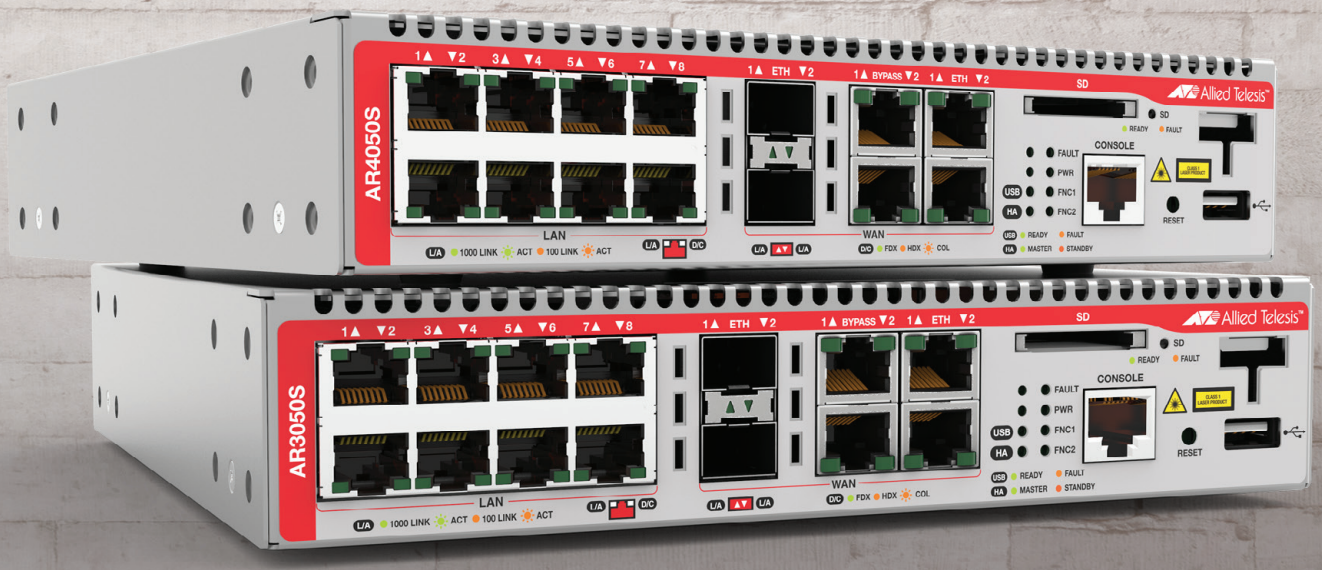
Technical Guide

Allied Telesis™

Feature Overview and Configuration Guide

Advanced Network Protection



AlliedWare Plus™
OPERATING SYSTEM

alliedtelesis.com

C613-22104-00 REV D

Acknowledgments

This product includes software developed by the University of California, Berkeley and its contributors.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. For information about this see www.openssl.org/. Copyright ©1998-2008 The OpenSSL Project. All rights reserved.

This product includes software licensed under the GNU General Public License available from: www.gnu.org/licenses/gpl2.html

Source code for all GPL licensed software in this product can be obtained from the Allied Telesis GPL Code Download Center at: www.alliedtelesis.com/support/default.aspx

Allied Telesis is committed to meeting the requirements of the open source licenses including the GNU General Public License (GPL) and will make all required source code available.

If you would like a copy of the GPL source code contained in Allied Telesis products, please send us a request by registered mail including a check for US$15 to cover production and shipping costs and a CD with the GPL code will be mailed to you.

GPL Code Request
Allied Telesis Labs (Ltd)
PO Box 8011
Christchurch
New Zealand

Contents

Introduction **5**

Products and software versions that apply to this guide 6

Related documents 7

Licensing 8

Feature overview **9**

Intrusion Prevention System (IPS) 10

Antivirus 12

IP Reputation 13

Malware Protection 15

Web Control 17

URL Filtering 20

UTM Offload 21

Selecting a security solution **23**

Proxy versus stream-based security processing 23

Packet flow architecture 25

Selecting a UTM firewall 28

URL Filtering or Web Control? 31

Antivirus or Malware Protection? 32

Firewall/NAT rules, entities and performance 33

Configuring Intrusion Prevention System (IPS) **35**

Configuring Antivirus **36**

Configuring IP Reputation **37**

Configuring Malware Protection **39**

Configuring Web Control **40**

How to configure basic Web Control 40

How to configure Web Control default action per-entity 42

How to discover which Web Control category a website URL belongs to 44
Configuring Web Control with firewall enabled 45

Configuring URL Filtering 47
How to use URL Filtering 47
Configuring URL Filtering 50

Setting up and configuring UTM Offload 55
Setting up UTM Offload 55
About the offload image 57
Configuring UTM Offload on VMware ESXi Server 58
Security considerations 63
Configuring Firewall and NAT allowing UTM Offload on the AR4050S 64
UTM Offload glossary 65

Logging 66
Log message filtering—general 66
Reading log messages 67
Firewall log messages 67
UTM log messages 68
IPS log messages 69
IP Reputation log messages 70
Malware Protection log messages 71
URL Filtering log messages 72
Web Control log messages 74
Antivirus log messages 74
Firewall connection logging 75
UTM Offload logging 77

Introduction

This guide describes the Advanced Network Protection features on AR-Series UTM firewalls AR4050S and AR3050S and how to configure them. It also describes the performance effects when various combinations of advanced security features are in use.

AlliedWare Plus Advanced Network Protection features provide the first line of defense against a wide range of malicious content. In addition to protecting the local network by blocking threats in inbound traffic, they also prevent compromised hosts or malicious users from launching attacks. This is essential for protecting your organization's reputation.

By partnerships with third-party security specialists, the security features below can be used in combination with associated signature databases that are regularly updated to keep on top of the latest attack mechanisms.

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

Additionally, on the AR4050, the UTM Offload feature can be used to improve network forwarding performance by offloading some of the advanced security features to a second physical or virtual machine that is automatically managed by the AR4050S.

This document provides:

- Overviews of each feature, in "Feature overview" on page 9
- Performance considerations and guidance for choosing which features and combinations may be appropriate for your network, in "Selecting a security solution" on page 23
- Guidance for selecting a UTM firewall based on security and performance requirements of your network, in "Selecting a UTM firewall" on page 28
- How to configure each of the security features, including examples
- Descriptions of logging available for each of the security features, in "Logging" on page 66.

Products and software versions that apply to this guide

This guide applies to AlliedWare Plus™ products that support Advanced Network Threat Protection features, running version **5.4.5** and later.

To see whether your AR-Series UTM Firewall supports a particular feature or command, see the following documents:

- The product's Datasheet
- The product's Command Reference

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

The features described in this document are supported from AlliedWare Plus 5.4.5 or later as follows:

Intrusion Prevention System:

- Version 5.4.5

Antivirus:

- Version 5.4.5

IP Reputation:

- Version 5.4.5

Malware Protection

- Version 5.4.5

Web Control

- Version 5.4.5 and later support Web Control.
- Version 5.4.6-2 and later support Web Control configuration of default action on a per-entity basis.
- Version 5.4.7-1.x and later support categorization of HTTPS websites using Transport Layer Security Server Name Indication (TLS SNI).
- Version 5.4.7-2.x and later supports a command to inquire about the web control category of a website URL.

URL Filtering

Version 5.4.6-0.x and later support URL Filtering.

Version 5.4.7-1.x and later support:

- Logging of all URL requests
- URL Filtering of HTTPS web sites using Transport Layer Security Server Name Indication (TLS SNI).

UTM Offload

- Version 5.4.8-1.2 supports UTM Offload (AR4050S only).

Logging

- Version 5.4.7-1.x assigns facility local5 for all log messages generated by firewall UTM features.
- Version 5.4.7-1.x and later support firewall connection logging.

Related documents

The following documents give more information about related features on AlliedWare Plus products:

- The product's Command Reference
- Firewall and Network Address Translation (NAT) Feature Overview and Configuration Guide
- Getting Started with the UTM Firewall GUI (AR4050S, AR3050S)
- Logging Feature Overview and Configuration Guide
- Update Manager Feature Overview and Configuration Guide
- Application Awareness Feature and Configuration Overview Guide
- Triggers Feature Overview and Configuration Guide

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

- This document is not applicable to Secure VPN routers. For information about Secure VPN routers, see the AR-Series VPN Router range.

Licensing

The AR-Series UTM firewalls have two subscription licensing options for the advanced security features. The following table shows the features included in those licenses, and whether they are proxy or stream-based processes:

License Type	Features included
Base	Intrusion Prevention System (IPS)
Next-Gen Firewall (NGFW)	Application Awareness Web Control
Advanced Threat Protection (ATP)	IP Reputation Malware Protection Antivirus URL Filtering
UTM Offload	UTM Offload ■ UTM Offload requires an AT-FL-UTM-OFFLOAD-xYR subscription license. Select from the 1, 3, or 5 year options. ■ The UTM Offload feature is installed on the forwarding device (the AR4050S), rather than the offload device. ■ Licenses for the UTM features (IP Reputation, URL Filtering and Malware Protection) are installed on the forwarding device. There is no need to get new licenses for the same feature on the offload device.

For information about installing licenses, see the ‘Subscription Licenses’ section of the Licensing Feature Overview and Configuration Guide.

Feature overview

This section provides a brief description of each of the Advanced Network Protection features available on the AR-Series UTM firewalls.

- **Intrusion Prevention System (IPS)**

  IPS is a stream-based intrusion detection and prevention system that is positioned at the perimeter of a network and effectively protects the network security. It can monitor, analyse and log suspicious network activity and proactively prevent malicious threats.

  For more information about how it works, see "Intrusion Prevention System (IPS)" on page 10. To configure this feature, see "Configuring Intrusion Prevention System (IPS)" on page 35.

- **Antivirus**

  Proxy-based Antivirus provides desktop level protection to prevent known threats from passing through the network. These threats include but are not limited to: viruses, trojans, worms, malware, spyware, rootkits, keyloggers and botnets.

  For more information about how it works, see "Antivirus" on page 12. To configure this feature, see "Configuring Antivirus" on page 36.

- **IP Reputation**

  An IP address may have a good or bad reputation. An IP address earns a bad reputation when suspicious activity, such as spam or viruses originating from that address is detected. AlliedWare Plus IP Reputation provides an extensive library of IP addresses of negative reputation, with each IP address being scored, categorized by type of activity. Stream-based AlliedWare Plus IP Reputation can effectively identify and block malicious threats from entering the network. With AlliedWare Plus IP Reputation, users can decide with confidence which IP addresses are safe to allow access into the network.

  For more information about how it works, see "IP Reputation" on page 13. To configure this feature, see "Configuring IP Reputation" on page 37.

- **Malware Protection**

  Stream-based Malware Protection scans traffic as it traverses the device in real-time for known malware and blocks the traffic once a threat has been detected.

  For more information about how it works, see "Malware Protection" on page 15. To configure this feature, see "Configuring Malware Protection" on page 39.

- **Web Control**

  Proxy-based Web Control offers an easy way to monitor and control the types of websites viewed by employees. It dynamically assigns URLs to categories, and applies policy to control access to inappropriate categories of websites.

  For more information about how it works, see "Web Control" on page 17. To configure this feature, see "Configuring Web Control" on page 40.

- **URL Filtering**

  Stream-based URL Filtering provides a fast, efficient method of controlling access to websites that are known to be undesirable. It acts on a global basis and should be used when traffic is to be blocked for everyone on the blacklist, or allowed for selective URLs as configured in a whitelist.

  For more information about how it works, see "URL Filtering" on page 20. To configure this feature, see "Configuring URL Filtering" on page 47.

Updating service files

Some of these features involve a partnership with a third-party security specialist. These specialists provide algorithmic engines and pattern files to match signatures of known viruses, attack sequences and the like. The pattern files are frequently updated (some are updated multiple times a day) and made available for download on the Allied Telesis update server. The AR-Series UTM firewalls automatically checks the Allied Telesis download server for new updates to pull down.

Performance

Enabling advanced network protection features significantly increases traffic processing and therefore CPU load. For information and guidance about the performance and security implications of enabling these features, and of stream and proxy processing methods, see "Selecting a security solution" on page 23.

On the AR4050S, the **UTM Offload** feature can improve network forwarding performance by offloading some of the advanced security feature processing to another virtual or physical machine. This is automatically managed by the AR4050S. See "UTM Offload" on page 21.

Intrusion Prevention System (IPS)

This feature is supported from AlliedWare Plus version 5.4.5 or later.

AlliedWare Plus Intrusion Prevention System (IPS) inspects inbound and outbound traffic to identify and log suspicious network activity; it proactively counteracts malicious threats. IPS uses the Suricata IDS/IPS engine to monitor and compare threats against an IDS database of known threat signatures.

This section describes how IPS works. To configure this feature, see "Configuring Intrusion Prevention System (IPS)" on page 35.

AlliedWare Plus IPS monitors inbound and outbound traffic and identifies suspicious or malicious traffic which may bypass your firewall or could be originating from inside your network.

AlliedWare Plus IPS enhances your network visibility and allows you to control the network by enforcing compliance with security policy.

AlliedWare Plus IPS is stream-based and there is no delay in detection and prevention. The IPS engine monitors network traffic and detects malicious activity in real-time by comparing the threat's characteristics and patterns against known malicious threats stored in a signature database.

Once threats or attacks are detected, the IPS engine can take the following actions:

- Alert: generate a log message (default action)
- Deny: drop matching packets

The firewall is used in conjunction with the IPS engine. The IPS engine is the first line of defense and it captures the traffic before it reaches the firewall. The firewall primarily filters predetermined packets and tracks connection to ensure sessions initiated from the private network are allowed.

AlliedWare Plus IPS supports a set of built-in categories. The categories are listed below:

- checksum: Invalid checksums, e.g. IPv4, TCPv4, UDPv4, ICMPv4,TCPv6, UDPv6, ICMPv6.
- ftp-bounce: GPL FTP PORT bounce attempt.
- gre-decoder events: GRE anomalies, e.g. GRE packet too small, GRE wrong version, GRE v0 recursion control, GRE v0 flags, GRE v0 header too big, GRE v1 checksum present, GRE v1 routing present, GRE v1 strict source route, GRE v1 recursion control.
- http-events: HTTP anomalies, e.g. HTTP unknown error, HTTP gzip decompression failed, HTTP request field missing colon, HTTP response field missing colon, HTTP invalid request chunk len, HTTP invalid response chunk len, HTTP status 100-Continue already seen, HTTP unable to match response to request, HTTP invalid server port in request.
- icmp-decoder-events: ICMP anomalies, e.g. IPv6 with ICMPv4 header, ICMPv4 packet too small, ICMPv4 unknown type, ICMPv6 truncated packet, ICMPv6 unknown version.
- ip-decoder-events: IPv4 & IPv6 anomalies, e.g. IPv4 packet too small, IPv4 header size too small, IPv4 wrong IP version, IPv6 packet too small, IPv6 duplicated Routing extension header, IPv6 duplicated Hop-By-Hop Options extension header, IPv6 DSTOPTS only padding, SLL packet too small, Ethernet packet too small, VLAN header too small, FRAG IPv4 Fragmentation overlap, FRAG IPv6 Packet size too large, IPv4-in-IPv6 invalid protocol, IPv6-in-IPv6 packet too short.
- ppp-decoder-events: PPP anomalies, e.g. PPP packet too small, PPP IPv6 too small, PPP wrong type, PPPoE wrong code, PPPoE malformed tags.
- smtp-events: SMTP anomalies, e.g. SMTP invalid reply, SMTP max reply line len exceeded, SMTP tls rejected, SMTP data command rejected.
- stream-events: TCP anomalies, e.g. 3way handshake with ack in wrong dir, 3way handshake async wrong sequence, 3way handshake right seq wrong ack evasion, 4way handshake SYNACK with wrong ACK, STREAM CLOSEWAIT FIN out of window, STREAM ESTABLISHED SYNACK resend, STREAM FIN invalid ack, STREAM FIN1 ack with wrong seq, STREAM

TIMEWAIT ACK with wrong seq, stream-events TCP packet too small, stream-events TCP duplicated option).

- udp-decoder-events: UDP anomalies, e.g. UDP packet too small, UDP header length too small, UDP invalid header length.

AlliedWare Plus IPS supports the following key IPS features:

Basic Operation

- IPS protection is disabled by default
- IPS is deployed in stream mode
- IPS processing occurs before the firewall

Configuration

- All categories have a default action of alert
- The list of categories and their configured actions can be displayed
- Category actions can be configured

Antivirus

This feature is supported from AlliedWare Plus version 5.4.5 or later.

AlliedWare Plus™ Antivirus provides the first line of defense against a wide range of malicious content, guarding against threats, such as viruses, Trojans, worms, spyware and adware. In addition to protecting the local network by blocking threats in inbound traffic, it also prevents compromised hosts or malicious users from launching attacks. This is essential for protecting your organization's reputation.

The scanning is performed by the Kaspersky Antivirus engine. The signature database used by the engine containing known threat patterns is regularly updated.

This section describes how AlliedWare Plus™ Antivirus works. To configure this feature, see "Configuring Antivirus" on page 36.

How antivirus works

AlliedWare Plus™ Antivirus uses proxy-based detection to scan traffic. Proxy-based detection can provide the best detection rate. Proxy-based detection looks for known patterns in the traffic, using signature analysis. A signature database containing a list of known threat patterns is kept up-to-date to ensure the effectiveness of the detection. Heuristics analysis is also used to look for suspect

behaviors of executable code and malware. Heuristics analysis can therefore detect unknown viruses as well as known polymorphic malware, which cannot be identified by using signature analysis.

When AlliedWare Plus Antivirus detects a virus, it blocks HTTP responses.

AlliedWare Plus Antivirus provides the following features:

- Scans HTTP responses
- Supports Kaspersky Antivirus
- Blocks HTTP responses in which a virus has been detected
- Scans packed, compressed or encoded object files
- Scans objects up to 10MB in size
- Scans 100MB of objects concurrently
- Extracts nested files up to 3 levels deep
- User configurable action upon scan failure
- User configurable action when any limit is exceeded

IP Reputation

This feature is supported from AlliedWare Plus version 5.4.5 or later.

IP Reputation uses Proofpoint's Emerging Threats (ET) Intelligence to identify and categorize IP addresses that are known sources of spam, viruses and other malicious activity. This can improve the success of Intrusion Prevention System (IPS) by reducing false positives. It provides an extra variable to the prevention decision, which allows rules to be crafted to drop packets only if the reputation exceeds a chosen threshold.

With real-time threat analysis, and regular updates to reputation lists, IP Reputation delivers accurate and robust scoring, increasing the precision with which intrusion protection policies can be applied.

This section describes AlliedWare Plus™ IP Reputation and its configuration. To configure this feature, see "Configuring IP Reputation" on page 37.

How IP Reputation works

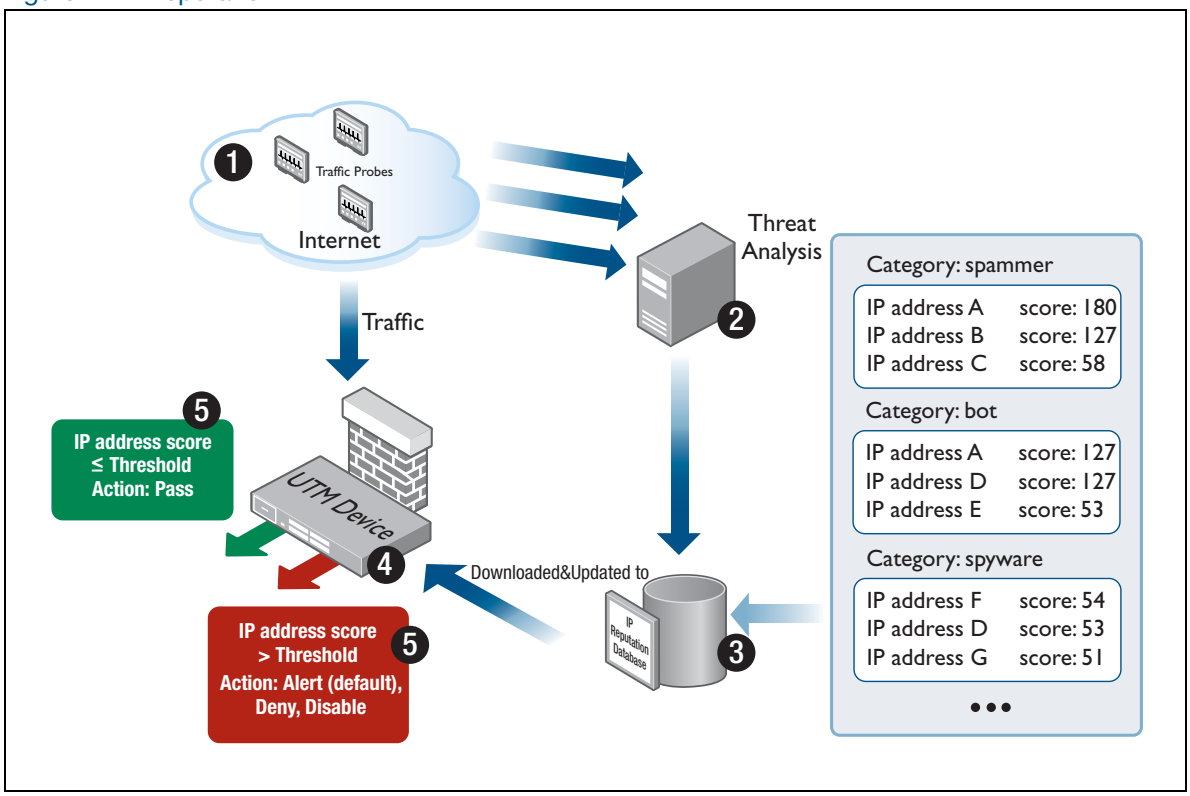
AlliedWare Plus IP Reputation uses categories, which is a grouping of criteria, to classify the nature of a host's reputation. For example, IP addresses associated with questionable gaming sites will be categorized as OnlineGaming.

A host may have a reputation in multiple categories. A score is rated for each IP address and the score is used to compare to a threshold to determine the action taken upon the IP address.

The reputation of a host changes dynamically. A host may degrade its reputation due to active engagement in unwanted activity, for example, the host launches a spam campaign. Conversely, absence of malicious activity will result in improved reputation.

AlliedWare Plus IP Reputation provides comprehensive IP reputation lists through Proofpoint's signature database. Proofpoint provides an IP Reputation database downloaded to the device. The database is updated regularly and can deliver the latest information and scores of identified and potentially harmful IP addresses. Figure 1 shows how AlliedWare Plus IP Reputation works.

Figure 1: IP Reputation



AlliedWare Plus IP Reputation delivers accurate and robust scoring, ensuring that malicious IP addresses are identified and strong local policies can be carried out with confidence.

AlliedWare Plus IP Reputation provides the following key features and benefits:

- Significantly enhances the ability of device to perform detection and intrusion prevention
- Advanced algorithm to reduce the number of false positives
- IP Reputation is disabled by default
- Supports Emerging Threats (ET) Intelligence™ Rep List of IPv4 addresses, categories and reputation scores provided by Proofpoint.
- Accurate and detailed information on 100,000+ IP addresses that have been identified as the source of spam, viruses, and other malicious activity
- Over 30 IP Reputation categories
- Real-time threat analysis

- Checks both the source and destination IP addresses in the packet
- User configurable action for each IP Reputation category
- Alert action logs the packet and allows the packet to continue
- Drop action logs the packet and silently discards the packet
- Disable action ignores the IP Reputation category
- The default action for each category is alert
- A whitelist to override IP Reputation provider lists and allow up to 128 specified IP addresses.

IP Reputation whitelist

Sometimes one of the IP Reputation providers adds an address to their list that you wish to allow access to in spite of its bad reputation. For example:

- A hosting site uses an IP address for a wide range of domains, some of which have been identified as ‘bad’, but most of which are acceptable. A user may wish to access the acceptable domains.
- An address may have been subject to some malicious activity and gained a ‘bad’ reputation. Once the activity has been resolved, a user may urgently need to regain access to the site before the address's reputation has been restored.

You can override the IP Reputation provider lists for up to 128 specified IP addresses by adding them to the whitelist. IP Reputation will allow traffic from IP addresses that are in the whitelist regardless of whether they appear in a provider list.

Note that there are risks associated with whitelisting an address that has been blacklisted by an IP Reputation provider—it removes the IP Reputation protection for this IP address.

Any other security features enabled on the device are still applied, even though a flow might match an IP Reputation whitelist address.

For more information, see "Configuring IP Reputation" on page 37 and "IP Reputation log messages" on page 70.

Malware Protection

The AlliedWare Plus Malware Protection feature is supported from AlliedWare Plus version 5.4.5 or later.

Stream-based Malware Protection scans traffic as it traverses the device real-time for known malware and blocks the traffic once a threat has been detected.

AlliedWare Plus Malware Protection provides the first line of defense against a wide range of malicious content. In addition to protecting the local network by blocking threats in inbound traffic, it

also prevents compromised hosts or malicious users from launching attacks. This is essential for protecting your organization's reputation.

Stream-based high performance anti-malware technology is employed 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 including web, email and instant messaging.

The Kaspersky anti-malware signature database is updated regularly to keep on top of the latest attack mechanisms.

This section describes how AlliedWare Plus™ Malware Protection works. To configure this feature, see "Configuring Malware Protection" on page 39.

How Malware Protection works

AlliedWare Plus Malware Protection uses stream-based detection to scan traffic. A stream engine is used to extract Layer 7 payload from the stream of traffic passing through the device. The stream engine looks for known patterns in the traffic, using signature analysis. A signature database containing a list of known threat patterns is kept up-to-date to ensure the effectiveness of the detection.

AlliedWare Plus Malware Protection provides the following features:

- Detects and blocks known malware by inspecting the traffic stream passing through the device real-time.
- Scans the Layer 7 payloads of packets intercepted by the stream engine
- Supports updating resource files
- Supports Kaspersky Safestream II Malware byte signatures

Note: AlliedWare Plus Malware Protection also provides MD5 scanning of HTTP and SMTP. Malware Protection uses stream-based scanning to compare the MD5 hash to values provided by the Kaspersky Safestream II list of malicious objects. Streams that match the MD5 hash of known malware will be blocked. POP and IMAP do not use the MD5 hash, and are instead scanned by the byte-stream process described above.

Web Control

The Web Control feature is supported in version 5.4.5 or later.

AlliedWare Plus Web Control provides a new level of service for business productivity management, compliance and web security. It offers an easy way to monitor and control the types of websites viewed by employees. It stops staff members visiting inappropriate websites that:

- Drain their productivity
- Contain questionable content
- Are bandwidth intensive and hence put a strain on resources
- Pose potential security threats to the organization

Web Control provides dynamic URL coverage, assigning websites or pages into around 100 categories, and allowing or blocking website access in real-time.

Once a particular URL has been categorized, the result is cached in the device so that any subsequent web requests with the same URL can be immediately processed according to the policy in place.

The Web Control process uses Digital Arts' active rating system.

This section describes AlliedWare Plus Web Control. To configure this feature, see "Configuring Web Control" on page 40.

How Web Control works

Integrated with Digital Arts' Active Rating System (ARS), AlliedWare Plus Web Control provides comprehensive and dynamic website coverage with high accuracy of categorization. AlliedWare Plus™ Web Control is capable of accurately assigning millions of websites or pages into around 100 categories and allowing or blocking website access in real-time.

AlliedWare Plus Web Control provides the following features:

- Categorizes a vast number of websites in multiple languages
- Covers millions of the most relevant websites in around 100 categories
- Supports multiple categorizations for a single website
- Supports management and configuration of categories, rules and website categorization provider

AlliedWare Plus Web Control uses a website classifier engine and caching mechanism to filter HTTP and HTTPS traffic.

When an HTTP request passes through the device, the associated TCP session transporting the HTTP data is proxied. The embedded URL of the website is intercepted and sent to the website classifier engine to retrieve the category the website belongs to.

In the case of HTTPS, if the server name indicator (SNI) is present in the TLS handshake exchange, it is extracted and sent to the URL classifier engine for categorization. The SNI only includes the hostname of the website, not the full path of the URL requested. If no SNI is present, the categorization will be based on the destination IP address of the request.

The SNI field is contained within the Client Hello message supplied during the TLS handshake when a client Web browser first attempts to access a secure HTTPS server website. The SNI information is supplied in clear-text, and represents the domain part of the URL of the HTTPS request. The SNI field is used by secure Web servers hosting multiple secure websites, and allows a Secure Web server with a single public IP address to host multiple websites. It allows the Secure Web Server to supply the correct digital certificate containing the correct domain name(s) to the requesting web browser client, so that the negotiation of the encrypted connection to Website can proceed.

To categorize the website, the website classifier engine queries Digital Arts' constantly updated Active Rating System (ARS) which contains about 100 pre-defined categories. The categorization provider then returns the category of the website. The website classifier engine also queries the custom static engine, which can be customized to suit individual business needs. The custom categorization is used in preference to, and can, override Digital Arts categorization. This means if a website matches match criteria from custom categories, then the website will not be sent for categorization by Digital Arts.

Once the website has been categorized, the device can filter the website according to a set of rules defined per category. The user is unable to visit the blocked website and will get a notification page if the website is blocked. Conversely, the user can get the resulting page from the website if the website is allowed.

Categorized websites are cached in the device. The device can check its local cache for a matching website against the HTTP or HTTPS request passing through it.

The Web Control process operates by determining the URL to which a session is destined, and consulting with a cloud-based server to check whether this URL may or may not be accessed.

If all of the traffic traversing the device consists of new HTTP 1.1 Get requests, and proxy-based Web Control is enabled, then TCP connections need to be formed and proxied for each connection request, and the URLs in the connection requests will be accumulated into bulk categorization requests, and then sent off to the cloud-based URL categorization service.

And so various external factors, such as

- latency of the Internet
- response time of the categorization servers in the Cloud
- processing of responses

will slow down the overall connections per second for traffic processed via this proxy service.

Figure 2: Web Control block action

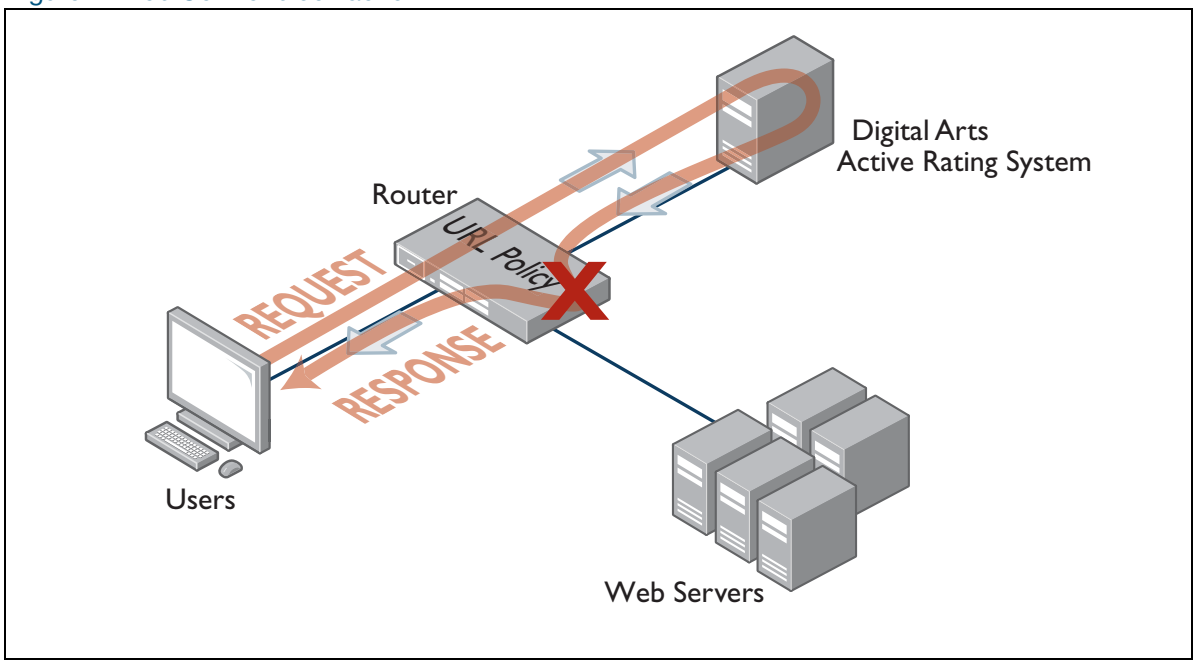
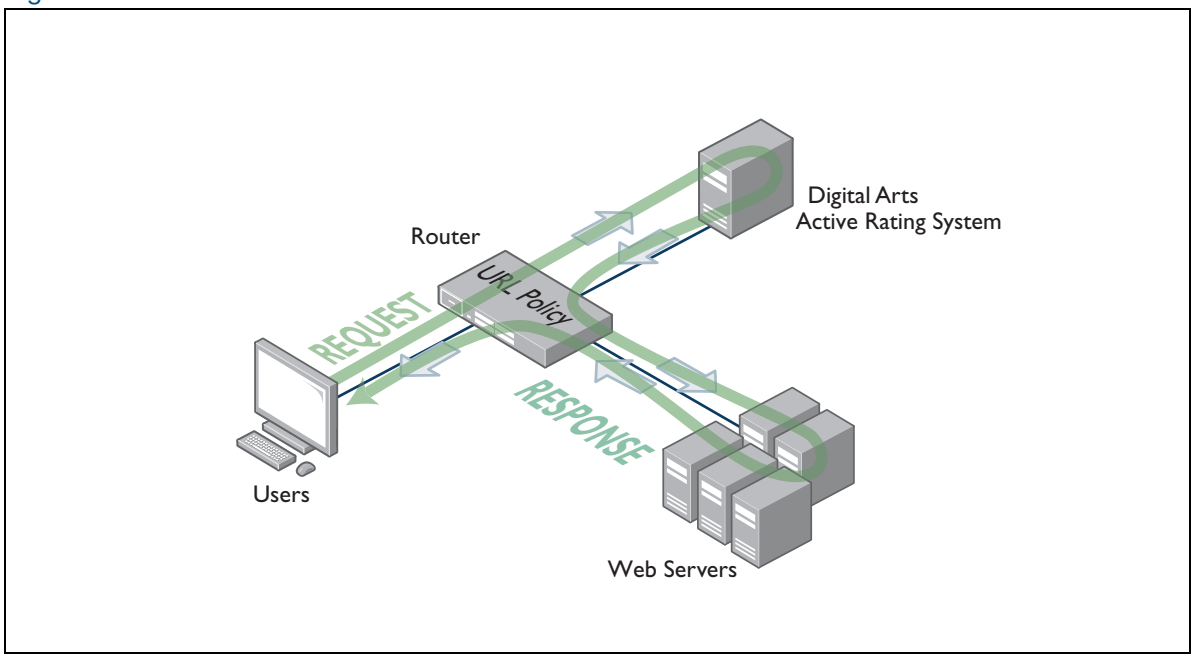


Figure 3: Web Control allow action



URL Filtering

The URL Filtering feature is supported in AlliedWare Plus version 5.4.6 or later.

URL Filtering provides an option for controlling access to website URLs.

Access to particular websites can be allowed (whitelist) or blocked (blacklist), providing businesses with simple website access management.

URL Filtering blocks all HTTP and HTTPS access to a list of websites or portions of web sites.

- A **whitelist** is a list of URLs that are known to comply with organisational policies.
- A **blacklist** is a list of URLs that are known to violate organisational policies.
- **Kaspersky** is a subscription-based service that classifies websites among dozens of pre-defined categories of content that will not comply with some organisations' policies.
  If you subscribe to the Kaspersky service, you can create additional blacklists to block extra URLs or whitelists to allow URLs that the Kaspersky service blocks.

The white and black lists can be from two sources, which can be used simultaneously. You can specify a short list of websites to control access to (up to 1000 blacklist and 1000 whitelist rules), and/or subscribe to the blacklist service offered by Kaspersky.

If Kaspersky-sourced lists are being used, the device will automatically download list updates from the Allied Telesis update server.

URL Filtering provides a fast efficient (stream-based) method of blocking web traffic from locations that are known to be undesirable. It acts on a global basis and should be used when traffic is to be blocked for everyone on the blacklist, or allowed for selective URLs as configured in a whitelist.

This contrasts with Web Control, which has finer grained control as URLs are proxied and categorized and access to websites are controllable on a per-category and per-firewall entity basis. And since the Web Control service is proxy-based there is increased latency compared to the (stream-based) URL Filtering service.

It is possible to use Web Control and URL Filtering at the same time. Connections must be permitted by both URL Filtering and Web Control in order to be allowed through the device. A block action in either feature will cause a failure to load the web page.

How Does URL Filtering Work?

URL filtering works by sniffing traffic as it traverses the AR-Series firewall and detecting the HTTP and HTTPS transactions that are taking place. These transactions are then processed, and when an HTTP Request is detected, the URL in question is compared against the whitelists (if any) and blacklists configured.

In AlliedWare Plus version 5.4.7-1 and later, the URL Filtering feature includes the ability to filter SSL-protected websites. For these HTTPS requests, the original URLs are encrypted, therefore they

are not visible for processing. Instead the domain name specified in TLS SNI (Transport Layer Security Server Name Indication) for each HTTPS request is used as the URL for matching.

The SNI field is contained within the Client Hello message supplied during the TLS handshake when a client web browser first attempts to access a secure HTTPS server website. The SNI information is supplied in clear-text, and represents the domain part of the URL of the HTTPS request. The SNI field is used by secure web servers hosting multiple secure websites, and allows a secure web server with a single public IP address to host multiple websites. It allows the secure web server to supply the correct digital certificate containing the correct domain name(s) to the requesting web browser client, so that the negotiation of the encrypted connection to the website can proceed.

- If a whitelist match is found, the traffic will not be blocked (it will be logged if configured to do so).
- If a blacklist match is found, the request will be dropped (and logged if configured to do so)—it will not be forwarded to the destination.
- If neither whitelist nor blacklist matches are found, the traffic will not be blocked.
- Pattern checking stops as soon as a match is found. So if traffic matches any configured whitelist, then it will be allowed though the device. Or if traffic matches any configured blacklist then it will immediately be blocked. That same traffic will not be subsequently checked against additional whitelists or blacklists.

For information about how to use URL Filtering, see "Configuring URL Filtering" on page 47.

UTM Offload

The UTM Offload feature is supported in version 5.4.8-1.2 or later on the AR4050.

How does UTM Offload work?

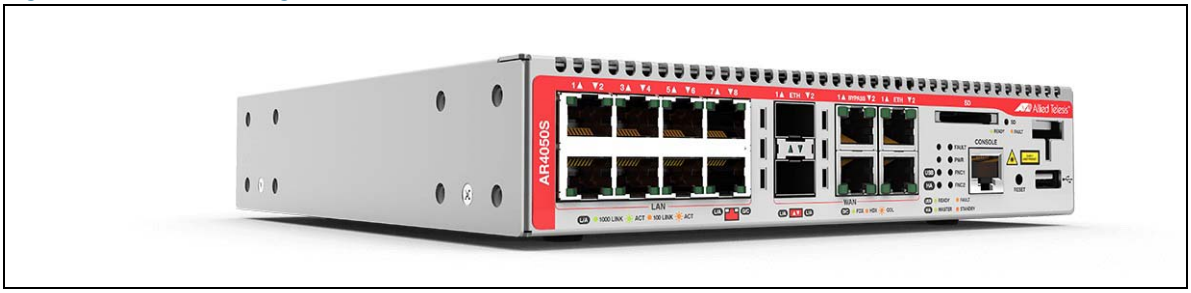
UTM Offload enables some security and threat protection features (IPS, IP Reputation, Malware Protection, and URL Filtering) to be offloaded to a secondary physical or virtual machine that is automatically managed by the AR4050S.

UTM Offload can up to double WAN connection throughput when using these features for real-time threat protection.

The forwarding device—AR4050S:

- boots and manages the offload device.
- configures the offload device.
- presents the status of all features, whether being processed locally on the AR4050S, or on the offload device.
- uses Service Function Chaining (SFC) methodology to send received traffic to the offload device for processing.
- gets the result of that processing back from the offload device and continues packet processing as normal.

Figure 4: The forwarding device—AR4050S



Which UTM features can be Offloaded?

Security features are configured as normal on the AR4050S device, but whenever UTM Offload is enabled, the following advanced threat protection features are all offloaded, if they are configured:

- IPS
- IP Reputation
- Malware Protection
- URL Filtering

The AR4050S automatically manages the offload device for you. You don't need to configure the offload device, as configuration and the status of all features is presented the same whether offloaded or not.

See also "Setting up and configuring UTM Offload" on page 55.

Selecting a security solution

This section describes in more detail the following:

- "Proxy versus stream-based security processing" on page 23
- "Packet flow architecture" on page 25, including UTM CPU processing requirements
- "Selecting a UTM firewall" on page 28, provides information to guide you in selecting a suitable firewall for your network requirements. This includes performance versus security guidelines.
- "URL Filtering or Web Control?" on page 31
- "Antivirus or Malware Protection?" on page 32
- "Firewall/NAT rules, entities and performance" on page 33

Proxy versus stream-based security processing

There are two types of scanning processes used by these advanced security features—proxy-based processes and stream-based processes.

Both types of processes focus on delivering secure and robust network protection via application-level inspection and scanning. However, each works in a different way with a distinctly different impact upon network latency and performance.

- Proxy-based processes are those in which the security device acts as a proxy for the data's destination. The security device will receive and reconstruct a whole file, and examine it for threats, before passing it on to the eventual destination.

  Proxy-based features on AR-Series firewalls are: Antivirus and Web Control.

- Stream-based processes are those in which packets are examined in real-time as they pass through the device. When a threat is detected, the data is then blocked.

  The stream-based features on AR-Series firewalls are: IPS, Malware Protection, IP reputation, and URL Filtering.

Proxy-based processing

Proxy-based engines act as an intermediary; they terminate each session from a client, establish an associated session to the target server, and monitor the associated session state in a transparent manner. They perform threat scanning by extracting the stored object data that is being transported in a data stream, and matching that data against various known threat signatures contained in the threat signature database files.

Large amounts of memory and system CPU resources can be used performing object file extraction, packet re-ordering and re-assembly, scanning, and object file re-transfer. Also, proxying the TCP session reduces the overall data throughput.

By the nature of its operation, proxy-based scanning provides the best detection, and is equivalent to desktop computer based antivirus systems. However, it is also more memory and CPU resource-intensive, and therefore inherently slower than stream-based scanning.

A single-user connection to a single website can potentially involve managing multiple simultaneous sessions.

Stream-based processing

In contrast, stream-based scanning processes data simply in the order that the packets come along.

Stream-based engines are designed for maximum throughput with minimum latency, as they do not inherently suffer from the overhead of having to proxy connections, and do not have to wait to receive, store, and scan entire objects contained in data transfers prior to forwarding them across a security boundary.

Data is scanned on a layer-by-layer approach as it arrives. It is deeply scanned against various threat signatures in real-time—from comparing source and destination IP addresses against an IP Reputation list (if IP Reputation is configured), through Layer 5 information (such as HTTP/1.1 Get requests embedded in HTTP packets), through to embedded application data within the stream, such as a Torrent or Skype, and so on.

There is inherently slightly less protection using this approach compared to proxy-based protection, as data is allowed to pass through the security boundary up until the point that a threat is detected, at which point it is blocked.

Stream-based security scanning engines consume noticeably less system memory and CPU processing power compared to proxy-based engines. This is because entire files traversing the security device do not need to be individually downloaded. Also, file fragments do not need to be re-assembled prior to scanning and subsequent fragmentation and forwarding.

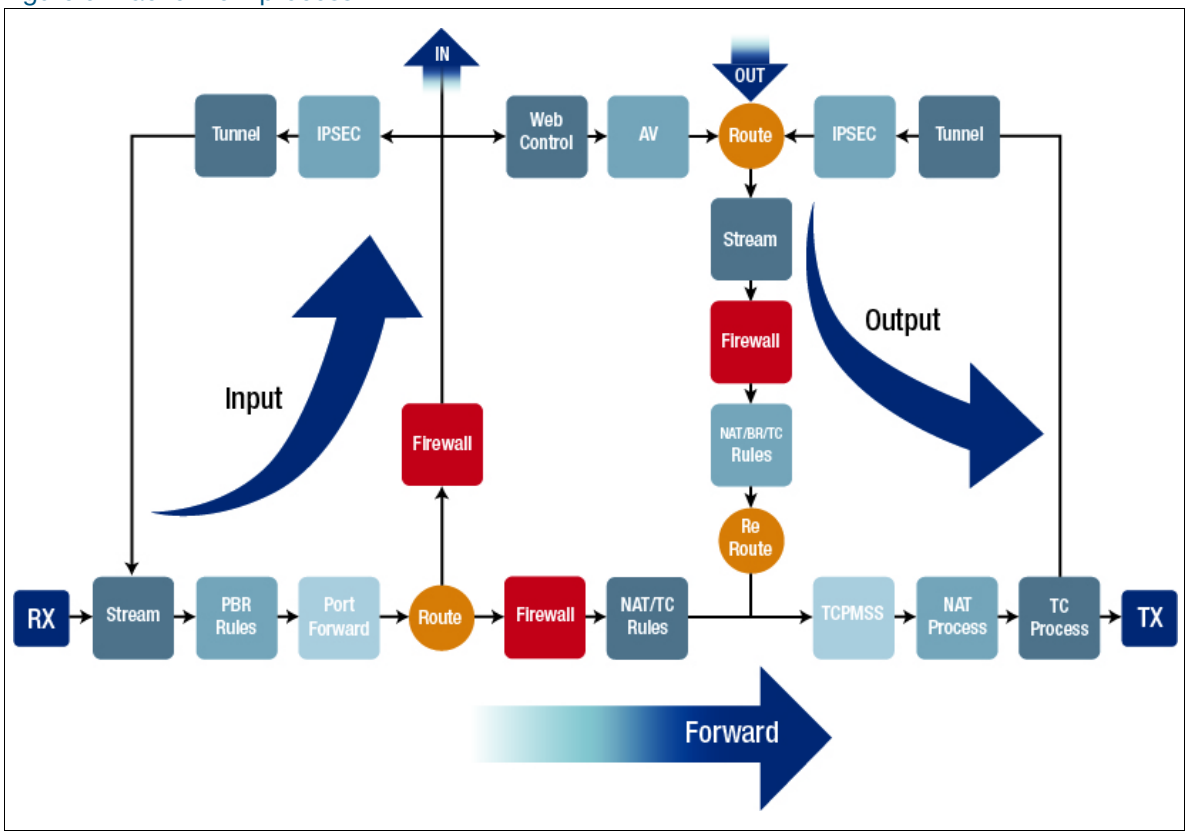
The stream-based features supported by AlliedWare Plus/ AR-Series firewalls are:

- IPS
- Malware Protection
- IP reputation
- URL Filtering.

Packet flow architecture

When protecting private networks from the Internet, packets are most commonly forwarded by the firewall. Network packets pass through the firewall using a fixed set of processing steps as illustrated in the diagram below:

Figure 5: Packet flow process



Before you configure different firewall features, it is important to understand the packet processing order.

This is the packet processing order:

1. Packets are received on one of the firewall's physical interfaces (LAN or WAN) and follow the **Forward** path shown in Figure 5 on page 25.
2. Stream processing always happens straight after the packet is received on the physical interface. Stream processing is DPI, IPS, IP Reputation, Malware Protection, and URL Filtering.
3. Policy Based Routing and Port Forwarding is applied before packets are routed to their destination.
4. After routing, firewall and NAT rules are matched.
5. Finally, NAT processing and traffic control is applied before packet transmission.

The other two important processing packet paths in the firewall are **Input** and **Output**.

- The **Input** path is applied to packets that are destined to the firewall itself:

  Along with management and network protocol packets received by the firewall, this also includes tunnel packets for which the firewall is the tunnel decapsulation endpoint and proxied packets where the firewall terminates both sides of HTTP(S) connections (web-control and antivirus).

- The **Output** path is applied to packets generated by the firewall itself:

  Along with management and network protocol packets generated by the firewall, this also includes tunnel packets encapsulated by the firewall and proxied packets where the firewall terminates both sides of HTTP(S) connections.

  Note that because packets generated by the firewall were never received on a physical interface, stream processing is also applied first in the **Output** path.

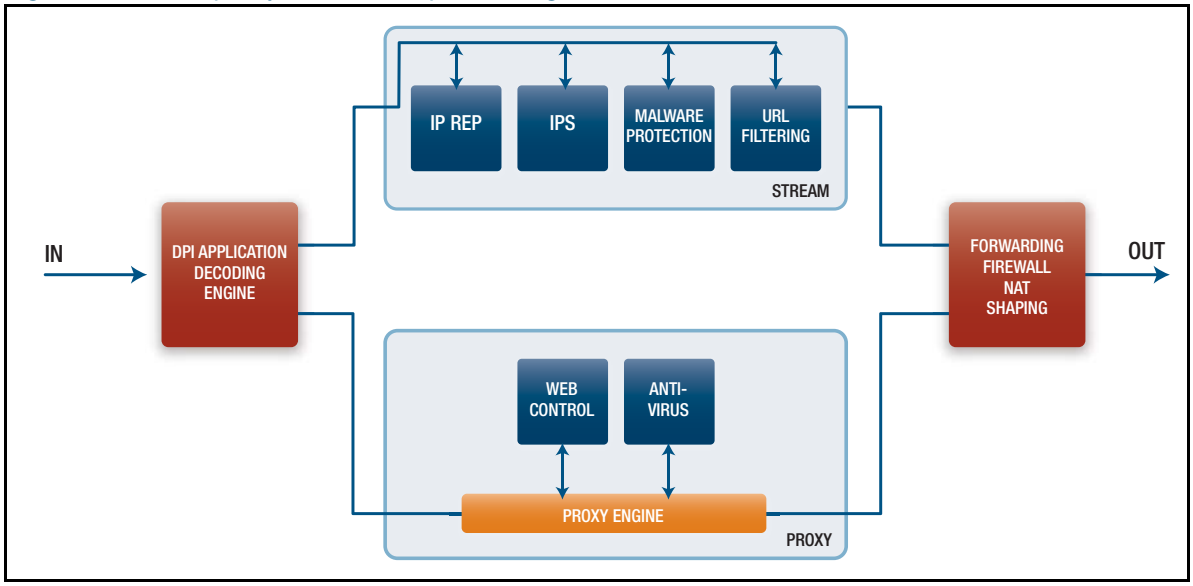
Be aware that when tunnel packets are encapsulated or decapsulated they skip stream processing the second time around unless **tunnel security-reprocessing** is enabled in a configuration.Pacekt file.

Basic security architecture

Stream-based features are capable of performing high-throughput low-latency threat protection. However, as discussed above, when proxy-based features are also enabled, performance can decrease and latency will increase as the proxy connections are formed, and data is processed and completely re-scanned through each security feature in turn. This can lead to valid concerns around effects on performance, connections per second, latency, and so on as each security feature is used.

Firstly, let's take a look at the basic security architecture.

Figure 6: Firewall proxy and stream processing order



DPI

As data ingresses the firewall, it is first identified by the DPI application decoding engine if application awareness feature is enabled. If selected, the inbuilt DPI engine contains a static library of a around a 100 or so common Internet-based applications that it is capable of identifying. However, if the Procera Networks' Network Application Visibility Library (NAVL) is selected as part of Application Awareness feature then the number of identifiable applications added and stored in the DPI engine library increases to many thousands.

Firewall, NAT, Traffic Shaping and SD-WAN policy-based routing rules can be optionally configured to perform actions based on the application traffic identified via DPI.

DPI is **not** required for the proxy or stream-based security functions described in this guide to operate.

For more information about Application Awareness and DPI (Deep Packet Inspection), see the Application Awareness Feature and Configuration Overview Guide.

Stream and proxy engines

Once the application data is identified, it is processed via either the stream or proxy engine forwarding path, and whether both stream-based and proxy-based security features are enabled.

If both stream and proxy-based security features are simultaneously enabled, then data will initially be processed via the stream engine, and will subsequently be processed via the proxy engine.

All of the stream-based security features operate as a series of rule-sets within the **Suricata** Stream engine. As each stream-based security feature is enabled, an associated set of rules is enabled and applied in the stream engine. IP data is only processed by the security application rule-sets that it matches. For example, an HTTP/1.1 Get request containing a URL would be processed via the URL Filtering rule-set within the Suricata engine, whereas an IP data stream not containing a URL would not be matched against the URL Filtering rule-set.

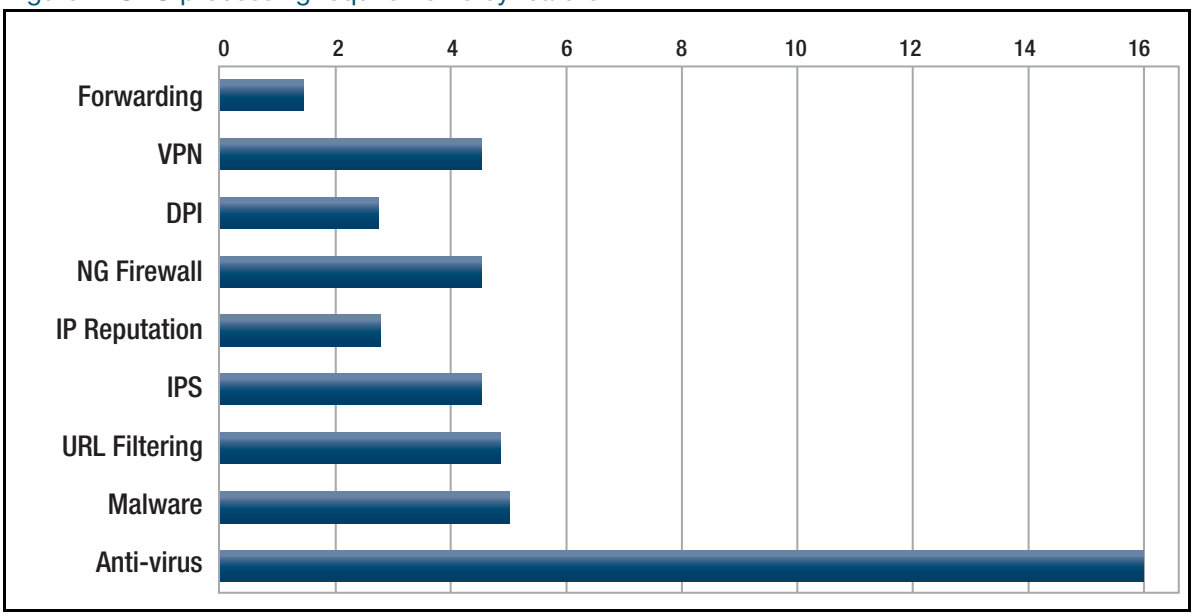
UTM CPU processing requirements

As each security function is enabled, the additional processing cost results in less CPU processing cycles being available to be dedicated to packet forwarding, so therefore overall throughput can be reduced.

The key point is that all packets are processed in software within the device and that security functions require much more processing per packet/byte than just forwarding a packet.

This diagram below is indicative only, based on test conditions, and highlights the number of CPU cycles that may be required for various functions.

Figure 7: CPU processing requirements by feature



Updates By default, a UTM firewall regularly checks for updates, and downloads and installs any updates available. In general, this will suit most networks. However, some of the resources can be large, so the process of downloading and installing them adds extra load to the firewall. In some busy networks, this may affect the general performance of the network while it is updating. If this is negatively affecting your network, you could consider disabling some or all of the automatic updates and scheduling regular updates (**update *<resource-name>* now** command, see the Update Manager Feature Overview and Configuration Guide) during off-peak times by using a time trigger (see the Triggers Feature Overview and Configuration Guide).

Selecting a UTM firewall

Use this section to select the appropriate UTM firewall router platform to meet your network security and forwarding performance requirements.

Each network is different, so we recommend fully auditing your current network application traffic flows, and assess your network security and performance requirements as part of your platform selection process.

Routers process packets in the CPU. As software features are enabled, they can consume additional CPU resources, which can reduce overall packet forwarding throughput.

This section provides estimates of performance impacts that the following UTM firewalls will experience as various combinations of security features are enabled, to aid selection.

UTM FIREWALL	
AR3050S	UTM Firewall
AR4050S	UTM Firewall

Usage scenarios

When positioning the UTM firewall in the network, it is very important to carefully consider what role it will take. You need to consider which feature combinations and protocols will be enabled on the device and how many users there will be.

This section describes five common use-cases:

- **VPN Aggregation**—Internet access protected by Stateful Inspection Firewall with Site-to-Site Virtual Private Networks to remote offices and remote access via SSL-VPN.
- **Application-Aware Firewall and Web Control**—Manage application use with the Deep Packet Inspection (DPI) Firewall, where policies are based on users and applications rather than IP addresses, ports and protocols. Also manage user access to websites with Web Control.
- **Real-Time Threat Protection**—High throughput stream-based packet scanning to provide real-time threat protection based on up-to-date threat data.
- **High Security Gateway**—Comprehensive desktop level protection that blocks viruses, trojans, worms, rootkits, spyware, and adware at the gateway to the network.

Note the differences between the following two scenarios:

1. **Real-Time Threat Protection** is a good option for customers wanting good protection without compromising throughput. It uses a combination of URL Filtering and a stream-based scanning engine to rapidly detect most common threats.
2. **High Security Gateway** offers the security of a comprehensive desktop level virus-scanner, but with increased latency. With this solution, all HTTP traffic associated with websites is proxied. Traffic is fully downloaded and scanned before passing through the security gateway to the internal hosts. This method of security is inherently more secure than stream-based scanning. However, this reduces the number of concurrent connections per second and the recommended number of users.

Features required for each scenario

The following table shows the features to use to support each scenario, and the licenses that contain each feature:

	LICENSE	VPN AGGREGATION	APPLICATION-AWARE FIREWALL AND WEB CONTROL	REAL-TIME THREAT PROTECTION	HIGH SECURITY GATEWAY
VPN	Unlicensed	Yes	Optional	Optional	Optional
Application Control	Advanced firewall license	-	Yes	-	-
Web Control		-	Yes	-	-
URL Filtering		-	-	Yes	-

	LICENSE	VPN AGGREGATION	APPLICATION-AWARE FIREWALL AND WEB CONTROL	REAL-TIME THREAT PROTECTION	HIGH SECURITY GATEWAY
IP Reputation	Advanced threat protection license	-	-	Yes	-
Malware Protection		-	-	Yes	-
Antivirus		-	-	-	Yes
UTM Offload[a]	UTM Offload	-	-	Optional	-

a. UTM Offload enables the router to offload processing of IP Reputation, Malware Protection, URL Filtering and IDS/IPS to a secondary physical or virtual machine that is automatically managed by an AR4050S. It is supported from version 5.4.8-1.2 onwards on AR4050S only. Use of UTM offload is not recommended with Web Control or Antivirus.

Performance guidelines

When deciding which scenario best matches your requirements, consider:

- The number of concurrent users.
- Other network functions or services the UTM Firewall is performing (for instance, BGP or AMF Master), as these could affect the available CPU resources.
- Whether to configure UTM Offload, which can potentially double WAN connection throughput for real-time threat protection.
- The level of protection your network really requires. While enabling all licensed features may give the strongest protection to the network, it will also give it the lowest throughput. Therefore, please consider the needs of your network carefully before selecting a specific platform and security feature combination.

The following table offers some guidelines for estimating the performance each UTM Firewall will experience under each scenario described above.

A	VPN AGGREGATION	APPLICATION-AWARE FIREWALL AND WEB CONTROL	REAL-TIME THREAT PROTECTION	HIGH SECURITY GATEWAY
Key to the table	■ Firewall throughput (UDP) ■ IPsec throughput (UDP) ■ Number of tunnels ■ Number of users[b]	■ Throughput (Enterprise Traffic Mix[c]) ■ Connections per second (TCP) ■ Number of flows ■ Number of users	■ Throughput (Enterprise Traffic Mix) ■ Connections per second (TCP) ■ Number of flows ■ Number of users	■ Throughput (HTTP) ■ Connections per second (TCP) ■ Number of users
AR3050S	■ 800 Mbps ■ 400 Mbps ■ 100 tunnels ■ 50 users	■ 83 Mbps ■ 150 connections per second ■ 10k flows ■ 20 users	■ 79 Mbps ■ 1000 connections per second ■ 33k flows ■ 20 users	

[a]	VPN AGGREGATION	APPLICATION-AWARE FIREWALL AND WEB CONTROL	REAL-TIME THREAT PROTECTION	HIGH SECURITY GATEWAY
AR4050S	■ 2000 Mbps ■ 1000 Mbps ■ 256 tunnels ■ 200 users	■ 128 Mbps ■ 450 connections per second ■ 22k flows ■ 100 users	■ 200 Mbps ■ 3000 connections per second ■ 90k flows ■ 50 users	■ 250 Mbps ■ 400 connections per second ■ 10 users
AR4050S with UTM Offload			■ 660 Mbps ■ 1300 connections per second ■ 90 flows ■ 250 users	

a. Actual performance may vary depending on network conditions and active services.
b. The number of users is a conservative estimate. When calculating the estimate, we assumed all users have a high level of **simultaneous** Internet activity. The actual number of attached workstations connecting via the UTM Firewall could be higher if not all are simultaneously and actively sending traffic.
c. The Enterprise Traffic Mix throughput figures are based on laboratory testing to simulate “real world” applications and web traffic associated with a small-to-medium sized business (SMB) enterprise. This test involves a mix of UDP, TCP and HTTP/HTTPS data types.

URL Filtering or Web Control?

URL Filtering and Web Control are two services that govern which websites users are allowed to access. The two services work in quite different ways, and therefore have different effects on performance.

URL Filtering

URL Filtering is a stream-based service. URLs are filtered using either a user-defined list (in which up to a thousand blacklist and/or whitelist URL entries can be configured), or a downloadable list (consisting of many thousands of known malicious website URLs) that can be **frequently updated**, obtained via Subscription.

URLs are extracted from GET, HEAD, POST, PUT, and DELETE HTTP requests for matching against white lists and black lists in real-time. URL Filtering might be used within an organization wanting to prevent access to a specific (user-defined) list of URLs via a low-latency stream-based service. Network administrators are allowed to statically configure any number of their own black-listed and white-listed URLs.

Web Control

Web Control is a **proxy-based** web-categorization service. This feature uses an external categorization service to provide **real-time protection**. The list of malicious and phishing websites is constantly updated in real-time by the categorization service provider. The AR-Series firewall caches the categorization responses from the external categorization service. This avoids unnecessary and repeated external lookups to URLs and improves performance.

An additional set of 50 user-defined category match criteria can be stored locally on the AR-Series firewall to provide specific access to a small list of user defined URLs for which an organization's access policy may differ to that of the external categorization service. For example, this allows an

organization to manually override and allow access to a URL that might otherwise be blocked by the external categorization service.

Summary

By its nature, **web control** provides **maximum protection** against malicious and phishing websites, as the cloud-based categorization lists are being constantly updated in real-time. But this comes at the expense of the latencies involved with a proxied service. URL Filtering, on the other hand, involves much less session latency, but involves a slightly larger risk of exposure to threats, as list updates occur less rapidly.

If both features (Web Control and URL Filtering) are simultaneously enabled, then URLs will be checked first via URL Filtering lists, then will subsequently be categorized via Web Control. Either feature can block a connection. If a connection is blocked by one feature, the decision cannot be over-ruled by the other feature.

While this provides a very high level of URL checking, it comes at the cost of additional session latency. The decision to operate both URL Filtering and Web Control needs to be carefully considered. Such a combination should only be deployed if the need for comprehensive URL checking takes priority over Internet-access performance.

In most situations, there is minimal benefit in using both features simultaneously.

Antivirus or Malware Protection?

Both the Malware Protection and Antivirus features perform a very similar service— detecting and blocking malicious code contained in content arriving from the Internet.

Antivirus

Antivirus is a proxy-based service that downloads an entire file object before scanning it to see if it contains an embedded virus and then allows or blocks it.

As part of this proxy behavior, if malicious content is detected, the AR-Series firewall is able to generate the ‘Access Denied’ HTTP web page and serve that to the client's web browser, so the user is explicitly notified that they have strayed onto an undesirable website.

Malware Protection

Malware Protection is a stream-based service, and so inherently introduces slightly less latency than Antivirus. This is because Antivirus does not forward a piece of content until it has been fully downloaded and scanned, whereas Malware Protection scans content as it passes through, so that the data is not held up waiting for the download to complete. As soon as Malware Protection detects a threat within a stream of data, it immediately stops forwarding any more of the stream.

However, Malware Protection does not have the ability to serve an ‘Access Denied’ notification web page to the user’s browser. The user experience is simply that the download of a page stalls until it eventually times out.

Not together

If both Antivirus and Malware Protection are simultaneously running in the AR-Series firewall, then typically Malware Protection would detect (and drop) any infected data before Antivirus has a chance to. This is because Malware Protection checks the data as it is arriving, whereas Antivirus does not scan a piece of content until it has all been downloaded.

Note, also, that if both services are operating, then the ‘Access Denied’ web page will not be served to the user’s browser if Malware Protection detects the infection and Antivirus does not get a chance to see the infection.

Choose one

In general, a network administrator should choose to use one of Malware Protection or Antivirus, rather than both.

Malware Protection should be chosen if maximum throughput (with good security protection) is a key business requirement for the device. Alternatively, the network administrator should consider use of the Antivirus feature if maximum protection (at the cost of slightly reduced throughput), and explicit user notification, are the key business requirements.

The use of both Malware Protection and Antivirus should be employed only if there is a need for extremely high security. The sets of threats that the two services can detect have a high level of overlap, but at any time each will likely detect a few threats that the other does not yet detect. Employing both services together slightly expands the aggregate set of threats that will be detected, with a very high throughput reduction.

Firewall/NAT rules, entities and performance

The numbers of zone entities, networks entities, host entities and associated firewall and NAT rules configured on an AR-Series firewall can also affect the Internet-access performance.

Firewall and NAT rules

Each additional NAT or firewall application rule configured on an AR-Series firewall adds an additional millisecond latency to the start of each new session as the session's content is checked against each relevant rule. Once a flow is established, it is cached in an internal connection tracking table, and not continually re-checked against the rules.

There is a configurable maximum of 500 NAT and/or Firewall rules combined to allow data for various applications to flow between firewall entity definitions. However, the practical limit will reduce as additional features are configured and used on the device, and depending on the system resources available.

In most situations, a single rule to masq any traffic from LAN to WAN is sufficient, without the need to configure NAT masq rules for each individual application. There may typically also be a few NAT port forwarding rules configured to allow external application traffic from the Internet to the public IP address to be translated to reach the internal addresses of internal servers.

A few dozen firewall rules to allow or deny specific application traffic to flow from one entity to another may also typically be configured.

Depending on what other features are in use on the device, as more rules are added, latencies for sessions will progressively worsen, eventually resulting in TCP connection timeouts and associated failure to load some website content. Also, as additional rules are configured, the time to load all the rules on device startup may increase device startup time.

Entities In terms of zones, the traditional three zone approach, that is, DMZ, private and public zones, covers the vast majority of needs. However, the structure of an organization may dictate the configuration of a larger number of zones.

The number of zone, network and host entities does not have any significant effect on forwarding performance.

Configuring Intrusion Prevention System (IPS)

This is an example of how to configure IPS.

By default, IPS protection is disabled; you need to explicitly enable it.

To show the list of built-in categories that AlliedWare Plus IPS supports, use the command:

```
awplus#show ips categories
```

Step 1: **Enter the IPS mode.**

```
awplus#configure terminal
awplus(config)#ips
```

Step 2: **Enable IPS protection.**

```
awplus(config-ips)#protect
```

Step 3: **(Optional) Configure action for a specified category.**

To drop packets categorized as **checksum**, enter the follow command:

```
awplus(config-ips)#category checksum action deny
```

Step 4: **Verify IPS configuration.**

```
awplus#show ips
```

Output 1: Example output from the console

```
awplus#show ips
Status:      Enabled (Active)
```

Configuring Antivirus

This section provides an example of how to configure Antivirus.

By default, antivirus protection is disabled and you need to explicitly enable it.

Step 1: **Enter the Antivirus mode.**

```
awplus#configure terminal
awplus(config)#antivirus
```

Step 2: **Set the provider and enable Antivirus protection.**

```
awplus(config-antivirus)#provider kaspersky
awplus(config-antivirus)#protect
```

Step 3: **(Optional) Set the action to take when a scan fails.**

By default, when a scan fails or when the limit is exceeded, the default action is **deny** (block). To allow HTTP traffic when a scan fails, enter the command:

```
awplus(config-antivirus)#action scan-failed permit
```

Step 4: **Show the information about the operation of Antivirus.**

```
awplus(config-antivirus)#do show antivirus
```

Output 2: Example output from the console

```
awplus#show antivirus
Status:      Enabled (Inactive Unlicensed)
Provider:    Kaspersky
Scan failed action:    block
Limit exceeded action: block
Resource version:          not set
Resource update interval: 1 hour
```

Configuring IP Reputation

This section shows an example of how to configure IP Reputation. For more information about IP Reputation, see "IP Reputation" on page 13, and the Command Reference.

By default, IP Reputation protection is disabled and you need to explicitly enable it.

Step 1: **Enter the IP Reputation mode.**

```
awplus#configure terminal
awplus(config)#ip-reputation
```

Step 2: **Set the IP Reputation database provider.**

```
awplus(config-ip-reputation)#provider proofpoint
```

Step 3: **Enable IP Reputation protection.**

```
awplus(config-ip-reputation)#protect
```

Step 4: **(Optional) Configure action for a category.**

```
awplus(config-ip-reputation)#category P2P action deny
```

Step 5: **(Optional) Add an IP address to the whitelist**

If you add an IP address to the whitelist, IP Reputation will allow it even if it is in a provider blacklist with a category that IP Reputation would otherwise alert or deny. We recommend only adding an IP address to the whitelist if it is necessary and you have reason to consider it safe and appropriate for your network.

You can add a maximum of 128 IP addresses to the whitelist; IP Reputation will not apply any further IP addresses to the traffic beyond that limit.

```
awplus(config-ip-reputation)#whitelist 10.1.1.1
```

If a whitelist address is logged as not matching a provider list, we recommend removing the address from the whitelist. This is important as it means you will be newly alerted and/or packets will be dropped if the address gets a bad reputation again at some time in the future.

```
awplus#configure terminal
awplus(config)#ip-reputation
awplus(config-ip-reputation)#no whitelist 10.1.1.1
```

Step 6: **Verify IP Reputation configuration.**

```
awplus#show ip-reputation
```

```
awplus#show ip-reputation
Status:      Enabled (Active)
Events:      0
Provider:    Proofpoint
    Resource version: iprep_et_rules_v12192
    Entry count:      85449
    Status:           Enabled
Whitelist:
    Entry count:      2
Resource update interval: 1 hour
```

To see:

- which IP addresses are configured in the whitelist, see the output from the **show running config** command.
- whether or not they match IP addresses in the whitelist that do not match entries in lists supplied by the provider, view log messages.

For more information, see "IP Reputation log messages" on page 70 and "IP Reputation whitelist" on page 15.

Configuration example: IP Reputation with whitelist

This example configuration extract sets:

- Proofpoint as the provider for the IP reputation database, and names this IP Reputation category Scanner.
- IP Reputation to deny any traffic from IP addresses in this database, except for a few specified IP addresses that it adds to the whitelist.

```
awplus#sh running-config ip-reputation
ip-reputation
 category Scanner action deny
 provider proofpoint
 whitelist 192.0.2.5
 whitelist 203.0.113.2
 protect
!
```

Configuring Malware Protection

This section shows an example of how to configure Malware Protection.

By default, Malware Protection is disabled and you need to explicitly enable it.

Step 1: **Enter the Malware Protection Configuration mode.**

```
awplus#configure terminal
awplus(config)#malware-protection
```

Step 2: **Set the provider and enable Malware Protection.**

```
awplus(config-malware)#provider kaspersky
awplus(config-malware)#protect
```

Step 3: **Show the information about the operation of Malware Protection.**

```
awplus#show malware-protection
```

Output 3: Example output from the console

```
awplus#show malware-protection
Status:      Enabled (Active)
Provider:    Kaspersky
Resource version:         1.0
Resource update interval: 1 hour
```

Configuring Web Control

This section provides examples of how to configure web control:

- "How to configure basic Web Control" on page 40
- "How to configure Web Control default action per-entity" on page 42
- "How to discover which Web Control category a website URL belongs to" on page 44

For more information about the web control feature, see "Web Control" on page 17.

How to configure basic Web Control

Example 1 By default, Web Control protection is disabled and you need to explicitly enable it.

Step 1: **Enter Web Control Configuration mode.**

```
awplus#configure terminal
awplus(config)#web-control
```

Step 2: **Set the website categorization provider and enable Web Control protection.**

```
awplus(config-web-control)#provider digitalarts
awplus(config-web-control)#protect
```

The command **show web-control categories** displays a list of predefined categories. You can optionally create your own named custom categories.

Step 3: **Configure a category and match criteria.**

To configure match criteria for the named custom category **movie**, use the Web Control command **match <word>** as follows:

```
awplus(config-web-control)#category movie
awplus(config-category)#match imdb
awplus(config-category)#match youtube
awplus(config-category)#match rottentomatoes
awplus(config-category)#exit
```

Match criteria are case-insensitive and matched up to the first appearance of '?' (query string marker) or '#' (fragment identifier) in a website URL. For example, URL ‘www.alliedtelesis.com/search.aspx?keyword=routers’ does not match the match criterion match router, but ‘www.alliedtelesis.com/routers’ does match that criterion.

When a URL matches a match criterion, the URL is categorized to the match criterion’s category. A URL can be matched to more than one category. Custom match criteria override and precede

provider categorization. If a URL or website matches custom criteria, then the URL will not be further sent for categorization by the provider criteria.

The provider performs the categorization of URLs into the appropriate category, so there is no need to configure specific match criteria for predefined categories.

As above, you can create your own custom categories which will match any website URLs against text strings in that category. This allows custom categories to be created to suit business needs.

You can create up to 50 match criteria in total, so a category can have a maximum of 50 match criteria, or 50 categories can each have one match criterion, as long as the total number of the match criteria does not exceed 50.

Step 4: **Configure an entity the rule applies to.**

```
awplus(config-web-control)#exit
awplus(config)#zone private
awplus(config-zone)#network engineering
awplus(config-network)#ip subnet 192.168.1.0/24 interface eth1
```

Step 5: **Create a rule for the category.**

```
awplus(config-network)#exit
awplus(config-zone)#exit
awplus(config)#web-control
awplus(config-web-control)#rule permit movie from private.engineering
awplus(config-web-control)#exit
awplus(config)#exit
```

URLs containing the match criteria associated with the custom category **movie** can now be accessed from the engineering network. Access to other URLs that do not match the custom category **movie** will be blocked by the default Web Control action.

Step 6: **Display information about the state of Web Control.**

```
awplus#show web-control
```

Output 4: Example output for basic web control configuration:

```
awplus#show web-control
Web Control protection is enabled
Web Control default action is deny
Web Control is licensed
Categorization provider is Digital Arts
Statistics:
 Categorization hits: 0/0  (0.0%)
 Rule hits:   0/0  (0.0%)
 Cache hits:  0/0  (0.0%)
 Cache size:  0
```

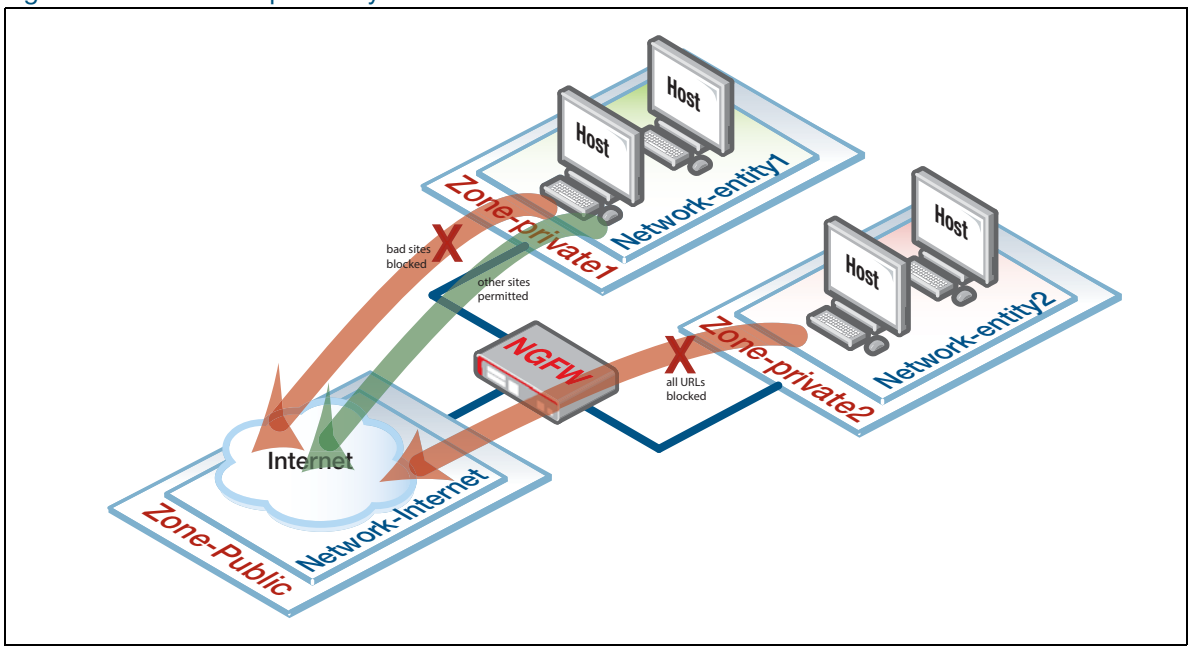
How to configure Web Control default action per-entity

The default action to take on uncategorized websites and categorized websites that do not hit any user-defined Web Control filter rules is to **deny** access to the website.

However, if there are multiple firewall entities configured in the device (such as multiple firewall zones), then you may wish to configure different default actions for each individual entity for any URLs that do not match filter rules.

A new reserved keyword **any** has been added to the parameter **<category>** in the rule command from version 5.4.6-2.x onwards. This reserved Web Control keyword overrides the default Web Control action for the specific entity that it is associated with. Rules containing this reserved keyword can be applied to all types of firewall entities, including zone, network and host entities. This new reserved keyword allows you to configure multiple firewall entities, with each entity having its own unique default action to apply to uncategorized URLs.

Figure 8: Web Control per entity



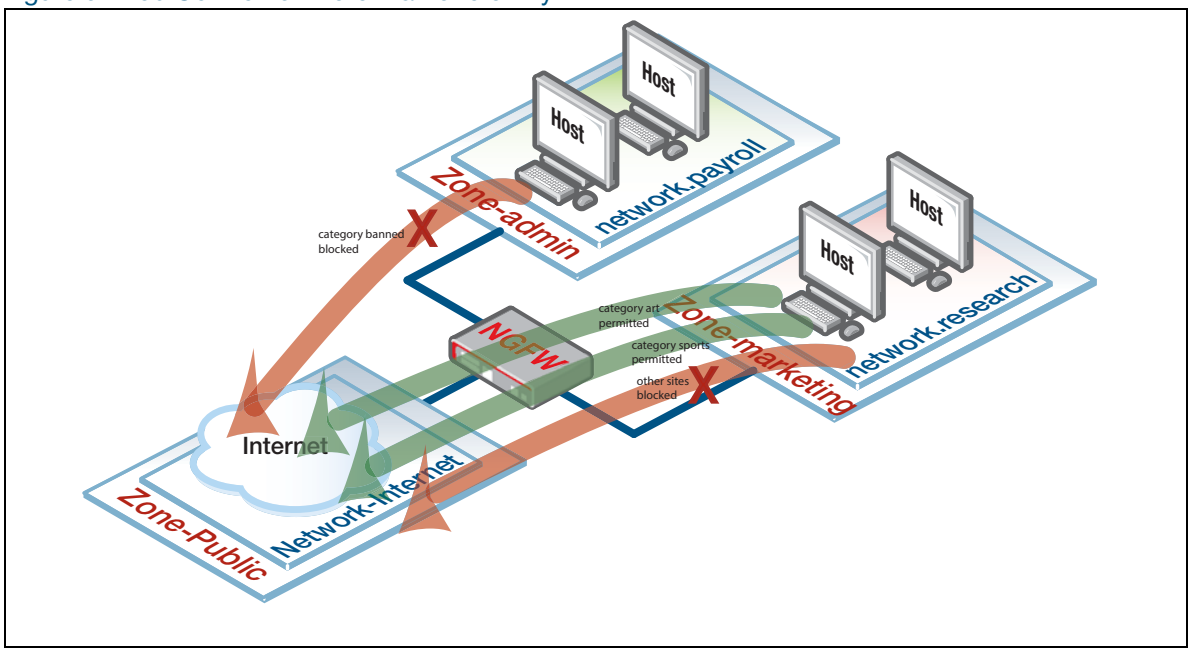
Example 2 Basic configuration to create a rule using the category keyword any:

```
awplus#configure terminal
awplus(config)#web-control
awplus(config-web-control)#rule deny badsites from private
awplus(config-web-control)#rule permit any from private
```

Rules are processed in order. In this example above the access to URLs associated with the named category **badsites** being accessed from the named firewall entity **private** will be blocked via the **deny** rule. Access to all other URLs originating from that specific firewall entity will be allowed via the subsequent **permit any** rule.

However, access to URLs from any other entity will not match the rules above, and so will be blocked via the Web Control default action.

Figure 9: Web Control for more than one entity



Example 3 The following shows how to configure two firewall entities, with a different default action being applied for each entity.

Access from the research network entity (within marketing zone) to URLs matching the **art** and **sports** categories are permitted, whilst access to any other URLs is denied.

Conversely, access from the payroll network entity (within the admin zone) to URLs matching the **banned** category are denied, whilst access to any other URLs is permitted.

Step 1: **Create the admin zone entity containing the payroll network entity and assign its IP subnet address.**

```
awplus#configure terminal
awplus(config)#zone admin
awplus(config-zone)#network payroll
awplus(config-network)#ip subnet 192.168.1.0/24
```

Step 2: **Create the marketing zone entity containing the research network entity and assign its ip subnet address.**

```
awplus(config-host)#zone marketing
awplus(config-zone)#network research
awplus(config-network)#ip subnet 192.168.2.0/24
```

Step 3: **Enter into Web Control configuration mode and set the website categorization provider.**

```
awplus(config-host)#web-control
awplus(config-web-control)#provider digitalarts
```

Step 4: **Configure custom categories and associated match criteria.**

```
awplus(config-control)#category banned
```

```
awplus(config-category)#match youtube
awplus(config-category)#match movies
awplus(config-category)#match gambling

awplus(config-category)#category art
awplus(config-category)#match contemporary
awplus(config-category)#match classic

awplus(config-category)#category sports
awplus(config-category)#match rugby
```

Step 5: **Create rules for the categories.**

```
awplus(config-category)#rule 10 permit art from marketing.research
awplus(config-web-control)#rule 20 permit sports from marketing.research
awplus(config-web-control)#rule 30 deny any from marketing.research
awplus(config-web-control)#rule 40 deny banned from admin.payroll
awplus(config-web-control)#rule 50 permit any from admin.payroll
```

Step 6: **Enable Web Control protection.**

```
awplus(config-web-control)#protect
```

How to discover which Web Control category a website URL belongs to

This feature is available from AlliedWare Plus version 5.4.7-2.1 and later.

You can send a categorization request to the web control provider to determine which web control category a website URL belongs to. A response from the provider's server contains the category or categories the URLs belong to. To use this feature, you need a license for web control, but web control does not need to be enabled. You can use this information to configure web control policies to more closely meet the needs of your organization.

Once you have discovered the categories that URLs belong to, you can apply or adjust web control rules to allow or deny access to particular categories.

Example 4 This example shows how to first inquire about categories, and then to deny access to some of the discovered categories.

Step 1: **Inquire about the categories for URLs.**

Inquire about which categories the URLs belong to. The provider returns a response for each URL. You can inquire about one or more URLs:

```
awplus#web-control categorize http://www.ebay.com http://www.amazon.com
```

```
awplus#web-control categorize http://www.ebay.com http://www.amazon.com
http://ebay.com ==> 54 (Online Auctions)
http://www.amazon.com ==> 55 (Online Shopping)
```

You can inquire about HTTPS URLs:

```
awplus#web-control categorize https://reddit.com/r/nfl
```

```
awplus#web-control categorize  https://reddit.com/r/nfl
https://reddit.com ==>  [Social Bookmarks(31)] [Forums(63)]
```

Step 2: **Enable web control and control access to categories**

Enable web control.

```
awplus(config)#web-control
awplus(config-web-control)# provider digitalarts
awplus(config-web-control)# protect
awplus(config-web-control)# action permit
```

Create rules to deny access to selected categories corresponding to the inquiries.

```
awplus(config-web-control)# rule 10 deny "Online Auctions" from any
awplus(config-web-control)# rule 10 deny "Online Shopping" from any
```

Note:

- If neither 'http://' nor 'https://' is specified in the URL, the default 'http://' is automatically added.
- Enquiries about HTTPS URLs will return only the high level category or categories associated with the domain, not those associated with the resources within the domain.
- For inquires about HTTPS URLs, only the domain part of the URL is sent to the web control provider for categorization, as in the 'reddit.com' example shown above. This is the expected behaviour with HTTPS traffic, where only the domain name specified in TLS SNI is available for access.
- If the server cannot categorize the URL, the response for it will be 'unknown category'.

Configuring Web Control with firewall enabled

The UTM firewall Web Control features integrate with the categorization provider Digital Arts' Active Rating System (ARS), which is regularly updated with about 100 predefined categories of web sites.

If the URL that a client wishes to visit is not cached, the AR-Series firewall will query the Digital Arts' ARS. The categorization provider then returns the category of the website. To allow this happen, a firewall rule to permit HTTP traffic originating from the AR-Series firewall to the Digital Arts server should be configured.

For example, the firewall rule below permits the HTTP traffic (containing categorization request) originating from the UTM firewall external interface (located with the public zone) to reach the Digital Arts ARS.

```
awplus(config-firewall)#rule permit http from PUBLIC.EXTERNAL.INTERFACE to
PUBLIC
```

For more information about firewall rules and zone, network, or host entities see the Firewall and Network Address Translation (NAT) Feature Overview and Configuration Guide.

Configuring URL Filtering

This section describes how to use, configure and monitor URL Filtering. For more information about the URL Filtering feature, see "URL Filtering" on page 20.

How to use URL Filtering

To use URL filtering, you can either use:

- a blacklist provided by Kaspersky
- custom lists (black/white)
- a combination of custom and Kaspersky lists.

Creating custom lists

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

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

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

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

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

```
example.com
```

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

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

Once this list is available to the system (stored in Flash, USB, or on an SD card), the configuration to enable URL filtering is straight forward, as described below in the section "Configuring URL Filtering" on page 47.

Details of the content of custom lists

A custom list is an ASCII formatted text file containing zero or more single-line pattern matches. So far, we have looked at the general syntax of the entries in these files. Here we look in more detail at the rules governing the content of these files:

- There is no ordering or precedence for patterns in the file.
- Spaces in the pattern are not allowed.
- The wildcard, asterisk '*' can be used in the pattern to indicate a match on zero or more characters.
- If there are no '/' or '*' characters present, then all content of the domain is blocked.
- "Match everything" patterns are not allowed (e.g. '*' or '*/*').
- Empty or comment lines (starting with '#' or ';') are ignored.
- The ‘www.’ prefix should not be included in the pattern. However patterns and URLs are normalized before matching. More specifically:
  - The ‘www.’ prefix and authentication prefix ‘login:<password>@’ that may pre-pend a URL are automatically stripped from the URL before pattern matching.
  - Patterns are converted to lower case.
  - Only the domain name should be specified for blocking HTTPS traffic because TLS SNI contains only the domain name for the HTTPS request.

The table below describes how the pattern ***mysite.com/** is matched (Blocked URLs) or not matched (Non-blocked URLs) for a blacklist.

Table 1: A pattern matching example with explanations.

THIS PATTERN	BLOCKS THE URLS	NON-BLOCKED URLS
*mysite.com/	mysub.mysite.com www.mysite.com	mysub.mysite.com/mypage
Pattern matching explanations	**mysub.mysite.com** is a match (and is therefore blocked) because: ■ The wildcard, asterix ‘*’ matches the prepended text ‘mysub’ in the URL, and the remaining text in the URL matches the pattern. **www.mysite.com** is a match because: ■ The “www.” prefix is stripped off prior to matching, and the remaining text in the URL matches the pattern.	**mysub.mysite.com/mypage** is not a match (and is therefore non-blocked) because: ■ The text ‘mypage’ in the URL is not part of the pattern.

The following table lists a series of blacklisted ‘domain and string pattern’ match criteria, and examples of URLs that would or would not be matched by these criteria.

Table 2: Blacklisted domain and string pattern match criteria

PATTERN	BLOCKED URLS	NON-BLOCKED URLS
com	www.mydotcomurl.com	myausurl.com.au
com.au	www.myausurl.com.au:8080/file.txt	mydotcomurl.com
ru	myrussian.pp.ru	myfakerussian.ru.org
z	faz.com auzi.id.au zulu.com me.kiwi.nz fish.com/folder1/file.gz www.google.co.nz/search?client=ubuntu&channel=fs&q=ziare&ie=utf-8&oe=utf-8&gfe_rd=cr&ei=ZfKWVqgtk5PABN6YtqgD	
*mysite.com/	mysub.mysite.com www.mysite.com	mysub.mysite.com/mypage
mysite.com/*	www.mysite.com/mypage.html www.mysite.com/ www.mysite.com	mysub.mysite.com/mypage www.mysite.com.au
mysite.com	mypage.mysite.com.au mysite.com.au www.mysite.com mypage.mysite.com/folder/file.txt somescript.sc?mysite.com.au	
mysite.com/*/filename*.exe	www.mysite.com/folder/filename.exe mysite.com/folder/filename-bad.exe mysite.com/subdomain/folder2/folder3.html/abcd/filename.exe mysite.com/folder/filename-bad/file.exe	www.myurl.mysite.com/subdomain/filename*.exe search-engine.com/search?q=mysite.com/folder/filename.exe mysite.com/filename.exe mysite.com/subdomain/file.exe mysite.com/subdomain/filename.exe1 mysite.com/subdomain/filename.html
192.168.1*/abcd-efgh/subdomain/*	192.168.10.com/abcd-efgh/subdomain/filename.exe 192.168.1.10/abcd-efgh/subdomain/filename.exe	192.168.2.10/abcd-efgh/subdomain/filename.exe 192.168.1.10/abcd-efgh/filename.exe 192.168.1.10/abcd-efgh/subdomain2/filename.exe

Limits

URL filtering is limited to 1000 custom whitelist and 1000 custom blacklist rules, spread over any number of list files.

Configuring URL Filtering

URL filtering is turned on by configuring a whitelist that uses a custom file, a blacklist that uses a custom file, or blacklisting that uses the Kaspersky service.

1. To add a **whitelist** that uses a custom file (that is stored on USB, for example) and then enable URL filtering, use the commands:

```
awplus#configure terminal
awplus(config)#url-filter
awplus(config-url-filter)#whitelist usb:/my_whitelist.txt
awplus(config-url-filter)#protect
```

2. To add a **blacklist** that uses a custom file (that is stored on Flash, for example) and then enable URL filtering, use the commands:

```
awplus#configure terminal
awplus(config)#url-filter
awplus(config-url-filter)#blacklist flash:/blacklist-example.txt
awplus(config-url-filter)#protect
```

3. To add a blacklist provided by **Kaspersky** and then enable URL filtering, use the commands:

```
awplus#configure terminal
awplus(config)#url-filter
awplus(config-url-filter)#provider kaspersky
awplus(config-url-filter)#protect
```

   - To check that Kaspersky is active, enter the command **show url-filter:**

```
awplus#show url-filter
Status:      Enabled (Loading)
Provider:    Kaspersky
 Status:              Enabled
 Resource version:    not set
 Update interval:     1 hour
 Blacklist entries:   -
Custom blacklists   Entries
 blacklist-example.txt  3
Custom whitelists   Entries
```

   - Invalid entries in URL filter lists are ignored (not loaded).
   - Expiry of the Kaspersky URL Filtering Subscription License will cause URL filtering to reload without a Kaspersky blacklist.

Using multiple whitelists and blacklists

The AR-Series firewall support pattern checking against multiple whitelists and multiple blacklists.

Multiple custom whitelists or blacklists can be configured and checked as follows:

```
awplus(config)#url-filter
awplus(config-url-filter)#blacklist blacklist1.txt
awplus(config-url-filter)#blacklist blacklist2.txt
awplus(config-url-filter)#blacklist blacklist3.txt
awplus(config-url-filter)#whitelist whitelist1.txt
awplus(config-url-filter)#whitelist whitelist2.txt
awplus(config-url-filter)#whitelist whitelist3.txt
awplus(config-url-filter)#protect
```

You can check the configuration using the **show url-filter**, **show running-config url-filter** and **dir** commands:

```
awplus#show url-filter
Status:      Enabled (Active)
Provider:    not set
Custom blacklists   Entries
 blacklist1.txt       18
 blacklist2.txt       23
 blacklist3.txt       39
Custom whitelists   Entries
 whitelist1.txt       11
 whitelist2.txt       26
 whitelist3.txt       33
```

```
awplus#show running-config url-filter
url-filter
 blacklist blacklist1.txt
 blacklist blacklist2.txt
 blacklist blacklist3.txt
 whitelist whitelist1.txt
 whitelist whitelist2.txt
 whitelist whitelist3.txt
 protect
!
```

```
awplus#dir
       107 -rw- May 11 2016 04:52:44  whitelist1.txt
       229 -rw- May 11 2016 04:52:39  whitelist2.txt
       318 -rw- May 11 2016 04:52:32  whitelist3.txt
       372 -rw- May 11 2016 04:51:50  blacklist3.txt
       202 -rw- May 11 2016 04:51:38  blacklist2.txt
       170 -rw- May 11 2016 04:51:31  blacklist1.txt
```

Rules for processing lists

The order of processing of lists is:

- First—whitelists
- Second—custom blacklists
- Third—Kaspersky-provided blacklists

The matching logic is that as soon as a URL matches an entry in a list that it is being compared against, then comparing stops and the relevant action (allow, if the match occurs in a whitelist, or deny if the match occurs in a blacklist) is taken.

Because whitelist matching precedes blacklist matching, you can use custom whitelists to override any corresponding blacklist entries. An HTTP or HTTPS request that has a URL matching an entry in a whitelist will be permitted immediately, and the URL will not be matched against any blacklists.

So, if websites you actually want to access are being blocked by the Kaspersky blacklist, or some subsection of an otherwise dangerous site is desirable, a whitelist may be created.

Example For this example, the ***example.net/viruses/research*** folder contains information that is needed within the otherwise completely blocked site.

This can be allowed by creating a whitelist file named ‘whitelist-example.txt’ in Flash memory, with the contents:

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

And configuring it as follows:

```
awplus#configure terminal
awplus(config)#url-filter
awplus(config-url-filter)#whitelist whitelist-example.txt
awplus(config-url-filter)#protect
```

This whitelist will be processed prior to the blacklist, and will allow matching traffic through.

Updating lists

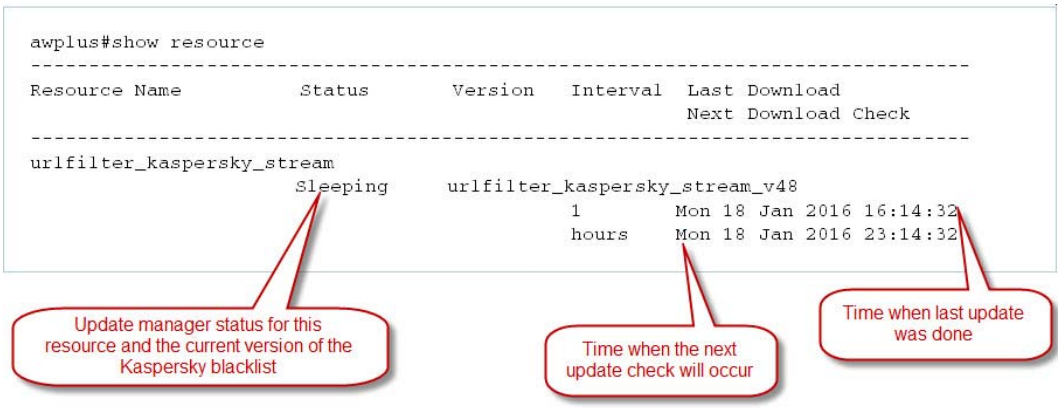
Updating the Kaspersky blacklist

When subscribed to the Kaspersky URL Filter service, updates to the Kaspersky blacklist will be made available. By default URL filtering checks for updates to the Kaspersky blacklist every hour.

You can configure the update interval via the **update-interval** command in **url-filter** configuration mode. The update process is managed by the Update Manager utility.

You can see the update status in two show command outputs: **show url-filter** and **show resource**.

```
awplus#show url-filter
Status:      Enabled (Loading)
Provider:    Kaspersky
 Status:              Enabled
 Resource version:    urlfilter_kaspersky_stream_v48
 Update interval:     1 hour
 Blacklist entries:   63457
...
```



When the Update Manager finds a new version is available, it downloads and instructs URL Filter to start using the new blacklist. An update check can be manually initiated with the **update urlfilter_kaspersky_stream now** or **update all now** commands.

Updating a user-defined blacklist or whitelist

You can modify blacklist and whitelist files that you have created. Once you have completed all the desired changes, use the **url-filter reload custom-lists** command to reload the modified files.

When a new blacklist or whitelist is configured and URL filter is already enabled, it automatically starts using the new file.

Monitoring URL Filtering

The **show url-filter** command displays a summary of the state of URL filtering, including the provider state, and counts of entries in each provided list. Any lists that contain too many entries to load will be noted here.

```
awplus#show url-filter
Status:      Enabled (Active)
Provider:    Kaspersky
 Status:              Enabled
 Resource version:    not set
 Update interval:     1 hour
 Blacklist entries:   -
Custom blacklists   Entries
 blacklist-example.txt  3
Custom whitelists   Entries
 whitelist-example.txt  1
```

Setting up and configuring UTM Offload

Setting up UTM Offload

These are the steps, described in more detail below, are required to set up UTM Offload:

- Purchase, download, and install the UTM Offload license on the AR4050S
- Enable UTM Offload on the AR4050S (the forwarding device)
- Set up the offload device

Purchasing, downloading, and installing the UTM Offload license

You only require a UTM Offload subscription license on the AR4050S, you do not need a license on the offload device as well. For information on purchasing, downloading, and installing the UTM Offload subscription license, see the Licensing Feature Overview Guide.

Enabling UTM Offload on the AR4050S

To enable UTM Offload on the AR4050S, you must have a direct Ethernet connection between the offload device and the AR4050S, i.e. from the Gigabit eth1 or eth2 port on the AR4050S to an Ethernet port on the offload device. The Ethernet connection must support a MTU of 1588 or higher. For more detail, see "Setting up the offload device" on page 56.

As an example, to enable UTM Offload and configure interface eth2 and subnet 192.168.100.0/24 to boot and communicate with, and manage the offload device, use the following commands:

```
awplus#configure terminal
awplus(config)#utm-offload interface eth2 subnet 192.168.100.0/24
```

To disable UTM Offload, use the following command:

```
awplus(config)#no utm-offload
```

Configuration notes

The MTU of the UTM Offload device interface is set to 1582 to support the overhead required for the standard Ethernet frames. You can not change this setting.

When configured, the interface of the forwarding device, which connects to the UTM Offload device, is automatically assigned an IP address which is the lowest usable address in the subnet. The interface is reserved for communication with the UTM Offload device and you should not manually configure this interface. The configured IP subnet used for UTM Offload is visible in the **show utm-offload** command, However the assigned IP address is not visible.

The AR4050S manages the offload device and offloads traffic automatically.

Setting up the offload device

The offload device can be any physical computer or virtual machine (VM). To use the UTM Offload feature, there must be a direct Ethernet connection from the forwarding device (AR4050S) to the offload device. The offload device must be configured to PXE boot (network boot) from the forwarding device.

Virtual machine

For instructions on setting up a virtual machine as an offload device, see "Configuring UTM Offload on VMware ESXi Server" on page 58.

Physical computer

If you want to set up a physical computer as an offload device, then the computer must:

- have a serial port, even if nothing is connected to that serial port.
- have a direct Ethernet connection between itself and the AR4050S, i.e. from the Gigabit eth1 or eth2 port on the AR4050S to an Ethernet port on the offload device. The Ethernet connection must support a MTU of 1588 or higher.
- be configured to network boot from the AR4050S. This will usually be done by changing the BIOS settings on the offload device and enabling PXE boot.
  - PXE boot does not currently support IPv6, therefore the Ethernet interface used for off loading is configured with IPv4.
  - The PC vendors website will have information about how to enable PXE boot. For example, to enable PXE Boot for Intel Desktop Boards, see Intel Support.

Specifications

The offload device must have the following minimum specifications:

UTM Offload Device Specifications
■ Multi-core 64-bit x86 processors
■ i5 CPU with 4 cores and 2.3-2.8GHz clock speed
■ 2GB of RAM
■ 4GB of Flash/HDD
■ VMware ESXi Hypervisor 6.x (Note: VMware is the only supported hypervisor if UTM Offload is not run directly on the offload device.)
■ A network card (NIC). Supported models: ■ Intel e1000 ■ Intel e1000e ■ Intel igb ■ VMware vmxnet3
■ At least one non USB storage device
■ Storage devices: Devices that support AHCI mode. ■ If using a SATA HDD, the SATA controller (which the SATA drive connects to) needs to support AHCI

About the offload image

The Allied Telesis Next Generation Firewall Appliance (AFA) software release is the image that is automatically downloaded and installed into the UTM Offload device.

The offload image is downloaded from the Update Server by the forwarding device and used to network boot the offload device. The forwarding device automatically downloads a compatible offload image version from the Update Server. Offload image version numbering aligns with other AlliedWare Plus software versions.

For example, an AR4050S running 5.4.8-1.1 downloads the 5.4.8-1.1 version of the AFA image. This process is automatically managed by the Update Server which ensures the correct version is offered to the AR4050S. You do not have to worry about getting the right version of AFA image to match your AlliedWare Plus software release. It is not possible for the forwarding device to boot the offload device with the wrong release.

Checking for image updates on the offload device

New offload device images are automatically downloaded by the forwarding device when detected.

The **default** interval used to detect offload image updates is 60 minutes. You can manually change this setting.

For example:

To change the time interval to 12 hours, use the following commands:

```
awplus#configure terminal
awplus(config)#utm-offload update interval hours 12
```

Figure 10: The **utm-offload update-interval** command parameters

```
awplus#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
awplus(config)#utm-offload update-interval ?
  days     Interval in days
  hours    Interval in hours
  minutes  Interval in minutes
  never    Never update the resource
  weeks    Interval in weeks
awplus(config)#utm-offload update-interval hours 12
```

The offload device image is downloaded from the resource server. The offload resource is tied to the release of software that the AR4050S is running. For more information on the AlliedWare Plus Update Manager, see the Update Manger Feature Overview and Configuration Guide.

Note: Configuring the update interval to **never** and upgrading the forwarding device to a later release without using the command **update afa_offload now** may result in the offload device not working.

Configuring UTM Offload on VMware ESXi Server

Many enterprises today have bare-metal hypervisor technology such as VMware ESXi Server running on powerful server hardware locally, to provide business critical applications and resources. This is a great use case for UTM Offload as businesses can utilize already existing hardware, simply by creating a new VM instance (virtual machine) to provide throughput improvements with the AR4050S while using the Advanced Threat Protection feature set.

There must be a direct Ethernet connection from the forwarding device (AR4050S) to the virtual machine. The virtual machine must be configured to PXE boot (network boot) from the forwarding device.

The PXE boot process make it very easy to setup UTM Offload in ESXi, in addition to the basic UTM Offload requirements for the AR4050S:

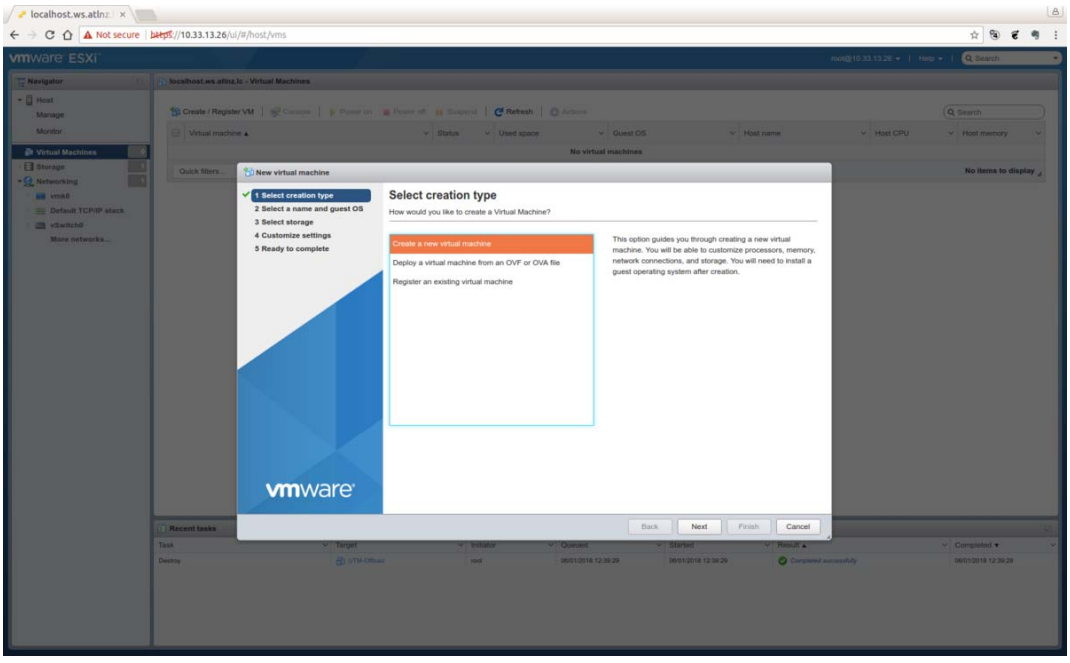
- UTM Offload licence (loaded on to the AR4050S)
- Internet access
- DNS server configuration
- Single UTM Offload configuration command on the ESXi

Simply follow the VMware configuration wizard as shown below, set the MTU of your virtual machine to be at least 1600 bytes, and click **Play**.

Using the configuration wizard

Open the VMware ESXi application, and perform the following steps:

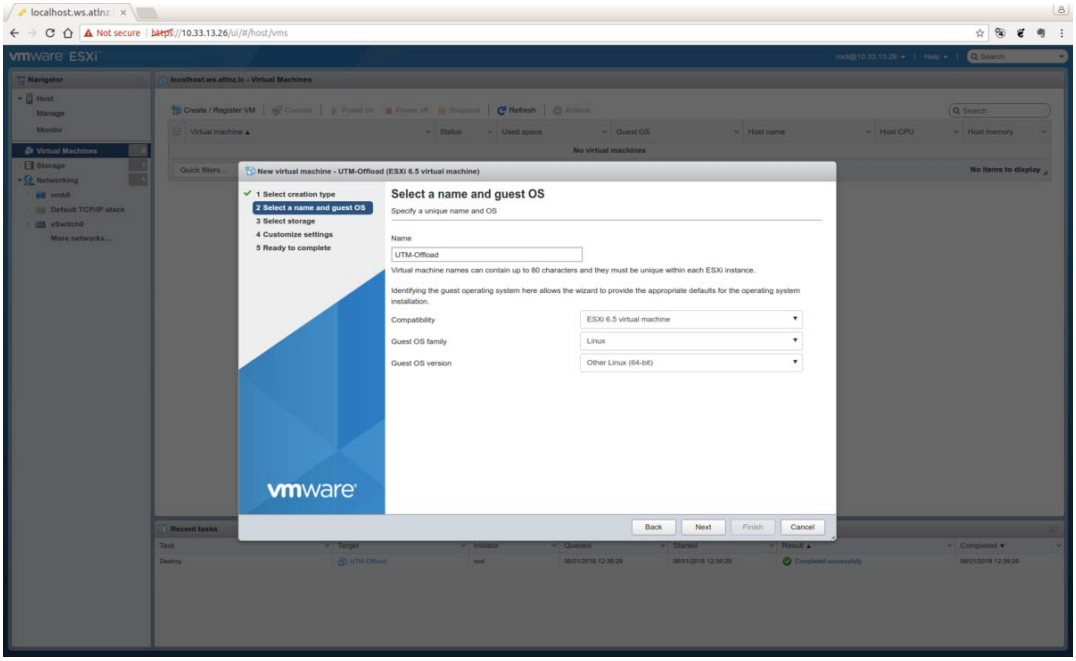
1. From the left side menu, select **Virtual Machines**
2. From the top tabs, select **Create/Register VM** to start the Wizard.



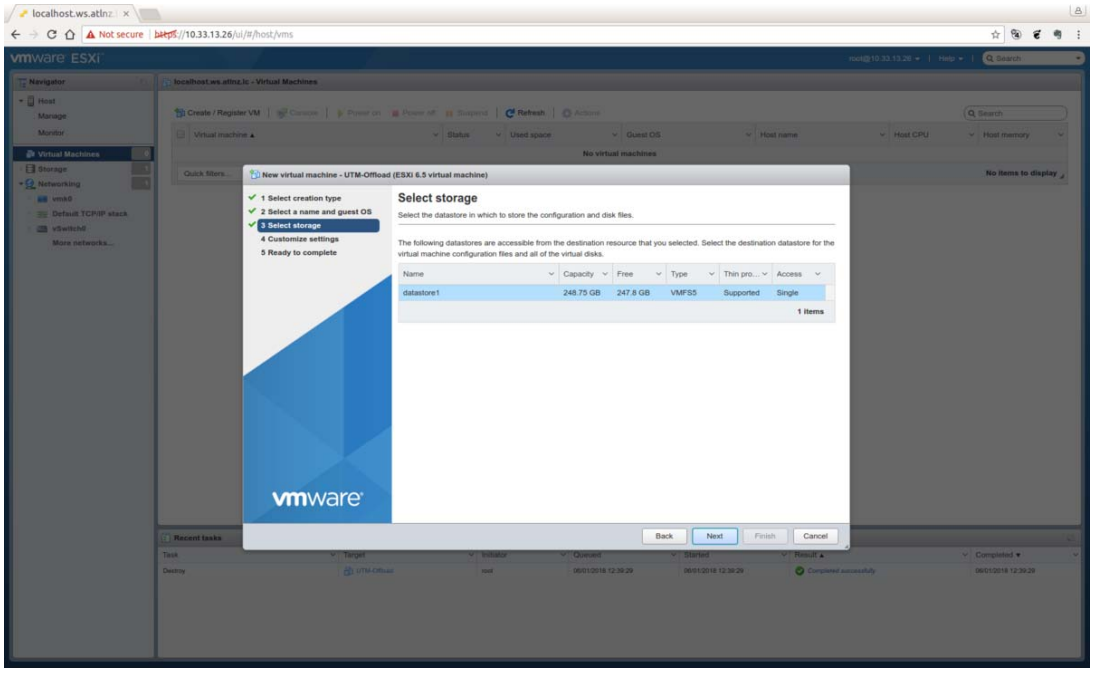
Note: The offload device must have an unused serial port.

3. From the **Select a name and guest OS** page, enter a unique **Name**

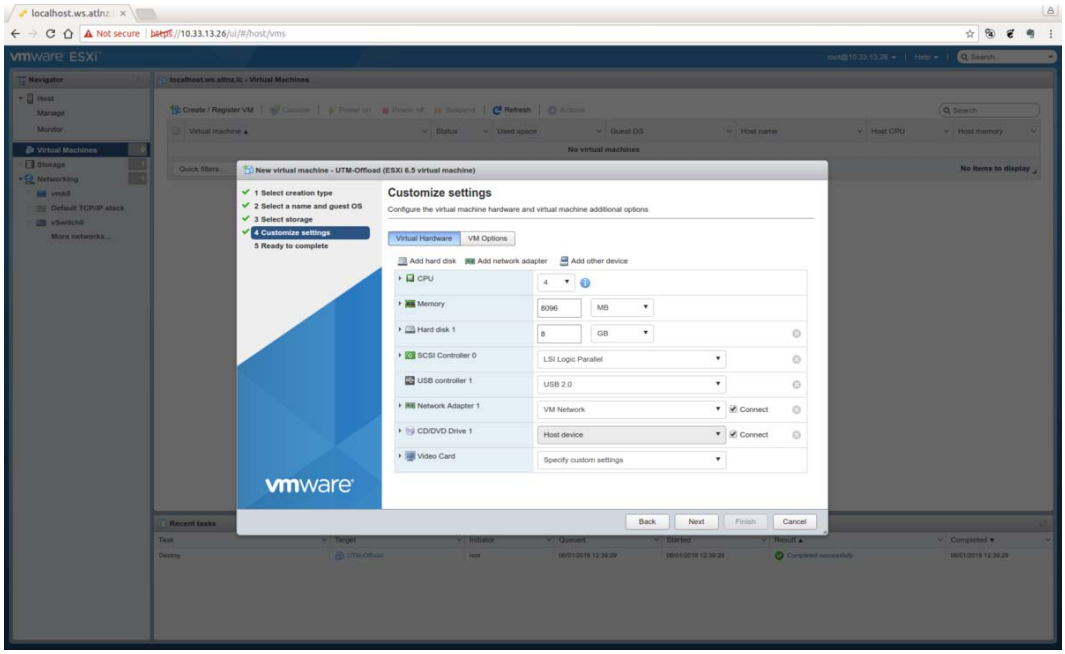
4. Use the drop down boxes to select, **Compatibility**, **Guest OS family**, and **Guest OS version**.



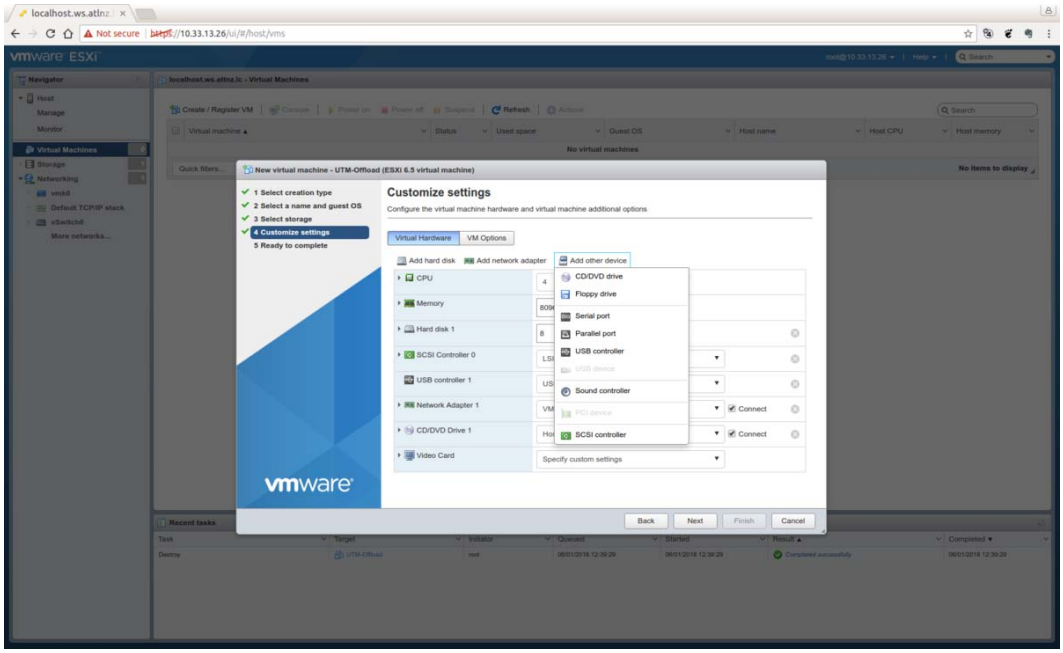
5. From the **Select storage** page, select the **datastore** for your configuration.



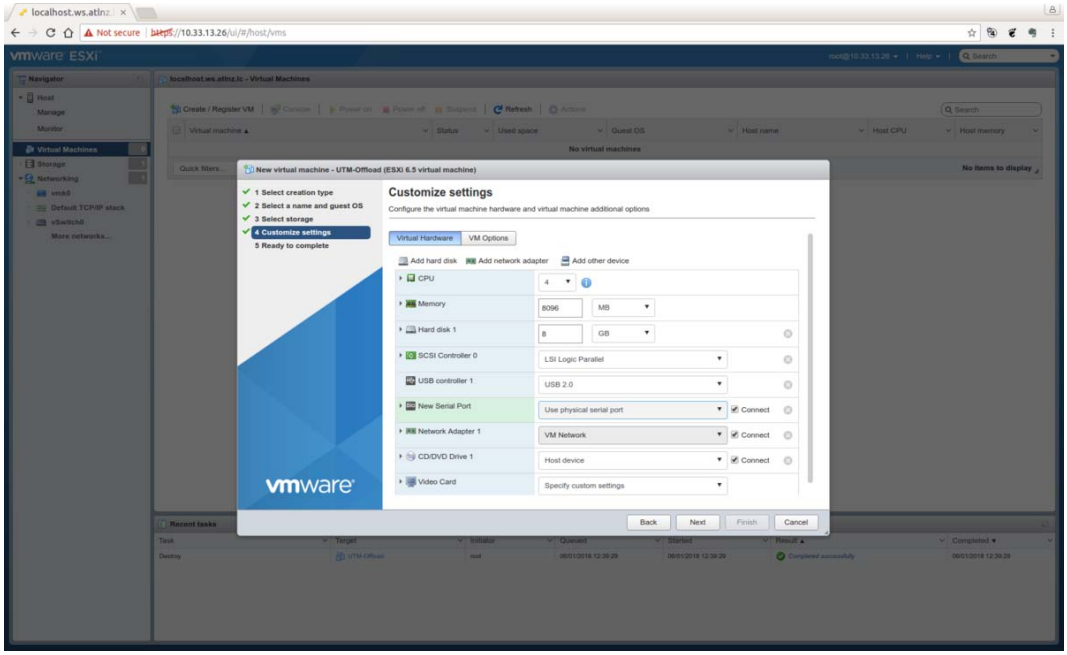
6. From the **Customize settings** page, configure the **Virtual Hardware** and **VM Options**.



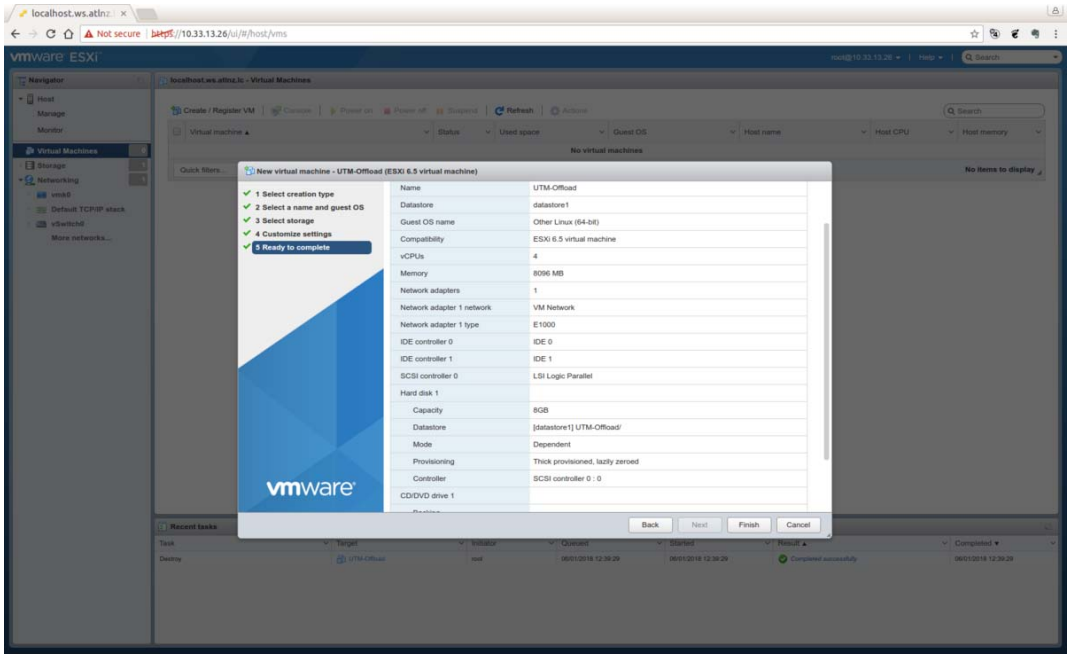
- Select **Serial port**.



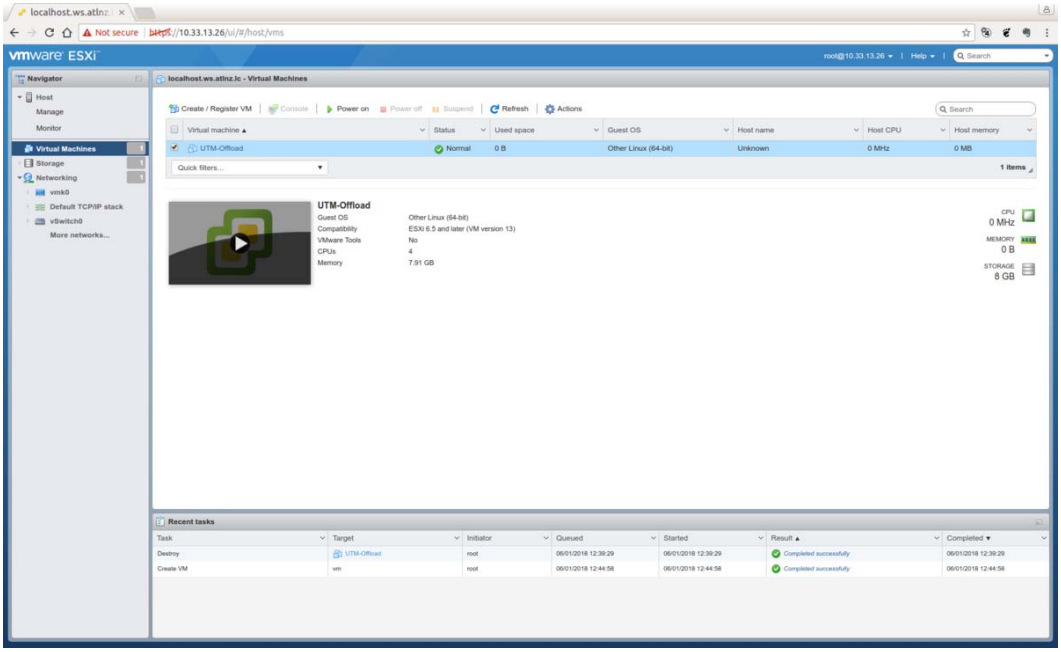
- Select **Connect**

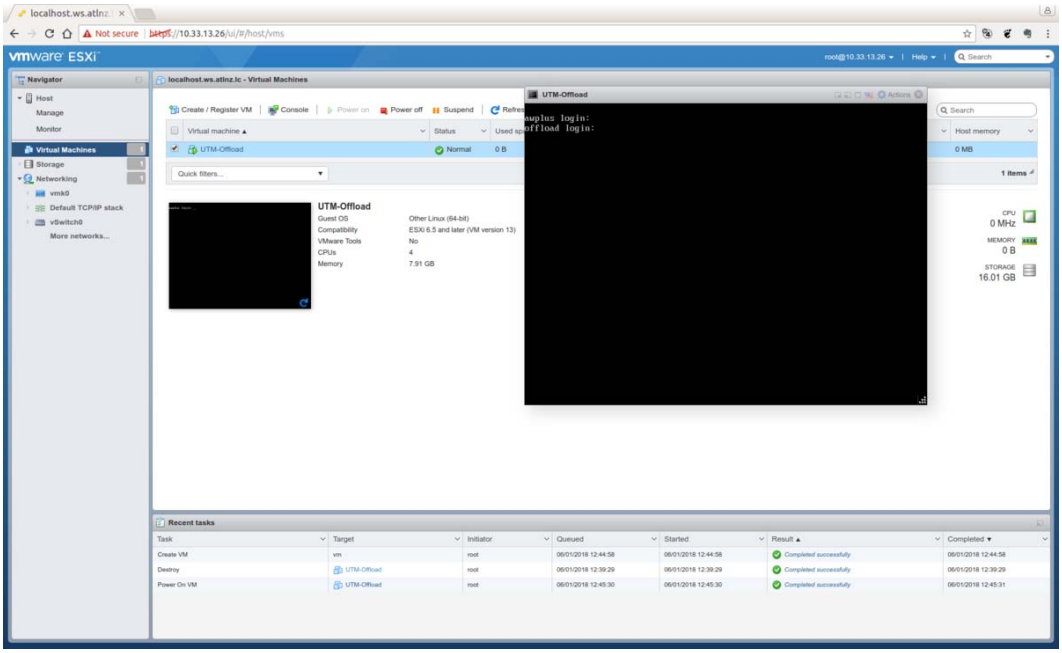


- Check the settings and click **Finish**.

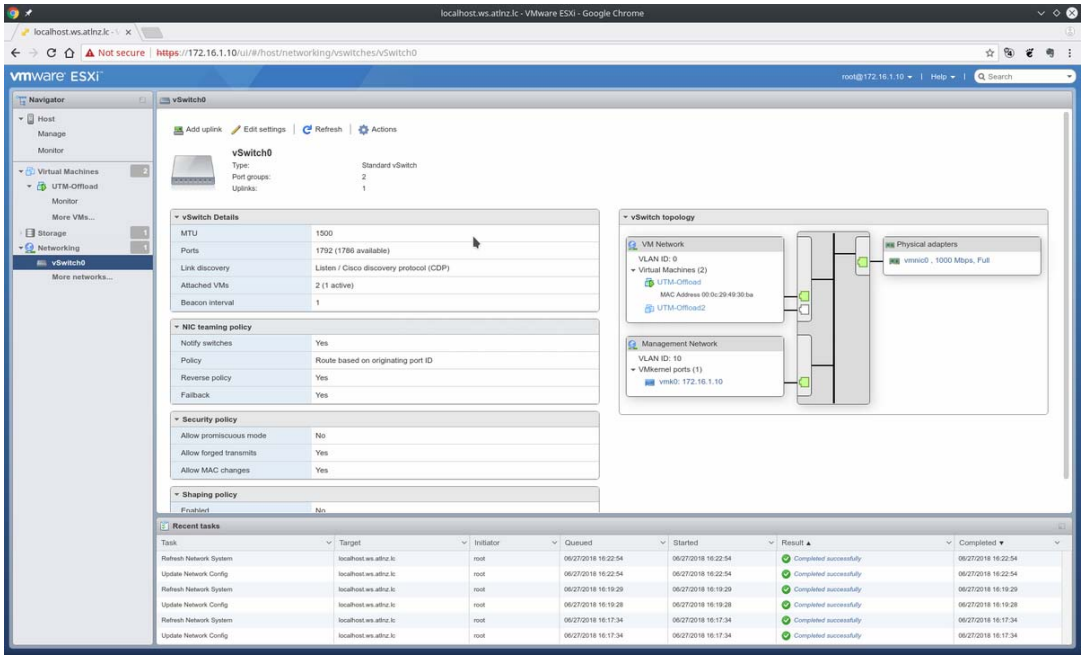


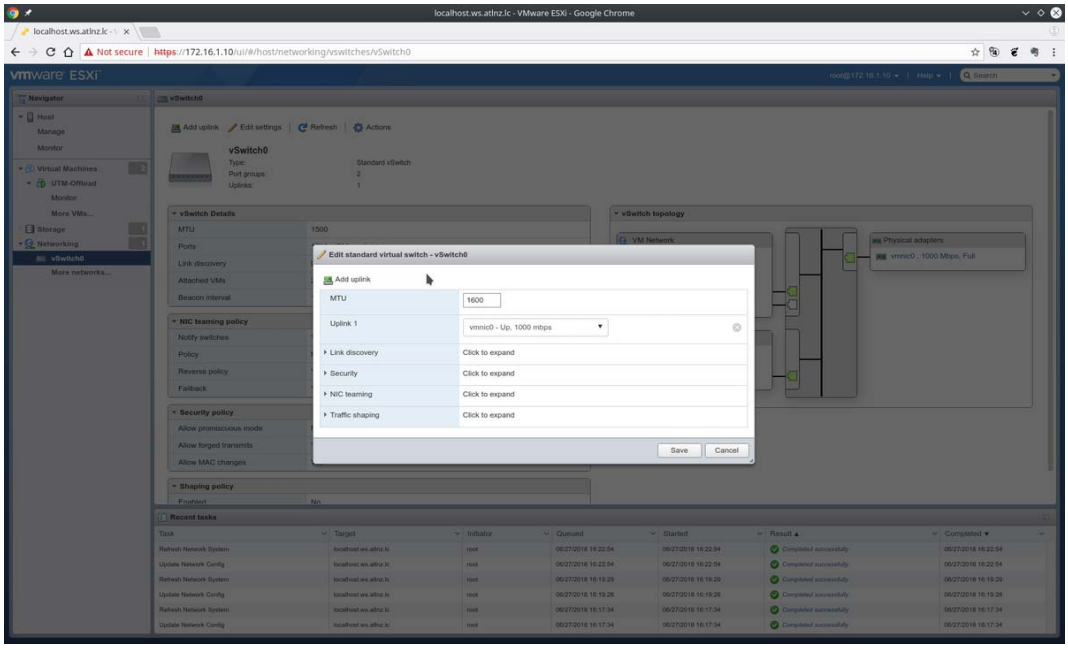
- Click **Play**


vmware ESXi
Navigator
Host
Manage
Monitor
Virtual Machines
Storage
Networking
vmk0
Default TCP/IP stack
vSwitch0
More networks...
localhost.ws.atlnz.lc - Virtual Machines
Create / Register VM
Console
Power on
Power off
Suspend
Refresh
Actions
Virtual machine
Status
Used space
Guest OS
Host name
Host CPU
Host memory
UTM-Offload
Normal
0 B
Other Linux (64-bit)
Unknown
0 MHz
0 MB
Quick filters...
1 items
UTM-Offload
Guest OS
Other Linux (64-bit)
Compatibility
ESXi 6.5 and later (VM version 13)
VMware Tools
No
CPUs
4
Memory
7.91 GB
CPU
0 MHz
MEMORY
0 B
STORAGE
8 GB
Recent tasks
Task
Target
Initiator
Queued
Started
Result
Completed
Destroy
Create VM


vmware ESXi
Navigator
Host
Manage
Monitor
Virtual Machines
Storage
Networking
vmk0
Default TCP/IP stack
vSwitch0
More networks...
localhost.ws.atlnz.lc - Virtual Machines
UTM-Offload
uplus login:
offload login:
Create / Register VM
Console
Power on
Power off
Suspend
Virtual machine
Status
Host memory
UTM-Offload
Normal
0 MB
Quick filters...
1 items
UTM-Offload
Guest OS
Other Linux (64-bit)
Compatibility
ESXi 6.5 and later (VM version 13)
VMware Tools
No
CPUs
4
Memory
7.91 GB
CPU
0 MHz
MEMORY
0 B
STORAGE
16.01 GB
Recent tasks
Task
Target
Initiator
Queued
Started
Result
Completed
Create VM
Destroy
Power On VM

7. Expand the **Networking** drop down menu and select the vSwitch that attaches to the UTM Offload device and set the **MTU** to be **1600 bytes**.





Security considerations

In all use cases UTM Offload should be deployed on a physically secured network because data traffic between the forwarding device and offload device has no additional security applied. LAN and WAN traffic are exposed on the offload network. UTM Offload does not increase the vulnerability of the forwarding device, as long as the physical link from the forwarding device to the offload device is secure.

Configuring Firewall and NAT allowing UTM Offload on the AR4050S

The following is a simple configuration for firewall and NAT allowing UTM Offload.

Configuration notes

- Rule 30 will allow the device to access the Update Manager.
- You need to configure a DNS Server address to allow communication with the update manager.
- The offload device synchronizes the time from the forwarding device. This ensures log messages are correctly time-stamped. Therefore, NTP is configured on the forwarding device (AR4050S).

```
!
zone private
  network lan
  ip subnet 192.168.10.0/24 interface vlan1
network offload
  ip subnet 192.168.100.0/24 interface eth2
!
zone public
 network all
  ip subnet 0.0.0.0/0 interface eth1
 host router
  ip address dynamic interface eth1
!
firewall
 rule 10 permit any from private to private
 rule 20 permit any from private to public
 rule 30 permit any from public.all.router to public
 protect
!
nat
 rule 10 masq any from private to public
 enable
!
ntp server <URL>
!
utm-offload interface eth2 subnet 192.168.100.0/24
!
ip name-server <x.x.x.x>
!
interface vlan1
 ip address 192.168.10.1/24
!
interface eth1
 ip address dhcp
!
```

UTM Offload glossary

- **Forwarding device (AR4050S)**

  The device that intercepts packets, sends them to the offload device for processing and finally forwards the packets when they return. It also manages the configuration of the offload device.

- **Offload Device**

  The headless device that provides UTM packet processing offload for the forwarding device. A headless device is a device that does not have a user-facing User interface.

- **Offload Image**

  Full software release that runs on the offload device. The offload image is downloaded from the Update Server by the forwarding device and used to network boot the offload device.

- **PXE Boot**

  Pre-boot Execution Environment (PXE) is the standard method used to boot off the shelf hardware across a network without first needing to install software on that hardware. The forwarding device functions as a PXE boot server to boot the offload device using the offload image.

- **Service Function Chaining (SFC)**

  SFC is a standardized mechanism for how network service functions are applied to packets. Packets are classified and matched by local policy to a configured Service Function Path (SFP).

  Those packets are then forwarded by the Service Function Forwarder (SFF) to each Service Function (SF) in the order specified in the path. SFC is used internally in UTM Offload as the underlying mechanism for offloading packets to the remote UTM engine.

- **UTM**

  In the context of UTM Offload, consists of one or more of the following security features:

  - **IDS/IPS.** Detects packets/flows that may threaten the network and when run in inline mode, prevents that threat.
  - **IP Reputation.** Categorizes public hosts based on their global reputation so that undesirable traffic can be blocked.
  - **URL Filtering.** Blocks access to websites that are known to contain resources that could potentially cause harm to endpoints.
  - **Malware Protection.** Scans traffic byte streams for signatures of common Malware and prevents that Malware from entering the network.

- **Bare-Metal Hypervisor**

  A hypervisor or virtual machine monitor (VMM) is computer software, firmware or hardware that creates and runs virtual machines. A bare-metal hypervisor, also known as a Type 1 hypervisor, is virtualization software that has been installed directly onto the computing hardware and does not require the installation of an additional underlying operating system.

Logging

This section gives a brief summary of what you can log in AlliedWare Plus devices, including how to read AlliedWare Plus log messages, followed by details about logging for each of the UTM features, and a simple configuration example.

- "Log message filtering—general" on page 66
- "Reading log messages" on page 67
- "Firewall log messages" on page 67
- "UTM log messages" on page 68
- "IPS log messages" on page 69
- "IP Reputation log messages" on page 70
- "Malware Protection log messages" on page 71
- "URL Filtering log messages" on page 72
- "Web Control log messages" on page 74
- "Antivirus log messages" on page 74
- "Firewall connection logging" on page 75
- "UTM Offload logging" on page 77

For detailed information about configuring logging, see the Logging Feature Overview and Configuration Guide and the 'Logging Commands' chapter in the Command Reference for your product.

Log message filtering—general

You can selectively log messages generated by AlliedWare Plus according to the severity level, the program that generates them, the facility assigned to them, or a specified string contained in the message. This allows you to select and log all the messages of particular severity levels or for a particular feature or facility with a single filter.

Reading log messages

Log messages generated by AlliedWare Plus show information in the following format:

```
<date> <time> <facility>.<severity> <hostname> <program>[<pid>]: <message>
```

Table 3: Elements in log messages

ELEMENT	DESCRIPTION
`<date> <time>`	The date and time when the log message was generated, according to the device's clock.
`<facility>`	The facility assigned for the message.
`<severity>`	The severity level of the message, indicating its importance.
`<hostname>`	The device's hostname, as configured by the **hostname** command (default: awplus).
`<program>`	Within the modular operating system, the particular program that generated the message. Some programs correspond to particular features (e.g., MSTP, EPSR), while others correspond to internal functions in the operating system (e.g. kernel).
`<pid>`	The process ID (PID) of the current instance of the software program that generated the message. A particular process ID does not always correspond to the same program. Some log messages, such as kernel messages, may not include a process ID.
`<message>`	The specific content of the log message. This may include some variable elements, such as interface names, and some strings that are fixed.

Firewall log messages

Firewall log messages are logged with facility 'kern', and have severity level 'info' (6). The message part includes information in the following format:

```
Firewall [rule <rule>]: <action> IN=<input-interface> OUT=<output-
interface> SRC=<source-ip> DST=<dest-ip> MARK=<mark> ...
```

Table 4: Elements in firewall log messages

Message element	Description
`<rule>`	The number of the firewall rule applied. If a packet is dropped by the default deny policy, there is no rule number.
`<action>`	The action applied to the packet or flow by the firewall; one of DENY, LOG, PERMIT or REJECT.
`<input-interface>`	The interface via which the traffic was received by the firewall.
`<output-interface>`	The interface via which the traffic was to be transmitted by the firewall.
`<source-ip>`	The source IP address of the packet.
`<dest-ip>`	The destination IP address of the packet.
`<mark>`	The DPI mark—the last 3 digits are the DPI application index in hexadecimal.
`...`	Any other packet details available.

Output 5: Example firewall log messages

```
2016 Nov 28 23:26:34 kern.info awplus kernel: Firewall rule 10: PERMIT IN=
OUT=eth0 SRC=192.168.5.2 DST=192.168.5.1 LEN=84 TOS=0x00 PREC=0x00 TTL=64
ID=7935 DF PROTO=ICMP TYPE=8 CODE=0 ID=2406 SEQ=1
2016 Nov 25 14:10:38 kern.info awplus kernel: Firewall: DENY probe FIN IN=vlan1
OUT=eth1 MAC=00:00:cd:38:00:bc:52:54:6b:6b:0f:1e:08:00 SRC=192.168.1.1
DST=172.16.1.2 LEN=40 TOS=0x00 PREC=0x00 TTL=63 ID=54219 PROTO=TCP SPT=6000
DPT=21 WINDOW=512 RES=0x00 UG PSH FIN URGP=0
2016 Nov 25 18:38:36 kern.info awplus kernel: Firewall rule 20: PERMIT IN=eth1
OUT=vlan1 MAC=00:00:cd:38:00:96:52:54:78:36:8f:a6:08:00 SRC=172.16.1.2
DST=192.168.1.1 LEN=239 TOS=0x00 PREC=0x00 TTL=63 ID=20563 DF PROTO=TCP SPT=80
DPT=46254 WINDOW=905 RES=000 ACK PSH URGP=0 MARK=0x1053
```

UTM log messages

The log messages from various UTM security features may come from a variety of sources and it is sometimes not obvious to users which program names they need to specify in order to get the logs from different features.

Log messages related to the firewall UTM features are generated by different programs, but from AlliedWare 5.4.7-1.x they are all now assigned the facility ‘local5’. This means you can easily filter log messages for all UTM messages via a single filter, for instance, to send all UTM log messages from multiple devices to a single destination.

The UTM log messages are generated by these programs:

- The program IPS generates messages for the Suricata stream-based security features Intrusion Prevention System, IP Reputation, Malware Protection, URL Filtering.
- The UTM program generates messages for the proxy-based features Web Control and Antivirus.

Configuration example: logging UTM messages

To configure an AR-Series firewall to generate log messages for any UTM features in use and send them to a syslog server at IP address 192.168.1.1, use the commands:

```
awplus# configure terminal
awplus(config)# log host 192.168.1.1 facility local5
```

To configure an AR-Series firewall to generate and send log messages for any UTM features in use into the buffered log, use the commands:

```
awplus# configure terminal
awplus(config)# log buffered facility local5
awplus(config)# exit
```

To selectively view only the log messages that have been sent to the buffered log that contain the facility local5, use the command line interface:

```
awplus# show log |grep local5
```

For each specific UTM feature, particular information will be generated in the log messages, as described below.

IPS log messages

IPS log messages have severity ‘info’ (6). The message part includes information in the following format:

<***action***> IPS: <***alert-msg***> [URL:<***url***>] <***protocol***> <***source-ip***>:<***source-port***> -> <***dest-ip***>:<***dest-port***>

Table 5: Elements in IPS log messages

Message element	Description
<action>	The action applied; [ALERT] or [DROP].
<alert-msg>	The rule specific message.
<url>	The requested URL if the flow is HTTP.
<protocol>	The protocol e.g., SMTP, HTTP, TCP, ICMP
<source-ip>:*<source-port>*	The source IP address and source port for the packet.
<dest-ip>:*<dest-port>*	The destination IP address and source port for the packet.

Output 6: Example IPS log messages

```
2016 Nov 17 02:49:57 local5.info awplus IPS[2369]: [Alert] IPS: smtp-events SMTP
no server welcome message [smtp] 172.16.92.2:25 -> 192.168.92.1:35992
2016 Nov 17 02:55:18 local5.info awplus IPS[2682]: [Alert] IPS: icmp-decoder-
events ICMPv4 unknown type [icmp] 172.16.92.2 -> 192.168.92.1
2016 Nov 17 03:15:23 local5.info awplus IPS[2398]: [Alert] IPS: checksum UDPv4
invalid checksum [udp] 192.168.92.1:2718 -> 172.16.92.2:0
2016 Nov 17 03:08:01 local5.info awplus IPS[2064]: [Drop] IPS: icmp-decoder-
events ICMPv4 unknown type [icmp] 192.168.92.1 -> 172.16.92.2
```

IP Reputation log messages

IP Reputation log messages have severity ‘info’ (6). The message includes information in the following format:

```
<action> IPREP: <alert-msg> (URL:<url>) <protocol> <source-ip>:<source-port> -> <dest-ip>:<dest-port>
```

Table 6: Elements in IP Reputation log messages

Message element	Description
<action>	The action applied by the IP reputation feature; [ALERT] or [DROP].
<alert-msg>	The rule specific message.
<url>	The requested URL if the flow is HTTP.
<protocol>	The protocol e.g., SMTP, HTTP, TCP, ICMP
<source-ip>	The source IP address for the packet.
<dest-ip>	The destination IP address for the packet.

Output 7: Example IP Reputation log message when traffic from a blacklisted IP address is alerted

```
2016 Nov 17 02:48:19 local5.info awplus IPS[2015]: [Alert] IPREP: DDoSAttacker:
IPREP DDoS Source [icmp] 172.16.92.2 -> 172.16.92.1
```

Output 8: Example IP Reputation log message when traffic from a blacklisted IP address is dropped

```
2016 Nov 17 02:48:01 local5.info awplus IPS[2014]: [Drop] IPREP: DDoSAttacker:
IPREP DDoS Source [icmp] 172.16.92.2 -> 172.16.92.1
```

Whenever IP Reputation starts up or is reloaded due to a new provider resource becoming available, or due to a change in configuration, log messages are generated. A log message is generated for each whitelist entry showing whether or not it matches an entry in a provider blacklist. For example:

Output 9: Example IP Reputation log messages at startup or when provider resource updated

```
2019 Oct 17 13:27:50 local5.info awplus streamd[1115]: IP-Reputation Whitelist:
192.0.2.4 matches provider blacklist (cat Scanner)
```

Output 10: Example IP Reputation log messages at startup or when provider resource updated

```
13:27:50 local5.alert awplus streamd[1115]: IP-Reputation Whitelist:
198.51.100.3 doesn't match provider blacklist(s)
```

If a whitelist address is reported as not matching a provider list, we recommend removing the address from the whitelist. This is important as it means you will be newly alerted if the address gets a bad reputation again some time in the future.

There is a limit of 128 whitelist entries. If more than this number are configured, the excess addresses are not applied. If too many addresses have been configured, IP Reputation will generate log messages showing which addresses haven't been applied. For example:

```
13:27:50 awplus streamd[1115]: IP-Reputation Whitelist: 203.0.113.2 not
applied. Already at whitelist entry limit (128 entries)
```

To update the whitelist, see "Configuring IP Reputation" on page 37. For more information, see "IP Reputation" on page 13.

Malware Protection log messages

Malware protection log messages have severity info (6). The message part includes information in the following format:

```
<action> MALWARE: <alert-msg> [URL:<url>] <protocol> <source-ip>:<source-
port> -> <dest-ip>:<dest-port>
```

Table 7: Elements in Malware Protection log messages

Message element	Description
<action>	The action applied by malware protection; [ALERT] or [DROP]
<alert-msg>	The rule specific message.
<url>	The requested URL if the flow is HTTP.
<protocol>	The protocol e.g., SMTP, HTTP, TCP, ICMP
<source-ip>:*<source-port>*	The source IP address and source port for the packet.
<dest-ip>:*<dest-port>*	The destination IP address and source port for the packet.]

Output 11: Example Malware Protection log messages

```
2016 Nov 17 02:13:08 local5.info awplus IPS[1939]: [Drop] MALWARE: Virus
detected by signature URL:http:/[172.16.92.2]/data/byte/sample.exe [http]
172.16.92.2:80 -> 192.168.92.1:60784
2016 Nov 17 02:32:02 local5.info awplus IPS[2014]: [Drop] MALWARE: Virus
detected by signature [tcp] 172.16.92.2:42168 -> 192.168.92.1:45528
2016 Nov 17 02:33:59 local5.info awplus IPS[1913]: [Drop] MALWARE: File with
known bad MD5 detected (ITW) URL:http:/[172.16.92.2]/data/md5/EICAR-Test-File
[http] 172.16.92.2:80 -> 192.168.92.1:60820
2016 Nov 17 02:36:32 local5.info awplus IPS[2004]: [Drop] MALWARE: File with
known bad MD5 detected (ITW) [smtp] 192.168.92.1:45820 -> 172.16.92.2:25
```

URL Filtering log messages

By default, URL Filtering messages are generated when there are:

- Blacklist and whitelist hits—logged at severity **info (6)** level.
- Invalid match criteria, detected while loading third party and custom blacklist and whitelist files—logged at **err (3)** level.
- Missing configured custom blacklist and/or whitelist files, while starting/restarting the feature—logged at **warning (4)** level.

From AlliedWare Plus version 5.4.7-1.x, you can turn on additional URL request logging to log **all** URL requests, including permitted requests. Use the following commands:

```
awplus(config)# url-filter
awplus(config-url-filter)# log url-requests
```

Log messages for blacklist or whitelist hits include information in the following format:

```
<action> URLFILTER: [URL:<url>] <protocol> <source-ip>:<source-port> ->
<dest-ip>:<dest-port>
```

Table 8: URL Filtering log message elements

Message element	Description
<action>	Which action is applied; [ALERT], [DROP] or [http].
<url>	The requested URL if the flow is HTTP.
<protocol>	The protocol e.g., SMTP, HTTP, TCP, ICMP.
<source-ip>:*<source-port>*	The source IP address and source port for the packet.
<dest-ip>:*<dest-port>*	The destination IP address and source port for the packet.

Output 12: Example URL filtering log message for a dropped URL request

```
2016 Nov 17 02:02:21 local5.info awplus IPS[2039]: [Drop] URLFILTER: URL:http:/
kdskspb.ru/ [http] 192.168.1.1:58272 -> 172.16.1.2:80
```

Output 13: Example URL filtering log message for a permitted URL request when **log url-requests** is configured

```
2017 Apr 12 03:47:21 local5.info awplus IPS[3885]: [Http] URL:http://172.16.1.2/
192.168.1.1:53698 -> 172.16.1.2:80
```

By default, URL Filtering only logs dropped requests. However, from 5.4.7-1.x, you can turn on additional URL request logging to log **all** URL requests, including permitted requests. Use the following commands:

```
awplus(config)# url-filter
```

```
awplus(config-url-filter)# log url-requests
```

Note: This is supported in all AR-Series firewalls.

By default, URL Filtering messages are generated when there are:

- Blacklist and whitelist hits—logged at severity **info (6)** level.
- Invalid match criteria, detected while loading third party and custom blacklist and whitelist files—logged at **err (3)** level.
- Missing configured custom blacklist and/or whitelist files, while starting/restarting the feature—logged at **warning (4)** level.

Log messages for blacklist or whitelist hits include information in the following format:

```
<action> URLFILTER: [URL:<url>] <protocol> <source-ip>:<source-port> ->
<dest-ip>:<dest-port>
```

Table 9: URL Filtering log message elements

Message element	Description
<action>	Which action is applied; [ALERT], [DROP] or [http].
<url>	The requested URL if the flow is HTTP.
<protocol>	The protocol e.g., SMTP, HTTP, TCP, ICMP.
<source-ip>:*<source-port>*	The source IP address and source port for the packet.
<dest-ip>:*<dest-port>*	The destination IP address and source port for the packet.

Output 14: Example URL Filtering log message for a dropped URL request

```
2016 Nov 17 02:02:21 local5.info awplus IPS[2039]: [Drop] URLFILTER: URL:http:/
kdskspb.ru/ [http] 192.168.1.1:58272 -> 172.16.1.2:80
```

Output 15: Example URL Filtering log message for a permitted URL request when **log url-requests** is configured

```
2017 Apr 12 03:47:21 local5.info awplus IPS[3885]: [Http] URL:http://172.16.1.2/
192.168.1.1:53698 -> 172.16.1.2:80
```

Web Control log messages

The message part includes information in the following format:

```
Web_Control: <action> <url> requested by <source-ip>: <category>, <order>
```

Table 10: Elements in Web Control log messages

Message element	Description
<action>	The action applied by the Web Control feature; either BLOCK or ALLOW.
<url>	The requested URL.
<source-ip>	The IP address of the requester.
<category>	The Web Control category of the website.
<order>	The Web Control rule number.

Web control block messages have severity level ‘warning’ (4); allow messages have severity level ‘info’ (6).

Output 16: Example Web Control log message

```
2016 Nov 26 08:11:15 local5.warning awplus UTM[828]: Web_Control: BLOCK http:/
/www.piracy.com/ requested by 192.168.1.1: Piracy, 0
```

Antivirus log messages

When Antivirus detects a virus named in its database it generates messages with the following format:

```
antivirus: Virus <virus> detected in <url> to <client-ip>
```

Antivirus can also generate messages in the following formats for issues related to scanning the traffic:

```
antivirus: Unable to scan <url> to <client-ip>: <reason>
antivirus: Unable to allocate memory to scan <url> to <client-ip>
antivirus: Max scan depth exceeded for <url> to <client-ip>
```

All the above Antivirus log messages have severity level ‘warning’ (4).

Table 11: Elements in Antivirus log messages

Message element	Description
<virus>	The name of the virus detected.
<url>	The requested URL.
<client-ip>	The IP address of the requester.
<reason>	Reason for failure to scan.

Output 17: Example Antivirus log message

```
2016 Nov 25 10:15:51 local5.warning awplus UTM[802]: antivirus: Virus EICAR-
Test-File[certain] detected in http://www.example.com/data/infected/sample.txt
to 192.168.1.1
```

Firewall connection logging

This feature is supported from AlliedWare Plus version 5.4.7-1.

Firewall connection logging can be enabled to provide additional logs that show the start and end of connections passing through the firewall. These messages are assigned facility local5. They have severity ‘info’ (6).

To enable logging of new connections, closed connections, or both passing through the firewall, use the commands:

```
awplus# configure terminal
awplus(config)# connection-log events {new|end|all}
```

To show the configuration of firewall connection logging, use the following command:

```
awplus# show connection-log events
```

Output 18: Example output from show connection-log events

```
awplus#show connection-log events
Log new connection events:    Disabled
Log connection end events:    Enabled
```

New connection log messages includes information in the following format for a newly started firewall connection:

```
NEW proto={tcp|udp|icmp|...|<number>} orig_src={<ipv4-addr>|<ipv6-addr>}
orig_dst={<ipv4-addr>|<ipv6-addr>} [orig_sport=<source-port>]
[orig_dport=<dest-port>] reply_src={<ipv4-addr>|<ipv6-addr>}
reply_dst={<ipv4-addr>|<ipv6-addr>} reply_sport=<source-port>
reply_dport=<dest-port>
```

Closed connection log messages includes information in the following format for a firewall connection that has ended:

```
END proto=[tcp|udp|icmp|...|<protocol-number>] orig_src={<ipv4-addr>|
<ipv6-addr>} orig_dst={<ipv4-addr>|<ipv6-addr>} [orig_sport=<source-port>]
[orig_dport=<dest-port>] orig_pkts=<packets> orig_bytes=<bytes>
reply_src={<ipv4-addr>|<ipv6-addr>} reply_dst={<ipv4-addr>|<ipv6-addr>}
reply_sport=<source-port> reply_dport=<dest-port> reply_pkts=<number>
reply_bytes=<number>
```

Table 12: Elements in firewall connection log messages

Message elements	Description
`proto={tcp|udp|icmp|<protocol>|<number>}`	The protocol or protocol number for the connection.
`orig_src={<ipv4-addr>|<ipv6-addr>}`	The source IPv4 or IPv6 address of the packet originating the connection.
`orig_dst={<ipv4-addr>|<ipv6-addr>}`	The destination IPv4 or IPv6 address for the packet originating the connection.
`orig_sport=<source-port>`	The source port number of the originating packet.
`orig_dport=<dest-port>`	The destination port number of the originating packet.
`orig_pkts=<packets>`	The total number of packets passed in the originating direction.
`orig_bytes=<bytes>`	The total number of bytes passed in the originating direction.
`reply_src={<ipv4-addr>|<ipv6-addr>`	The source IPv4 or IPv6 address of the returning packets.
`reply_dst={<ipv4-addr>|<ipv6-addr>`	The destination IPv4 or IPv6 address of the returning packets.
`reply_sport=<source-port>`	The source port number of the returning packets.
`reply_dport=<dest-port>`	The destination port number of the returning packets.
`reply_pkts=<number>`	The total number of returning packets.
`reply_bytes=<number>`	The total number of returning bytes.

Note that the original source and destination addresses and ports may differ from the reply source address and destination addresses and ports depending on whether NAT is applied and the type of NAT.

Output 19: Example connection log messages for TCP connection

```
NEW proto=TCP orig_src=192.168.1.100 orig_dst=192.168.1.1 orig_sport=55532
orig_dport=80 reply_src=192.168.1.1 reply_dst=192.168.1.100 reply_sport=80
reply_dport=55532

END proto=TCP orig_src=192.168.1.100 orig_dst=192.168.1.1 orig_sport=55532
orig_dport=80 orig_pkts=7 orig_bytes=522 reply_src=192.168.1.1
reply_dst=192.168.1.100 reply_sport=80 reply_dport=55532 reply_pkts=4
reply_bytes=811
```

Output 20: Example connection log messages for ICMP connection

```
NEW proto=ICMP orig_src=192.168.1.1 orig_dst=192.168.1.100
reply_src=192.168.1.100 reply_dst=192.168.1.1

END proto=ICMP orig_src=192.168.1.1 orig_dst=192.168.1.100 orig_pkts=2
orig_bytes=168 reply_src=192.168.1.100 reply_dst=192.168.1.1 reply_pkts=2
reply_bytes=168
```

UTM Offload logging

The following UTM Offload items are logged:

- Change in state of the offload device.
- Communication failure between the AR4050S and the offload device.
- Existing UTM feature log messages appear in the AR4050S log transparently.
- Other general log messages generated by the offload device appear in the AR4050S log transparently.
- Messages from the offload device appearing in the AR4050S log have the offload device's IP address, the timestamp for when the message was generated and the string "offload" inserted.

When the AR4050S detects the offload device is no longer present it will:

- output a log message
- stop sending packets to the offload device for processing
- install a rule to block traffic from being forwarded across the forwarding device (this allows management of the forwarding device to continue, but continues to protect the user)

Checking the UTM offload status

To see the status of the offload device, use the command:

```
awplus#show utm-offload
```

Figure 11: Output from **show utm-offload**

```
awplus#show utm-offload
Status:       Enabled (Booted)
Interface:    eth2
Subnet:       192.168.100.0/24
Resource update interval: 1 hour

awplus#show resource
------------------------------------------------------------------------------
Resource Name          Status       Version    Interval  Last Download
                                                          Next Download Check
------------------------------------------------------------------------------
dpi_procera_app_db     Sleeping     dpi_procera_app_db_v66
                                               1         None
                                               hour     Sun  1 Jul 2018 21:58:54
afa_offload            Sleeping     afa_main_offload_v51
                                               1         None
                                               hour     Sun  1 Jul 2018 21:47:41
iprep_et_rules         Sleeping     iprep_et_rules_v8582
                                              1        Mon  2 Jul 2018 04:05:06
                                               hour     Mon  2 Jul 2018 06:05:03
```