Cisco Secure Network Analytics

Alarm Suppression 7.4

Table of Contents

Overview **3**
Alarms You Can Suppress 3
Rule Configuration 9
Rule Properties 10
Attribute Details 12
API Examples 16
Contacting Support **17**

Overview

You can configure rules, based on alarm attributes, for known communication between devices which is expected and known to never be malicious. When the communication matches the rule criteria (such as ports, protocols, IP addresses), Analytics suppresses any alarms that would normally be generated, resulting in a less noisy and more efficacious system.

Each time Analytics processes a configuration file, it overwrites the previous file. No Flow Collector synching occurs since this action is limited to the Manager (formerly Stealthwatch Management Console).

You can suppress 23 of the available alarms and for any of your domains.

- Analytics supports alarm suppression for Cisco Secure Network Analytics (formerly Stealthwatch) version 7.4.0.
- Syslogs are not sent out for Response Management.
- A log of suppressions is preserved but is not recorded in the audit log.
- When you perform a configuration backup, the alarm suppression file should be included (but only if you have successfully previously processed this file). However, we recommend that you create a configuration backup of this file on the Manager.

Alarms You Can Suppress

You can suppress the following alarms:

Alarm Type (Alarm ID)	Alarm Attributes you can Suppress
Addr (Address) Scan/tcp (276) The source host is attempting to contact multiple hosts (using TCP) within a natural class C network (/24) on the same port and most connection attempts are either being rejected (TCP Reset) or the target hosts are not responding at all. This is used to trigger the Worm Activity and Worm Propagation alarms. These are commonly seen during network	• source_ip • source_groups • protocol • destination_ip_range • destination_port

Alarm Type (Alarm ID)	Alarm Attributes you can Suppress
scanning or enumeration.	
Addr (Address) Scan/udp (286) The source host is attempting to contact multiple hosts (using UDP) within a natural class C network (/24) on the same port and most connection attempts are either being rejected (ICMP port unreachable) or the hosts are not responding at all. These are commonly seen during network scanning or enumeration. This is used to trigger the Worm Activity and Worm Propagation alarms.	• source_ip • source_groups • protocol • destination_ip_range • destination_port
Beaconing Host (39) An IP communication between an inside and outside host (with traffic in only one direction) exceeds the "Seconds required to qualify a flow as long duration" setting.	• source _ip • source_groups • source_port • destination_ip • destination_groups • destination_port • protocol
Bot Infected Host - Attempted C&C Activity (41) The source host is attempting to contact a command and control (C&C) server using a port identified in the C&C Server list. The communication is one-way only, indicating the C&C server has not responded. The inside host, as the initiator, accumulates Concern Index (CI) points. If the C&C	• source_ip • source_groups • source_port • destination_ip • destination_groups • destination_port • protocol

Alarm Type (Alarm ID)	Alarm Attributes you can Suppress
server it attempts to contact is also an inside host, then that C&C server accumulates Target Index (TI) points.	
Bot Infected Host - Successful C&C Activity (42) The source host has successfully contacted a C&C server using a port identified in the C&C Server list. The communication is two-way, indicating the C&C server has responded. The inside host, as the initiator, accumulates Concern Index (CI) points. If the C&C server it contacts is also an inside host, then that C&C server accumulates Target Index (TI) points.	• source_ip • source_groups • source_port • destination_ip • destination_groups • destination_port • protocol
Brute Force Login (58) The host detects a series of short TCP connections consistent with an attempt at brute force password cracking through repeated logins.	• source_ip • source_groups • source_port • destination_ip • destination_groups • destination_port • protocol
High SMB Peers (60) This security event indicates that host has many Server Message Block (SMB) sessions to the outside, which is consistent with worm propagation.	• source_ip • source_groups • source_port • protocol • flows_count
High Traffic (30)	• source_ip

Alarm Type (Alarm ID)	Alarm Attributes you can Suppress
The host traffic rate averaged over a 5-minute period has exceeded the limit of acceptable traffic values.	• source_groups • bytes_ per_second
ICMP Flood (7) The source host has sent an excessive number of ICMP packets in a 5-minute period.	• source_ip • source_groups • packets
Packet Flood (8) The source host has sent an excessive number of short packets to the target host. This security event is seen as a result of brute force attacks, DoS attacks, and malfunctioning network applications.	• source_ip • source_groups • source_port • destination_ip • destination_groups • destination_port • protocol
Ping Oversized Packet (278) The source host has sent an ICMP echo request or reply that has more than 90 data bytes. These events may be harmless network health checks or may contain a covert data channel.	• source_ip • source_groups • destination_ip • destination_groups • protocol
Ping Scan (277) The source host is sending Echo Request packets to many hosts with a natural class C network (/24) range of addresses. This is often done to identify the active hosts on a network.	• source_ip • source_groups • protocol • destination_ip_range
Port Scan (55) The source IP has attempted to	• source_ip • source_groups

Alarm Type (Alarm ID)	Alarm Attributes you can Suppress
connect to an excessive number of ports on the target IP.	• source_port • destination_ip • destination_groups • destination_port • protocol
Scanner Talking (63) This security event indicates that a host that has been scanning your network now has a two-way conversation with one of the target hosts that it scanned. It is enabled by default in the Inside Hosts policy and the Outside Hosts policy. It is, however, disabled by default in the Network Management Scanners role policy.	• source_ip • source_groups • source_ports • destination_ip • destination_group • destination_port • protocol
SSH Reverse Shell (61) Detects an SSH session that appears to be a reverse shell. More data is being sent to the outside host than is being received.	• source_ip • source_groups • source_port • destination_ip • destination_groups • destination_port • protocol
Stealth Scan/tcp (272) The source host has used the same source port to connect to different ports on the target host at the same time. This behavior indicates applications that have used raw	• source_ip • source_groups • source_port • destination_ip • destination_groups

Alarm Type (Alarm ID)	Alarm Attributes you can Suppress
sockets to create TCP or UDP connections. The security event shows the last target port accessed before the security event was recognized.	• destination_port • protocol
Stealth Scan/udp (271) A crafted UDP scan with re-use of port numbers by the source host. This often indicates "packet crafting" is being done by the scanning host which may be looking for hosts to attack.	• source_ip • source_groups • source_port • destination_ip • destination_groups • destination_port • protocol
Suspect Data Hoarding (315) The source host has downloaded an unusual amount of data from one or more hosts.	• source IP Address • source Group List • bytes
Suspect Data Loss (40) Indicates that an inside host has uploaded an abnormal amount of data to outside hosts.	• source_ip • source_groups • bytes
Suspect UDP Activity (24) The source host has been identified scanning multiple hosts on a UDP port and has successfully sent a large UDP packet to another previously scanned host. This type of behavior is consistent with many single-packet UDP-based worms such as "SQL Slammer" and "Witty." Investigate this security event immediately.	• source_ip • source_groups • source _port • destination_ip • destination_groups • destination_port • protocol

Alarm Type (Alarm ID)	Alarm Attributes you can Suppress
SYN Flood (5) The source host has sent an excessive number of TCP connection requests (SYN packets) in a 5-minute period. This may indicate a DoS attack or non-stealthy scanning activity.	• source_ip • source_groups • packets
UDP Flood (6) The source host has sent an excessive number of UDP packets in a 5-minute period. This may indicate a DoS attack or non-stealthy scanning activity.	• source_ip • source_groups • packets
Worm Propagation (36) The host has scanned and connected on a particular port across more than one subnet, and the host was previously scanned and connected to by a host for which the Worm Activity alarm has been raised.	• source_ip • source_groups • source_port • destination_ip • destination_groups • destination_port • protocol • initial_infected_host

For more information about these alarms, see Security Event List.

Rule Configuration

You must use APIs to configure alarm suppression rules. These APIs contain the following endpoints:

- **Get** Displays the current suppression configuration.
- **Put** Uploads and configures the rules to suppress alarms.
- **Delete** Deletes all suppression configuration.

Both Admin and Primary Admin users can configure alarm suppression rules.

Example: Following is an example of an alarm type rule. Its definition is "For an Address Scan TCP alarm with a device ID corresponding to 400 or 401, AND a domain ID other than 300 or 301, AND source groups corresponding to 22,23, or 24, AND a source IP corresponding to 1.1.1.1 or 1.1.1.2."

```
{
"rules": [
{
"type": 276,
"filters": [
{ "field": "device_id", "operator": "In", "value": [400, 401] }

,
{ "field": "domain_id", "operator": "NotIn", "value": [300, 301] }

,
{ "field": "source_groups", "operator": "In", "value": [22,23,24] }

,
{ "field": "source_ip", "operator": "In", "value": ["1.1.1.1", "1.1.1.2"] }

]
}
]
}
```

Rule Properties

Refer to the following guidelines when configuring rules:

- If an alarm type does have more than one rule, then either one of those rules (OR operation across rules) may suppress the alarm.
- The raised alarm should match all the attributes defined in the rule of a specific alarm type that you want to be suppressed.
- If you use the operator "IN" within a value, then any of the values within that expression can be true (OR operations across values within an expression).
- The same alarm type can have more than one rule.
- You can configure a maximum of 500 rules irrespective of alarm type.

Following are two rules for Address Scan TCP. The JSON for the full set of rules is shown in these two rules. Its definition is as follows:

" (For an Address Scan TCP alarm in a domain with ID 123 AND with a device ID of 12)

OR

(For an Address Scan TCP alarm in a domain with ID 234 AND with a device ID of 432)."

```
{
"rules": [
{
"type": 276,
"filters": [
{ "field": "domain_id", "operator" : "Equal", "value": 123}
,
{ "field": "device_id", "operator" : "Equal", "value": 12}
]
},
{
"type" : 276,
"filters": [
{ "field": "domain_id", "operator" : "Equal", "value": 234}
,
{ "field": "device_id", "operator" : "Equal", "value": 432}
]
}
]
}
```


When a host performs an address scan (TCP/UDP) on the same subnet with multiple ports, even though many security events are generated, only one condition is generated and one alarm is logged in host_alarm database on the Manager.

To suppress alarms of this kind, use the following rule:

Option 1: Give one port per expression

```
{
"rules" : [ {
"type" : 276,
"filters" : [
{ "field" : "destination_port", "operator" : Equal, "value" : 2049}
]
}, {
"type" : 276,
"filters" : [
{ "field" : "destination_port", "operator" : Equal, "value" : 2055}
,
```

Option 2: Give additional criteria (be more granular). See example below for available attributes

```
{
"type": 276,
"filters": [
{ "field": "device_id", "operator": "Equal", "value": 301 }
,
{ "field": "domain_id", "operator": "Equal", "value": 301 }
,
{ "field": "source_groups", "operator": "In", "value": [65534] }
,
{ "field": "source_ip", "operator": "In", "value": ["10.1.0.9", "10.1.0.8", "10.1.0.7", "10.1.0.6","10.1.0.5"] }
,
{ "field": "destination_ip_range", "operator": "In", "value": ["10.10.0.0"] }
,
{ "field": "protocol", "operator": "In", "value": ["tcp"] }
,
{ "field": "destination_port", "operator": "In", "value": [50] }
]
}
```

Attribute Details

The attributes you can suppress on an alarm fall into one of the following attribute types. You can use any of these operators that match a particular attribute type when building a rule. The following attributes may or may not be common across alarms.

> Entries are not case sensitive. As an example, for the protocol attribute you can use TCP, tcp, TcP, etc. These are all valid entries.

Attribute	Type	Operators	Description
bytes	Long	Equal, NotEqual, GreaterThan, GreaterThanEqual, LessThan, LessThanEqual	Positive whole number between 0 and 4294967296.
bytes_per_second	Long	Equal, NotEqual, GreaterThan, GreaterThanEqual, LessThan, LessThanEqual	Positive whole number between 0 and 4294967296.
device_id (This is the Flow Collector ID.)	integer or Set<Integer>	If Integer: Equal, NotEqual, GreaterThan, GreaterThanEqual, LessThan, LessThanEqual	Positive whole number.
		If Set<Integer>: In, NotIn	Set of whole numbers enclosed within [ ] up to 100 values.
destination_ip	Set<IPAddress>	In, NotIn	Set of IP addresses or subnet address range enclosed within [ ] up to 100 values.
destination_ip_range	Set<IPAddress>	In, NotIn	Set of subnet addresses enclosed within [ ] up to 100 values.
destination_groups	Set<Integer>	In, NotIn	Set of whole numbers

Attribute	Type	Operators	Description
			representing host group ID enclosed within [ ].
destination_port	Integer or Set<Integer>	If Integer: Equal, NotEqual, GreaterThan, GreaterThanEqual, LessThan, LessThanEqual	Positive whole number.
		If Set<Integer>: In, NotIn	Set of whole numbers enclosed within [ ] up to 100 values.
domain_id	integer or Set<Integer>	If Integer: Equal, NotEqual, GreaterThan, GreaterThanEqual, LessThan, LessThanEqual	Positive whole number.
		If Set<Integer>: In, NotIn	Set of whole numbers enclosed within [ ] up to 100 values.
flows_count	Long	Equal, NotEqual, GreaterThan, GreaterThanEqual, LessThan, LessThanEqual	Positive whole number between 0 and 4294967296.
initial_infected_host	Set<IPAddress>	In, NotIn	Set of IP addresses enclosed within [ ] up to 100 values.

Attribute	Type	Operators	Description
packets	Long	Equal, NotEqual, GreaterThan, GreaterThanEqual, LessThan, LessThanEqual	Positive whole number between 0 and 4294967296.
protocol	Protocol or Set<Protocol>	If Protocol: Equal, NotEqual	Single valid protocol name enclosed in double quotes Example: ["TCP"].
		If Set<Protocol> In, NotIn	Set of valid protocol names enclosed within [ ] up to 100 values Example: ["TCP", "UDP"].
source_ip	Set<IPAddress>	In, NotIn	Set of IP addresses or subnet address range enclosed within [ ] up to 100 values.
source_ groups	Set<Integer>	In, NotIn	Set of whole numbers representing host group ID enclosed within [ ] up to 100 values.
source_port	Integer or Set<Integer>	If Integer: Equal, NotEqual, GreaterThan, GreaterThanEqual, LessThan,	Positive whole number.

Attribute	Type	Operators	Description
		LessThanEqual	
		If Set<Integer>: In, NotIn	Set of whole numbers enclosed within [ ] up to 100 values.

API Examples

To read an overview of our APIs that contain endpoints (along with their request and response schema), do one of the following:

Option 1

1. Enter this URL: **https://[manager_ip_address]/api-docs**
2. Scroll to the link entitled "Alarm Suppression API" in the APIs section and click this link.

   The corresponding page opens.

Option 2

Enter this URL: **https://[manager_ip_address]/legacy-detections/v1/docs**

The corresponding API documentation is displayed.

Contacting Support

If you need technical support, please do one of the following:

- Contact your local Cisco Partner
- Contact Cisco Support
- To open a case by web: http://www.cisco.com/c/en/us/support/index.html
- To open a case by email: tac@cisco.com
- For phone support: 1-800-553-2447 (U.S.)
- For worldwide support numbers: https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

Copyright Information