Technical Guide

IP Reputation

FEATURE OVERVIEW AND CONFIGURATION GUIDE

Introduction

This guide describes AlliedWare Plus IP Reputation and its configuration.

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. 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.

Contents

Products and software version that apply to this guide

This Guide applies to AlliedWare Plus IP Reputation, 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

AlliedWare Plus™ OPERATING SYSTEM

- 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.

How IP Reputation Works

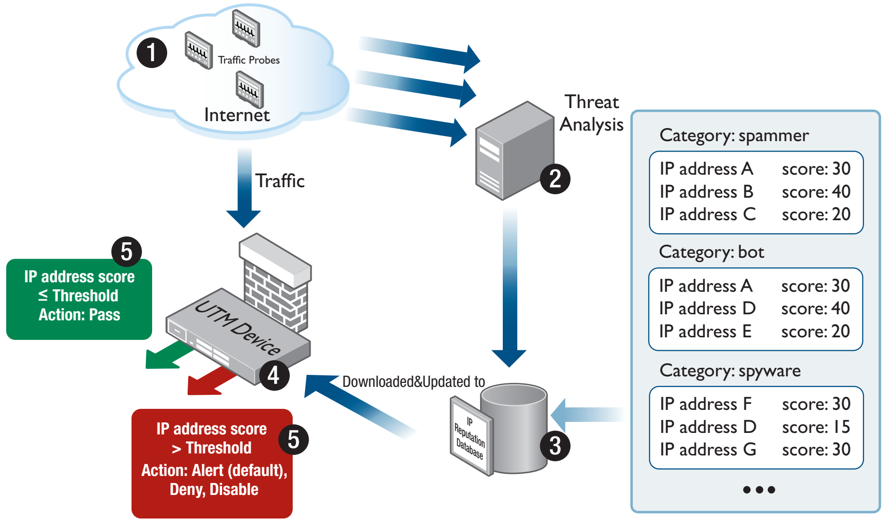
AlliedWare Plus IP Reputation uses category, which is a grouping of criteria, to classify the nature of a host's reputation. For example, IP addresses associated with questionable gaming sites will be categorized as OnlineGaming.

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 compressive IP reputation lists through Emerging Threats. Emerging Threats 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



Category: spammer

IP address A	score: 30
IP address B	score: 40
IP address C	score: 20

Category: bot

IP address A	score: 30
IP address D	score: 40
IP address E	score: 20

Category: spyware

IP address F	score: 30
IP address D	score: 15
IP address G	score: 30

•••

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 the Emerging Threats IQRisk™ Rep List of IPv4 addresses, categories and reputation scores
- Accurate and detailed information on 200,000+ 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

Configuration Example

This example shows how to configure IP Reputation.

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 emerging-threats
```

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: Verify IP Reputation configuration

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

Below is an example output from the console.

```
awplus#show ip-reputation
Status:      Enabled (Active)
Provider:    emerging-threats
Resource version:        1.0
Resource update interval: 1 hour
```

Allied Telesis™ the **solution :** the **network**

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