# CounterACT Firewall-1® SAM Client Plugin

## Configuration Guide

Version 2.1.0 and Above

# Table of Contents

# About the Firewall-1® SAM Client Plugin

The CounterACT Firewall-1® SAM Client Plugin forwards block requests to an external Check Point Firewall-1® Suspicious Activity Monitor (SAM) server, allowing you to block sources with a CounterACT device and with the firewall. If a source is blocked by the firewall and the engine is stopped or the system is in Listen Only mode, firewall blocking continues.

## Requirements

- CounterACT version 6.3.4.0 or higher.
- FireWall-1® NG Feature Pack 3.

# Configuration

After installing the plugin, you must:

- Configure the SAM server for the selected CounterACT device.
- Configure firewall interoperability at the CounterACT Console.

## Configuring the SAM Server

You must configure the SAM client when blocking infected hosts using FireWall-1 and a CounterACT device. If the SAM client is configured using the sslca authentication method, you must register the CounterACT device at the Check Point SmartCenter. Messages regarding sslca communication are displayed at the SmartCenter in the SmartView™ status window. Contact your ForeScout support representative for information about connecting to SmartCenter.

**To configure the SAM server:**

1. Log in to the CounterACT device running the plugin.
2. Run the following command:

   **`fstool opsec`**

   The OPSEC configuration menu appears.
3. Select the **`Configure SAM Client`** option. The following messages appear:

```
SAM server IP address :

SAM server port [18183] :

Choose SAM server (X.X.X.X) communication type:

1) sslca : Certificate based authentication (recommended)
2) clear : No authentication (use for debugging only)
3) auth_opsec : Check Point proprietary (for backward
compatibility)

Choice : 1
```

4. Enter the required parameters for the server.
5. Select an authentication option. If you choose option 1, your CounterACT device must be registered at the Check Point SmartCenter Management Station.

   A series of messages appear with guidelines for configuring the Firewall-1 SAM server according to the authentication method chosen.

   The final message appears:

```
Appliance should be restarted for changes to be applied

Restart Appliance (yes/no) [yes] :
```

6. Press **Enter** to apply the configuration.

# Configuring Firewall Interoperability

Firewall interoperability values can be set from the CounterACT Console.

**To view or update firewall interoperability values:**

1. Select the **Options** icon from the Console toolbar and then select **Plugins**.
2. Select **Firewall-1(R) SAM Client** and then select **Configure**.

   The Firewall-1(R) SAM Client Plugin Configuration dialog box opens.

The following table summarizes Firewall-1 SAM Client configuration options:

| Field Name | Description |
|---|---|
| Firewall-1 Group | The firewalls at which source sessions are dropped or rejected.<br>▪ All: All the firewalls managed by the Check Point SmartCenter Server<br>▪ Gateways: All the firewalls managed by the Check Point SmartCenter Server that are defined as gateways and have VPN-1 or FireWall-1 installed |
| Block Method | Drop: Packets will be dropped<br>Reject: Packets will be rejected |
| Block Existing Connections | True: Block existing connections<br>False: Block only new connections |

| Field Name | Description |
|---|---|
| Source-Block Logging Type | The type of source blocking log messages that you want to send to the SmartView Tracker |
| Service-Block Logging Type | The type of service blocking log messages that you want to send to the SmartView Tracker |
| Maximum Concurrent Blocked Sources | The maximum number of concurrent blocked sources |
| Maximum Concurrent Blocked Services | The maximum number of concurrent blocked sources (the firewall may become overloaded if it has to handle an extensive number of sources)<br>Note: Protected services defined from the Firewall Policy dialog box may generate extensive Firewall-1 rules. If the number of rules generated exceeds the default, the rules will not be added. |

# Known Issues

Port blocking is not supported.

If a protected service rule is defined in a CounterACT policy, the rule will be implemented by the CounterACT device only - not by the CounterACT device and the Firewall.

# Legal Notice



Send comments and questions about this document to: documentation@forescout.com

May 2015