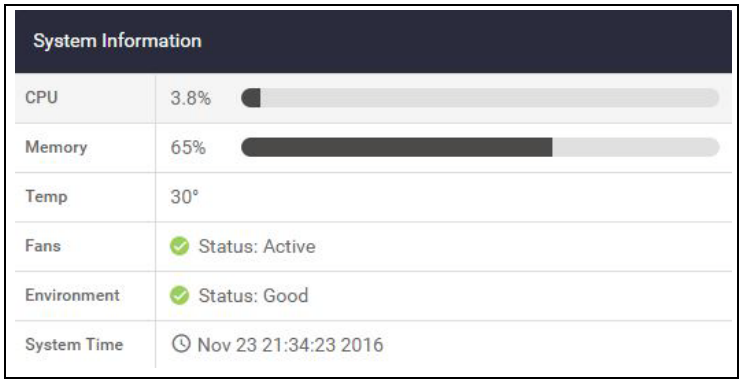


Currently there is a **System Information** widget that displays details about the firewalls status. The **Traffic** widget show traffic through the firewall, or per interface. The **Security Monitoring** widget shows the various security features, statistics, and allows you to turn the features on or off, with the option to go and configure them further.

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

System Information

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



Interface Traffic

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

Firewall Traffic

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

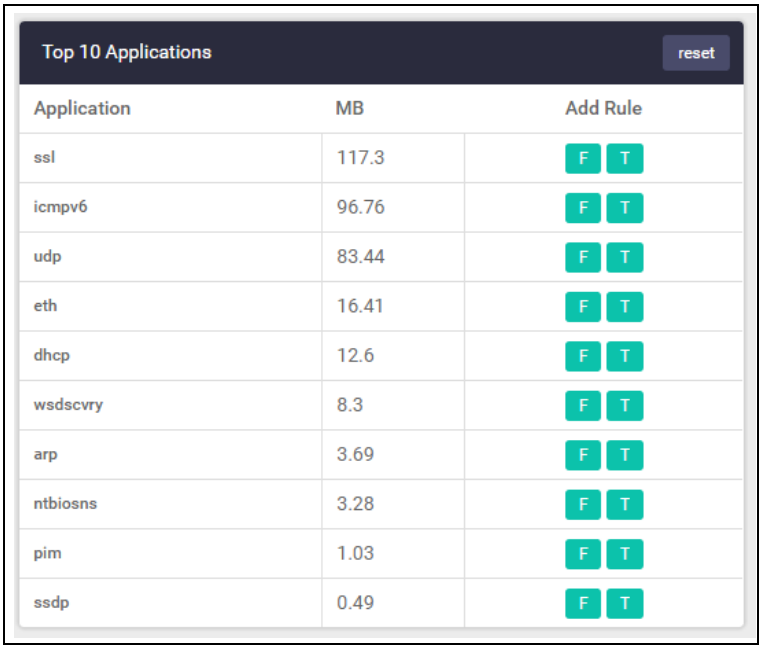
Security monitoring

The **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, and enable or disable from right here on the widget. You can select **edit** to go to that features dedicated page to configure it further.

You can also see how many rules are configured for the various features, and statistics. Web Control statistics show how many hits categories and rules are getting, while Antivirus statistics show files scanned, viruses found and so on.

Top 10 Applications

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 Categories

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

System Page

Further system information is available on the **System** page, such as model, serial number, firmware and GUI versions, and so on.