Integrating Juniper Sky Advanced Threat Prevention (ATP) and ForeScout CounterACT® for Infected Host Remediation

Configuration Example

March 2018
Contents

Introduction .............................................................................................................................................................. 4
Customer Use Case .................................................................................................................................................... 4
Technical Overview ................................................................................................................................................... 4
Configuration Example .............................................................................................................................................. 5
  Introduction .......................................................................................................................................................... 5
  Requirements ....................................................................................................................................................... 5
  Topology .............................................................................................................................................................. 5
  Configuration ....................................................................................................................................................... 6
  Verification ......................................................................................................................................................... 16
Introduction

This document illustrates how to integrate ForeScout CounterACT with Juniper Sky Advanced Threat Prevention (ATP) to reduce the attack surface, detect advanced threats and automate threat response. This document includes an example with step-by-step instructions for configuring Sky ATP, SRX Series devices, and CounterACT to collaborate in environments where they are deployed together.

Customer Use Case

Juniper Sky ATP is an advanced malware detection solution deployed in the cloud that detects sophisticated zero-day and unknown threats. Using state-of-the-art machine learning, Juniper Sky ATP continuously analyzes web and email files for evasive malware. Juniper Sky ATP integrates with SRX Series next-generation firewalls to deliver deep inspection, inline blocking, and actionable alerts.

By extending Sky ATP to also integrate with ForeScout CounterACT’s agentless network security, you can automate control and protection of potentially malicious endpoints at the network layer, even in 3rd-party or heterogeneous network environments, and prevent the lateral spread of malware and zero-day threats.

Summary of advantages

- Ensure automated protection against malicious endpoints at both the perimeter and network level
- Agentless integration requires no additional software installation to ensure enforcement and control of endpoints on the network

Technical Overview

By integrating Juniper Sky ATP and ForeScout CounterACT, automated protection against malware and zero-day threats becomes a reality. As highlighted in Figure 1, once an indicator of compromise (IOC) or threat is detected, Sky ATP informs CounterACT via the SRX device about the endpoint. CounterACT can then take the necessary action on the endpoint. With its ability to interface with any switches and wireless controllers, combined with the ability to take a variety of actions on the endpoint, ForeScout CounterACT offers the ability to limit malware propagation and minimize data breaches.
Integrating ForeScout CounterACT® and Juniper Sky ATP

Figure 1: Juniper Sky ATP and ForeScout CounterACT integrated threat mitigation workflow

Once CounterACT discovers a security problem on an endpoint, its sophisticated policy manager can automatically execute a range of responses, depending on the severity of the problem. Minor violations might result in a warning message sent to the end user; employees and contractors who bring their own devices can be redirected to an automated onboarding portal; serious violations could result in actions such as blocking or quarantining the device, reinstallation of a security agent, re-starting of an agent or process, triggering the endpoint to fetch an operating system patch, or other remediation actions based on the policies defined for CounterACT.

Configuration Example

Introduction
This configuration example illustrates how to configure and integrate ForeScout CounterACT to Juniper Sky ATP via an SRX Services Gateway.

Requirements
- ForeScout CounterACT hardware appliance or virtual appliance running version 7.0 or later
- Juniper SRX device running Junos OS Release 15.1X49-D70 or later
- Juniper SRX and Sky ATP installed and configured (refer to steps 19 and 20 for installation and configuration links)

Topology
Figure 2 shows the lab topology used for this configuration example.
Configuration
This configuration example provides step-by-step instructions to configure the ForeScout CounterACT instance:

1. In the CounterACT GUI, open the Options tab and select Advanced Tools Plugin to verify that it has been installed.
If not, install the Advanced Tools Plugin. This (free) base plugin and can be downloaded from the ForeScout website at https://pact.ly/S1lnt3.

2. Launch a terminal or SSH connection to CounterACT, and navigate to the following directory:

/usr/local/forescout/plugin/syslog

3. Edit the install.properties file and add the following configuration:

```
#Juniper SkyATP Infected Host Syslog
template.infected_host.type = juniper_skyatp
template.infected_host.regexp = .*?\(HOST\_INFECTED\).*?ip=(\b\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}\b).?threat-level=([7|8|9]|1[0])
template.infected_host.properties = $goodies_label_list,$ip
#Juniper SkyATP Malware Event Syslog
template.malware_event.type = juniper_skyatp
```
4. In the same directory, edit the `local.properties` file and add the following configuration:

```properties
#Custom Juniper SkyATP
config.type1.option.juniper_skyatp= Juniper SkyATP
config.type2.option.juniper_skyatp= Juniper SkyATP
config.type3.option.juniper_skyatp= Juniper SkyATP

#Juniper SkyATP Infected Host Syslog
template.infected_host.type = juniper_skyatp
template.infected_host.regexp = .*?(HOST_INFECTED).*?ip=(\b\d{1,3}\.|\d{1,3}\.|\d{1,3}\.|\d{1,3}\b).?threat-level=([7|8|9]|1\[0])
template.infected_host.properties = $goodies_label_list,$ip

#Juniper SkyATP Malware Event Syslog
template.malware_event.type = juniper_skyatp
template.malware_event.regexp = .*?(MALWARE_EVENT).*?ip=(\b\d{1,3}\.|\d{1,3}\.|\d{1,3}\.|\d{1,3}\b).*?mw-score=([7|8|9]|1\[0])
template.malware_event.properties = $goodies_label_list,$ip
```

5. Return to the CounterACT GUI, navigate to the Plugins section and select `Syslog`.

6. On the **Send Events To** tab, configure a local server with IP address 127.0.0.1 as follows:
7. On the Default Action Configuration tab, configure similar settings, as follows:

8. Right-click on Syslog and select Start Plugin.

9. Close the Options tab in the CounterACT GUI.
10. From the console or SSH session, restart the plugin by entering the following command:

   `fstool syslog restart`

   **Note:** Starting the syslog plugin above instantiates the process; restarting the plugin here activates the configuration settings.

11. In the CounterACT GUI, re-open the **Options** tab and navigate to **Plugins > Syslog**.

12. Click on the **Receive From** tab. Juniper Sky ATP should now appear as a source type in the drop-down list. Select **Juniper SkyATP** as the syslog source and enter the IP address of the SRX device.

13. In the CounterACT GUI, navigate to the **Policy** section. Create a new policy for Sky ATP. It will appear as shown below.
14. The configuration details about the Infected Host policy can be seen by clicking on the section as highlighted below.

**Note:** In an actual deployment, you also have the option of automated blocking of the endpoint with a Switch Block if desired.

15. Click **OK**.
16. Click on **Juniper SkyATP-2** to look at the configuration details of **Juniper SkyATP Malware Event**. **Note:** In an actual deployment, you also have the option of automated blocking of the endpoint with a Switch Block if desired.


17. Click **OK**. Then close the **Options** tab.

18. In the CounterACT GUI, navigate to the **Action** section and select **HTTP Notification**. On the **Message** tab, enter an appropriate message and click **OK**.
19. Install and configure Sky ATP and the SRX device using the following links:
   - Installing Sky ATP
   - Configuring Sky ATP and SRX (see next step for more detail on SRX configuration)

20. On the SRX device, be sure to perform the following steps:
   - Configure a profile to identify **compromised hosts**, and/or **outbound requests to C&C servers**
   - Configure a **security intelligence policy** to enable the profiles
   - Configure an **anti-malware** policy
   - Configure a **firewall policy** to include the security intelligence policies

Use the links as needed for more information. The resulting configuration should look similar to the example shown below.

```plaintext
root@tme-srx340-05> show configuration services security-intelligence
profile threat-prevention-basic-Infected-Hosts {
  category Infected-Hosts;
  rule Rule-1 {
    match {
      threat-level [ 1 2 3 4 5 6 ];
    }
    then {
      action {
        permit;
      }
    }
```
 Integrating ForeScout CounterACT® and Juniper Sky ATP

```plaintext
log;
}
}
rule Rule-2 {
  match {
    threat-level [ 7 8 9 10 ];
  }
  then {
    action {
      block {
        drop;
      }
      log;
    }
  }
}
policy threat-prevention-basic {
  Infected-Hosts {
    threat-prevention-basic-Infected-Hosts;
  }
}
root@tme-srx340-05> show configuration services advanced-anti-malware
connection {
  url https://srxapi.us-west-2.sky.junipersecurity.net;
  authentication {
    tls-profile aamw-ssl;
  }
}
policy threat-prevention-basic {
  http {
    inspection-profile default_profile;
    action block;
    notification {
      log;
    }
  }
  verdict-threshold 6;
  fallback-options {
    action permit;
    notification {
      log;
    }
  }
  default-notification {
    log;
  }
  whitelist-notification {
    log;
  }
  blacklist-notification {
    log;
  }
}
root@tme-srx340-05> show configuration security policies
from-zone Corp to-zone Untrust {
  policy CorpOutbound {
    match {
      source-address any;
      destination-address any;
      application any;
    }
    then {
      permit {
        log;
      }
    }
  }
```
21. To verify basic communication between the SRX device and Sky ATP, enter the following command:

```
root@tme-srx340-05> show services advanced-anti-malware status
Server connection status:
  Server hostname: srxapi.us-west-2.sky.junipersecurity.net
  Server port: 443
  Control Plane:
    Connection time: 2017-09-26 05:01:15 UTC
    Connection status: Connected
  Service Plane:
    master
    Connection active number: 1
    Connection retry statistics: 18
```
Verification
To validate that CounterACT is blocking access to infected endpoints:

1. Login to one of the endpoints (behind the EX switch). In this example the host uses IP address 192.168.3.107.

2. Attempt to download a malware test file. A common file can be found at [http://www.eicar.org/86-0-Intended-use.html](http://www.eicar.org/86-0-Intended-use.html) (review the information on the page, and then click on the DOWNLOAD link at upper-left).

3. The endpoint is redirected to a Web page that shows the notification configured earlier.

4. CounterACT should receive a notification from the SRX device that the endpoint is attempting to download a malicious file. In the CounterACT GUI, navigate to the Policy section and click on SkyATP. In this section, select either Juniper SkyATP Infected Host or Juniper SkyATP Malware Event.

5. Click on 192.168.3.107. On the Profile tab of the Host Details page, the Assigned Label field is populated with entries related to the event.
6. The **Policy Actions** tab provides further detail on the events and actions taken by CounterACT.
7. In the Sky ATP portal, you can validate that the malware test file was seen and categorized by Sky ATP. Navigate to File Scanning > HTTP File Download to see the offending file listed in the output.

8. Click the file signature of the offending file to view more detailed information.
## Integrating ForeScout CounterACT® and Juniper Sky ATP

### File Details

<table>
<thead>
<tr>
<th>Status</th>
<th>File Name</th>
<th>Category</th>
<th>File Hashes</th>
<th>Other Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat Level</td>
<td>c4431b9435f257a598...</td>
<td>Executable (exe)</td>
<td>c4431b9435f257a598...</td>
<td>md5: 719d044f1d057a49698d142c2be5c930a0408e8</td>
</tr>
<tr>
<td>Global Prevalence</td>
<td>Low</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Last Scanned</td>
<td>2017-05-24 5:48 PM</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>