Distributed IPS Integration with Extreme Networks Network Access Control (NAC)

Bill Banks
SE – North Florida
December, 2018

Abstract

Extreme Networks provides software-driven networking solutions for Enterprise and Service Provider customers. Providing a combined end-to-end solution from the Data Center to the Access Point, Extreme Networks designs, develops, and manufactures wired and wireless network infrastructure equipment and develops the software for network management, policy, analytics, security and access controls. In 2017, Extreme Networks acquired Enterasys Networks that included their Network Access Control software.

The Extreme Networks ExtremeControl NAC solution is business-oriented visibility and control over individual users and applications in multi-vendor infrastructures. NAC protects existing infrastructure investments since it does not require the deployment of new switching hardware or that agents be installed on all end systems. Extreme Networks NAC performs multi-user, multi-method authentication, vulnerability assessment and assisted remediation.

ExtremeControl can integrate with Check Point Threat Protection to accept threat intelligence and use that intelligence to enforce NAC policy changes to endpoints. Check Point forwards the threat logs to the Extreme Networks ExtremeControl solution, which then can quarantine devices that have been flagged by the Check Point Threat Policy.

This integration works with Check Point Log Exporter built into R80.20. The Log Exporter package for R77.30 and R80.10 can be found at SK122323. This document assumes you are using R80.20 or have installed Log Exporter.

Check Point Configuration

1. Configure Log Exporter to send the logs to the ExtremeControl server.

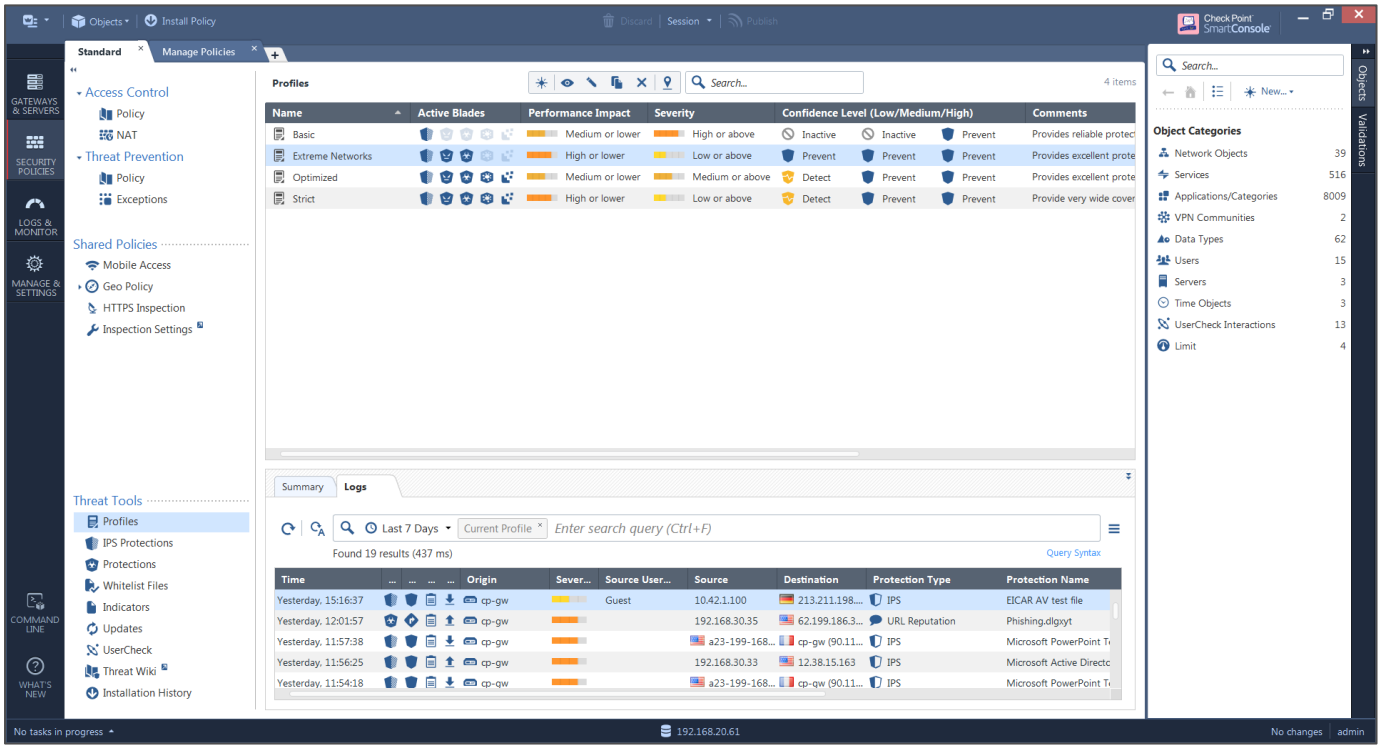
```
#cp_log_export add name Extreme target-server “xmc ip address” target-port 514
protocol udp format generic
```

2. Edit the log exporter configuration file.

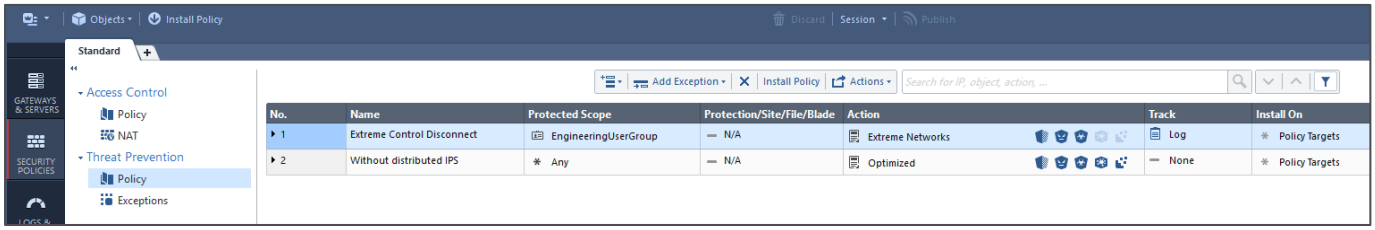
```
#cd /opt/CPrt-R80/log_exporter/targets/Extreme(name of the export Name)/
#vi targetConfiguration.xml
```

```
<is_enabled>true</is_enabled><!--Is the process allowed to run, and start on cpstart--
>
  <!-- Destination section defines the properties of the export target -->
  <destination type="syslog"> <!-- Target output type -->
    <ip>X.X.X.X</ip><!--the ip of the syslog server-->
    <port>514</port><!--the port on which the syslog is listening to-->
<filter filter_out_by_connection="true">
              <field  name="product">
```

3. Log into SmartConsole and clone threat profile with the desired protections enabled. Below is a cloned strict profile named ‘Extreme Networks’.



4. Create a threat rule that is applied to the scope of the devices you want ExtremeControl to use Check Point threat intelligence for NAC policy. You can use the name of the rule in Extreme Connect match conditions = Services. The Track must be set to Log to generate the syslog message.

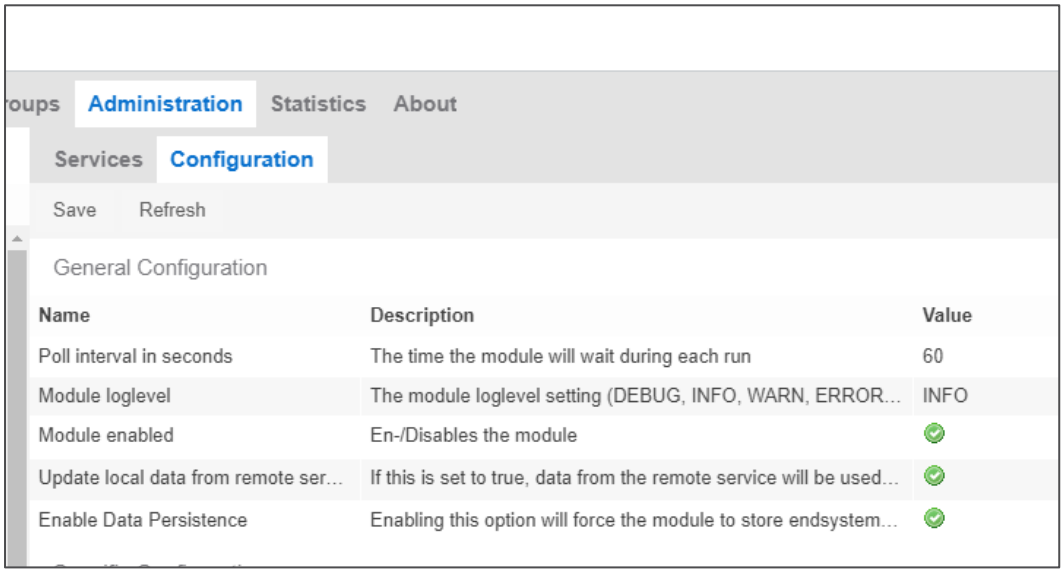


Extreme Networks Configuration

1. Log into ExtremeControl dashboard and access the 'Administration tab'. Check Point Log Exporter will inform the Extreme Connect by syslog messages.

2. Edit regex key value to reflect the threat policy name we created in the Check Point SmartConsole threat policy. The policy we created was called 'Extreme Control Disconnect'. This interoperability will only work if the threat policy name matches the regex key value.

3. Click the 'Configuration' tab and set the module to active to enable the protections.



Reference:

Pala, Z. (2018, August). extremenetworks/Integrations. Retrieved from https://github.com/extremenetworks/Integrations/blob/master/CheckPoint/dips/README.md

