Technical Guide

Intrusion Prevention System (IPS)

Feature Overview and Configuration Guide

Introduction

This guide describes AlliedWare Plus™ Intrusion Prevention System (IPS) and its configuration.

AlliedWare Plus IPS is an intrusion detection and prevention system that is positioned at the perimeter of a network and effectively protects the network security. It can monitor, analyze and log suspicious network activity and proactively prevent malicious threats.

Products and software version that apply to this guide

This guide applies to AlliedWare Plus IPS, running version **5.4.5** or later.

To see whether a product supports IPS, see the following documents:

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

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

Feature support may change in later software versions. For the latest information, see the above documents.

Contents

How IPS works

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 deployed in inline mode and there is no delay 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*>]**.

The IPS built-in 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 key features

Basic Operation

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

Configuration

You can:

- Display the list of categories and their configured actions
- Set category actions to ‘alert’, ‘deny’, or ‘disable’. The default action for all categories is either ‘alert’ or ‘disable’.
- Configure rule actions in categories to eliminate unnecessary or troublesome rules for a specific deployment.
- Enable Rate limiting of IPS alerts.
- Configure a third party category provider, currently this is Proofpoint.
- Configure the Update interval of the third party resource.

Configuration example

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
```