Review or Dispute IPS False Positives with Umbrella

Contents

Introduction

This document describes how to review or dispute Intrusion Prevention Service (IPS) false positives with Cisco Umbrella.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on Cisco Umbrella.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Overview

Cisco Umbrella's Intrusion Prevention System detects (and optionally blocks) packets which are deemed to be associated with a known threat, vulnerability, but also simply when the format of the packet is unusual.

Administrators choose which IPS signature list is used to detect threats based on these default lists:

- Connectivity Over Security
- Balanced Security and Connectivity

- Security Over Connectivity
- Maximum Detection

It is important to remember that the chosen signature list can greatly impact the number of IPS False Positives encountered. The most secure modes (such as Maximum Detection and Security Over Connectivity) are expected to create unwanted IPS detections as they place emphasis on security. The most secure modes are only recommended when total security is required, and the Administrator must anticipate the need to monitor and review large numbers of IPS events.

For more information on the different modes, review the IPS Documentation.

Review IPS Detections

Use the Activity Search on the Umbrella Dashboard to view IPS Events. For each event there are two important pieces of information:

- IPS Signature ID/Category/Name. Searchable on https://snort.org
- CVE Number (if applicable). Searchable on https://www.cve.org/

Not all IPS detections indicate a known exploit/attack. Many of the signatures (particularly in Max Detection mode) simply indicate the presence of a certain type of traffic, or a protocol violation. It is important to review the sources of information mentioned earlier along with other details about the event (like source/destination) to determine if the event requires further investigation from your security team.

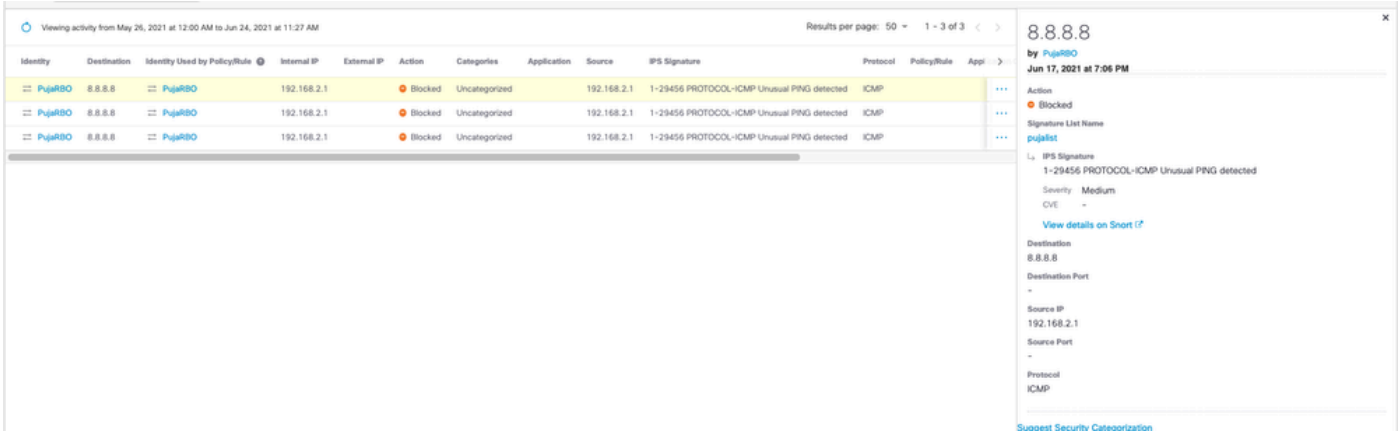
The signature category can be useful in providing additional context about the type of IPS detection. Review the categories available on snort.org.

Protocol Violations

In this example, an IPS Event is linked to this signature :
https://www.snort.org/rule_docs/1-29456

The description of the signature is:

"The rule looks for PING traffic coming into the network that doesn't follow the normal format of a PING."



4403885889428

In this case, the Snort rule is not necessarily detecting any particular exploit, but is instead detecting a malformed ICMP packet that was blocked. Based on the information available on snort.org, and other details about the event (like source/destination), the Administrator can decide that this event requires no

further investigation

Application Compatibility

Some legitimate applications are not compatible with IPS signatures, particularly when the more aggressive (Max Detection) modes are configured. In these scenarios, the application can be blocked for reasons discussed in the Protocol Violation section. The application can use a protocol in an unexpected way, or use a custom protocol over a port that is normally reserved for other traffic.

Even though the application is legitimate, these detections are often valid and cannot always be corrected by Cisco.

If a legitimate application is blocked by IPS, Umbrella recommends contacting the vendor of the application with details of the event/signature. Third party applications must be tested for compatibility with the IPS signatures at snort.org.

It is currently not possible to exclude an individual Application/Destination from IPS scanning.

Disabling IPS Signatures

If a signature is found to cause compatibility issues with a third party application, the signature can be disabled (either temporarily or permanently). This must only be done when you trust the application and you have determined that the value of the application outweighs the security benefits of the specific signature.

Complete the steps in the Add a Custom Signature List documentation for information on creating a custom signature list. You can use your current settings as a template and then disable the desired rules by setting them to **Log Only** or **Ignore**.

Support

Historical Events

Umbrella Support is unable to provide additional details about **historical** IPS Events. IPS Events inform you that traffic did not match the IPS signature. Details of the signature are publicly available on snort.org. Umbrella does not store a copy of raw traffic/packets and is therefore unable to provide further context or confirmation about the nature of an IPS event.

IPS Problems / False Positives

If you wish to dispute a **current** IPS problem (such as a False Positive), please contact Umbrella Support.

In order to investigate these problems, a packet capture is required by Umbrella Support. The raw contents of packets are needed to determine how the traffic triggered the IPS detection. You must be able to replicate the issue in order to generate the packet capture.

Before raising a ticket, use a tool such as Wireshark to generate the packet capture when replicating the issue. Instructions are available in our knowledge base.

Alternatively, Umbrella Support can assist with generating the packet capture. They need to schedule a time when the issue with the affected user or application can be recreated.