Technical Guide

Application Awareness

Feature Overview and Configuration Guide

Introduction

This guide describes application awareness in AlliedWare Plus™, and its configuration.

Application awareness enhances the network functions of AlliedWare Plus by providing real-time multi-layer classification of network traffic. The DPI engine inspects every packet and accurately identifies today's most common applications (social networking, P2P, instant messaging, file sharing, streaming, enterprise and web 2.0 applications). Application awareness enables network functions to operate with dramatically improved accuracy and provide a more human-friendly view of traffic classification than with traditional IP and port-based rules.

Contents

Products and software versions that apply to this guide

This Guide applies to products supporting AlliedWare Plus Application Awareness (DPI), running version **5.4.5** or later.

- Versions 5.4.5 or later support Deep Packet Inspection (DPI) using Procera subscription-based application libraries on the UTM Firewalls.
- Versions 5.4.7-2 or later add support for Deep Packet Inspection (DPI) using the built-in library of applications.
- Versions 5.4.7-2.1 and later support more application information in the output from the **show application detail** command.
- Versions 5.4.8-1.x and later support FQDN lookup
- Versions 5.5.2-1.1 and later support tab completion for application and entity names
- Version 5.5.2-0.1 and later support DPI functionality utilized with Web-categorization
- Version 5.5.2-2 and later support DPI Web-categorization using OpenText subscription-based application libraries.

To see whether a product supports a command, see the product's Command Reference.

Related documents

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

- Firewall and Network Address Translation (NAT) Feature Overview and Configuration Guide
- Traffic Control Feature Overview and Configuration Guide.
- Policy-based Routing Feature Overview and Configuration Guide
- The product's Command Reference

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

Applications

An application serves as a high-level abstraction to categorize packets within network traffic. Achieving traffic matching for applications involves various techniques, such as matching packets based on port numbers or identifying application signatures in packet flows. The device is capable of recognizing different types of applications, allowing configuration of source port, destination port, protocol, ICMP code, and ICMP type for each application.

For an application to be considered valid, its protocol, source, and destination must be appropriately configured. For instance, an application is invalid if it lacks a configured protocol, or if source and destination ports are assigned to protocols other than TCP, UDP, or SCTP.

There is an built-in library of many more applications that can be identified in traffic if Deep Packet Inspection (DPI) is enabled.

The extensive up-to-date library of applications maintained by Procera is available by subscription. When DPI is enabled, the device recognizes these applications.

You can use the **show application** and **show application detail** commands to display the detail of these applications.

If applications have the same name, precedence in all application-aware features is:

1. user-configured applications
2. applications identified by DPI
3. built-in predefined list

Entities

An entity is a high level abstraction of an individual network device, an individual network, or a group of networks or subnets. There are three types of entity:

- Zone
- Network
- Host

Zone is a high level abstraction for a logical grouping or segmentation of physical networks. This is the highest level of partitioning that firewall and NAT policy can be applied to. Zone establishes the security border of your networks. A zone defines a boundary where traffic is subjected to policy restrictions as it crosses to another region of your networks. The minimum zones normally implemented would be a trusted zone for the private network behind the firewall and a untrusted zone for the Internet. Other common zones are a Demilitarized Zone (DMZ) for publicly visible web servers and a Virtual Private Network (VPN) zone for remote access users or tunnels to other networks.

A **network** is a high level abstraction of a logical network in a zone. This consists of the IP subnets and interfaces over which it is reachable. Subnets are grouped into networks to apply a common set of rules among the subnets.

Host is a high level abstraction of a single node in a network. This is commonly used if a particular device, for example a server, has a static IP address that needs to be specified, for instance in a firewall policy. It can also be used for an address that is dynamically learned.

An entity is the instance that a number of features can be applied to, including firewall and NAT policies, Web Control policies, Traffic Control and Policy-Based Routing (PBR).

What is Application Awareness?

Rather than being limited to determining applications based on network layer and transport layer information, for example well-known protocols and ports, AlliedWare Plus Application Awareness is capable of drilling further down into the packet and determine the actual application associated with that packet.

AlliedWare Plus Application Awareness identifies applications by looking at the relationships between packets rather than individual packets in isolation and matching those packets to a database of predefined application signatures.

This allows enterprises to differentiate business-critical from noncritical applications and enforce security and acceptable-use policies in ways that make sense for the business in contrast to black-and-white policies.

AlliedWare Plus Application Awareness uses information that is defined for particular applications. If Deep Packet Inspection (DPI) is enabled, it can use either:

- a licensed version of Procera Networks' Network Application Visibility Library (NAVL) to respond to the fast changing and complex applications, if this is enabled.
- or (from version 5.4.7-2.x) an internal (built-in) library, which supports a smaller fixed subset application list.

  and

- from version 5.5.2-0.1x, Web categorization of hostnames, statically configured and/or provided by a subscription service (Digital Arts).
- from version 5.5.2-2, Web categorization of hostnames can be provided by Webroot subscription service.

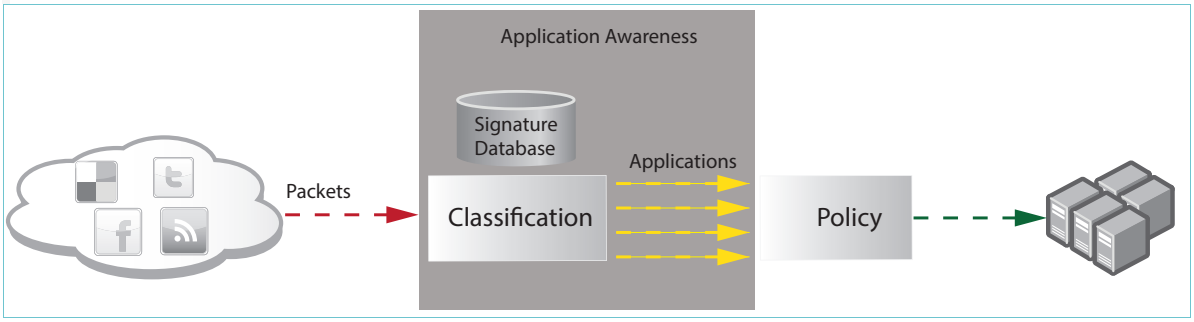
These DPI tools use a combination of deep packet and deep flow inspection techniques to provide real-time identification of network applications. The NAVL library will detect more applications and is dynamic and updated frequently, the internal library is fixed for the duration of a release. Web categorization takes the hostnames detected in the HTTP transaction or TLS negotiation to identify the application being provided by a server.

What is Application Awareness used for?

By matching packets against pre-defined application signatures, DPI allows you to see what kinds of traffic are flowing in the network, and enhance network processing accordingly. This information can be used in the following ways.

- Network Visibility— you can enhance your view of the traffic in your network by seeing how many packets and bytes are associated with each application.
- Application Control—you can use firewall rules to determine not only which applications are allowed, but under what circumstances and by whom.
- Traffic Control—with traffic control rules, you can prioritize the organisations important applications, and limit bandwidth to non-critical applications.
- Policy-based Routing (PBR)—you can configure PBR rules to automatically select low-latency paths for time-critical applications (such as VOIP), and route other traffic to other paths.

The figure below shows how application awareness can be used to enhance the way features such as firewall, traffic control and PBR can apply their application-based policies.



Configuring and Monitoring Application Awareness with DPI plus Web-categorization

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
```

Viewing application information

When DPI is enabled, you can display more detailed information about applications:

- inspected by DPI
- the device can recognise

Display applications inspected by DPI

To display a list of applications detected by DPI and the number of packets and bytes associated with each, use the command:

```
awplus# show dpi statistics
```

```
awplus#show dpi statistics
Application  Packets            Bytes
-------------------------------------------------
http         30                 2020
icmp         348                29232
telnet       45                 2553
```

Display detailed counters per entity

To display transmit and receive counters for each entity, use the **counters detailed** command to set DPI mode. These counters will require system resources and need to be configured when required. Use the **no** variant of the **counters detailed** command when finished to stop using system resources.

To set DPI mode, use the commands:

```
awplus# configure terminal
awplus# dpi
awplus# counters detailed
```

Then, to display counters of traffic that is transmitted and received by devices for an entity, use the command **show dpi statistics *<entity-name>***. While the simple statistics are incremented after each packet is processed, these counters are only incremented after each flow is completed.

For example, to display detailed counters for the “lan” entity, use the command:

```
awplus# show dpi statistics lan
```

```
awplus#show dpi statistics lan
Statistics for entity: lan
Application TX Packets RX Packets TX Bytes RX Bytes
-------------------------------------------------------------------------------
microsoft          984       2692   404370  3366235
ssl               2241       3413   999433  2703874
google            1493       2840   163543  3477037
amazon             822       1595   127254  1681665
http_download       33        318     2415   470665
googleservice      213        334    22377   353958
cloudflare          79        197    10908   188997
windowsupdate       99        133    12122   129162
http               117        103    17741   34089
msn                 23         24     6141   13599
office 365          19         18     2038   11745
spotify             10          9     1084   4330
facebook             9         10     1350   3993
```

Display applications the device can recognise

To display details about the applications the device can recognize, use the command:

```
awplus# show application detail
```

From version 5.4.7-2.x, the following information is displayed about these applications:

- Application mark—the hexadecimal DPI application index representing each protocol or application
- Application name—the short name used when referenced from application aware features (for instance firewall)
- Description—a longer description of the type of traffic this traffic relates to. For applications identified by the Procera application list, the description includes the following additional information:
  - Category—a general and high-level category for the application.
  - Productivity—an index value between 1 and 5 that rates the potential for each application to improve or increase the overall productivity of network users. For instance, applications with a low productivity index (e.g. games and social networking) can be expected to have a negative impact on productivity.
  - Risks—an index value between 1 and 5 that rates the potential for each protocol or application to allow undesirable content onto your network. The higher the risk index, the greater the chance of letting in something that could be dangerous or destructive.

```
awplus#show application detail
Name              Mark    Detail
-------------------------------------------------------------------------------
050plus           0x435   DPI: The traffic consists of data from logging in or
                            making calls with the 050Plus application.
                            (Cat=Messaging, Prod=2, Risk=2)
12306cn           0x292   DPI: 12306.cn is the only China Railway customer
                            service center (Cat=Web Services, Prod=4, Risk=1)
123movie          0x64D   DPI: Free movie streaming/downloading site
                            (Cat=Streaming Media, Prod=1, Risk=5)
126com            0x293   DPI: 126.com is a free webmail service of Netease
                            (Cat=Mail, Prod=4, Risk=2)
17173             0x30B   DPI: General browsing, interaction, and game play on
                            the social gaming network 17173.com (Cat=Social
                            Networking, Prod=2, Risk=2)
1fichier          0x779   DPI: Online cloud storage.(Cat=File Transfer,Prod=1,
                            Risk=5)
2345com           0x2BE   DPI: General browsing of navigation portal 2345.com
                            (Cat=Web Services, Prod=3, Risk=1)
247inc            0x36D   DPI: Data and advertisements hosted by [24]7 Inc.
                            (Cat=Web Services, Prod=3, Risk=1)
```

To find a particular application or application mark or in the output from the **show application detail** command, you can filter it:

```
awplus#show application detail | grep 0x5A
icmp              0x5A    DPI: Internet Control Message Protocol
```

You can use this information to interpret references to the application mark in log messages, for instance those generated by the firewall:

```
2022 Jul 11 00:50:29 kern.info awplus kernel: Firewall: DENY in policy IN=vlan1
OUT= MAC=00:00:cd:38:00:a7:80:1f:02:ff:e8:1a:08:00 SRC=192.168.100.1
DST=192.168.100.2 LEN=84 TOS=0x00 PREC=0x00 TTL=64 ID=53865 DF PROTO=ICMP TYPE=8
CODE=0 ID=31014 SEQ=9 MARK=0x5a
```

Once you've identified this traffic, for instance, configure a firewall rule to permit ICMP.

Configuration: Apply firewall rules with DPI

DPI itself does not control or apply rules to the traffic. You can use firewall rules to enforce security policy and apply rules to DPI applications.

Step 1: **Create public zone.**

```
awplus# configure terminal
awplus(config)# zone public
awplus(config-zone)# network wan
awplus(config-network)# ip subnet 0.0.0.0/0 interface eth2
awplus(config-network)# exit
```

Step 2: **Create DMZ zone.**

```
awplus(config-zone)# zone dmz
awplus(config-zone)# network servers
awplus(config-network)# ip subnet 172.16.0.0/24 interface eth1
awplus(config-zone)# exit
```

Step 3: **Apply firewall rule for an application.**

```
awplus(config)# firewall
awplus(config-firewall)# rule 10 deny facebook from public to dmz
```

Step 4: **Enable firewall protection.**

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

When using DPI with the firewall, sufficient packets must be permitted to pass in order to allow DPI to identify the application contained in the flow. Before the application has been identified, DPI will mark the packets as ‘undecided’. A firewall rule is required to permit these undecided packets to pass. Once the application has been identified by DPI, the firewall will reassess the flow against its rules and decide if the flow should continue to be permitted or not. A special application type ‘undecided’ is used to create this rule. (For the rare situations when DPI cannot identify the application, they will eventually be marked as ‘unknown’.)

For example, if HTTP traffic is to be permitted from the private to the public zone, in addition to the permit rule for HTTP, add the following rule to allow ‘undecided’ traffic until DPI has finished identifying the application.

```
awplus(config-firewall)# rule 20 permit undecided from private to public
```

Apply Firewall Rules with DPI

DPI itself does not control or apply rules to the traffic. You can use firewall rules to enforce security policy and apply rules to DPI applications.

Step 1: **Create public zone.**

```
awplus# configure terminal
awplus(config)# zone public
awplus(config-zone)# network wan
awplus(config-network)# ip subnet 0.0.0.0/0 interface eth2
awplus(config-network)# exit
```

Step 2: **Create DMZ zone.**

```
awplus(config-zone)# zone dmz
awplus(config-zone)# network servers
awplus(config-network)# ip subnet 172.16.0.0/24 interface eth1
awplus(config-zone)# exit
```

Step 3: **Apply firewall rule for an application.**

```
awplus(config)# firewall
awplus(config-firewall)# rule 10 deny facebook from public to dmz
```

Step 4: **Enable firewall protection.**

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

When using DPI with the firewall, sufficient packets must be permitted to pass in order to allow DPI to identify the application contained in the flow. Before the application has been identified, DPI will mark the packets as ‘undecided’. A firewall rule is required to permit these undecided packets to pass. Once the application has been identified by DPI, the firewall will reassess the flow against its rules and decide if the flow should continue to be permitted or not. A special application type ‘undecided’ is used to create this rule. (For the rare situations when DPI cannot identify the application, they will eventually be marked as ‘unknown’.)

For example, if HTTP traffic is to be permitted from the private to the public zone, in addition to the permit rule for HTTP, add the following rule to allow ‘undecided’ traffic until DPI has finished identifying the application.

```
awplus(config-firewall)# rule 20 permit undecided from private to public
```

Migrating from URL Filtering to DPI with Web-Categorization

From software release 5.5.2-0.1 onwards, existing URL Filtering deployments should be migrated to DPI **Web Categorization** to take advantage of improved throughput and HTTPS traffic support. The migration involves two steps:

- migrating provider rules
- migrating custom whitelists and blacklists.

Migrating provider rules

URL filtering uses a third-party auto-updated blacklist, which blocks all traffic that matches the blacklist.

DPI Web Categorization classifies traffic into categories, allowing greater control over what is blocked. For example, two categories are 'business-economy' and 'gambling'. While many administrators may want to block 'gambling', not all will choose to block 'business-economy'.

Below is an example output of the command **show applications detail**. DPI Web Categorization provider category descriptions are prefixed with 'DPI: Web Categorization'.

```
awplus#show application detail
Name                        Mark   Detail
-------------------------------------------------------------------------------
...
business-economy  0xXX DPI: Web Categorization - Business firms, corporate
                            websites,business information,economics,
                            marketing,management,and entrepreneurship.
...
gambling          0xXX DPI: Web Categorization - Gambling or lottery
                            websites that invite the use of real or virtual
                            money. Information or advice for placing wagers,
                            participating in lotteries, gambling, or running
                            numbers; virtual casinos and offshore gambling
                            ventures; sports picks and betting pools; virtual
                            sports and fantasy leagues that offer large rewards
                            or request significant wagers. Hotel and Resort
                            sites that do not enable gambling on the site are
                            categorized in "travel" or "local-information"
...!
```

In order to block the category 'gambling':

```
awplus# configure terminal
awplus(config)# firewall
awplus(config-firewall)# rule 10 deny gambling from lan to wan
```

Migrating custom blacklists and whitelists

URL Filtering blocks all HTTP access to a list of websites or portions of web sites. DPI Web Categorization uses custom applications instead. For example, a URL Filter blacklist may have been configured to use the following blacklist:

```
mysite.com
ru
```

with the following URL Filter configuration:

```
awplus# configure terminal
awplus(config)# url-filter
awplus(config-url-filter)# whitelist flash:my_blacklist.txt
awplus(config-url-filter)# protect
```

Using DPI Web Categorization, this configuration could be mirrored by configuring an application with hostnames:

```
awplus# configure terminal
awplus(config)# application my_blacklist
awplus(config-application)# hostname mysite.com
awplus(config-application)# hostname ru
```

and adding a firewall rule to drop the traffic that matches the custom application:

```
awplus# configure terminal
awplus(config)# firewall
awplus(config-firewall)# rule 10 deny my_blacklist from lan to wan
```

Many rules can be migrated from URL-filtering to DPI Web Categorization. However, there are some differences in how URL Filtering and DPI Web Categorization match hostnames. These differences are described below, using the above example:

URL Filtering pattern	DPI Web Categorization application	URL Filtering matched URLs	URL Filtering unmatched URLs	DPI matched URLs	DPI unmatched URLs
com	application my_blacklist hostname com	www.bad.com	www.bad.com.au	www.bad.com	www.bad.com.au
com.au	application my_blacklist hostname com.au	www.bad.com.au:8080/file.txt	www.bad.com	www.bad.com.au:8080/file.txt	www.bad.com
badstuff.*	application my_blacklist hostname badstuff.com hostname badstuff.au hostname badstuff.ru	www.badstuff.com www.badstuff.au www.badstuff.ru www.badstuff.io		www.badstuff.com www.badstuff.au www.badstuff.ru	www.badstuff.io

As URL Filtering operates over (unencrypted) HTTP traffic, it can match full URLs including the path and query e.g. mysite.com/*/*.exe. With modern traffic using HTTPS, DPI Web Categorization matches on TLS SNI and therefore matches on the hostname of URLs (mysite.com in the example) and cannot match on the path of URLs.

Migrating from Web Control to DPI Web-Categorization

We recommend migrating Web Control configurations to use to Web-categorization with DPI to benefit from improved throughput and decreased memory usage.

- Version 5.5.2-0.1 and later support DPI functionality used with Web-categorization.
- Version 5.5.2-2 and later support DPI Web-categorization using OpenText subscription-based application libraries.

Migrating Web Control Provider

Web Control provider services are similar to DPI Web Categorization provider services, but instead of providing automatically updated application entities, they provide Web Control categories. For this reason, migrating from a Web Control provider to a DPI Web Categorization provider is as simple as moving Web Control rules to Firewall rules. For example, both Web Control and DPI Web Categorization have the provider categories business-economy and gambling.

```
awplus#show application detail
Name                      Mark    Detail
-------------------------------------------------------------------------------
...
business-economy  0xXX  DPI: Web Categorization - Business firms, corporate
                                        websites, business information, economics,
                                        marketing, management, and entrepreneurship.
...
gambling                  0xXX  DPI: Web Categorization - Gambling or lottery
                                        websites that invite the use of real or virtual
                                        money. Information or advice for placing wagers
                                        participating in lotteries, gambling, or running
                                        numbers; virtual casinos and offshore gambling
                                        ventures; sports picks and betting pools; virtua
                                        sports and fantasy leagues that offer large rewards
                                        or request significant wagers. Hotel and Resort
                                        sites that do not enable gambling on the site are
                                        categorized in "travel" or "local-information"
...!
```

The Web Control rule to block gambling would look like this:

```
awplus# configure terminal
awplus(config)# web-control
awplus(config-web-control)# rule deny gambling from lan
```

This rule could be translated into Web Categorization as follows:

```
awplus# configure terminal
awplus(config)# firewall
awplus(config-firewall)# rule deny my_blacklist from lan to wan
```

In Web Control, traffic is matched to rules before firewall rules are processed. Since DPI Web Categorization categories are matched by firewall rules, the translated rules should have low rule IDs to ensure existing firewall rules do not permit traffic that should be dropped.

Migrating Web Control custom categories

Web Control supports custom categories, similar to DPI Web Categorization, with some minor differences. For example, Web Control could be configured to block the following:

```
mysite.com
ru
```

with the following Web Control configuration:

```
awplus# configure terminal
awplus(config)# web-control
awplus(config-web-control)# category my_blacklist
awplus(config-category)# match mysite.com
awplus(config-category)# match ru
awplus(config-web-control)# rule deny my_blacklist from lan
```

In DPI Web Categorization, this configuration could be mirrored by configuring an application with hostnames:

```
awplus# configure terminal
awplus(config)# application my_blacklist
awplus(config-application)# hostname mysite.com
awplus(config-application)# hostname ru
```

and adding a firewall rule to drop the traffic that matches the custom application:

```
awplus# configure terminal
awplus(config)# firewall
awplus(config-firewall)# rule 10 deny my_blacklist from lan to wan
```

Many rules can be migrated from Web Control to DPI Web Categorization. However, there are some differences in how Web Control and DPI Web Categorization match hostnames. These differences are described below, using the above example:

Web Control match	DPI Web categorization application	Web Control matched URLs	Web Control unmatched URLs	DPI matched URLs	DPI unmatched URLs
category my_blacklist match com	application my_blacklist hostname com	www.bad.com	www.bad.com.au	www.bad.com	www.bad.com.au
category my_blacklist match com.au	application my_blacklist hostname com.au	www.bad.com.au	www.bad.com	www.bad.com.au www.bad.com	
category my_blacklist match bad	application my_blacklist hostname badstuff.com hostname badstuff.au hostname badstuff.ru	www.badstuff.com www.badstuff.au www.badstuff.ru www.badstuff.io		www.badstuff.com www.badstuff.au www.badstuff.ru	www.badstuff.io www.badminton.com

A Web Control category match matches a URL if the match string is a sub-string of the URL. This method can match more URLs with one match, but can also match undesired URLS, like www.badminton.com in the above example. The difference between DPI Web Categorization and Web Control must be considered when migrating custom categories to applications.

Fully Qualified Domain Name (FQDN) Lookup for Entities

FQDN lookup for host entities provides an alternative mechanism to match web traffic destined to a web server or cloud-based service. It does this by allowing a host entity to store a list of IP addresses that is dynamically updated from DNS. The user achieves this by creating a named host entity that specifies an FQDN. Then the IP addresses stored in the device's DNS cache (as A and AAAA records) that match the FQDNs are copied into the entity's IP address list for use during packet matching operations. This means the IP addresses associated with a particular Internet service will always be as up-to-date as the addresses that are provided by DNS for that service.

Overview of FQDN lookup

In our system, ingress traffic is matched against application-based Firewall, PBR, and Traffic Control rules. Applications can be statically defined, or can be identified by the DPI engine.

Static applications can be configured to match on:

- protocol
- source and destination port
- DSCP value
- ICMP type and code

Alternatively, applications can be identified by the inbuilt, or 3rd party DPI engine. However, DPI engines are only capable of matching applications that they already know about, which may be problematic for customers if they are using an obscure application or a region-specific service that may be unknown to the DPI provider.

Given these limitations, it may be difficult for a customer to set up application-based rules to selectively match specific applications, and control access to Internet-based services. Web services are highly likely to use the same destination/source ports, and the web services may not be reliably recognized by any of the DPI providers that AlliedWare Plus supports.

A named host entity can be configured to match a specific IP address. This is fine, if the IP address is known. FQDN lookup for host entities provides an alternative mechanism to match traffic to specific IP address(es) which can be identified via DNS lookup.

The feature is configured by specifying an FQDN on a host entity instead of an IP address. Traffic flows destined to the list of IP addresses resolved by DNS lookup to the FQDN are matched.

The following shows how to configure a named host entity that will match traffic to all IP address(es) (resolved via DNS lookup) to facebook.com:

```
zone public
 network all
  ip subnet 0.0.0.0/0 interface eth1
 host facebook
  ip address dynamic fqdn facebook.com
```

How does FQDN lookup work?

1. The router needs to be configured with the DNS relay feature so that all DNS requests sent by clients within the network are intercepted by the router itself.
2. When an FQDN is configured and a client makes a DNS request for that FQDN, the router will copy the IP address(es) learned into the firewall host entity IP address list table associated with that FQDN.
   - Domain names will be matched based on the most specific FQDN entity, allowing subdomains to match on a less specific FQDN. This behavior is similar to a wildcard DNS record.
     For instance, if you have the following FQDN entities configured: "com," "google.com," and "maps.google.com," then "microsoft.com" will match with "com," "drive.google.com" will match with "google.com," and "maps.google.com" will match with "maps.google.com." However, it's important to note that "maps.google.com" will not match with "google.com.
3. Domains that are added into the cache can then be seen in the output of the **show ip dns forwarding cache** command and added into firewall entities as appropriate.

DNS configuration is required in order for the AR-Series Firewall to perform DNS resolution and cache the results.

Note: The optional parameter **via-relay** is appended to the **ip domain-lookup** command. This parameter forces all DNS requests originating from the router itself to be parsed through the DNS relay feature (DNS forwarding). This is because the DNS relay has a cache of recently resolved domains which is required for this feature to work.

```
!
ip name-server 10.0.0.1
ip domain-lookup via-relay
ip dns forwarding
ip dns forwarding cache size 1000 timeout 1800
!
```

For examples of how to configure FQDN Lookup, refer to "Configuration: FQDN Lookup" on page 22.

Limitations

There are several limitations when identifying applications based purely on IP address(es) learned via DNS lookup to a specific FQDN.

- Cloud-based Web Services may be hosted within a geographically distributed CDN. This can result in multiple services sharing a common IP address with other related services that the network administrator may wish to treat in a different manner. This can be problematic if one service needs to be permitted and another needs to be denied. If they share the same IP address then this will not work correctly; either both will be permitted or both will be blocked depending on rule order. Office365 and GoogleDocs are examples of applications where related services may share IP address (for example, Excel365 and Word365). An example of dissimilar services sharing the same IP address is www.google.com and www.youtube.com; it is quite conceivable that a network administrator may want to block access to YouTube but not Google Search.
- Some services (especially ones hosted by a CDN) may be initially accessed by a single FQDN known by the user. However once the connection has been established, the user's computer will need to make multiple requests to new IP addresses that were not registered in DNS under the original FQDN, but were learned as part of the first connection. If PBR rules are configured to selectively route all traffic for a given service out a particular interface based on FQDN, then it is likely that traffic **not** registered with an IP address under the original FQDN will be routed out a different interface in this case, resulting in communications errors. Domains requested by network clients can be seen in the output of **show ip dns forwarding cache** so the administrator will be able to discover and add missing FQDNs to their configuration. However as domains change over time they will need to periodically refresh the list of FQDNs they monitor. Office365 is an example of an application that behaves in this manner. In this instance, the user should consider alternative technology options, such as PAC files loaded into workstations to control traffic path selection at source.
- Firewall rules must be present to prevent clients from using other DNS servers. The client's device must use the router as their DNS server IP to ensure that future requests to the service's IP addresses use the same IP addresses that the router has resolved for that service.
- Some services may have IP addresses registered in DNS, but upon accessing that IP address, the client is sent a redirect to a secondary IP address, to which subsequent communications may be directed. Because the secondary IP address was not included in the DNS reply, the Host entity will not be able to correctly match all traffic sent to the secondary address.
- The device relies on DNS queries in order to populate the list of IP addresses to match traffic against. This means any Internet resources that are accessed directly by IP address from network clients (and therefore don't generate DNS requests) won't be able to be matched by the device. This may require the user to manually configure explicit entities to match against those IP addresses. Providers of web-based services often publish lists of URLs and IP addresses associated with their services.
- Any DNS requests that are not sent using standard unencrypted DNS queries to port 53 cannot be intercepted by the device. This means traffic destined to FQDNs that have been resolved via these protocols won't be able to be matched by the device as it will have no record of the IP addresses used by the domain. These alternative DNS protocols do not yet have widespread

adoption, but are under active development at present, for example, DNS over HTTPs, DNS over TLS, or DNSCrypt.

- IP addresses matched by FQDN entities are only updated when the DNS records are updated by DNS request. Expired DNS records still exist in the DNS cache but are not displayed to the user. When a DNS request is made, the DNS cache is traversed for expired entries and deleted then. For example, a user performs DNS requests for “facebook.com” and “google.com” so these are added to the DNS cache. After some time these will expire and they are not deleted from the DNS cache yet. The user performs a DNS request for “google.com”, the record for “google.com” is updated and the record for “facebook.com” is now deleted.
- When an FQDN is used as part of a firewall rule to explicitly permit traffic from a source IP address that would otherwise be denied, it means the IP address is not statically configured in the firewall's configuration and is instead learned via a DNS lookup of the configured FQDN. Because DNS requests are vulnerable to spoofing, firewall rules that rely on DNS resolution may be circumvented by an attacker that substitutes their own chosen IP address instead of the genuine IP address for the configured FQDN, thus bypassing firewall rules that ordinarily would block their access. Therefore use of a firewall deny rule to restrict DNS traffic is advised.

Configuration: FQDN Lookup

This example shows configuration for Fully-Qualified Domain Name (FQDN) lookup with firewall and NAT used to block access to Facebook and to restrict access to the DNS.

```
!
zone private
 network lan
  ip subnet 192.168.1.0/24
!
zone public
 network all
  ip subnet 0.0.0.0/0 interface eth1
 host wan
  ip address 172.16.0.2
 host facebook
  ip address dynamic fqdn facebook.com
 host dns
  ip address 10.0.0.1
!

firewall
 rule 10 deny any from private to public.all.facebook
 rule 20 permit any from private to private
 rule 30 permit any from private to public
 rule 40 permit dns from public.all.wan to public.wan.dns
 rule 50 deny dns from public to public
 rule 60 permit any from public.all.wan to public
 protect
!
nat
 rule 10 masq any from private to public
 enable
!
ip name-server 10.0.0.1
ip domain-lookup via-relay
!
```

```
interface eth1
 ip address 172.16.0.2/24
!
interface vlan1
 ip address 192.168.1.1/24
!
ip route 0.0.0.0/0 172.16.0.1
!
ip dns forwarding
ip dns forwarding timeout 600
ip dns forwarding cache size 1000 timeout 600
!
```

The following example shows configuration for using FQDN lookup with Policy-Based Routing (PBR) to selectively policy-route traffic to Facebook.

```
!
zone private
 network lan
  ip subnet 192.168.1.0/24
!
zone public
 network all
  ip subnet 0.0.0.0/0
  host facebook
  ip address dynamic fqdn facebook.com
 host eth1
  ip address 172.16.0.2
 host eth2
  ip address 172.16.1.2
!

firewall
 rule 10 permit any from private to private
 rule 20 permit any from private to public
 rule 30 permit any from public.all.eth1 to public
 rule 40 permit any from public.all.eth2 to public
 protect
!
nat
 rule 10 masq any from private to public
 enable
!

policy-based-routing
 ip policy-route 10 match http from private to public.all.facebook nexthop
172.16.1.1
 policy-based-routing enable
!
ip name-server 10.0.0.1
ip domain-lookup via-relay
!
interface eth1
 ip address 172.16.0.2/24
!

interface eth2
 ip address 172.16.1.2/24
!
interface vlan1
 ip address 192.168.1.1/24
!
ip route 0.0.0.0/0 172.16.0.1
ip route 0.0.0.0/0 172.16.1.1 10
!
ip dns forwarding
ip dns forwarding timeout 600
ip dns forwarding cache size 1000 timeout 600
!
```

The following example shows configuration for using FQDN lookup with traffic control to limit upload bandwidth to Facebook.

```
!
zone private
 network lan
  ip subnet 192.168.1.0/24
!
zone public
 network all
  ip subnet 0.0.0.0/0
  host facebook
  ip address dynamic fqdn .com
 host eth1
  ip address 172.16.0.2
!

firewall
 rule 10 permit any from private to private
 rule 20 permit any from private to public
 rule 30 permit any from public.all.eth1 to public
 protect
!
nat
 rule 10 masq any from private to public
 enable
!
traffic-control
 policy RESTRICT priority
  class LOW priority-level 5 max 1mbit
 rule 10 match http from private to public.facebook policy RESTRICT.LOW
   traffic-control enable
!

interface eth1
 ip address 172.16.0.2/24
!
interface vlan1
 ip address 192.168.1.1/24
!
ip route 0.0.0.0/0 172.16.0.1
!
ip dns forwarding
ip dns forwarding timeout 600
ip dns forwarding cache size 1000 timeout 600
!
```

Show commands

Here is an example of the **show running-config entity** command:

```
awplus#show running-config entity
zone public
 network all
  ip subnet 0.0.0.0/0 interface eth1
 network fqdn
  host facebook
   ip address dynamic fqdn facebook.com
```

To see resolved IP addresses, use the **show entity** command:

```
awplus#show entity
Zone:          public
 Network:      public.all
  Subnet:      0.0.0.0/0 via eth1
 Network:      public.fqdn
  Host:        public.fqdn.facebook
   FQDN IPv4:  facebook.com
   Address:    157.240.8.35 (dynamic)
```

To see the DNS cache entries, use the **show ip dns forwarding cache** command:

```
awplus#show ip dns forwarding cache
IPv4 addresses in cache:      1
IPv6 addresses in cache:      0
Cache size: 10000
Host
 Address                                              Expires Flags
facebook.com
 157.240.8.35                                             101
```

NAT Rules with DPI

You can configure firewall rules to allow or deny specific application traffic to flow from one entity to another. And most commonly, when using DPI in combination with NAT, it is sufficient to configure a single rule to masq any traffic from LAN to WAN without the need to configure NAT rules for each application. You may also configure a few NAT port forwarding rules to allow external traffic from the Internet to the public IP address to be translated to reach the internal addresses of internal servers.

For example:

```
awplus(config)# nat
awplus(config-nat)# enable
awplus(config-nat)# rule masq any from lan to wan
awplus(config-nat)# exit
awplus(config)# exit
```

However, if you configure NAT rules to selectively apply address translation to specific application traffic only, you may find that the application traffic matching the NAT rules will not be forwarded even with DPI enabled. This is because the DPI engine cannot positively identify the application until after the first few packets associated with the application flow have been seen. Therefore, NAT does not know what to do with the initial packets of a new flow, as they will not match any defined application-specific NAT rules.

There are two solutions to this problem:

Solution 1: Create a new custom definition

The first alternative for allowing DPI-permitted traffic through NAT rules is to create a new custom definition for the application for the NAT rule.

Step 1: **Create a new custom application definition.**

Create a new custom definition for the application for the NAT rule. For example:

```
awplus(config)# application customapp
awplus(config-application)# protocol tcp
awplus(config-application)# sport 300 to 65535
awplus(config-application)# dport 45
```

Step 2: **Apply this application to NAT rules.**

```
awplus(config)# nat
awplus(config-nat)# enable
awplus(config-nat)# rule masq customapp from lan to wan
awplus(config-nat)# exit
awplus(config)# exit
```

Confirm that the NAT rules with the specified application are valid.

```
awplus#show nat rule

[* = Rule is not valid - see "show nat rule config-check"]

-------------------------------------------------------------------------
  ID     Action     From                    With (dst/src) Entity   Hits
         App        To                      With dport
-------------------------------------------------------------------------
  10     masq       lan                     -                       0
         customapp  wan                     -
```

Solution 2: Override the DPI definition

The second alternative for allowing DPI-permitted traffic through NAT rules is to statically configure an application with the same name as the DPI application. The statically configured application overrides any previously defined DPI-based settings. For example:

```
awplus(config)# application mail
awplus(config-application)# protocol tcp
awplus(config-application)# sport 500 to 10000
awplus(config-application)# dport 50
awplus(config-application)# exit
awplus(config)# nat
awplus(config-nat)# rule masq mail from lan to wan
awplus(config-nat)# end
```

Confirm that the NAT rules with the specified application are valid.

```
awplus#show nat rule

[* = Rule is not valid - see "show nat rule config-check"]
-------------------------------------------------------------------------
  ID      Action      From                    With (dst/src) Entity   Hits
          App         To                      With dport
-------------------------------------------------------------------------
  10      masq        lan                     -                       0
          mail        wan
```

When DPI is enabled, because there is a user-defined application called ‘mail’, it will not be replaced by the DPI definition. The user-defined application has priority.

Allied Telesis NETWORK SMARTER

North America Headquarters | 19800 North Creek Parkway | Suite 100 | Bothell | WA 98011 | USA | T: +1 800 424 4284 | F: +1 425 481 3895
Asia-Pacific Headquarters | 11 Tai Seng Link | Singapore | 534182 | T: +65 6383 3832 | F: +65 6383 3830
EMEA & CSA Operations | Incheonweg 7 | 1437 EK Rozenburg | The Netherlands | T: +31 20 7950020 | F: +31 20 7950021

alliedtelesis.com