Overview of the Tenable Network Monitor

The Tenable Network Monitor (TNM), a client used by Tenable's Log Correlation Engine (LCE), is a tool used to receive all traffic from a main switch or router to monitor inbound and outbound sessions. The TNM can report UDP, TCP (where it also tracks the session size), ICMP, and IGMP traffic. This information feeds LCE's TASLs, particularly the threatlist TASL that monitors for connections to botnets and other IP addresses that are known to be suspect. The IP address threatlist is updated daily to keep up with emerging threats. More details about how TNM uses the threatlist are described in this Discussions Forum post:

https://discussions.nessus.org/message/19302#19302

TNM logs can also be used to report traffic anomalies and long TCP sessions. TNM events feed other alerts as well, such as crowd surge, which is described in the following Discussions Forum post:

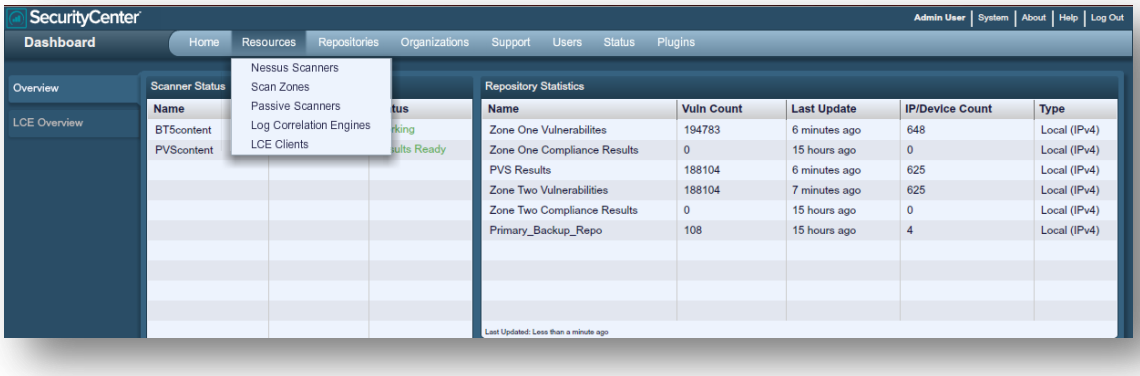
https://discussions.nessus.org/message/21035#21035

One particularly useful feature of TNM is that it can be used to monitor syslog traffic. While many systems have the capability to forward syslog data, what if you have to cross a DMZ to get back to LCE? You certainly don't want sensitive log data to be subject to sniffing in the DMZ. The TNM can be set up on the syslog server to monitor some or all of the syslog traffic and send that information to the LCE server over an encrypted connection.

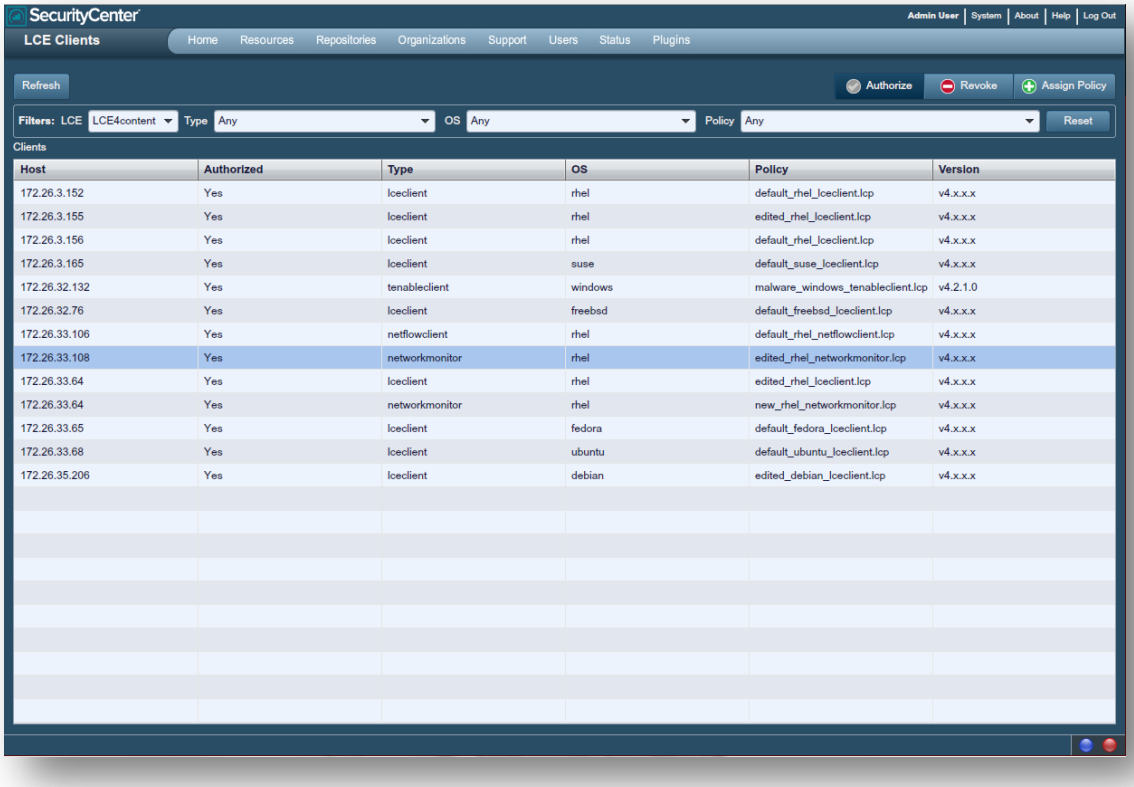
Configuring Tenable Network Monitor to Gather Syslog

To gather syslog traffic using the Tenable Network Monitor, you will need to edit a copy of the default policy. To obtain a copy of the default policy to edit, use the following steps.

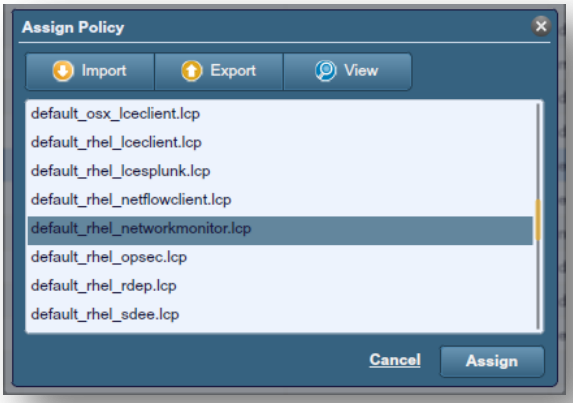
First, log into SecurityCenter as an admin user, and navigate to the "LCE Client" section.



Next, select the host that has the Tenable Network Monitor client installed, and choose “Assign Policy”:



Once the “Assign Policy” window opens, scroll down until the “default_rhel_networkmonitor.lcp” file is found. Select the “default_rhel_networkmonitor.lcp” file and choose “Export”. Save the file, and then open it in a text editor.



The default policy downloaded will be similar to the one shown below:

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<options xmlns:xi="http://www.w3.org/2003/XInclude">
```

```
<!-- Network Monitor log messages are stored in files named according to the date
    in the following directory. -->
<log-directory>./</log-directory>

<!-- The Network Monitor automatically generates a tcpdump filter expression that
   selects
    which network packets will be processed. This expression is based on the
   syslog
    monitoring settings below. The following option allows the default filter to
   be
    overridden with a custom expression.  -->
<!-- filter-expression>tcp or icmp or udp port 514</filter-expression -->

<!-- The network monitor will report traffic from only the interfaces listed
   below. -->
<!-- interface>eth0</interface -->
<interface>eth0</interface>

<!-- Traffic containing syslog messages is forwarded to the LCE server for the
   hosts
    matching the filtering criteria in the final section. The following specifies
   the
    protocol/port pairs for which all traffic will be processed as syslog
   messages.
    These settings should match the syslog or syslog-ng configuration.  -->
<monitor-syslog-port>udp/514</monitor-syslog-port>
<monitor-syslog-port>tcp/1468</monitor-syslog-port>

<!-- When the below option is set to yes, only syslog messages are reported, and
   all
    all other traffic is ignored.  -->
<syslog-only>no</syslog-only>

<!-- The following section defines the networks on which syslog will be monitored.
     The network monitor will report syslog messages received at the above
   specified
     ports for any IP address matching the filter criteria. -->
<include-networks>
    <filter>192.168.20.5/32</filter>
    <filter>127.0.0.1</filter>
</include-networks>
<exclude-networks>
</exclude-networks>

<!-- The heartbeat-frequency option defines the number of seconds between each
   pair
    of client heartbeat messages that are sent to the server. -->
<heartbeat-frequency>300</heartbeat-frequency>

<!-- The LCE client provides the option of periodically sending a log file
   containing
    performance statistics to the LCE server. The following option determines the
    number of minutes between each performance statistics report. When the next
   line
    is commented out or removed, performance reporting is disabled. -->
<statistics-frequency>60</statistics-frequency>
```

```
    <!-- LCE clients can compress log data prior to sending it to the LCE server,
       saving bandwidth.
         For debugging purposes, event packet compression may be disabled, but this
       will
        increase the bandwidth required to send data from LCE clients to the LCE
       server.
        Setting the following option to 0 will disable compression only during
       transmission. -->
    <compress-events>1</compress-events>

</options>
```

To configure the Tenable Network Monitor to only monitor syslog traffic, first make sure that the port and protocol are specified in the "**monitor-syslog-port**" tag. The example below is used to monitor syslog traffic on UDP port 514:

```
<monitor-syslog-port>udp/514</monitor-syslog-port>
```

A network to monitor also needs to be specified. An example of the "**include-networks**" section is shown below:

```
<include-networks>
<filter>192.168.0.0/22</filter>
<filter>127.0.0.1</filter>
</include-networks>
```

Finally, to monitor only syslog with the Tenable Network Monitor, the following tag needs to be set to "yes", as shown in the example below:

```
<syslog-only>yes</syslog-only>
```

If the interface is different than the default (eth0), it will also need to be changed to the appropriate network interface. In this example, the interface used is eth1, as shown below:

```
<interface>eth1</interface>
```

The complete edited policy is shown below:

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<options xmlns:xi="http://www.w3.org/2003/XInclude">

<!-- Network Monitor log messages are stored in files named according to the date
        in the following directory. -->
<log-directory>./</log-directory>

<!-- The Network Monitor automatically generates a tcpdump filter expression that
       selects
        which network packets will be processed. This expression is based on the
       syslog
        monitoring settings below. The following option allows the default filter to
       be
        overridden with a custom expression.  -->
```

```
<!-- filter-expression>tcp or icmp or udp port 514</filter-expression -->

<!-- The network monitor will report traffic from only the interfaces listed below. --
      >
<!-- interface>eth0</interface -->
<interface>eth1</interface>

<!-- Traffic containing syslog messages is forwarded to the LCE server for the hosts
       matching the filtering criteria in the final section. The following specifies
      the
       protocol/port pairs for which all traffic will be processed as syslog
      messages.
       These settings should match the syslog or syslog-ng configuration.  -->
<monitor-syslog-port>udp/514</monitor-syslog-port>
<monitor-syslog-port>tcp/1468</monitor-syslog-port>

<!-- When the below option is set to yes, only syslog messages are reported, and all
       all other traffic is ignored.  -->
<syslog-only>yes</syslog-only>

<!-- The following section defines the networks on which syslog will be monitored.
The network monitor will report syslog messages received at the above specified
ports for any IP address matching the filter criteria. -->
<include-networks>
<filter>172.26.0.0/22</filter>
<filter>127.0.0.1</filter>
</include-networks>
<exclude-networks>
</exclude-networks>

<!-- The heartbeat-frequency option defines the number of seconds between each pair
       of client heartbeat messages that are sent to the server. -->
<heartbeat-frequency>300</heartbeat-frequency>

<!-- The LCE client provides the option of periodically sending a log file containing
       performance statistics to the LCE server. The following option determines the
       number of minutes between each performance statistics report. When the next
      line
       is commented out or removed, performance reporting is disabled. -->
<statistics-frequency>60</statistics-frequency>

<!-- LCE clients can compress log data prior to sending it to the LCE server, saving
      bandwidth.
For debugging purposes, event packet compression may be disabled, but this will
       increase the bandwidth required to send data from LCE clients to the LCE
      server.
       Setting the following option to 0 will disable compression only during
      transmission. -->
<compress-events>1</compress-events>

</options>
```

Configuring Tenable Network Monitor to Gather Additional Data

To gather syslog data and additional network traffic data set the “syslog-only”” option to “no” as shown below:

```
<syslog-only>no</syslog-only>
```

Next, uncomment the “filter expression” section (which is commented out by default). An example of the default commented line is shown below followed by the uncommented line with the appropriate filter to gather the most data:

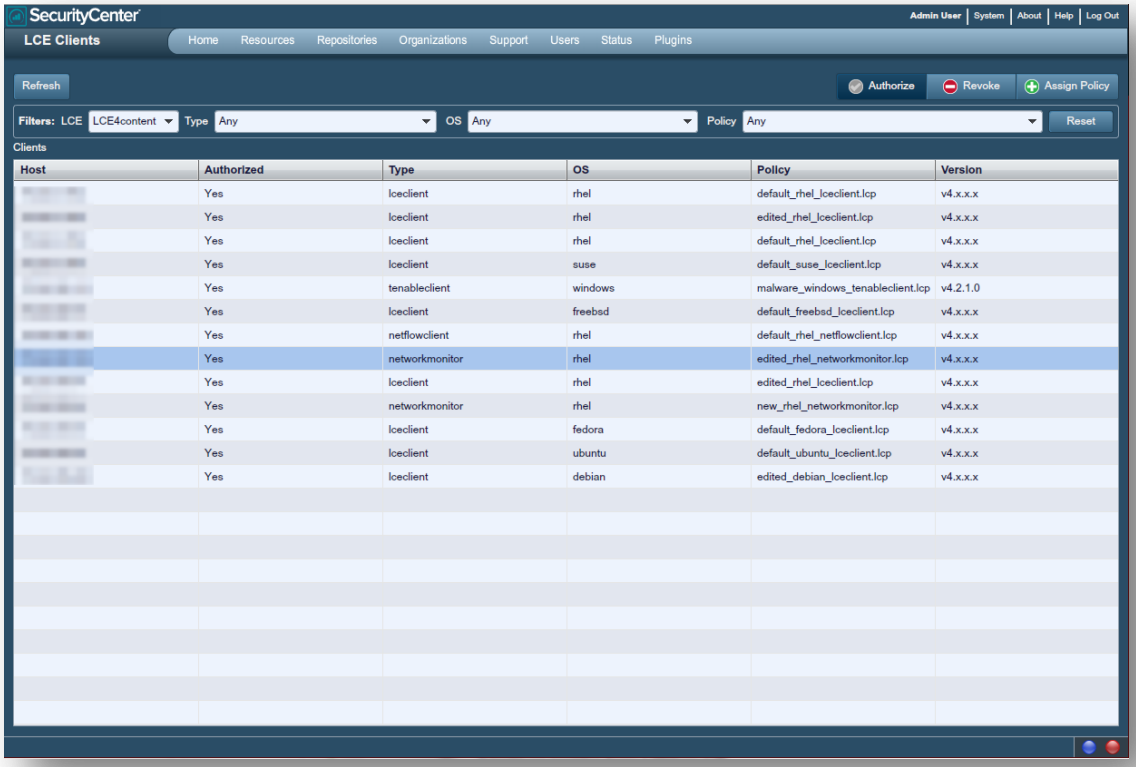
```
<!-- filter-expression>tcp or icmp or udp port 514</filter-expression -->

<filter-expression>udp or tcp or icmp or igmp</filter-expression>
```

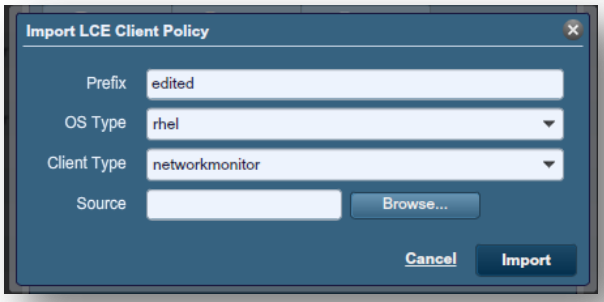
Configuring the client in this way allows the most information to be forwarded to the Log Correlation Engine server. A sample of events is shown below:

Importing the Edited Policy

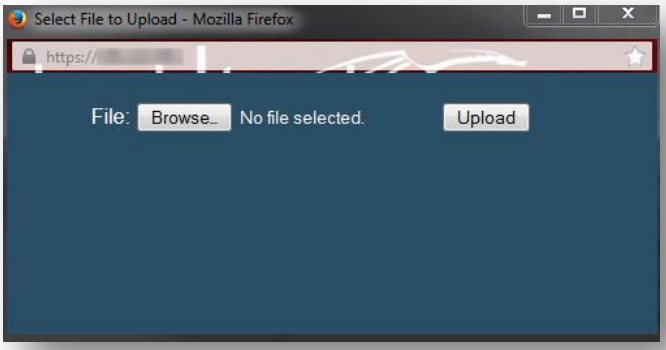
After the policy has been modified, you will need to import the new policy. To do this, select the "**networkmonitor**" client from the list of clients, and choose "**Assign Policy**" from the "**LCE Clients**" menu.



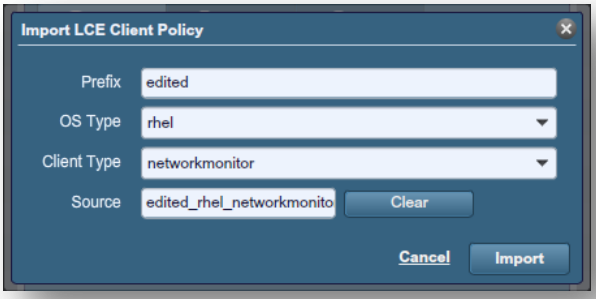
The "**Import LCE Client Policy**" menu will be displayed. Select "**Browse**" to start the policy upload process.



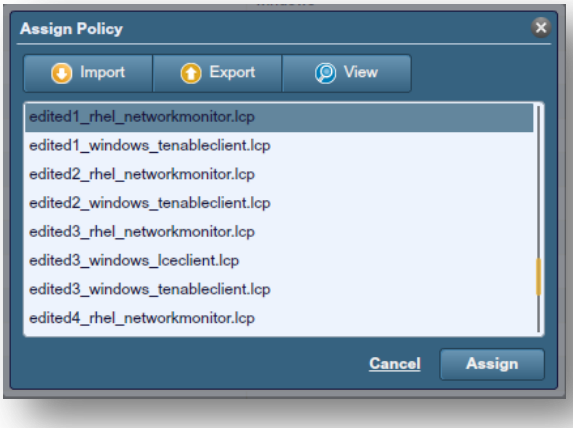
The next menu for file upload will be displayed. Select "**Browse**" to locate the policy file, and after the file has been chosen, select "**Upload**".



Finally, select "**Import**" to complete the policy upload.



Choose the policy from the "**Assign Policy**" menu, and select "**Assign**".



The new policy will now be in effect on the chosen Tenable Network Monitor client.

For More Information

Tenable has produced a variety of additional documents detailing the LCE's deployment, configuration, user operation, and overall testing. These documents are listed here:

- Log Correlation Engine Architecture Guide – provides a high-level view of LCE architecture and supported platforms/environments.
- Log Correlation Engine Administrator and User Guide – describes installation, configuration, and operation of the LCE.
- Log Correlation Engine Quick Start Guide – provides basic instructions to quickly install and configure an LCE server. A more detailed description of configuration and management of an LCE server is provided in the "LCE Administration and User Guide" document.
- Log Correlation Engine Client Guide – how to configure, operate, and manage the various Linux, Unix, Windows, NetFlow, OPSEC, and other clients.
- LCE High Availability Large Scale Deployment Guide – details various configuration methods, architecture examples, and hardware specifications for performance and high availability of large scale deployments of Tenable's Log Correlation Engine (LCE).
- LCE Best Practices – Learn how to best leverage the Log Correlation Engine in your enterprise.
- Tenable Event Correlation – outlines various methods of event correlation provided by Tenable products and describes the type of information leveraged by the correlation, and how this can be used to monitor security and compliance on enterprise networks.
- Tenable Products Plugin Families – provides a description and summary of the plugin families for Nessus, Log Correlation Engine, and the Passive Vulnerability Scanner.
- Log Correlation Engine Log Normalization Guide – explanation of the LCE's log parsing syntax with extensive examples of log parsing and manipulating the LCE's `.prm` libraries.
- TASL Reference Guide – explanation of the Tenable Application Scripting Language with extensive examples of a variety of correlation rules.
- Log Correlation Engine Statistics Daemon Guide – configuration, operation, and theory of the LCE's statistic daemon used to discover behavioral anomalies.
- Log Correlation Engine Large Disk Array Install Guide – configuration, operation, and theory for using the LCE in large disk array environments.
- Example Custom LCE Log Parsing - Minecraft Server Logs – describes how to create a custom log parser using Minecraft as an example.

Documentation is also available for Nessus, the Passive Vulnerability Scanner, and SecurityCenter through the Tenable Support Portal located at https://support.tenable.com/.

There are also some relevant postings at Tenable's blog located at http://www.tenable.com/blog and at the Tenable Discussion Forums located at https://discussions.nessus.org/community/lce.

For further information, please contact Tenable at support@tenable.com, sales@tenable.com, or visit our web site at http://www.tenable.com/.

About Tenable Network Security

Tenable Network Security is relied upon by more than 20,000 organizations, including the entire U.S. Department of Defense and many of the world's largest companies and governments, to stay ahead of emerging vulnerabilities, threats and compliance-related risks. Its Nessus and SecurityCenter solutions continue to set the standard to identify vulnerabilities, prevent attacks and comply with a multitude of regulatory requirements. For more information, please visit www.tenable.com.

GLOBAL HEADQUARTERS

Tenable Network Security
7021 Columbia Gateway Drive
Suite 500
Columbia, MD 21046
410.872.0555
www.tenable.com