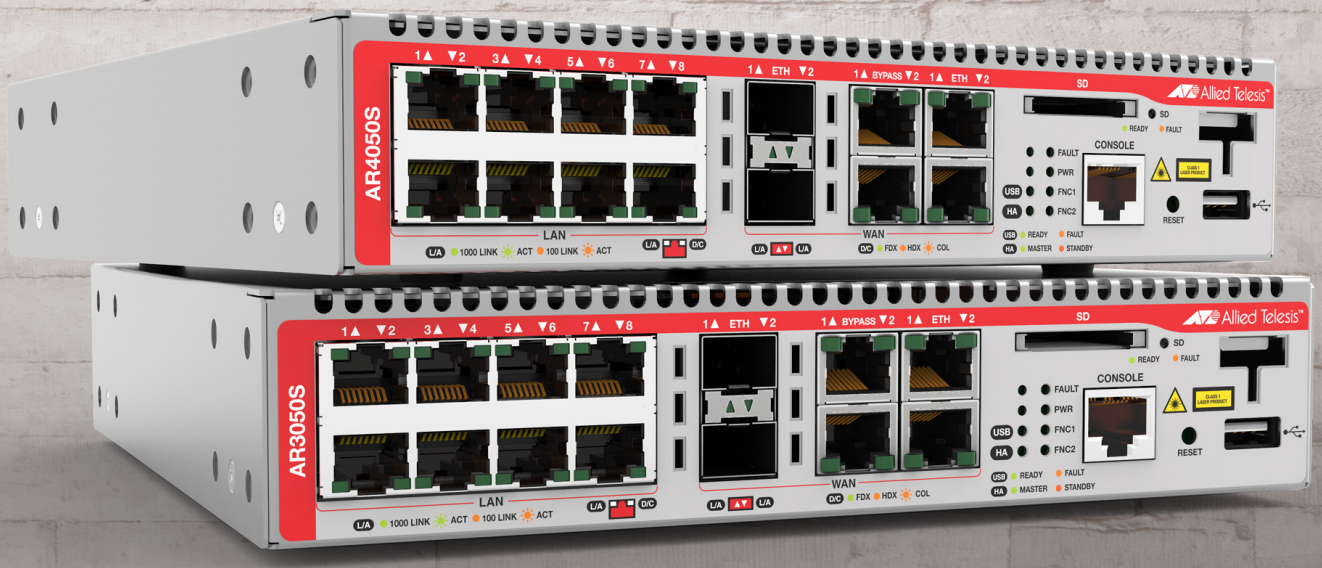
Technical Guide

Allied Telesis™

Feature Overview and Configuration Guide

Advanced Network Protection



AlliedWare Plus™
OPERATING SYSTEM

alliedtelesis.com

C613-22104-00 REV H

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

IP Reputation 13

Web Categorization for blocking web traffic by category 15

Web Control 16

UTM Offload 19

Selecting a security solution **21**

Packet flow architecture 21

Selecting a UTM firewall 24

Firewall/NAT rules, entities and performance 26

Configuring Intrusion Prevention System (IPS) **27**

Configuring IP Reputation **29**

Configuring Web-Categorization to block web traffic by category **31**

Configuring Web Control **34**

How to configure basic Web Control 34

How to configure Web Control default action per-entity 36

How to discover which Web Control category a website URL belongs to 40

Setting up and configuring UTM Offload **42**

Setting up UTM Offload 42

About the offload image 44

Configuring UTM Offload on VMware ESXi Server 45

Security considerations 51

Configuring Firewall and NAT allowing UTM Offload on the AR4050S or AR4050S-5G 51
UTM Offload glossary.....52

Logging 54
Log message filtering—general.....55
Reading log messages 55
Firewall log messages 55
UTM log messages 56
IPS log messages.....57
IP Reputation log messages 58
Malware Protection log messages 59
URL Filtering log messages 60
Web Control log messages 61
Antivirus log messages 62
Firewall connection logging.....62
UTM Offload logging 64

Appendix: Features using providers Digital Arts or Kaspersky 66
Security feature licenses 66
Selecting a solution 66
Web-Categorization using provider Digital Arts 68
Web Control using provider Digital Arts 68
Antivirus using provider Kaspersky.....69
Malware Protection using provider Kaspersky.....72
URL Filtering using provider Kaspersky 74

Introduction

This guide describes the Advanced Network Protection features on AlliedWare Plus UTM firewalls 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
- IP Reputation
- Web Categorization
- Web Control
- Application Control
- URL Filtering

Also, on the AR4050S and AR4050S-5G, 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 and AR4050S-5G.

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 21
- Guidance for selecting a UTM firewall based on security and performance requirements of your network, in "Selecting a UTM firewall" on page 24
- How to configure each of the security features, including examples
- Descriptions of logging available for each of the security features, in "Logging" on page 54.
- An appendix for features using providers Digital Arts or Kaspersky in "Appendix: Features using providers Digital Arts or Kaspersky" 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 AlliedWare Plus 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
- version 5.5.2-2.1 and onwards support Advanced IPS.

IP Reputation

- Version 5.4.5

Web-categorization

- Version 5.5.2-0.1 and onward support DPI with web-categorization.

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.
- Version 5.5.4-1.2 and later Web Control uses streaming processes (earlier versions were proxy-based).

UTM Offload

- Version 5.4.8-1.2 supports UTM Offload (AR4050S and AR4050S-5G 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.

Malware Protection

- Version 5.4.5

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).

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 Device GUI on UTM Firewalls
- 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 does not describe to Secure VPN routers. For information about Secure VPN routers, see the AR-Series Secure VPN Router range.

Licensing

The AlliedWare Plus UTM firewalls have subscription licensing options for the advanced security features. The following table shows the features included in those licenses:

Table 1: UTM feature licenses

License	Description	Features included
Base license		Intrusion Prevention System (IPS)
AT-AR3-UTM-01-xYR (AR3050S) AT-AR4-UTM-01-xYR (AR4050S, AR4050S-5G, 10GbE UTM Firewall, AR4000S Cloud)	Advanced Firewall x indicates 1, 3 or 5 years	Application Control (DPI) (provider Procera) Web Categorization (provider OpenText) Web Control (provider OpenText)
AT-AR4-UTM-02-xYR [a] (AR4050S or AR4050S-5G, 10GbE UTM Firewall, AR4000S Cloud)	Advanced Threat Protection x indicates 1, 3 or 5 years	Advanced IPS (provider Proofpoint) IP Reputation
AT-FL-UTM-OFFLOAD-xYR (AR4050S, AR4050S-5G)	UTM Offload license x indicates 1, 3 or 5 years	UTM Offload Install the UTM Offload license and the offloadable UTM feature license on the forwarding device (the AR4050S or AR4050S-5G), not the offload device.

a. From AlliedWare plus version 5.5.4-1 onwards, you can use licences AT-AR4-UTM-01 and AT-AR4-UTM-02 together on the AR4050S/AR4050-5G, 10GbE UTM Firewall, or AR4000S Cloud.
In earlier versions, AT-AR4-UTM-01 and AT-AR4-UTM-02 cannot be used together.

To obtain a license, contact your authorized Allied Telesis service and support centre.

For more information about:

- security and feature licenses, see the UTM Firewalls and AR4050S-5G Datasheets
- installing licenses, see the ‘Subscription Licenses’ section of the Licensing Feature Overview and Configuration Guide
- Application Control, see Application Awareness Feature Overview and Configuration Guide .

Feature overview

This section provides a brief description of each of the Advanced Network Protection features available on the AlliedWare Plus UTM firewalls.

- **Advanced 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 27.

- **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 29.

- **Web Categorization with Application Awareness**

  You can use Web Categorization with Application Awareness to determine which web traffic to block or permit in your network based on which categories the traffic the traffic belongs to. Web Categorization uses third party categorization service OpenText to assess which categories of traffic the hostnames are associated with.

  For more information about how it works, see "Web Categorization for blocking web traffic by category" on page 15. To configure this feature, see "Configuring Web-Categorization to block web traffic by category" on page 31.

- **Web Control**

  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 16. To configure this feature, see "Configuring Web Control" on page 34.

For information about features that use third-party provider Kaspersky, see "" on page 65.

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 AlliedWare Plus 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 21.

On the AR4050S and AR4050S-5G, 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 or AR4050S-5G. See "UTM Offload" on page 19.

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 27.

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
- 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 and third-party provided categories, currently provided by Proofpoint. Use the command **show ips categories** to show the categories. For extra information about all categories, or a specific category, use the command **show ips categories detail [<*category*>]**.

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 (inline) 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

Advanced IPS support

From version 5.5.2-2.1 onwards, AlliedWare Plus provides Advanced IPS (Intrusion Prevention System) functionality.

This is made possible by the addition of the third-party vendor Emerging Threat (ET) Intelligence Pro Ruleset from ProofPoint. The Proofpoint ET Pro Ruleset detects and blocks advanced threats. Updated daily, it covers malware delivery, command and control, attack spread, in-the-wild exploits and vulnerabilities, and credential phishing. It also detects and blocks distributed denial-of service attacks (DDoS), protocol and application anomalies, exploit kits and supervisory control and data acquisition (SCADA) attacks.

Both the advanced, and built-in IPS rules-sets are utilised by the Suricata IPS engine. The basic built-in IPS rule-set includes up to several hundred categorized rules, which provides protection against basic known common threats. Conversely, the third party IPS provider has an ever expanding, global set of sensors and Intelligence feeds to detect new threats in real-time. The associated threats are analysed, and categorized, resulting in an Advanced IPS rule-set consisting of tens of thousands of rules, which are updated regularly.

Advanced IPS requires a license, which is available in the bundle pack: AT-AR4-UTM-02-1/ 3/5YR. Contact your authorized Allied Telesis service and support centre to obtain a license.

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 29.

How IP Reputation works

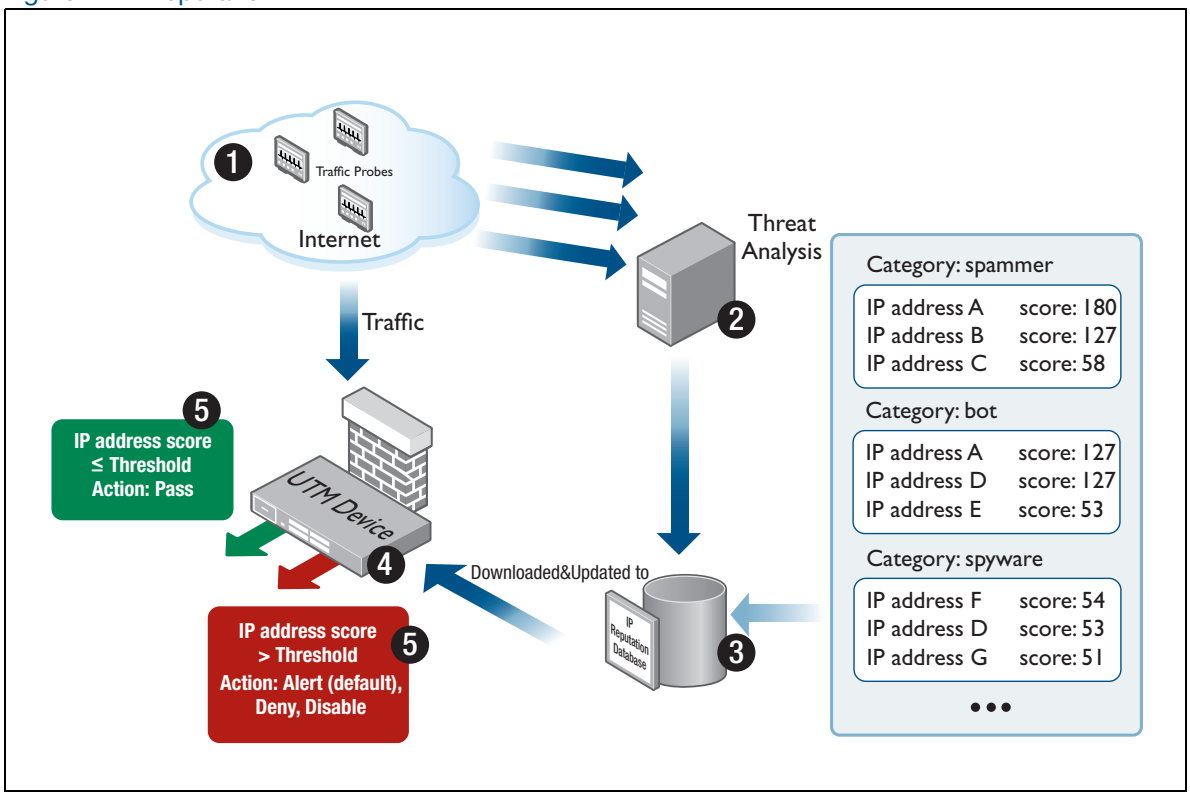
AlliedWare Plus IP Reputation uses categories, which is a grouping of criteria, to classify the nature of a host's reputation. For example, IP addresses associated with questionable gaming sites will be categorized as OnlineGaming.

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 29 and "IP Reputation log messages" on page 58.

Web Categorization for blocking web traffic by category

From software release 5.5.2-0.1 onwards, DPI can be enhanced with Web Categorization. Web Categorization helps protect users on the network based on the type of website they access. It enables businesses to manage the types of website their staff can access.

The DPI engine does this by scanning packets traversing the system and identifying HTTP hostnames or TLS server names and passing these to the Web Categorization engine for subsequent processing. Web Categorization then matches the hostname against custom hosts configured under the ‘application’ configuration mode, and/or sends it to the third party categorizer for processing. So for example, you could block all ‘Gambling’ websites. Once a category has been determined, the packet flow will match rules that specify that category in their application field, for example, Firewall, NAT or PBR rules.

From version 5.4.5 and onwards, AlliedWare Plus includes Web Control. From 5.5.2-0.1 onwards, you can use Web Categorization for faster and more flexible stream-based processing with Deep Packet Inspection (DPI). Both Web Categorization and Web Control use provider OpenText. DPI uses provider Procera or the built-in provider that doesn't require a license.

To use Web Categorization on your device, you need to configure a DPI provider, enable Web Categorization and enable DPI. Hosts are categorized by type (if they are identified by the provider), or in the absence of a category by their usual DPI application.

To configure Web Categorization with Application Control, see "Configuring Web-Categorization to block web traffic by category" on page 31.

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.

This Web Control implementation uses third party website categorization providers.

This section describes AlliedWare Plus Web Control. To configure this feature, see "Configuring Web Control" on page 34.

From software version 5.5.2-0.1 onwards, you can instead use Web-Categorization for more flexible processing with Deep Packet Inspection (DPI). For more information on this, see "Web Categorization for blocking web traffic by category" on page 15.

How Web Control works

Integrated with OpenText, 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 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 the OpenText 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 classifier engine uses custom classification in preference to, and to override, the OpenText categorization. This means if a website matches match criteria from custom categories, then the website will not be sent for categorization by OpenText.

Once the website has been categorized, the device can filter the website according to a set of rules defined per category. If a website is blocked, the user cannot load pages from it. If using HTTP, the user will also see a notification page. Conversely, if the website is allowed, the user can load pages from it.

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.

Figure 2: Web Control block action

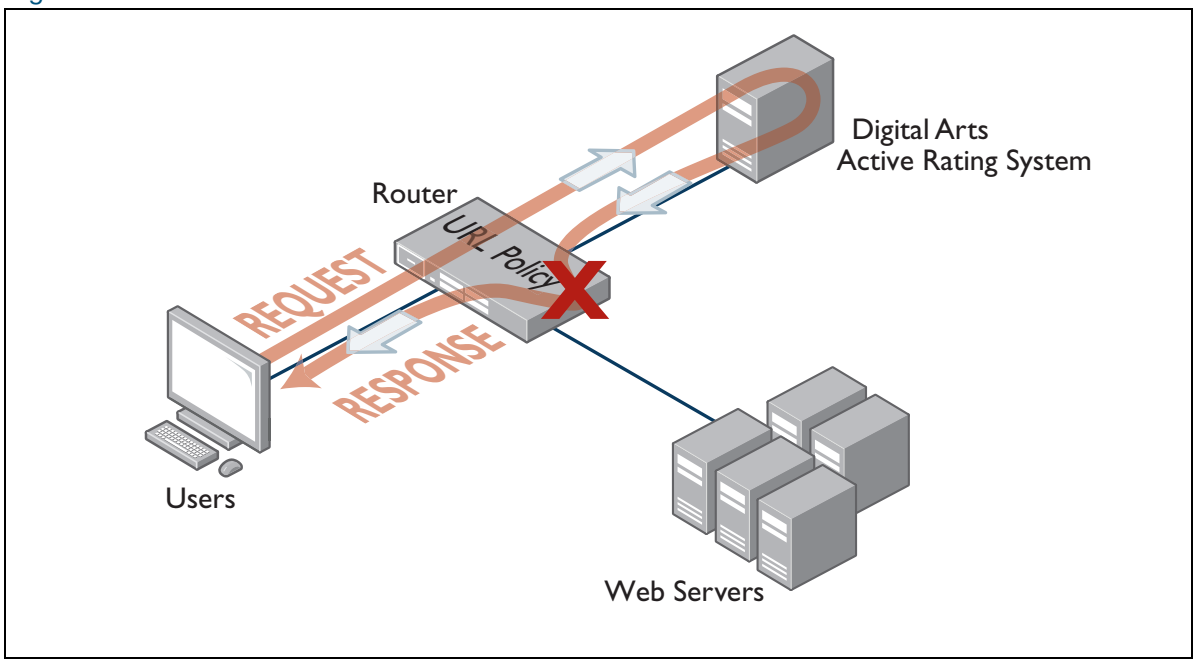
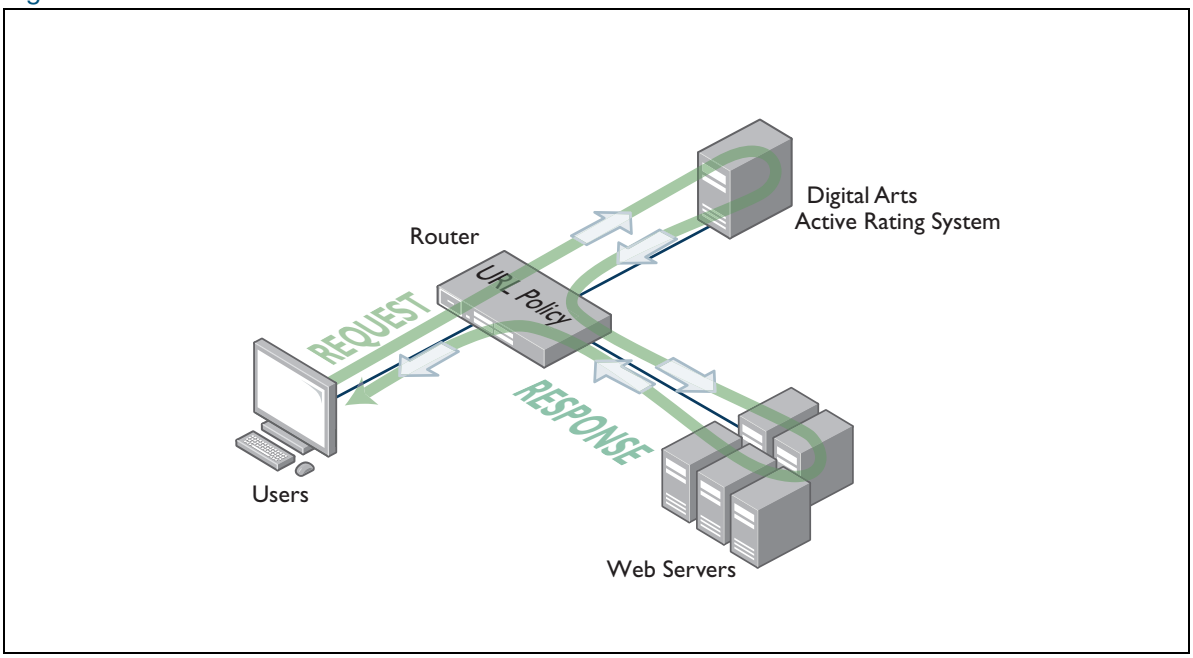


Figure 3: Web Control allow action



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 or AR4050S-5G.

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

The forwarding device—AR4050S or AR4050S-5G:

- boots and manages the offload device.
- configures the offload device.
- presents the status of all features, whether being processed locally on the AR4050S or AR4050S-5G, 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 or AR4050S-5G 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 or AR4050S-5G 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 42.

Selecting a security solution

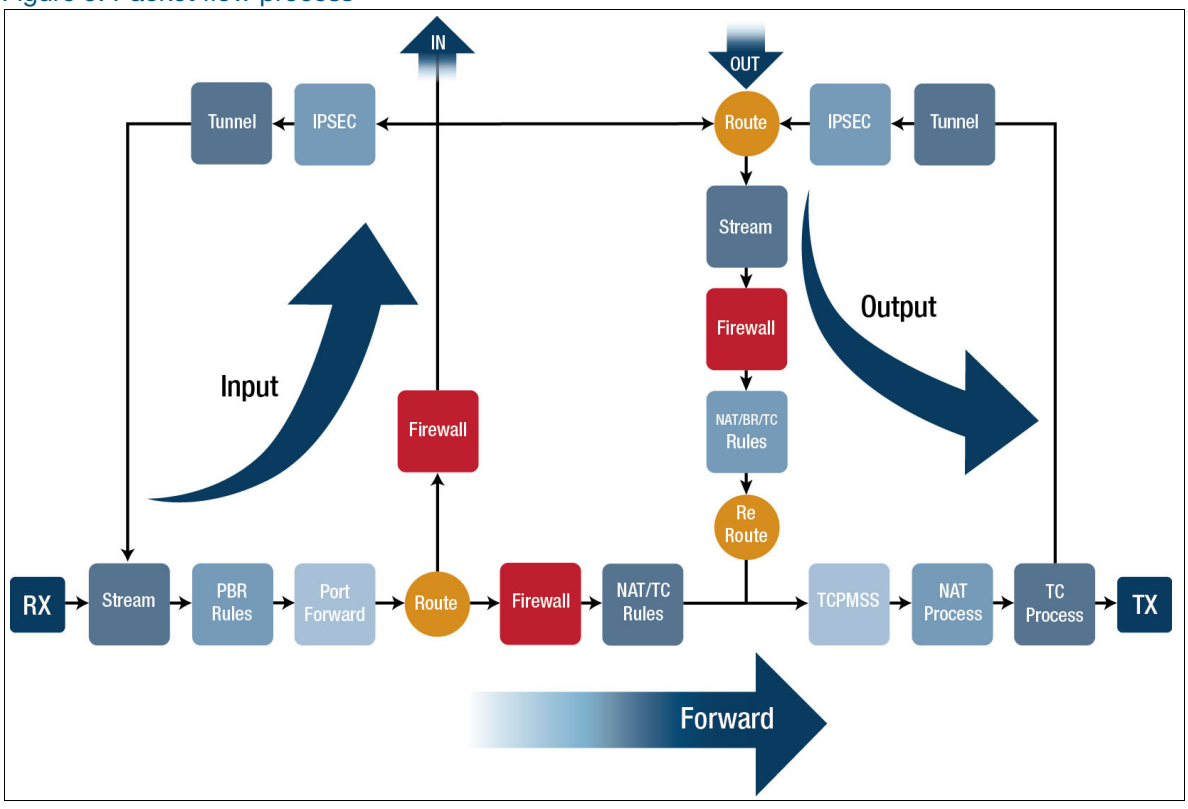
This section describes in more detail the following:

- "Packet flow architecture" on page 21, including UTM CPU processing requirements
- "Selecting a UTM firewall" on page 24, provides information to guide you in selecting a suitable firewall for your network requirements. This includes performance versus security guidelines.
- "Firewall/NAT rules, entities and performance" on page 26

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 above.
2. Stream processing always happens straight after the packet is received on the physical interface. Stream processing includes IPS, Advanced IPS, IP Reputation, Web control, Web Categorization 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.

- 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.

  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.

When tunneling encrytped traffic, we recommend enabling tunnel inline processing. This decrypts traffic prior to stream processing. The earlier method, tunnel security reprocessing, is also supported. If neither of these is enabled, tunneled packets cannot be processed.

Application Awareness (DPI)

As data ingresses the firewall, it is first identified by the DPI application decoding engine if the application awareness feature is enabled. If selected, the inbuilt DPI engine contains a static library of 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 the Application Awareness feature then the number of identifiable applications added and stored in the 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 does not have to be turned on for the security functions described in this guide to operate.

For more information about Application Awareness, see the Application Awareness Feature and Configuration Overview Guide.

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.

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:

- AR3050S
- AR4050S
- AR4050S-5G
- 10GbE Virtual UTM Router (as an app running on VST-APL)

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 Firewall and Web Categorization, where policies are based on users and applications rather than IP addresses, ports and protocols. Also manage user access to websites with Web Categorization or 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.

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 with web-categorization	Real-time threat protection	Application-aware firewall with web-categorization and real-time threat protection[a]
VPN	Unlicensed	Yes	Optional	Optional	Optional
Application Awareness (DPI)	Advanced firewall license	-	Yes	-	Yes
Web-Categorization		-	Yes	-	Yes
IP Reputation	Advanced threat protection license	-	-	Yes	Yes
Advanced IPS		-	-	Yes	Yes
UTM Offload[b]	UTM Offload	-	-	Optional	Optional

a. The scenario Application Aware Firewall with Web Categorization and Real-time Threat Protection is supported on the AR4050S, AR4050S-5G, AR4000S Cloud and 10GbE UTM firewalls.

b. UTM Offload enables the router to offload processing to a secondary physical or virtual machine that is automatically managed by an AR4050S and AR4050S-5G. It is supported from version 5.4.8-1.2 onwards on AR4050S and AR4050S-5G only. UTM Offload is only beneficial when using IP Reputation and IDS/IPS.

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.

Firewall/NAT rules, entities and performance

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

Firewall and NAT rules

Each additional NAT or firewall application rule configured on an AlliedWare Plus 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 example shows how to configure IPS.

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

Step 1: **Enter the IPS mode**

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

Step 2: **(Optional) Select an IPS provider**

```
awplus(config-ips)# provider proofpoint
```

By default, IPS will only use the built-in categories. If you select a provider, IPS can use a lot more categories. Built-in categories are available alongside provider categories.

Step 3: **Enable IPS protection**

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

Step 4: **Verify IPS configuration**

```
awplus# show ips
```

```
awplus#show ips
Status:              Enabled (Active)
Provider:            proofpoint
Events:              0
Alert Thresholding:  Enabled (default)
Resource version:    2.0
Update interval:     1 hour
```

Step 5: **Verify IPS categories**

```
awplus(config)# show ips categories detail
```

A category is a label that helps to classify the nature of traffic, for example, whether it is spammer, spot or spyware and so on. Once IPS protection is enabled, traffic is categorized according to the available IPS categories. You can use the **show ips categories detail** command to view the categories and their actions. In this way, you can decide if category actions should be changed to suit your network's specific needs.

```
awplus#show ips categories detail
Rule Statistics:
 Usage:              176/176
 Alert:              176
 Deny:               0
 Disable:            0

  Category (* = invalid) Action  Rules Description
-------------------------------------------------------------------------
  active-ftp             alert   2     Signatures for detecting when an FTP
                                         connections uses active mode. Active
                                         mode FTP is where the server tries to
                                         initiate the data connection to client
  checksum               alert   7     Signatures for detecting invalid
                                         checksums in IP, TCP, UDP, and ICMP
                                         headers
  ...
  ...
  ...
```

Step 6: **(Optional) Change the actions of categories**

A categories default action can change with time, depending on the current security recommendations. If this is not desired, you can explicitly set a category action to avoid any future changes during updates.

For example, to set the action ‘deny’ on the category ‘active-ftp’, use the command:

```
awplus(config-ips)#category active-ftp action deny
```

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 58 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 Web-Categorization to block web traffic by category

From software release 5.5.2-0.1 onwards, DPI functionality can be used with Web-Categorization. Web-Categorization helps protect users on the network based on the type of website they access. Organizations can use this to manage the types of website their staff can access.

The DPI engine does this by scanning packets traversing the system and identifying HTTP hostnames or TLS server names (SNI) and passing these to the Web Categorization engine for subsequent processing. This hostname is then matched against custom hosts configured under the 'application' configuration mode and/or sent to the third party categorizer (OpenText) for processing. Once a category has been assigned (either custom or via third party categorizer) the traffic can be matched against rules where the category is specified by the "application" parameter (for example, using Firewall or Policy Based Routing).

The earlier method of web categorization (Web Control) also uses OpenText as a website categorization provider. However, its filtering mechanism is much simpler and less flexible. From 5.5.2-0.1 onwards, we recommend using Web-Categorization.

This example shows how to configure application awareness and Web-categorization using Deep Packet Inspection (DPI). By default, application awareness is disabled and you need to explicitly enable it.

Step 1: Enter the DPI mode

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

Step 2: Select Web-Categorization with categorization provider OpenText

```
awplus(config-dpi)# web-categorization opentext
```

Step 3: Select the DPI provider and enable DPI

```
awplus(config-dpi)# provider {procera|built-in}
awplus(config-dpi)# enable
```

Step 4: Add custom web-categorization (optional)

By default, website URLs will be automatically categorized by the external third party provider, so custom web-categorization is optional. Custom matching will take precedence over any third party categorization.

Note: Add hostnames with a leading period to include all sub-domains. These applications can overlap with existing DPI applications.

```
awplus(config-dpi)# application companies
awplus(config-dpi-application)# hostname www.alliedtelesis.co.nz
```

```
awplus(config-dpi-application)# hostname .alliedtelesis.com
```

Note: You can enquire about which categories the URLs belong to. The provider returns a response for each HTTP or HTTPs URL. For example:

```
awplus#dpi categorize http://www.ebay.com http://www.amazon.com
http://www.ebay.com: ==> 54 (online auctions)
http://www.amazon.com: ==> 55 (online shopping)
awplus#dpi categorize https://reddit.com/r/nfl
https://reddit.com: [social-bookmarks (31)] [forums (63)]
```

Step 5: **Configure firewall rules**

Configure firewall rules for access control.

Note: When DPI Web-Categorization is configured, DPI marks all traffic flows as uncategorized to begin with. You can configure a rule to decide what initial action to take the first time a user accesses any given website not yet categorised.

Note: If using DPI Web-Categorization with an external provider (OpenText), and together with firewall which is the usual case, then a new 'system' application needs to be permitted by firewall rule. The system application and associated permit rule is used to match and allow HTTPS-based categorization with the external provider.
If using DPI Web-categorization without an external provider (for example using only custom category without using an external provider), then this firewall application rule is not necessary.

From version 5.5.2-1.1 onwards, you can use the tab key to auto-complete application and entity names. This makes it easier to specify the name of an existing DPI application or firewall entity.

Here is a running configuration example showing how to configure DPI with web categorization and firewall.

The following is an example of how to configure:

- application awareness (DPI) using provider Procera and web-categorization provider OpenText
- a custom blacklist list as an application
- network zones for LAN, WAN and Internet
- firewall rules to permit or deny traffic between the zones, based on source and destination zones, the web category provided by OpenText, and the custom blacklist:
  Rule 30 allows the uncategorised traffic from the LAN to the Internet.
  Rule 40 blocks traffic that matches the custom black list.
  Rule 50 blocks traffic from the LAN to WAN that the provider categorizes as gambling
  Rule 60 permits the traffic from the WAN interface to the Internet that is required for the categorization service operate and to update resources.

```
!
application custom_host_URL_list
 hostname www.google.com
!
zone inet
 network all
 ip subnet 0.0.0.0/0 interface eth1
!
zone lan
 network lan
  ip subnet 192.168.1.0/24 interface vlan1
!
zone wan
 network wan
  ip subnet 0.0.0.0/0 interface eth1
  host wan_int
   ip address dynamic interface eth1
!
firewall
 rule 20 permit undecided from lan to wan
 rule 30 permit uncategorized from lan to wan
 rule 40 deny custom_host_URL_list from lan to wan
 rule 50 deny gambling from lan to wan
 rule 60 permit system from wan.wan.wan_int to inet
protect
!
nat
 rule 10 masq any from lan to wan
 enable
!
dpi
 provider procera
 web-categorization opentext
 enable
!
```

Step 6: **Verify DPI configuration**

```
awplus# show dpi
```

```
Status:      running
Provider:    procera
Mode:        assured
Counters:    global only
Providing application database: disabled
Web Categorization:          enabled
Web Categorization Provider: OpenText
Resource version:         1.0
Resource update interval: 1 hour
```

For more information about applications, about configuring firewall rules to use with DPI, and about migrating a Web Control configuration to use Web-Categorization with DPI, see the Application Awareness Feature Overview and Configuration Guide.

Configuring Web Control

This section provides examples of how to configure web control:

- "How to configure basic Web Control" on page 34
- "How to configure Web Control default action per-entity" on page 36
- "How to discover which Web Control category a website URL belongs to" on page 40

For more information about the Web Control feature, see "Web Control" on page 16.

Note that from AlliedWarePlus version 5.5.2-0.1, we recommend using Web Categorization with Application Awareness (DPI) in place of Web Control. This allows greater flexibility in controlling web traffic. For more information about Web Categorization, see "Web Categorization for blocking web traffic by category" on page 15 and "Configuring Web-Categorization to block web traffic by category" on page 31. For information about migrating a Web Control configuration to use Web Categorization, see the Application Awareness Feature Overview and Configuration Guide.

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 opentext
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.

From version 5.5.2-1.1 onwards, you can use the tab key to auto-complete application and entity names. This makes it easier to specify the name of an existing DPI application or firewall entity.

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
```

Note: In Firewall entities, you can specify an interface along with a particular subnet as part of the network configuration, so that it matches a particular subnet traversing a particular interface. Prior to AlliedWare Plus version 5.5.4-1.1, web-control rules included this interface in the match criteria when applying rules.

You may need to change your configuration if you use interface matching, particularly if you have a network entity such as 'ip subnet 0.0.0.0/0 interface <***interface-name***>'. You will need to specify a subnet or multiple subnets that cover the hosts that send traffic via that interface in order to achieve equivalent matching.

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 1: 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 OpenText
Statistics:
 Categorization hits: 0/0  (0.0%)
 Rule hits:   0/0  (0.0%)
 Cache hits:  0/0  (0.0%)
 Cache size:  0
```

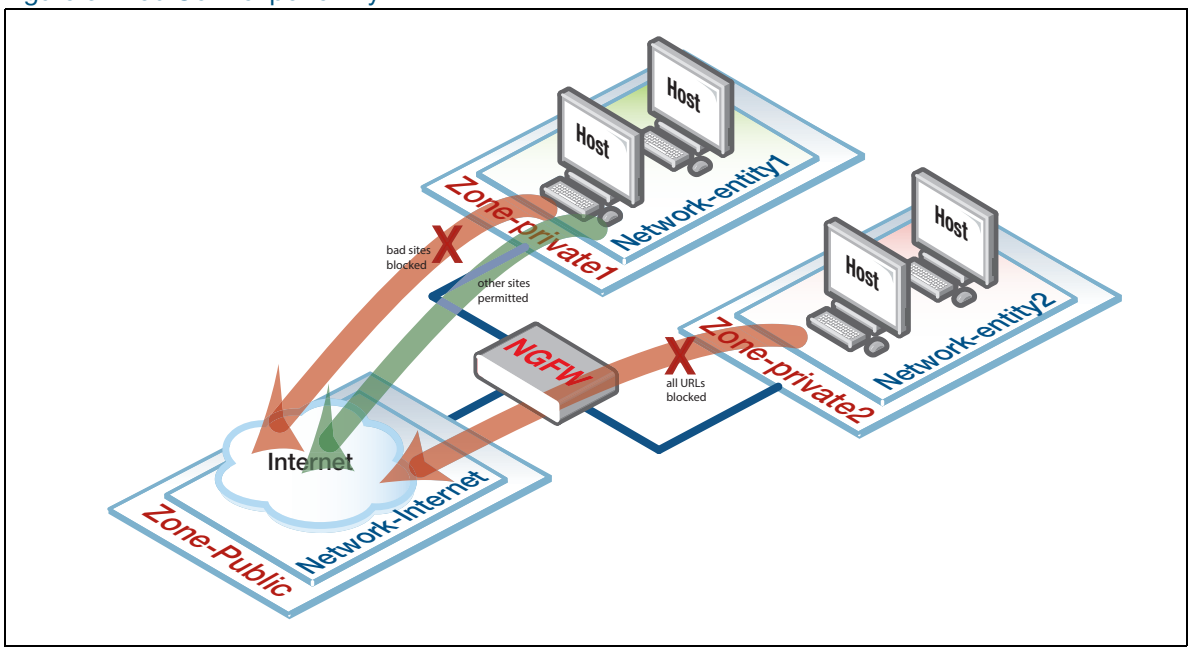
How to configure Web Control default action per-entity

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 6: Web Control per entity



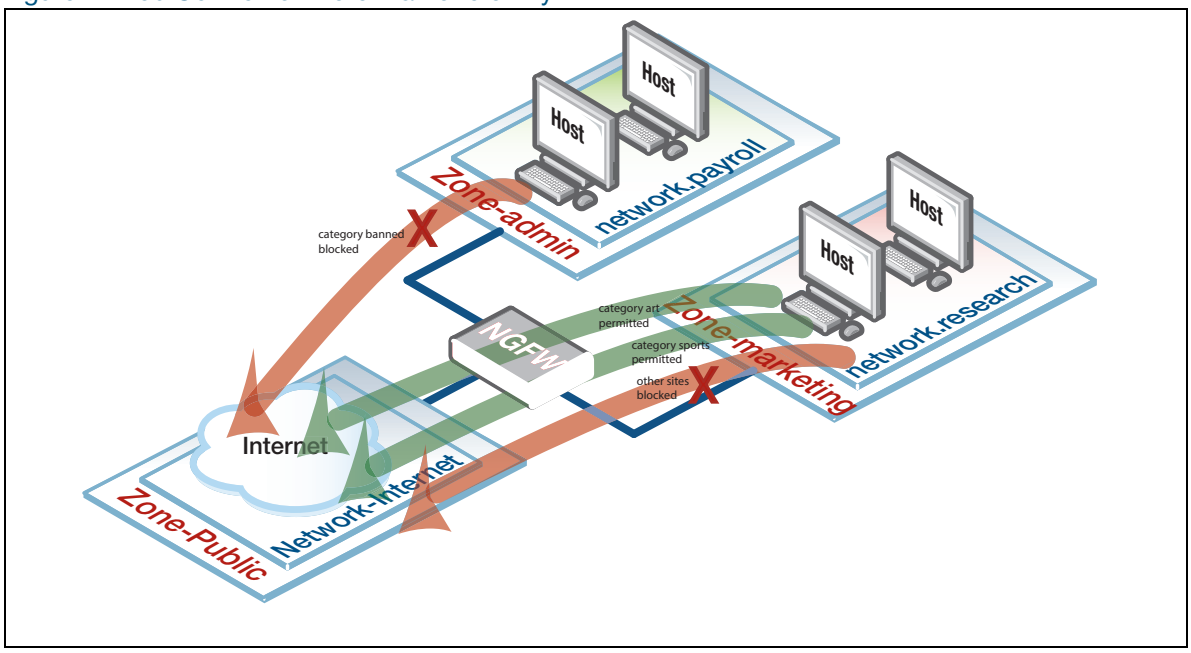
Example 2 Basic configuration to create a rule using the category keyword any:

```
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 7: 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 opentext
```

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
```

Example 4 Using Bypass rules to exempt certain traffic from Web Control ((from AlliedWare Plus version 5.5.4-1.1 onwards). Bypass rules allow certain traffic to be exempt from inspection by Web Control.

These can be used in 2 different scenarios:

- Certain clients are permitted unrestricted web access.
- Certain web servers contain only trusted content.

Bypass rules specify the exempted host(s) using a Firewall entity. Bypass rules check the entity against both the source and destination of the packet. If one or other matches, the rule is applied.

The web servers on a company's intranet do not need to be filtered by Web Control, therefore a bypass rule can be added.

Step 1: **To configure a bypass rule on a company Intranet**

```
awplus# configure terminal
awplus(config)# web-control
awplus(config-web-control)# bypass-web-control company.intranet
```

Step 2: **To remove the bypass rule**

```
awplus# configure terminal
```

```
awplus(config)# web-control
awplus(config-web-control)# no bypass-web-control company.intranet
```

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 a web control provider. 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 5 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 opentext
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'.

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 or AR4050S-5G
- Enable UTM Offload on the AR4050S or AR4050S-5G (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 or AR4050S-5G, 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 or AR4050S-5G

To enable UTM Offload on the AR4050S or AR4050S-5G, you must have a direct Ethernet connection between the offload device and the AR4050S or AR4050S-5G, i.e. from the Gigabit eth1 or eth2 port on the AR4050S or AR4050S-5G 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 43.

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 or AR4050S-5G 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 or AR4050S-5G) 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 45.

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 or AR4050S-5G, i.e. from the Gigabit eth1 or eth2 port on the AR4050S or AR4050S-5G 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 or AR4050S-5G. 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

UTM Offload Device Specifications
■ 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 or AR4050S-5G 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 or AR4050S-5G. 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 8: 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 or AR4050S-5G 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 or AR4050S-5G while using the Advanced Threat Protection feature set.

There must be a direct Ethernet connection from the forwarding device (AR4050S or AR4050S-5G) 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 or AR4050S-5G:

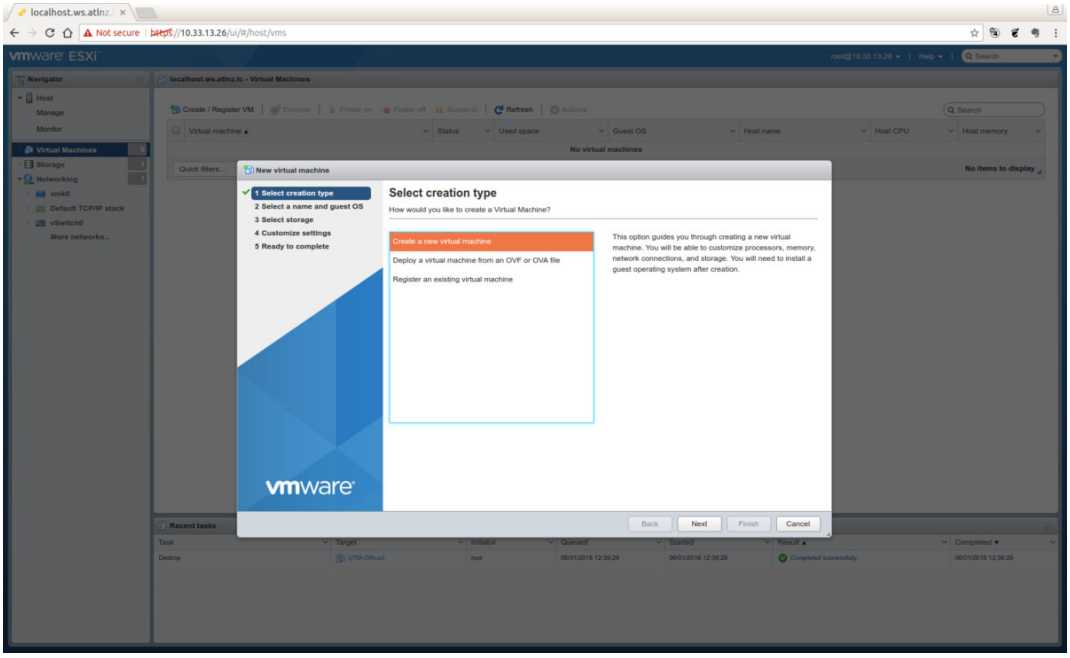
- UTM Offload licence (loaded on to the AR4050S or AR4050S-5G)
- Internet access
- DNS server configuration
- Single UTM Offload configuration command on the ESXi

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:

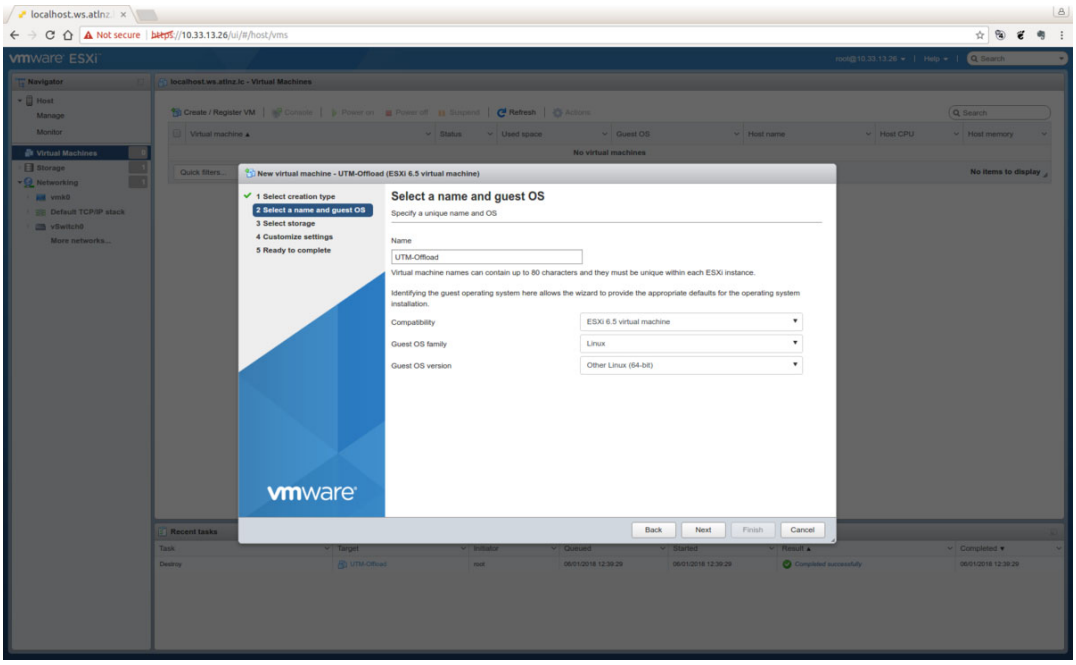
1. From the left side menu, select **Virtual Machines**
2. From the top tabs, select **Create/Register VM** to start the Wizard.



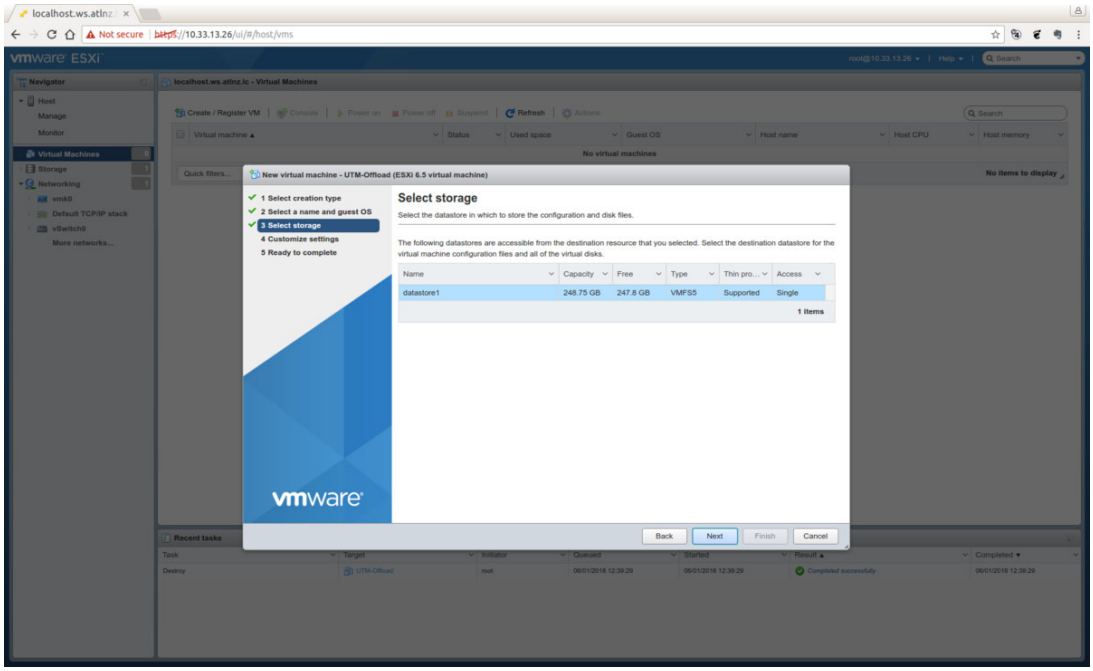
Note: The offload device must have an unused serial port.

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

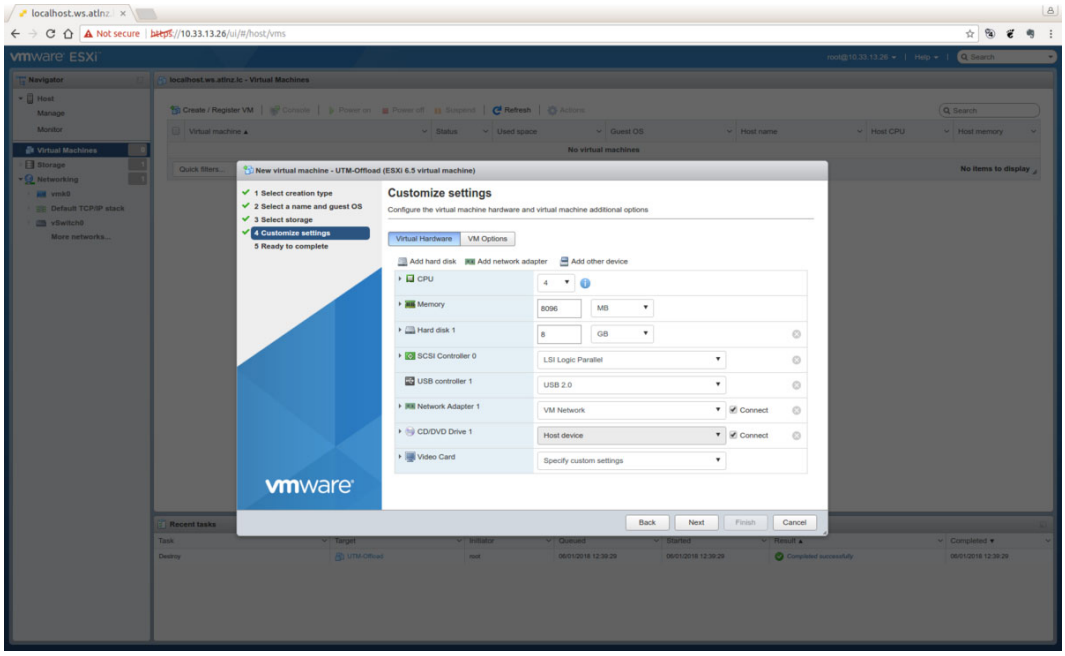
4. Use the drop down boxes to select, **Compatibility**, **Guest OS family**, and **Guest OS version**.



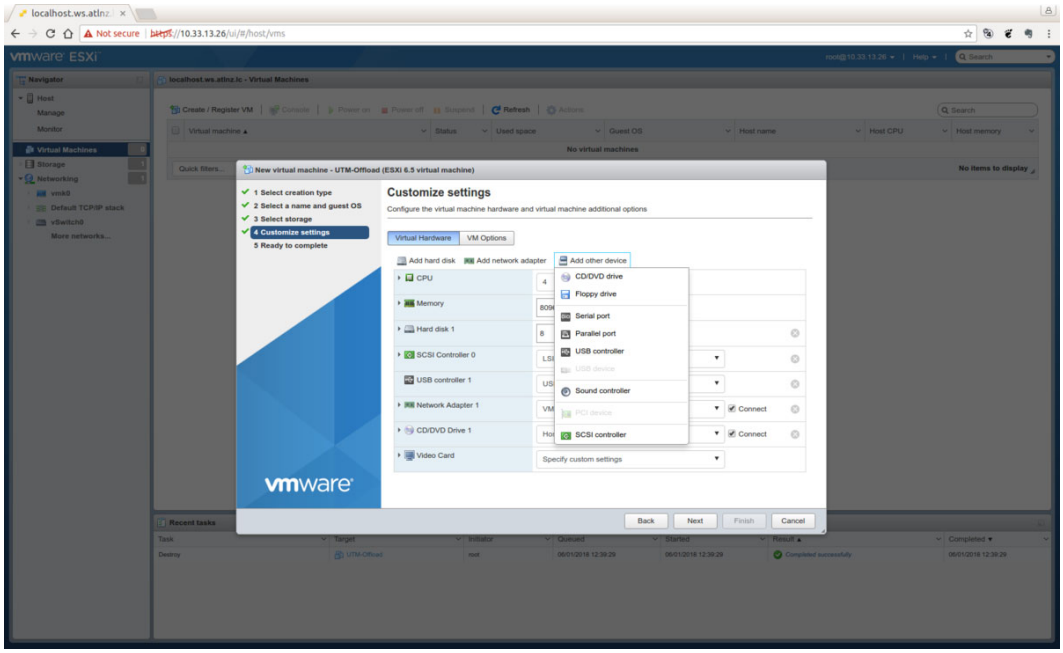
5. From the **Select storage** page, select the **datastore** for your configuration.



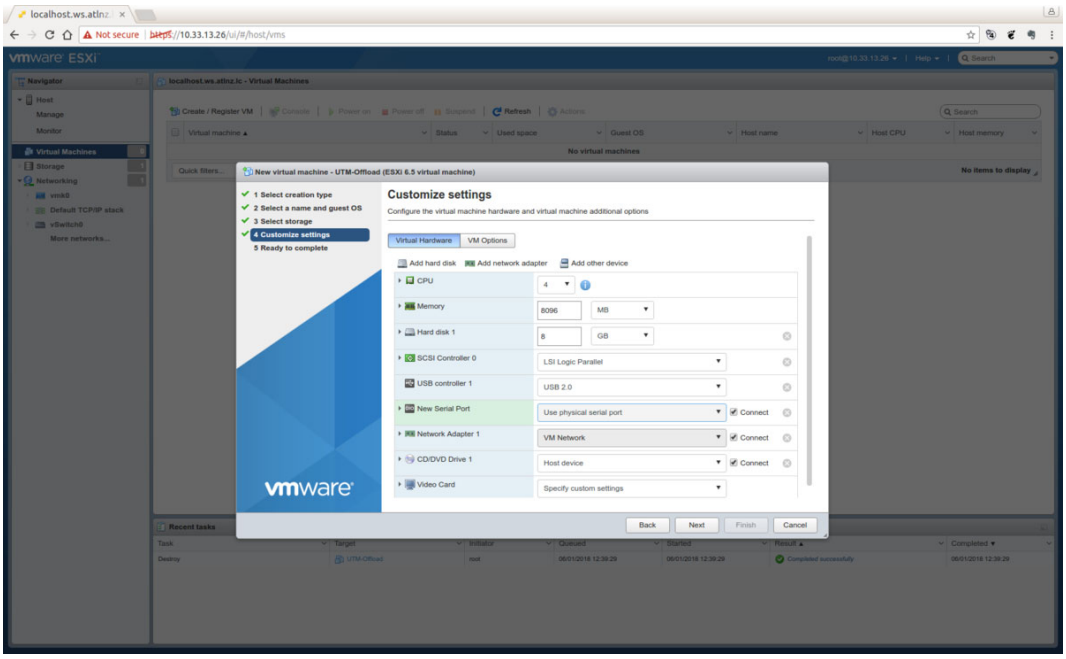
6. From the **Customize settings** page, configure the **Virtual Hardware** and **VM Options**.



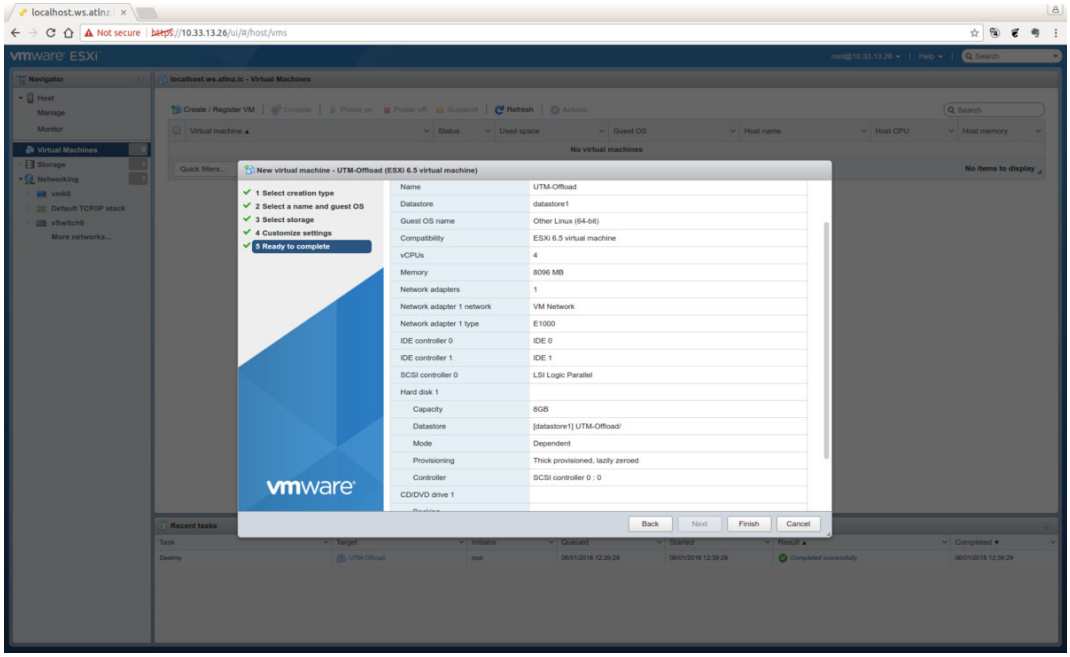
- Select **Serial port**.



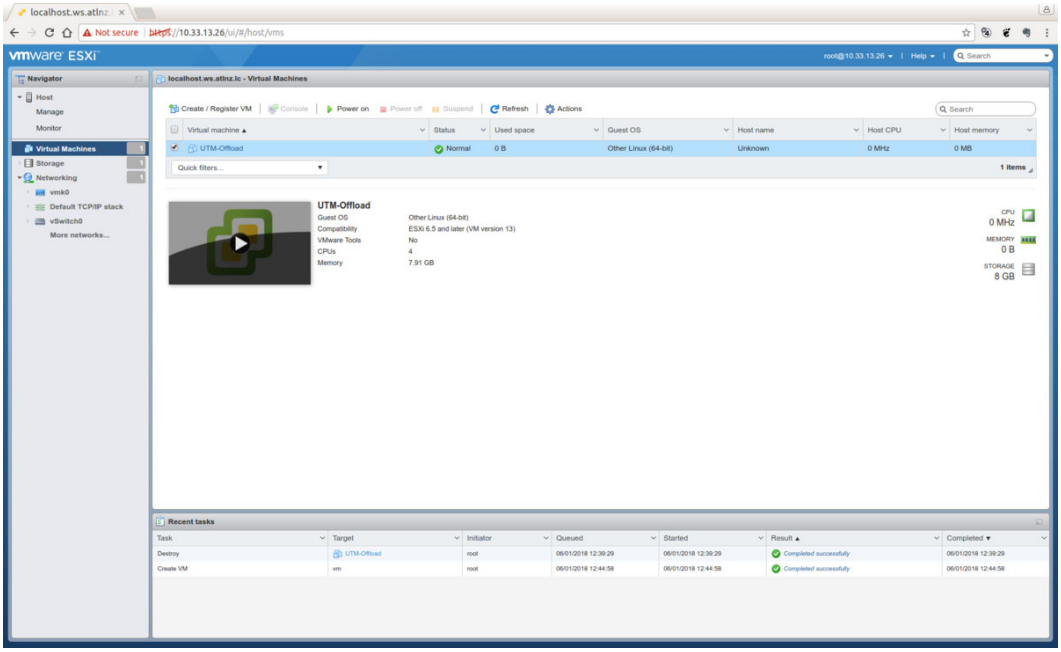
- Select **Connect**

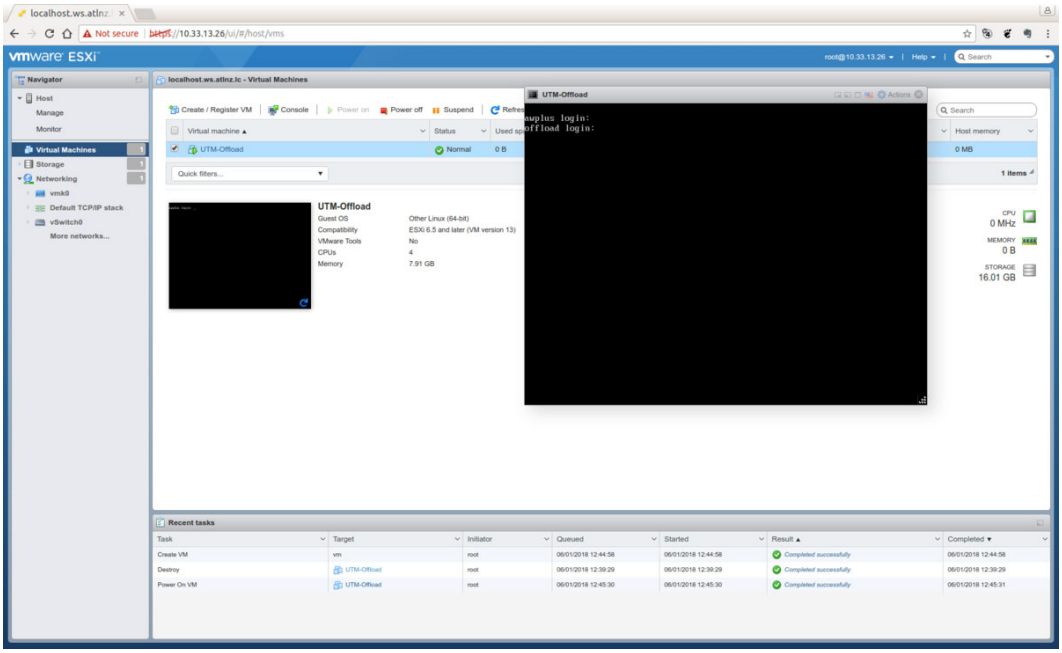


- Check the settings and click **Finish**.

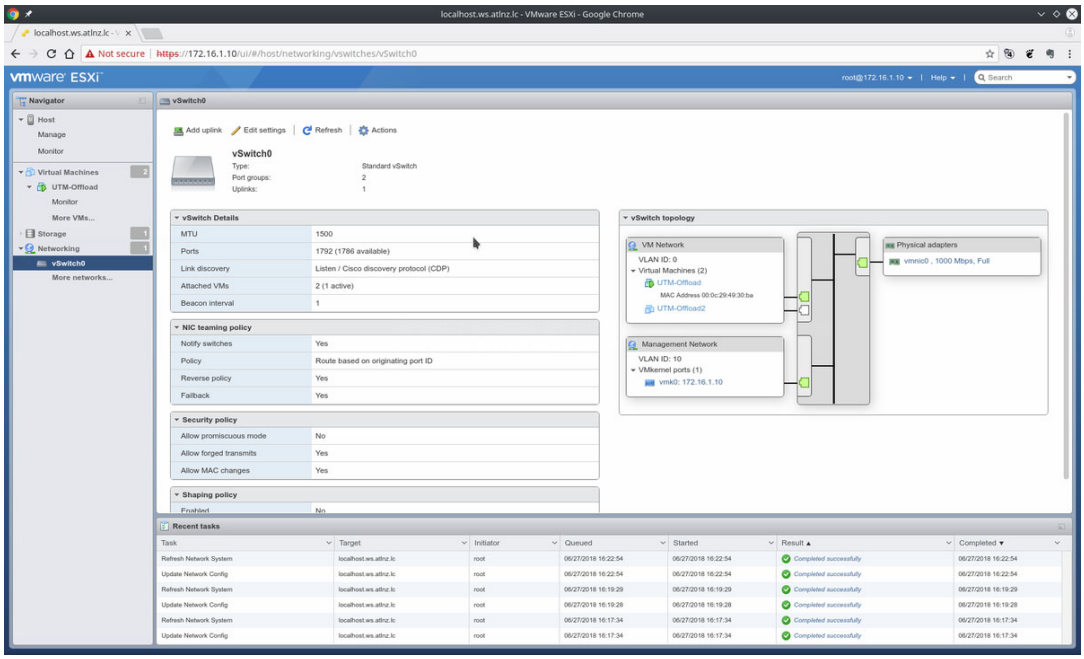


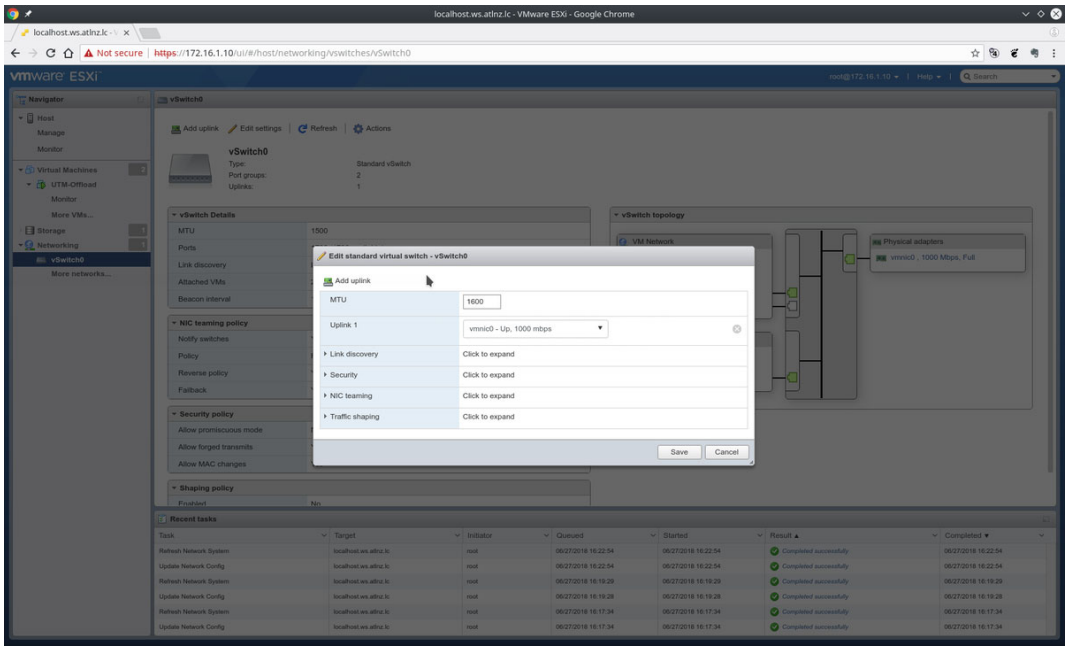
- Click **Play**





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 or AR4050S-5G

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 or AR4050S-5G).

```
!
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 or AR4050S-5G)**

  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 55
- "Reading log messages" on page 55
- "Firewall log messages" on page 55
- "UTM log messages" on page 56
- "IPS log messages" on page 57
- "IP Reputation log messages" on page 58
- "Malware Protection log messages" on page 59
- "URL Filtering log messages" on page 60
- "Web Control log messages" on page 61
- "Antivirus log messages" on page 62
- "Firewall connection logging" on page 62
- "UTM Offload logging" on page 64

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 2: 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 'local5', 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 3: 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 2: Example firewall log messages

```
2022 Jul 28 23:26:34 local5.info awplus ulogd[432]: 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
2022 Jul 25 14:10:38 local5.info awplus ulogd[432]: 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
2022 Jul 25 18:38:36 local5.info awplus ulogd[432]: 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 AlliedWare Plus 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 a 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>
```

From software version 5.5.2-2 onwards, the **<sid>** element is included in the IPS log message:

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

Table 4: 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
<sid>	The signature ID
<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 3: 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
```

Output 4: Example IPS log message (version: 5.5.2-2 onwards)

```
2022 Nov 17 02:49:57 local5.info awplus IPS[2369]: [Alert] IPS: smtp-events SMTP
no server welcome message [sid:2220006] [smtp] 172.16.92.2:25 ->
192.168.92.1:35992
2022 Nov 17 02:55:18 local5.info awplus IPS[2682]: [Alert] IPS: icmp-decoder-
events ICMPv4 unknown type [sid:2200024] [icmp] 172.16.92.2 -> 192.168.92.1
2022 Nov 17 03:15:23 local5.info awplus IPS[2398]: [Alert] IPS: checksum UDPv4
invalid checksum [sid:2200075] [udp] 192.168.92.1:2718 -> 172.16.92.2:0
2022 Nov 17 03:08:01 local5.info awplus IPS[2064]: [Drop] IPS: icmp-decoder-
events ICMPv4 unknown type [sid:2200024] [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 5: 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 5: 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 6: 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 7: 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 8: 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 29. 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 6: 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.

Table 6: Elements in Malware Protection log messages

Message element	Description
<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 9: 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 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 7: 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 10: 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 11: 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 8: 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 12: 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 9: 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 13: 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 14: 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 10: 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.

Table 10: Elements in firewall connection log messages

Message elements	Description
`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 15: 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 16: 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 or AR4050S-5G firewall and the offload device.
- Existing UTM feature log messages appear in the firewall's log transparently.
- Other general log messages generated by the offload device appear in the firewall's log transparently.
- Messages from the offload device appearing in the firewall's log have the offload device's IP address, the timestamp for when the message was generated and the string 'offload' inserted.

When the AR4050S or AR4050S-5G 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 9: 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
```

Appendix: Features using providers Digital Arts or Kaspersky

Security feature licenses

AlliedWare Plus security feature licenses purchased in 2023 or earlier may include subscriptions to providers Digital Arts or Kaspersky, as in the following table.

License	License name	Features (and providers)
AT-FL-AR3-NGFW-xYR (AR3050S) AT-FL-AR4-NGFW-xYR (AR4050S, AR4050S-5G)	Next-Gen Firewall (NGFW) x indicates 1, 3 or 5 years	Application Control (Procera) Web Control (Digital Arts) Web Categorization (Digital Arts)
AT-FL-AR3-ATP-xYR (AR3050S) AT-FL-AR4-ATP-xYR (AR4050S, AR4050S-5G)	Advanced Threat Protection (ATP) x indicates 1, 3 or 5 years	IP Reputation (ProofPoint) Malware Protection (Kaspersky) Antivirus (Kaspersky) URL Filtering (Kaspersky)

Selecting a solution

Protect from unwanted URLs with Web Categorization, Web Control or URL Filtering?

Each of these AlliedWare Plus features serves a similar purpose—you can use them to block or allow access to your network for Internet traffic from particular URLs.

- Web Categorization
  We recommend using Web Categorization with Application Awareness and firewall rules to categorize traffic from the Internet and block or allow as needed. Older security licenses include provider Digital Arts ("Web-Categorization using provider Digital Arts" on page 68. More recent licenses include provider OpenText ("Web Categorization for blocking web traffic by category" on page 15 and "Configuring Web-Categorization to block web traffic by category" on page 31).
- Web Control
  "Web Control using provider Digital Arts" on page 68 shows how to configure Web Control to use provider Digital Arts. Read this in conjunction with "Web Control" on page 16 and "Configuring Web Control" on page 34.
- URL Filtering
  "URL Filtering using provider Kaspersky" on page 74.

Protect from malicious code with Antivirus or Malware Protection?

Both the these AlliedWare Plus features perform a very similar service—detecting and blocking malicious code contained in content arriving from the Internet.

This Appendix describes how to use "Antivirus using provider Kaspersky" on page 69 and "Malware Protection using provider Kaspersky" on page 72.

You may choose to enable one of these features. In most situations, we recommend that you not enable both.

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 AlliedWare Plus 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 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.

Note 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.

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 using 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.

Web-Categorization using provider Digital Arts

To enable Web-Categorization and set it to use provider Digital Arts, use the steps below.

Step 1: **Enter the mode**

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

Step 2: **Select Web-Categorization with categorization provider Digital Arts**

```
awplus(config-dpi)# web-categorization digitalarts
```

Step 3: **Configure the rest Web-Categorization**

To configure the rest of Web-Categorization with DPI to manage URL access, see "Configuring Web-Categorization to block web traffic by category" on page 31. That is, replace the command **web-categorization opentext** in that section with the command **web-categorization digitalarts**. By default, application awareness is disabled and you need to explicitly enable it.

Web Control using provider Digital Arts

To enable Web Control and set it to use provider Digital Arts, use the steps below.

By default, Web Control protection and application awareness are disabled and you need to explicitly enable them.

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
```

Step 3: **Configure the rest Web Control**

To configure the rest of Web Control with DPI to manage URL access, see "Configuring Web Control" on page 34. That is, replace the command **provider opentext** in that section with the command **provider digitalarts**.

Note that from AlliedWare Plus version 5.5.2-0.1, we recommend using Web-Categorization with DPI to provide more flexible control of web traffic. For more information in the Application Awareness Feature Overview and Configuration Guide about:

- applications
- configuring firewall rules to use with DPI,
- migrating a Web Control configuration to use Web-Categorization with DPI.

Antivirus using provider Kaspersky

This section describes how AlliedWare Plus™ Antivirus works and how to configure it. This feature is supported from AlliedWare Plus version 5.4.5 or later.

Note that from AlliedWare Plus version 5.5.3-0.1 onward, we recommend using Advanced Intrusion Prevention System (IPS) to protect against a wide range of malicious content in encrypted and cleartext traffic. Advanced IPS is available from AlliedWare Plus version 5.5.2-2.1 onwards. For information about IPS and Advanced IPS, see "Intrusion Prevention System (IPS)" on page 10 and "Configuring Intrusion Prevention System (IPS)" on page 27. For information about licensing see "Licensing" on page 8.

Antivirus

AlliedWare Plus™ Antivirus provides a defense against a wide range of malicious content in cleartext traffic, 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 a third-party Antivirus engine. The signature database used by the engine containing known threat patterns is regularly updated.

How Antivirus works

AlliedWare Plus™ Antivirus uses proxy-based detection to scan cleartext 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:

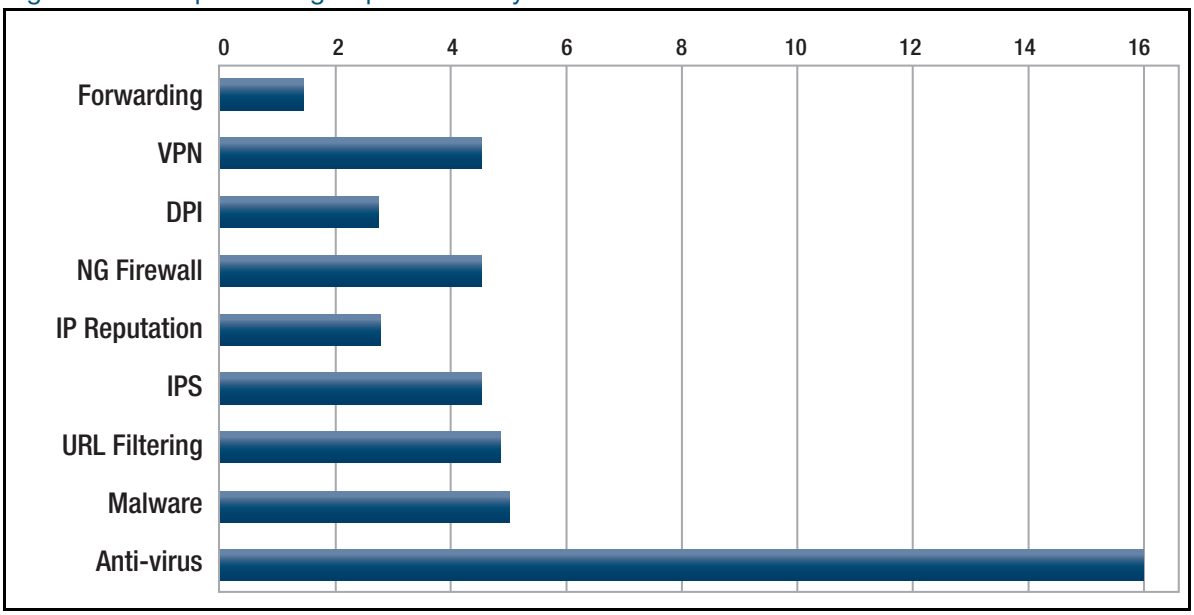
- Scans HTTP responses
- Supports third-party Antivirus
- Blocks HTTP responses in which a virus has been detected
- Scans packed, compressed or encoded object files
- Scans objects up to 10MB in size
- Scans 100MB of objects concurrently

- Extracts nested files up to 3 levels deep
- User configurable action upon scan failure

User configurable action when any limit is exceeded.

As each security function is enabled, overall throughput can be reduced. The diagram below is indicative only, based on test conditions, and highlights the number of CPU cycles that may be required for various functions. Note that enabling Antivirus can have significant effects on throughput.

Figure 10: CPU processing requirements by feature



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
```

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
```

Malware Protection using provider Kaspersky

This section describes how AlliedWare Plus™ Malware Protection works and how to configure it. The AlliedWare Plus Malware Protection feature is supported from AlliedWare Plus version 5.4.5 or later.

Note that from AlliedWare Plus version 5.5.3-0.1 onward, we recommend using Advanced Intrusion Prevention System (IPS) to protect against a wide range of malicious content in encrypted and cleartext traffic. Advanced IPS is available from AlliedWare Plus version 5.5.2-2.1 onwards. For information about IPS and Advanced IPS, see "Intrusion Prevention System (IPS)" on page 10 and "Configuring Intrusion Prevention System (IPS)" on page 27. For information about licensing see "Licensing" on page 8.

Malware Protection

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

Malware Protection provides a 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 cleartext traffic including web, email and instant messaging.

The third-party provider database is updated regularly to keep on top of the latest attack mechanisms.

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 third-party 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 third-party 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.

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 17: Example output from the console

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

URL Filtering using provider Kaspersky

This section describes how AlliedWare Plus™ URL Filtering works and how to configure it. This feature is supported from AlliedWare Plus version 5.4.6 and onwards.

Note that from 5.5.2-0.1 onwards, we recommend using AlliedWare Plus Web-Categorization with DPI to control access to website URLs. This provides more flexible control over categories and actions. For more information about Web Categorization, see "Web Categorization for blocking web traffic by category" on page 15. For information about licensing see "Licensing" on page 8. For information about migrating a URL Filtering configuration to use Web Categorization with DPI, see the Application Awareness Feature Overview and Configuration Guide.

URL Filtering

URL Filtering provides a stream-based method of controlling access to website URLs that are known to be undesirable. It globally allows (whitelist) or blocks (blacklist) access to particular websites, 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.
- **Third-party blacklists** provide 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 a service, you can create additional blacklists to block extra URLs or whitelists to allow URLs that the third-party service blocks.

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 the third-party providers.

If you use third-party-sourced lists, the device will automatically download list updates from the Allied Telesis update server.

URL Filtering provides a 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 via the blacklists (user-defined and third-party), or allowed for everyone via the whitelists. (This contrasts with Web Control, with which URLs are categorized and you can control access to websites on a per-category and per-firewall entity basis.)

It is possible to use Web Control and URL Filtering at the same time, but in most situations there is little benefit in this. 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?

To use URL filtering, you can either use:

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

URL filtering works by sniffing traffic as it traverses the AlliedWare Plus 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.

Configure URL Filtering

This section describes how to use, configure and monitor URL Filtering using the CLI. For more information about the URL Filtering feature, see "URL Filtering using provider Kaspersky" on page 74.

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 a third-party 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 a third party provider such as 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 a third party provider such as the Kaspersky URL Filtering Subscription License will cause URL filtering to reload without a Kaspersky blacklist.

Using multiple whitelists and blacklists

The AlliedWare Plus firewalls 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—third-party-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 third-party 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

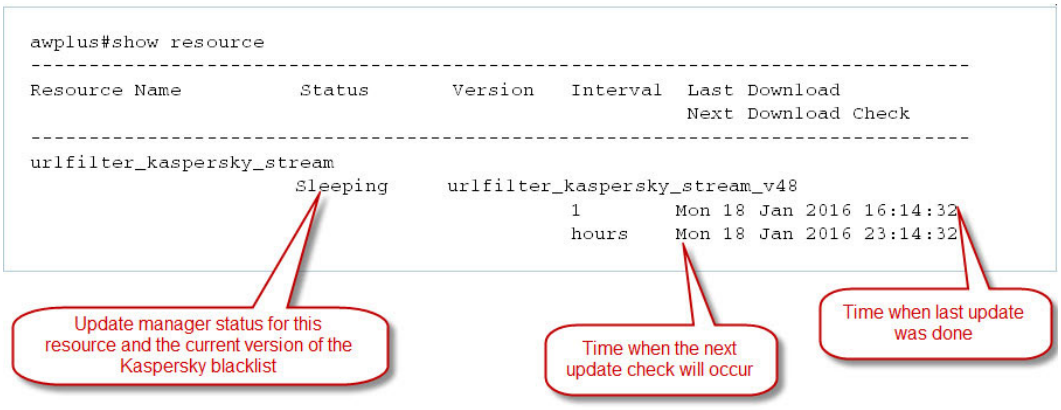
Updating the Kaspersky blacklist

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
```