Introduction

This guide describes AlliedWare Plus Application Control and its configuration.

AlliedWare Plus Application Control is a next-generation Deep Packet Inspection (DPI) software engine that provides real-time, multiple-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) while dramatically increasing the throughput and reducing latency.

Contents

Introduction ........................................................................................................................................................................ 1
Products and software version that apply to this guide................................................................. 1
What is Application Control? ................................................................................................................................. 2
Configuration Example...................................................................................................................................................... 3

Products and software version that apply to this guide

This Guide applies to AlliedWare Plus Application Control, running version 5.4.5 or later.

However, implementation varies between products. To see whether a product supports a feature or command, see the following documents:

- The product’s Datasheet
- The AlliedWare Plus Datasheet
What is Application Control?

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

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

AlliedWare Plus Application Control can also identify thousands of individual applications and establish rules determining not only which are allowed, but under what circumstances and by whom. 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 Control utilizes Procera Networks’ Network Application Visibility Library (NAVL) to respond to the fast changing and complex applications. NAVL uses a combination of deep packet and deep flow inspection techniques to provide real-time identification of network applications. Figure 6 shows how Application Control works.

**Figure 6: Deep Packet Inspection**

AlliedWare Plus Application Control is used by the firewall to match packets against pre-defined application signatures and provide Layer 7 filtering for firewall rules.

**Configuration Example**

This example shows how to configure Application Control using Deep Packet Inspection (DPI).

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

The product’s Command Reference

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

Feature support may change in later software versions. For the latest information, see the above documents.
Step 1: Enter the DPI mode.
```
awplus#configure terminal
awplus(config)#dpi
```

Step 2: Set the DPI provider and enable DPI protection.
```
awplus(config-dpi)#provider procera
awplus(config-dpi)#enable
```

Step 3: Verify DPI configuration
```
awplus#show dpi
```
Below is an example output from the console.
```
awplus#show dpi
Status: running
Provider: procera
Resource version: 1.0
Resource update interval: 1 hour
```

Step 4: Show applications inspected by DPI
```
awplus#show dpi statistics
```
```
awplus#show dpi statistics
Application | Packets | Bytes
-------------|--------|------
http         | 30     | 2020 |
icmp         | 348    | 29232|
telnet       | 45     | 2553 |
```

Step 5: Apply firewall rules
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.
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
```
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
```
Apply firewall rule.
awplus(config-zone)#exit
awplus(config)#firewall
awplus(config-firewall)#rule 10 permit http from public to dmz
Enable firewall protection.
awplus(config-firewall)#protect
When using DPI with 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 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