NetFort LANGuardian
Change Log

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Modified By</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>June 2018</td>
<td>Conor Shovlin</td>
<td>Draft TechNote</td>
</tr>
<tr>
<td>1.0</td>
<td>August 2018</td>
<td>Conor Shovlin</td>
<td>First Published Version</td>
</tr>
</tbody>
</table>

Copyright

© Copyright 2018 Hewlett Packard Enterprise Development LP.

Open Source Code

This product includes code licensed under the GNU General Public License, the GNU Lesser General Public License, and/or certain other open source licenses. A complete machine-readable copy of the source code corresponding to such code is available upon request. This offer is valid to anyone in receipt of this information and shall expire three years following the date of the final distribution of this product version by Hewlett-Packard Company. To obtain such source code, send a check or money order in the amount of US $10.00 to:

Hewlett-Packard Company
Attn: General Counsel
3000 Hanover Street
Palo Alto, CA 94304
USA

Please specify the product and version for which you are requesting source code. You may also request a copy of this source code free of charge at HPE-Aruba-gplquery@hpe.com.
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>5</td>
</tr>
<tr>
<td>Software Requirements</td>
<td>6</td>
</tr>
<tr>
<td>ClearPass &amp; Netfort LANGuardian Versions used for Testing</td>
<td>9</td>
</tr>
<tr>
<td>Configuring ClearPass Policy Manager for the Netfort LANGuardian</td>
<td>9</td>
</tr>
<tr>
<td>Appendix A - Netfort XML File</td>
<td>20</td>
</tr>
<tr>
<td>Appendix B - Sample Alert Rule Templates for Netfort LANGuardian</td>
<td>21</td>
</tr>
</tbody>
</table>

© 2017 Hewlett Packard Enterprise Development LP. All Rights Reserved.
Figures

Figure 1: Overview of the CPPM & Netfort LanGuardian Integration ................................................................. 7
Figure 2: ClearPass Access Tracker Example of workflow with a Netfort Detection ........................................... 7
**Figure 3:** Sample ClearPass & Netfort Use Cases ............................................................................................... 8
**Figure 4:** Netfort Syslog Example ……………………………………………………………………………………… 9
Figure 5: Importing the IEE Netfort Dictionary …………………………………………………………………………… 10
Figure 6: Configure an Enforcement profile ……………………………………………………………………………… 10
**Figure 7:** Enforcement Profile ws_update_endpoint_Netfort …………………………………………………………… 11
**Figure 8:** Endpoint Attribute ……………………………………………………………………………………………… 11
**Figure 9:** ClearPass Netfort IEE Policy Summary ……………………………………………………………………….. 12
**Figure 10:** ClearPass example Policy creation based on Unauthorized DNS ..................................................... 12
**Figure 11:** ClearPass 802.1X Authentication Service for Aruba Switch checking Endpoint Compromised Variable. 13
**Figure 12:** ClearPass 802.1X Authentication Service for Aruba WLAN checking Endpoint Compromised Variable. 13
Introduction

This TechNote covers the setup/configuration and monitoring of the Ingress Event Engine [IEE] to NetFort LANGuardian.

The IEE delivers a new dimension to the capabilities on how ClearPass can interoperate with Devices and Users. Prior to this feature two types of events were able to trigger CPPM in to taking actions, the first was a typical WEB/802.1X network authentication, the second was the ability for a 3rd party system to utilize our exposed XMLAPI or RESTful API's.

In adding IEE, we have provided a 3rd dimension where an inbound syslog can be the trigger for CPPM to take action on the authenticated networks devices & users

NetFort LANGuardian Overview

NetFort LANGuardian is the industry’s leading deep packet inspection software for investigating, monitoring, and reporting on network and user activity. It is a passive network traffic analyzer, not inline, so it doesn’t impact on network performance. It can be downloaded and deployed on standard physical or virtual hardware, configured, connected to a SPAN or mirror port and monitoring activity at any location in minutes. Because it gathers information from raw network traffic, it is vendor agnostic and can be deployed at any location across the network. It does not require any agents, clients, logs or NetFlow.

Every device, user and application on the network leaves a traffic trail. LANGuardian continuously analyses this trail extracting rich metadata. This application specific network metadata is enriched with user names. The end result is granular detail and context retained for long periods. LANGuardian’ s real time and historical metadata is ideal for multiple security and operational use cases helping users to:

- Find out what users are doing internally
- Monitor Internet activity, proxy or non-proxy
- Troubleshoot bandwidth issues
- Find out who accessed, a file or folder on a Windows or UNIX network share
- Detect and alert on use of vulnerable protocols such as SMBv1
- Create a dashboard to track and alert on Ransomware attacks
- Alert on weak SSL/TLS encryption protocols and cipher sessions
- Create a continuous inventory of devices, users and applications
- Receive an immediate security alert on suspicious activity on the network
- Perform forensics to diagnose recent network issues
- Monitor MS SQL activity including all queries
- Define very specific alerts conditions on user or network activity
Software Requirements

ClearPass Software Version

At the time of writing, 6.7.5 version is the recommended software release. The TechNote also covers installation steps and screenshots from a ClearPass server running 6.6.10. CPPM runs on hardware appliances with pre-installed software or as a Virtual Machine under the following hypervisors. Hypervisors that run on a client computer such as VMware Player are not supported.

- VMware ESXi 5.5, 6.0, 6.5 or higher
- Microsoft Hyper-V Server 2012 R2 or 2016 R2
- Hyper-V on Microsoft Windows Server 2012 R2 or 2016 R2
- KVM on CentOS 6.6, 6.7, or 6.8 (Soon to be released for ClearPass 6.7)

Netfort LANGuardian Software Version

- LANGuardian Version 14.4.1 or higher

ClearPass Ingress Event Engine

Starting within the ClearPass 6.6 release we added a new feature to the ClearPass Exchange Framework called Ingress Event Engine (IEE) specific to our ability to consume inbound messages, parse them and trigger an action in the sense of an enforcement update for the user/endpoint. An example of this, could be we receive an update regarding the posture/health of the endpoint so we want to react by triggering an enforcement update for the device/user’s role/vlan/dACL or/and we might want to trigger an update to a data-center or internet access firewall based upon this new posture/health context we have just received.

Providing this new feature allows for event driven real-time enforcement to happen within the enterprise network and enables a more effective framework of protection.

The ClearPass IEE installation and deployment guide is located here:


Leveraging the IEE feature Aruba and Netfort have created a custom XML (see appendix A) that enables users of Netfort LANGuardian and Aruba ClearPass to invoke Network Access Control policy on client Endpoint subject to network monitoring rules created on Netfort LANGuardian
Figure 1: Overview of the CPPM & Netfort LanGuardian Integration

![Diagram of CPPM & Netfort LanGuardian Integration]

Steps:
1. Client Connects to the Network
2. ClearPass provides Access Control
3. Netfort sees an anomaly on the client Device
4. Netfort sends an IE Event to ClearPass
5. ClearPass updates Endpoint DB & initiates a CoA
6. Client re-Connects to the network on a Quarantined Network

Where:
- **employee** is the 802.1X User connected to the network.
- **ws_ArubaSwitch_802.1X** is the 802.1X Authentication Service on ClearPass on the Network
- **ws_IEE_Netfort** is ClearPass Service that manages the Inbound Event based on activity detected by Netfort LANGuardian

The following Use Cases have been identified as rules that Netfort LANGuardian admins can configure to invoke Network Policy on Client Devices use Aruba ClearPass
Figure 3: Sample ClearPass & Netfort Use Cases

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Clients scanning externally</td>
<td>Alert if an internal client is netscanning or port scanning IP addresses or ranges that are outside of the local network (or possibly sections of the internal network). Use this to identify if attacks or reconnaissance on 3rd party network originates from your managed network.</td>
</tr>
<tr>
<td>2</td>
<td>Use of weak SSL/TLS protocols and ciphers</td>
<td>Alert if versions of SSL/TLS older that TLS1.2 (actual version is configurable) are detected in use on the network. This is useful for ensuring PCI and GDPR compliance and good network hygiene. Also, can detect if older encryption algorithms are use (RC4/3DES etc.).</td>
</tr>
<tr>
<td>3</td>
<td>Use of SMBv1 protocol</td>
<td>Detect clients and servers using SMBv1 protocol. This filesharing protocol is obsolete and vulnerable to many attacks that have resulted in ransomware and Bitcoin Miners etc. Alert on connection attempts and connections established.</td>
</tr>
<tr>
<td>4</td>
<td>Clients using unauthorized DNS servers</td>
<td>Alert if a client on the network attempts to use a DNS server that is not on the approved list of DNS servers (configurable). Can indicate potential DNS settings hijack by malware</td>
</tr>
<tr>
<td>5</td>
<td>Inter subnet communication and applications</td>
<td>Monitor and alert on any inter subnet connection attempts, connection establishment or protocols that do not match a defined whitelist. In controlled production environments, the number of allowed protocols is typically very few and any changes or new protocols being used require immediate investigation</td>
</tr>
<tr>
<td>6</td>
<td>Ransomware detection from client behavior</td>
<td>Alert if any single client generates an excessive number of file rename or file write actions in a short period of time. While some ransomware variants can evade endpoint detection systems, the client actions on network shares cannot be hidden.</td>
</tr>
<tr>
<td>7</td>
<td>A VPN client attempting to access a specific file or folder</td>
<td>An external user using a VPN client to access data while working from home.</td>
</tr>
<tr>
<td>8</td>
<td>New Email server or any SMTP traffic from user machines</td>
<td>A new email server appearing on the network and sending email.</td>
</tr>
<tr>
<td>9</td>
<td>Specific email attachments</td>
<td>A SMTP email with an attachment containing a specific string.</td>
</tr>
<tr>
<td>10</td>
<td>Unusual file share activity</td>
<td>Large volumes of file copies or deletes over a short period.</td>
</tr>
</tbody>
</table>
ClearPass & Netfort LANGuardian Versions used for Testing

The following example is based on the following testing conditions:

- ClearPass Policy Manager – version 6.6.10
- Aruba 325 IAP – version 6.5.4
- Aruba 7005 Controller – version 8.2 (standalone)
- Aruba 2930F Switch – version 16.05
- Netfort LANGuardian – version 14.4.1

Configuring ClearPass Policy Manager for the Netfort LANGuardian

To configure the ClearPass Netfort LANGuardian you must complete the following steps:

1. Import the Netfort ClearPass IEE Dictionary
2. Enable the IEE Services on ClearPass
3. Configure a Netfort Enforcement Profile to Update the Endpoint DB
4. Configure a Netfort IEE Event Policy
5. Update\Create Standard Network Authentication Server to check for Netfort Endpoint Attributes

Introduction

To understand the ClearPass IEE process we need to understand the syslog that is being generated by Netfort.

**Figure 4: Netfort Syslog Example**

```
<69>Mar 20 13:04:54 languardian27.netfort.com NetFort LANGuardian 14.4.0.91: sen_id=1 app_id=21 sid=1 app=usdev name='User Defined' src_ip=10.31.1.100 dest_ip=10.2.100.216 src_mac=58:ef:68:e4:dd:b7 rule_name='Ransomware'
```

The key Element of the Syslog that allows ClearPass to control policy on the network is ‘rule_name’ in the example above this is ‘Ransomware’

As we build the ClearPass Service the Rule Name is the variable that allow us to build policy but also create different levels of network access policy based on the use cases available between ClearPass and Netfort LanGuardian

**Step 1.1: Import the Netfort Network IEE Dictionary**

First Step is to import the Netfort XML. Please see Appendix A & XML on [http://support.arubanetworks.com](http://support.arubanetworks.com)
Step 1.2: Enable the IEE Services on ClearPass

To enable the IEE Services on ClearPass please follow the CPPM TechNote - Ingress Event Engine V1.0


Step 1.3: Configure a Netfort Enforcement Profile to Update the Endpoint DB in ClearPass

Create a ClearPass Entity Update Enforcement Profile which will allow us to create & send a custom Attributes to the Endpoint DB.

Figure 6: Configure an Enforcement profile
Multiple or different attributes can be set here by the ClearPass admin. In the case of our Netfort example of Ransomware we are setting the Endpoint Compromised Attribute as True.

**Figure 7:** Enforcement Profile *ws_update_endpoint_Netfort*

![Enforcement Profiles - ws_update_endpoint_NetFort](image)

**Figure 8:** Endpoint Attribute

![Enforcement Profiles - ws_update_endpoint_NetFort](image)

**Step 1.4: Configure a Netfort IEE Event Policy**

We then create an Enforcement Event Policy based on the Netfort Event.

![Enforcement Policies](image)

In our example we are creating a rule based on the Event-Name (rule_name) as passed by the Netfort Syslog
Different Rules can be added depending on how the ClearPass admin would like to define policy.

Once the Policy has been determined apply an Enforcement Profile created in Step 1. In the case of the Ransomware example we set the Endpoint Compromised Attribute as True.

As well as creating an Endpoint Update on the Enforcement Profile we also add two additional actions on the Enforcement Profile to initiate an CoA on the client device

**[Aruba Terminate Session]** - Initiates a CoA on Aruba WLAN

**[HPE Bounce Host-Port]** - Initiates a CoA on Aruba Switch

In the example of 3rd party NAD you would enable ClearPass to do a CoA on these devices using standard CoA configuration
Step 1.5: Update/Create Standard Network Authentication Server to check for Netfort Endpoint Attributes

The final step is to check for the Endpoint Attribute as part of any client Authentication request to the network. This can be based on 802.1X, MAC, OnConnect, etc. on both the Wired or Wireless Services.

In the examples below this is based on an 802.1X authentication using Aruba Wired Switch and Aruba Wireless network.

Vlan & Role assignment is based on the end user credentials and they are assigned access to the network. In this case we check for the Attributes created as part of the Netfort Update and assign the relevant network access, in our example, we are assigning VLAN 34 which is the quarantine VLAN on this network.

**Figure 11:** *ClearPass 802.1X Authentication Service for Aruba Switch checking Endpoint Compromised Variable*

![Figure 11: ClearPass 802.1X Authentication Service for Aruba Switch checking Endpoint Compromised Variable](image1)

**Figure 12:** *ClearPass 802.1X Authentication Service for Aruba WLAN checking Endpoint Compromised Variable*

![Figure 12: ClearPass 802.1X Authentication Service for Aruba WLAN checking Endpoint Compromised Variable](image2)
Configuring Netfort LANGuardian Rules for ClearPass IEE

Netfort LANGuardian monitors user network activity, by analyzing network traffic and recording traffic flows and metadata events into its internal database. To create an integration with CPPM two configuration steps are required

1. Create a rule to identify alert conditions. The inputs to the rule are the metadata events generated by LANGuardian and some policy information from the network Administrator

2. A configuration to export an IEE syslog message to CPPM when an alert rule is triggered.

This section will describe how to perform these two steps using the LANGuardian GUI and a sample alert rule. Appendix B lists additional alert rule templates for a variety of alerting use cases.

Sample use case: Ransomware detection by monitoring client actions

Ransomware malware can be detected by endpoint/antivirus systems or by filtering gateways. However, polymorphic malware, root kits and sandbox detection evasion techniques mean that these methods are not guaranteed to detect all ransomware. An alternative or additional method is to monitor the behavior of client systems and their interaction with fileshares where most valuable data resides. When ransomware is active it encrypts file rapidly, attempting to encode as many files as possible before detection. This typically results in a high rate of file rename actions. LANGuardian's Fileshare monitoring module can detect when file rename actions occur. By applying a rate limit, LANGuardian can detect with a high degree of confidence when a ransomware infected client is encoding files. This allows rapid detection and response.

LANGuardian alert rules are created using the alert rules menu and have the following sample structure

<table>
<thead>
<tr>
<th>Module</th>
<th>Hook</th>
<th>Qualifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FileShare</td>
<td>File Rename</td>
<td>rlim=3/s</td>
<td>Identify when file SMB file rename actions exceed 3 per second.</td>
</tr>
</tbody>
</table>

Module and Hook name identify some meta events that LANGuardian generate from network traffic analysis.

An example module is File Share, any event that relates to activity on an SMB fileshare. The Hooks are the various action that can happen on Fileshares, such as file create, file read etc.

The qualifiers are dependent on the module and hook and generally include src IP, dst IP, protocol and rate limit etc.

For a more complete description of the rules syntax, please see [https://www.netfort.com/help/#custom-rules](https://www.netfort.com/help/#custom-rules)
Steps to add a new alert rule

Step 2.1: Access the Alert Rules configuration menu

Step 2.2: Click on Add New Rule

Step 2.3: Give the new rule a name

In this example we name the rule Ransomware.

Alert Rule name and IEE Policy name

The choice of rule name is arbitrary, but important. The chosen rule name must match exactly the named IEE policy as created in step 1.4 above. See also figures 4 and 6
Step 2.4: Select the module *File Share*
Step 2.5: Select the **Hook Rename File**

![New Rule](image)

- **Name**: Randomware
- **Module**: File Share
- **Hook**: Rename file

**Available variables**:
- **FIELD NAME**: src
- **VARIABLE**: 192.168.127.0/24 or 172.16.17.30

**Step 2.6: Add a rate limit and any other sub conditions for the rule**

![New Rule](image)

- **Name**: Randomware
- **Hook**: Rename file

**Rule**:

\[ \text{src=192.168.127.0/24} \& \text{rlim=3/s burst=10} \]

**Available variables**:

- **FIELD NAME**: src
- **VARIABLE**: 192.168.127.0/24
- **EXAMPLE**: 192.168.127.0/24 or 172.16.17.30

In this example the optional src parameter is included alerts will be generated only if the client renaming files belongs to the subnet 192.168.127.0/24.

The rlim specifies that alerts are generated if files are renamed at a rate higher than 3 files per second and that at least 10 files have to be renamed.
**Step 2.7: Click on Save**

This completes the creation of a new alert rule. The new rule detects clients from a certain subnet that are rapidly renaming files on Windows File Shares. When the rule triggers a new User Defined event will be created in the LANGuardian database. These steps must be repeated for each new rule that is created.

To notify ClearPass that ransomware activity has been detected, the LANGuardian configuration needs to be modified to forward a syslog when a User Defined event is generated.

**Steps to generate a syslog message**

**Step 3.1: Access the Syslog Forwarder configuration menu**

![Syslog Forwarder Configuration](image)

**Step 3.2: Enter the IP address of ClearPass Policy Manager**

![Syslog Forwarder Configuration](image)

**Step 3.3: Enable syslog message from User Defined events**
Step 3.4: Click on Save

This completes the syslog configuration for forwarding User Defined events to the CPPM.

This configuration has only to be completed once.
Appendix A – Netfort XML File

This example XML is available for download from support.arubanetworks.com

Find it here
### Appendix B – Sample Alert Rule Templates for Netfort LANGuardian

#### External Scanning

<table>
<thead>
<tr>
<th>Rule Name</th>
<th>Rule Module</th>
<th>Rule Hook</th>
<th>Rule Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>External Scanning</td>
<td>Port Scan</td>
<td>Port Scan</td>
<td><code>src=10/0 &amp;&amp; dst=!10/8</code></td>
<td>Source is internal, target is external</td>
</tr>
<tr>
<td>Weak Encryption</td>
<td>Cryptographic Protocol</td>
<td>Cipher Established or Exchanged</td>
<td><code>Proto=0x301</code></td>
<td><code>[0x0304, 'TLS v1.3'], [0x0303, 'TLS v1.2'], [0x0302, 'TLS v1.1'], [0x0301, 'TLS v1.0'], [0x0300, 'SSL v3.0'], [0x0002, 'SSL v2.0'], [0x0001, 'SSL v1.0'],</code></td>
</tr>
<tr>
<td>SMBV1</td>
<td>File Share</td>
<td>Read File</td>
<td><code>protover=1</code></td>
<td><code>[1' =&gt; 'SMB1'] [2' =&gt; 'SMB2 / SMB3']</code></td>
</tr>
<tr>
<td>Unauthorized DNS</td>
<td>DNS</td>
<td>DNS A Record Response</td>
<td><code>dst != 8.8.8.8 &amp;&amp; dst != 172.16.2.100</code></td>
<td>Exclude approved DNS servers (8.8.8.8 and 172.16.2.100). All other DNS servers generate alerts</td>
</tr>
<tr>
<td>Ransomware</td>
<td>File Share</td>
<td>rename</td>
<td><code>rlim=&quot;3/s burst 10&quot;</code></td>
<td>3 per second, min 10 events</td>
</tr>
<tr>
<td>VPN Client Folder Access</td>
<td>File Share</td>
<td>File read</td>
<td>src=172.16.100.0/24 &amp;&amp; name =~ finance</td>
<td>172.16.100 is the VPN subnet and finance is the folder of interest</td>
</tr>
<tr>
<td>-------------------------</td>
<td>------------</td>
<td>-----------</td>
<td>-----------------------------------------</td>
<td>-------------------------------------------------------------------</td>
</tr>
<tr>
<td>New Email servers or any SMTP traffic from user machines</td>
<td>Email</td>
<td>Email without attachment</td>
<td>src !=10.0.0.100</td>
<td>Exclude the authorized SMTP server (10.0.0.100), all other systems generating SMTP will generate alerts.</td>
</tr>
<tr>
<td>Specific email attachments</td>
<td>Email</td>
<td>Email with attachment</td>
<td>filename =~ customers</td>
<td>Any attachment with “customers” in the title</td>
</tr>
<tr>
<td>Unusual File share activity</td>
<td>File Share</td>
<td>Delete File</td>
<td>rlim = 10/m</td>
<td>More than 10 file deletes per minute generates an alert</td>
</tr>
</tbody>
</table>