Introduction

This document explains what Intrusion Prevention System (IPS) Event Summarization is and what the reasons are for IP addresses that show up as 0.0.0.0:0 in IPS signature events.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco IPS signature alerts configuration
- IPS event summarization configuration

**Note:** See [IPS Summarization Configuration Examples](#) for event summarization configuration examples.

Components Used

The information in this document is based on these software and hardware versions:

- Adaptive Security Appliance (ASA) 5500 or 5500x IPS modules
- IPS 4200, 4300, or 4500 Series IPS appliances
- Network Module Enhanced (NME) - IPS module
- IPS 7.x software

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, make sure that you understand the potential impact of any command.
Background Information

IPS event summarization is a method used to aggregate multiple events into a single alert. This results in a reduction of the volume of alerts processed and sent by the sensor.

Problem

Events generated on the IPS show the IP address of the attacker/victim as 0.0.0.0:0.

Solution

When the IPS generates signature alerts, it provides information such as Signature ID, Timestamp, IP address of the attacker/victim, and so on. Under certain conditions, the events generated show the IP address of the attacker/victim displayed as 0.0.0.0:0. The reason behind the IP addresses displayed as 0.0.0.0:0 is summarization. In order to configure summarization, either add a new custom signature or edit a current signature and select Alert Frequency > Summary Mode.

The available summarization options are:

- Fire-all - fires an alert every time a signature is triggered.
- Fire-once - fires an alert for an address set.
- Summarize - fires an alert the first time a signature is triggered. Additional alerts for that signature are summarized for the duration of the summary interval.
- Global-summarization - fires an alert for every summary interval.

What is the difference between Summary Key and Global Summary Threshold?

Summary Key is a key used by the IPS in order to conclude how to create a summary event. By default, this is an attacker address which means that if you have one attacker that triggers any signature, one regular event and one summary is generated. If you have two attackers, two regular and two summary events are generated for the configured summary interval. If you set the summary key to victim address and you have two attackers that target one victim, then two attackers will record only one regular and one summary event.

Summary Mode has two options; Summary Interval and Summary Key. Summary Interval is represented in seconds and it fires for every summary interval. Summary Key is a criterion by which the IPS decides on how to create the Summary event. By default, this is the Attacker address. The available Summary Key options include:

- Attacker address (default)
- Attacker address and victim port
- Attacker and victim addresses
- Attacker and victim addresses and ports
- Victim address
The previous example shows a signature summarized with a Summary Interval of 4 and Summary Key as attacker address. In this scenario, the signature fires a normal event the first time after which point the signature is summarized for an interval of 4 seconds.

<table>
<thead>
<tr>
<th>Severity</th>
<th>Date</th>
<th>Time</th>
<th>Device</th>
<th>Sig. Name</th>
<th>Sig. ID</th>
<th>Attacker IP</th>
<th>Victim IP</th>
<th>VI</th>
<th>T</th>
<th>...</th>
</tr>
</thead>
<tbody>
<tr>
<td>inf...</td>
<td>08/28...</td>
<td>02:45:55</td>
<td>sensor</td>
<td>ICMP Echo Request</td>
<td>2004/0</td>
<td>192.168.2.245</td>
<td>172.16.2.245</td>
<td>35</td>
<td>35</td>
<td></td>
</tr>
<tr>
<td>inf...</td>
<td>08/28...</td>
<td>02:45:55</td>
<td>sensor</td>
<td>ICMP Echo Reply</td>
<td>2000/0</td>
<td>172.16.2.245</td>
<td>192.168.2.245</td>
<td>35</td>
<td>35</td>
<td></td>
</tr>
<tr>
<td>inf...</td>
<td>08/28...</td>
<td>02:45:57</td>
<td>sensor</td>
<td>ICMP Echo Reply</td>
<td>2000/0</td>
<td>10.0.0.14</td>
<td>192.168.2.245</td>
<td>35</td>
<td>35</td>
<td></td>
</tr>
<tr>
<td>inf...</td>
<td>08/28...</td>
<td>02:45:59</td>
<td>sensor</td>
<td>ICMP Echo Request</td>
<td>2004/0</td>
<td>192.168.2.245</td>
<td>0.0.0.0</td>
<td>25</td>
<td>25</td>
<td></td>
</tr>
<tr>
<td>inf...</td>
<td>08/28...</td>
<td>02:45:59</td>
<td>sensor</td>
<td>ICMP Echo Reply</td>
<td>2000/0</td>
<td>172.16.2.245</td>
<td>0.0.0.0</td>
<td>25</td>
<td>25</td>
<td></td>
</tr>
<tr>
<td>inf...</td>
<td>08/28...</td>
<td>02:45:59</td>
<td>sensor</td>
<td>ICMP Echo Request</td>
<td>2004/0</td>
<td>192.168.2.245</td>
<td>10.0.0.14</td>
<td>35</td>
<td>35</td>
<td></td>
</tr>
<tr>
<td>inf...</td>
<td>08/28...</td>
<td>02:46:01</td>
<td>sensor</td>
<td>ICMP Echo Reply</td>
<td>2000/0</td>
<td>10.0.0.14</td>
<td>0.0.0.0</td>
<td>25</td>
<td>25</td>
<td></td>
</tr>
<tr>
<td>inf...</td>
<td>08/28...</td>
<td>02:46:03</td>
<td>sensor</td>
<td>ICMP Echo Request</td>
<td>2004/0</td>
<td>192.168.2.245</td>
<td>0.0.0.0</td>
<td>25</td>
<td>25</td>
<td></td>
</tr>
</tbody>
</table>

Global Summary Threshold - if global summary is not specified and if there are two attacker IP addresses seen, the IPS records two normal events. After a period of Summary Interval, two additional summarized events are generated, one for each attacker IP address. In total, you would have 4 events recorded within the specified interval.

With Global Summarization enabled with a Global Summary Threshold of say, two, and if you repeat the previous example, then the IPS records THREE events: two for initial hits for each attacker address and one summarized event for all attackers (two in this case) within the specified interval. Now if you scaled up the number of attackers and hits, you would see that a Global Summarization saves up a lot of events/logs and thus a processor cycles.

Global Summarization has only one sub-option which is "summary interval" that is configured in seconds. When the signature is set to global-summarization, it fires for every summary interval. That is, if the summary interval is set to '5', it fires an alert the first time the signature is triggered and thereafter it fires for every summary interval of 5 seconds.

In order to edit a signature, select **Configuration > Policies > Active signature** and then search for the relevant signature.

For example, the SIG ID for 'ICMP request' is 2004. Right-click the signature and select **Edit** in order to get to the dialog box shown here:
In the previous configuration snippet, the summary mode has been set to 'global summarize' with a summary interval of 5 seconds.

The sample of alerts show the signatures 'ICMP Echo Request' and 'ICMP Echo Reply', which have been summarized and hence display the attacker/victim IP addresses as '0.0.0.0'.

Do not confuse global summarization events with 'signature 1102.0 events (Impossible IP Packet)'. Hackers might try to evade an IPS with the use of all zeros for the source/destination IP addresses and port which could trigger this signature, which might look like a summarized event.
Related Information

- Cisco Intrusion Prevention System Signatures Frequently Asked Questions
- Cisco Intrusion Prevention System Sensor CLI Configuration Guide for IPS 7.1
- IPS Summarization Configuration Examples
- Technical Support & Documentation - Cisco Systems