END USER LICENSE AGREEMENT

The Pulse Secure product that is the subject of this technical documentation consists of (or is intended for use with) Pulse Secure software. Use of such software is subject to the terms and conditions of the End User License Agreement (“EULA”) posted at http://www.pulsesecure.net/support/eula/. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.
NOZOMI NETWORKS INTEGRATION USING HTTP ATTRIBUTE SERVER ............ 3
Purpose of this Guide ............................................................... 3
Prerequisites ............................................................................. 3
Use Cases .................................................................................. 3
Configuring HTTP Attribute Server ........................................... 3
PPS and Nozomi Networks Integration ......................................... 5
Overview .................................................................................... 5
Configuring PPS with Nozomi Networks ...................................... 6
Profiler and Nozomi Networks Integration ................................. 10
Configuring Nozomi Networks as Collector ............................... 10
Troubleshooting ........................................................................ 11
Appendix .................................................................................... 12

Alert Based Admission Control Using Nozomi Networks .............. 13
Overview .................................................................................... 13
Deployment of PPS with Nozomi Networks SCADAguardian .......... 13
Configuring PPS with Nozomi Networks ...................................... 14
Admission Control Template ...................................................... 15
Admission Control Policies ......................................................... 16
Admission Control Client ............................................................. 18
Configuring Nozomi Networks SCADAguardian .......................... 19
Troubleshooting ........................................................................ 20
Event Types Supported by Nozomi Networks .............................. 21
Requesting Technical Support ..................................................... 26
Self-Help Online Tools and Resources ....................................... 26
Opening a Case with PSGSC ....................................................... 26
Reporting Documentation Issues ............................................... 27
Nozomi Networks Integration using HTTP Attribute Server

Purpose of this Guide
This guide describes how Pulse Policy Secure (PPS) fetches Operational Technology (OT) device attributes from Nozomi Networks and use them in role mapping rules to provide network segmentation. The Profiler can fetch the OT device information for visibility purpose. It also describes about how Pulse Policy Secure (PPS) and Nozomi Networks together can provide threat detection and threat response in ICS/OT environment using Admission Control.

Prerequisites
This guide assumes you are familiar with the use of the following products and their related terminology.

- Pulse Policy Secure at version 9.1R8.
- Nozomi Networks

Use Cases
The following use cases are supported with PPS and Nozomi networks integration:

1. Role Based Access Control (RBAC) for the endpoints based on the device attributes received from HTTP attribute server (Nozomi Networks).
2. Periodic compliance check for the endpoint using HTTP attribute server.
3. OT devices can be profiled using Profiler.

Configuring HTTP Attribute Server
The default Nozomi Networks template provides the list of possible attributes that can be received from the network security device along with attribute value. The template also provides possible actions that can be taken for an attribute. PPS is loaded with default template for Nozomi Networks.

Note: This configuration is common for both PPS and Profiler.

To add the HTTP Attribute server in PPS:

2. Enter the name.
4. Enter the IP address or hostname of Nozomi Networks server.
5. Enter the user name and password (Admin credentials of Nozomi Networks).
6. Enter the backup host name/IP address, user name and password.
7. Click **Test Connection** to test connectivity between PPS and Nozomi Networks server.
8. Click **Save Changes**.

Figure 1  HTTP Attribute Server

![Authentication Servers](image1)

Figure 2  Template

![Template](image2)
Figure 3  Available Templates

Note:

- A subset of attributes supported by Nozomi Networks is added in the default template. A new template can be created by Admin and has to be uploaded on PPS for supporting any additional attributes apart from the one’s in the default template.

- Nozomi Networks does not support more than 4 simultaneous TCP connections (See Nozomi Documentation for more details). During high load, PPS may establish more than 4 connections. Hence, it is recommended to use Profiler as a device attribute server (with Nozomi Networks as a collector) to overcome this limitation.

PPS and Nozomi Networks Integration

- Overview
- Configuring PPS with Nozomi Networks

Overview

Nozomi Networks has the capability to fetch details of ICS devices managed by Operational Technology. Operational technology devices include valves, transmitters, switches, sensors and actuators. These devices rely on custom protocols for managing and communicating.

Nozomi Networks provides detailed information about OT devices like device category, OS, manufacturer, firmware version and so on. PPS integration with Nozomi Networks allows the retrieval of OT device details and use them for network segmentation by assigning enforcement policies based on VLAN or ACLs.

This section describes how to integrate Nozomi Networks device with PPS.

The authentication process is described below when PPS is configured for MAC address authentication:

1. Whenever a device tries to connect to the network, MAC Authentication request is generated to PPS. PPS can query Nozomi Networks for device attributes using device identifier like MAC address.

2. The retrieved attributes can be used in role mapping rules to determine role of the device. Based on the assigned role, device can be put in specific VLAN or ACL policies can be applied.

3. PPS periodically queries the Nozomi Networks for change in attributes and assigns the role accordingly.
Configuring PPS with Nozomi Networks

A high-level overview of the configuration steps needed to set up and run the integration is described below:

- The Administrator configures the basic PPS configurations such as creating an authentication server, authentication realm, user roles, and role mapping rules.
- Configure Nozomi Networks as HTTP attribute server in PPS.
- Configure the Switches/WLC as RADIUS Client in PPS (Endpoint Policy > Network Access > Radius Clients > New Radius Client). Switch should be configured with PPS as a RADIUS server.
- Configured HTTP attribute server has to be mapped as a "Device Attributes" under the realm configuration and role mapping rules can be used to assign the roles based on the attributes received from the attribute server.

1. Configure Nozomi Networks as HTTP attribute server in PPS “Configuring HTTP Attribute Server” on page 3

2. Select Endpoint Policy > MAC Address Realms, click New to create the authentication realm. Under Device Attributes, select the Nozomi HTTP attribute server created earlier or User Realms > Users > General, select the Nozomi Networks server created in Device Attributes
Figure 5  MAC Address Realms

3. Configure rules based on Device Attributes from **Endpoint Policy > MAC Address Realms** and click **Role Mapping > Role Mapping Rule**. Create a new rule, select Rule based on: **Device Attribute** and click **Update** or **User Realms > Users > Role Mapping > Role Mapping Rule**.

Figure 6  Device Attributes
4. Click **Save Changes**.

Once the role mapping rule is created, you can see the summary page as shown below. The following page shows the different rules created with the corresponding roles assigned.

**Note:** MAC Address is used as a device identifier to query attributes from Nozomi Networks. Without Host Checker, PPS doesn't learn the MAC address. For agentless sessions, Host Checker should be enabled to learn MAC address. For Agentless sessions/logins, pre-auth Host Checker must be enabled.
Profiler and Nozomi Networks Integration

The Nozomi Networks is configured as a HTTP Attribute Server and is available under Device Attribute Server settings. The server is manually selected as an active collector to collect information that is used to classify and categorize the devices. The attributes information helps for role mapping.

**Note:** The collector can only read devices that have a confirmed MAC address and are stored in the Profiler.

Configuring Nozomi Networks as Collector

To configure Nozomi Networks as a device attribute server to perform as an active collector:

1. Configure Nozomi Networks as HTTP attribute server in PPS “Configuring HTTP Attribute Server” on page 3
2. Under MAC Address Realms or User Realms, select the Nozomi HTTP attribute server created in Device Attributes.
3. Navigate to Profiler > Profiler Configuration > Advance Configuration. Under Device Attribute Server, select the HTTP server as the device attribute server.

The DDR page displays the endpoint information collected by Nozomi collector.
Troubleshooting

To verify the event logs on PPS, select System > Log/Monitoring > Events. You can verify that the event logs are generated every time when an event is received from Nozomi Networks.

To verify the user access logs, select System > Logs & Monitoring > User Access to verify the user login related logs like realm, roles, username and IP address.

Figure 11 Event Logs
You can also enable debug logs to troubleshoot any issues. Select Maintenance > Troubleshooting > Monitoring > Debug Log to enable debug logs.

Maintenance > Troubleshooting > User Session > Policy Tracing can be used to see which attributes are fetched from Nozomi Attribute Server or Profiler.

### Appendix

Attributes exposed by the default Nozomi Networks template. Admin can add more attributes to the list by creating a new template and uploading it to PPS. PPS performs normalization of few attributes as used and displayed by Profiler. These attributes are category, hostname, manufacturer, ip, os, and macaddr.

```json
"attributes" : [
    {
      "type" : "category",
      "label" : "hostname",
      "mac_vendor" : "manufacturer",
      "ip" : "ip",
      "os" : "os",
      "mac_address" : "macaddr",
      "vendor" : "vendor",
      "level" : "level",
      "roles" : "roles",
      "firmware_version" : "firmwareVersion",
      "product_name" : "productName",
      "level" : "level",
      "zone" : "zone",
      "is_broadcast" : "isBroadcast",
      "is_public" : "isPublic",
      "reputation" : "reputation",
      "is_confirmed" : "isConfirmed",
      "is_learned" : "isLearned",
      "is_disabled" : "isDisabled",
      "is_fully_learned" : "isFullLearned",
      "first_activity_time" : "firstActivityTime",
      "last_activity_time" : "lastActivityTime"
    }
]```
Alert Based Admission Control using Nozomi Networks

Overview
Nozomi Networks provides industry leading solution for real-time cyber security and visibility for Industrial Control Networks. It provides superior network and operational visibility and advanced threat detection. Nozomi Networks SCADAguardian uses behavior based anomaly detection and multiple types of signature and rule based detection. SCADAguardian also generates different kinds of alerts when potentially dangerous conditions are met. These alerts are originated from different engines (Protocol Validation, Learned Behaviour, Built-in checks, Custom checks) in SCADAguardian.

Pulse Policy Secure (PPS) can be deployed in ICS/OT network to provide authentication and access control. PPS can consume alerts generated by Nozomi Networks SCADAguardian and takes appropriate action to restrict access of anomalous device endpoint.

Deployment of PPS with Nozomi Networks SCADAguardian
This section describes the integration of PPS with Nozomi Networks. PPS receives the threat alert information from Nozomi networks solution and takes an action at the endpoint based on the admission control policies.
CS security vendors such as Nozomi Networks are deployed to passively analyse industrial protocol communication for automatic assert discovery and threat detection.

1. The device connects to PPS through Switch.
2. The device session is created on the PPS.
3. The device access details are pushed to Switch using ACL.
4. The Nozomi Networks SCADAguardian monitors the device traffic.
5. The Nozomi Networks SCADAguardian generates the syslog messages for the device.
6. The syslog message is sent to PPS if any suspicious traffic or activity is detected from the device.
7. Pulse Policy Secure (PPS) processes the received syslog message and actions are taken based on the configured policies.
8. New/Updated ACL details are pushed to Switch for updating the enforcement of the device.

**Configuring PPS with Nozomi Networks**

The network security devices are configured with PPS for admission access control. A high-level overview of the configuration steps needed to set up and run the integration is described below:

- The Administrator configures the basic PPS configurations such as creating an authentication server, authentication realm, user roles, and role mapping rules.
- Configure Nozomi Networks SCADAguardian as a client in PPS.
- Configure PPS details in SCADAguardian
• Configure PPS to block/quarantine the endpoint based on the SCADAguardian admission control template.

This section covers the following topics:

• “Admission Control Template” on page 15
• “Admission Control Policies” on page 16
• “Admission Control Client” on page 18

Admission Control Template

The admission control template provides the list of possible events that can be received from the network security device along with regular expression to parse the message. The template also provides possible actions that can be taken for an event.

Pulse Policy Secure (PPS) is loaded with default templates for SCADAguardian (nozomi-scadaguardian-cef.itmpl).

You can view the list of configured integration templates that provides the list of network security devices and the supported protocol type using Endpoint Policy > Admission Control > Templates.

To view the admission control templates:


Figure 13 Existing Template

Admin can also create templates and can upload it to PPS.
Admission Control Policies

The admission control policies define the list of actions to be performed on PPS for the user sessions. The actions are based on the event and the severity information received from the network security device.

To view and add the new integration policy:

1. Select **Endpoint Policy > Admission Control > Policies**.
2. Click **New Policy**.
3. Enter the policy name.
4. Select **Nozomi Networks-SCADAguardian-Syslog-CEF** as a template.
5. Under **Rule on Receiving**, select the event type severity score. Refer to Event Types supported by Nozomi Networks for more information on supported event types. The event types and the severity score are based on the selected template.
6. Under **then perform this action**, select the desired action.
   - Ignore (log the event) — Received syslog event details are logged on the PPS and no specific action is taken.
   - Terminate user session — Terminates the user session on the PPS for the received messages.
   - Block the endpoint from authenticating to the network — Blocks the endpoint from authenticating to the network.
   - Put the endpoint into a quarantine network by assigning this role — choose the role to put endpoint in quarantine role. Specify whether to apply the role assignment permanently or only for the session.

   **Note:** Admission Control Policy action is not taken for endpoints behind Network Address Translation (NAT).
7. Under **Roles**, specify:
   - Policy applies to ALL roles—To apply the policy to all users.
   - Policy applies to SELECTED roles—To apply this policy only to users who are mapped to roles in the Selected roles list. You must add roles to this list from the Available roles list.
   - Policy applies to all roles OTHER THAN those selected below—To apply this policy to all users except for those who map to the roles in the Selected roles list. You must add roles to this list from the Available roles list.

8. Click **Save changes**.

**Figure 14  Configuration Policies**

Once the policy is created, you can see the summary page as shown below. The following page shows the different policies created for different events with different user roles.
Admission Control Client

The admission control clients are the network security devices on which the syslog forwarding is enabled. The messages are received by the syslog server module running on PPS.

To add a client:

1. Select **Endpoint Policy > Admission Control > Clients.**
2. Click **New Client.**
3. Enter the name of the client.
4. Enter the description.
5. Enter the IP address of the Nozomi client.
6. Select the Protocol Type as Syslog.
7. Select the Vendor as Nozomi Networks.
8. Select Device Type as SCADAguardian.
9. Click **Save Changes.**
Configuring Nozomi Networks SCADAguardian

To receive the alert information, PPS details are added in SCADAguardian admin interface.

1. Select **Administration > Data Integration**.
   a. Click **Add** to add new Endpoint.
   b. Under Endpoint Configured as, select **Common Event Format (CEF)**.
   c. Under **To URL**, enter the Protocol (TCP or UDP), IP address of PPS, and port number.
   d. Select the checkbox **Enable sending Alerts**.
   e. Enter the filter query if only specific alert information should be sent to PPS.

For example, if administrator wants to send information to PPS for alerts with risk score of more than 6, specify "where risk > 6" in query filter.
Troubleshooting
To verify the event logs on PPS, select **System > Log/Monitoring > Events**.
You can verify that the event logs are generated every time when an event is received from SCADAguardian.

To verify the user access logs, select **System > Logs & Monitoring > User Access** to verify the user login related logs like realm, roles, username and IP address.
You can also verify whether the quarantined(blocked) host is listed in the Infected Devices report, which lists the mac address, IP address, and the device status. To verify the reports, select System > Reports > Infected Hosts.

![Infected Devices Report](image)

You can also enable debug logs to troubleshoot any issues. Select Maintenance > Troubleshooting > Monitoring > Debug Log to enable debug logs.

**Event Types supported by Nozomi Networks**

The following table describes the detailed description about events supported by Nozomi Networks.

<table>
<thead>
<tr>
<th>Category</th>
<th>Type ID</th>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Custom Checks</td>
<td>PROC:STALE-VARIABLE</td>
<td>Stale variable</td>
<td>A variable configured with: check_last_update N does not have its value updated for more than N seconds.</td>
</tr>
<tr>
<td>Learned Behavior/Custom Checks</td>
<td>PROC:CRITICAL-STATE-ON</td>
<td>Critical state on</td>
<td>The system has entered in a Process Critical State that has either been learned or inserted as a custom check</td>
</tr>
<tr>
<td>Custom Checks</td>
<td>PROC:INVALID-VARIABLE-QUALITY</td>
<td>Invalid variable quality</td>
<td>A variable configured with: check_quality N keeps its value with an invalid quality for more than N seconds.</td>
</tr>
<tr>
<td>Built-in Checks</td>
<td>NET:RST-FROM-SLAVE</td>
<td>Slave sent RST on Link</td>
<td>A slave closed the connection to the master. This can be due to the device restarting or behaving in a strange manner.</td>
</tr>
<tr>
<td>Custom Checks</td>
<td>NET:INACTIVE-PROTOCOL</td>
<td>Inactive protocol</td>
<td>A link configured with :check_last_activity N stays inactive for more than N seconds.</td>
</tr>
<tr>
<td>Category</td>
<td>Type ID</td>
<td>Name</td>
<td>Definition</td>
</tr>
<tr>
<td>------------------------</td>
<td>--------------------------------</td>
<td>----------------------------------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Built-in Checks</td>
<td>SIGN:TCP-SYN-FLOOD</td>
<td>TCP SYN flood</td>
<td>This kind of alert occurs when either one or many hosts send a great amount of TCP SYN packets to a single host.</td>
</tr>
<tr>
<td>Built-in Checks</td>
<td>SIGN:MALICIOUS-PROTOCOL</td>
<td>Malicious Protocol detected</td>
<td>Malicious Protocol detected</td>
</tr>
<tr>
<td>Built-in Checks</td>
<td>SIGN:FRAMEWORK-CHANGE</td>
<td>Firmware change requested</td>
<td>Firmware change requested</td>
</tr>
<tr>
<td>Built-in Checks</td>
<td>SIGN:MAN-IN-THE-MIDDLE</td>
<td>Man-In-the-middle attack</td>
<td>This kind of alert is raised when a Man-In-the-middle attack is detected.</td>
</tr>
<tr>
<td>Protocol Validation</td>
<td>SIGN:DHCP-OPERATION</td>
<td>DHCP operation</td>
<td>A DHCP request from an unknown device has been found in the network, as a sign of a new device which is trying to obtain an address.</td>
</tr>
<tr>
<td>Built-in Checks</td>
<td>SIGN:CPE:CHANGE</td>
<td>Installed software change detected</td>
<td>This kind of alert is raised after the detection of an installed software change.</td>
</tr>
<tr>
<td>Built-in Checks</td>
<td>SIGN:PROTOCOL-ERROR</td>
<td>Protocol error</td>
<td>A generic protocol error occurred, this usually relates to a state machine, option or other general violation of the protocol.</td>
</tr>
<tr>
<td>Built-in Checks</td>
<td>SIGN:ILLEGAL-PARAMETERS</td>
<td>A request with illegal parameters was asked</td>
<td>A request with illegal parameters was asked</td>
</tr>
<tr>
<td>Built-in Checks</td>
<td>SIGN:UNSUPPORTED-FUNC</td>
<td>Unsupported function was asked</td>
<td>An unsupported function has been called on the remote peer. It might me because of a malfunctioning software is trying to perform an operation without success or that a malicious attacker is trying to understand the functionalities of the device.</td>
</tr>
<tr>
<td>Built-in Checks</td>
<td>SIGN:MALICIOUS-DOMAIN</td>
<td>Malicious domain</td>
<td>Malicious domain</td>
</tr>
<tr>
<td>Built-in Checks</td>
<td>SIGN:NETWORK-SCAN</td>
<td>Network Scan</td>
<td>Network Scan</td>
</tr>
<tr>
<td>Built-in Checks</td>
<td>SIGN:PROGRAM:CHANGE</td>
<td>Program change detected</td>
<td>The program on the OT device has been uploaded and changed. This can be a legitimate operation during maintenance and upgrade of the software or an unauthorized tentative to read the program logic.</td>
</tr>
<tr>
<td>Built-in Checks</td>
<td>SIGN:CONFIGURATION-CHANGE</td>
<td>Configuration change requested</td>
<td>The configuration on the device has been uploaded and changed. This can be a legitimate operation during maintenance or an unauthorized tentative to modify the behaviour of the device.</td>
</tr>
<tr>
<td>Learned Behavior</td>
<td>VI:NEW-NODE:MALICIOUS-IP</td>
<td>Bad reputation ip</td>
<td>Bad reputation ip</td>
</tr>
<tr>
<td>Category</td>
<td>Type ID</td>
<td>Name</td>
<td>Definition</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------</td>
<td>-------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Built-in Checks</td>
<td>SIGN:OT_DEVICE-REBOOT</td>
<td>OT device reboot requested</td>
<td>The OT device has been requested to reboot by the sender host. This event may be something correct during Engineering operations on the OT device, for instance the maintenance. However, it may indicate suspicious activity of an attacker trying to disrupt the process being controlled by the OT device.</td>
</tr>
<tr>
<td>Custom Checks</td>
<td>PROC:NOST-ALLOWED-INVALID-VARIABLE</td>
<td>(Variable quality is not allowed)</td>
<td>A variable that has been configured with a specific check has been detected to have a not allowed quality.</td>
</tr>
<tr>
<td>Built-in Checks</td>
<td>SIGN:MULTIPLE-UNSUCCESSFUL-LOGINS</td>
<td>Multiple unsuccessful logins</td>
<td>This kind of alert occurs when a host is repeatedly trying to login to a service without success.</td>
</tr>
<tr>
<td>Custom Checks</td>
<td>PROC:SYNC-ASKED-AGAIN</td>
<td>Slave sync asked</td>
<td>A new general interrogation command is issued, this can be an anomaly since this command should be performed once per OT device.</td>
</tr>
<tr>
<td>Built-in Checks</td>
<td>SIGN:OT_DEVICE-STOP</td>
<td>OT device stop requested</td>
<td>The OT device program has been requested to stop by the sender host. This event may be something correct during Engineering operations on the OT device, for instance the maintenance of the program itself. However, it may indicate suspicious activity of an attacker trying to halt the process being controlled by the OT device.</td>
</tr>
<tr>
<td>Built-in Checks</td>
<td>SIGN:OT_DEVICE-START</td>
<td>OT device start requested</td>
<td>The OT device program has been requested to start again by the sender host. This event may be something correct during Engineering operations on the OT device, for instance the maintenance of the program itself or a reboot of the system for updates. However, it may indicate suspicious activity of an attacker trying to manipulate the state of the OT device.</td>
</tr>
<tr>
<td>Learned Behavior</td>
<td>VI:PROC:PROTOCOL-FLOW-ANOMALY</td>
<td>Protocol flow anomaly</td>
<td>This kind of alert is raised when the Process-related behavior of a protocol changes in a suspicious manner.</td>
</tr>
<tr>
<td>Built-in Checks</td>
<td>SIGN:DEV-STATE-CHANGE</td>
<td>Device state change</td>
<td>This kind of alert is raised when a change of the state of a device is detected, for example when an OT device is asked to enter in a new mode or a factory reset is issued.</td>
</tr>
<tr>
<td>Built-in Checks</td>
<td>SIGN:PROGRAM:UPLOAD</td>
<td>Program uploaded to device</td>
<td>The program of the OT device has been uploaded. This can be a legitimate operation during maintenance and upgrade of the software or an unauthorized tentative to disrupt the normal behavior of the system.</td>
</tr>
<tr>
<td>Category</td>
<td>Type ID</td>
<td>Name</td>
<td>Definition</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------------------</td>
<td>-----------------------------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Built-in Checks</td>
<td>SIGN:CLEARTEXT-PASSWORD</td>
<td>Cleartext password</td>
<td>Cleartext password</td>
</tr>
<tr>
<td>Built-in Checks</td>
<td>SIGN:TCP-SYN-FLOOD</td>
<td>TCP SYN flood</td>
<td>This kind of alert occurs when one or many host send a great amount of TCP SYN packets to a single host.</td>
</tr>
<tr>
<td>Built-in Checks</td>
<td>PROC:WRONG-TIME</td>
<td>Process time issue detected</td>
<td>A slave reported a wrong time regarding Process data. This may be due to incorrect time synchronization of the slave, a misbehavior or a sign of compromise of the device.</td>
</tr>
<tr>
<td>Protocol Validation</td>
<td>SIGN:SCADA-INJECTION</td>
<td>SCADA packet Injection4</td>
<td>A traffic injection of SCADA packets has been detected in the network.</td>
</tr>
<tr>
<td>Built-in Checks</td>
<td>SIGN:ARP:DUP</td>
<td>Duplicate IP</td>
<td>This kind of alert occurs when a duplicated IP is spotted on the network by analyzing the ARP protocol.</td>
</tr>
<tr>
<td>Built-in Checks</td>
<td>SIGN:PACKET-RULE</td>
<td>Packet rule match</td>
<td>A packet rule has matching a specific security check has matched. This Alert requires to thoroughly check what happened to verify if an attacker is trying to compromise one or more host.</td>
</tr>
<tr>
<td>Learned Behavior</td>
<td>VI:NEW-PROTOCOL:CONFIRMED</td>
<td>New protocol confirmed</td>
<td>A protocol between two nodes has been confirmed at Layer 4 (the endpoint has accepted the connection).</td>
</tr>
<tr>
<td>Custom Checks</td>
<td>NET:LINK-RECONNECTION</td>
<td>Link reconnection</td>
<td>A link configured as persistent has a new TCP handshake.</td>
</tr>
<tr>
<td>Built-in Checks</td>
<td>SIGN:MALICIOUS-IP</td>
<td>Bad ip reputation</td>
<td>Bad ip reputation</td>
</tr>
<tr>
<td>Learned Behavior</td>
<td>VI:PROC:VARIABLE-FLOW-ANOMALCY</td>
<td>Variable flow anomaly</td>
<td>The access over time to a variable has changed in an unexpected manner.</td>
</tr>
<tr>
<td>Built-in Checks</td>
<td>SIGN:PROC:MISSING-VAR</td>
<td>Missing Variable Requested</td>
<td>A tentative to access a nonexistent variable has been performed. This can be due to a reconnaissance activity or configuration change.</td>
</tr>
<tr>
<td>Learned Behavior</td>
<td>VI:NEW-NET-DEV</td>
<td>New network device detected</td>
<td>A new unseen network device, such as a switch, router or firewall has appeared in the network.</td>
</tr>
<tr>
<td>Learned Behavior</td>
<td>VI:PROC:NEW-VAR</td>
<td>New SCADA variable appeared</td>
<td>A new variable has been detected in a SCADA slave.</td>
</tr>
<tr>
<td>Learned Behavior</td>
<td>VI:NEW-FUNC-CODE</td>
<td>New function code detected</td>
<td>A node starts using a function code as never seen earlier.</td>
</tr>
<tr>
<td>Learned Behavior</td>
<td>VI:NEW-PROTOCOL:APPLICATION</td>
<td>New application detected</td>
<td>A Layer 7 protocol has been detected in a Layer 4 protocol.</td>
</tr>
<tr>
<td>Category</td>
<td>Type ID</td>
<td>Name</td>
<td>Definition</td>
</tr>
<tr>
<td>-------------------</td>
<td>--------------------------</td>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Built-in Checks</td>
<td>SIGN:MALWARE-DETECTED</td>
<td>Malware detected</td>
<td>A malicious payload has been transferred over the network.</td>
</tr>
<tr>
<td>Learned Behavior</td>
<td>VI:NEW-PROTOCOL</td>
<td>New protocol used</td>
<td>A new protocol has been tried between two nodes.</td>
</tr>
<tr>
<td>Learned Behavior</td>
<td>VI:NEW-LINK</td>
<td>New target used</td>
<td>A node tries to communicate with a node not contacted before.</td>
</tr>
<tr>
<td>Learned Behavior</td>
<td>VI:NEW-ARP</td>
<td>New ARP from unknown MAC addresses</td>
<td>A new unseen node appeared through ARP traffic. This Alert is useful to detect also devices that are connected near the sniff interfaces of SCADAguardian but are not sending relevant application-level packets through the network.</td>
</tr>
<tr>
<td>Learned Behavior</td>
<td>VI:NEW-NODE:TARGET</td>
<td>New target node appeared</td>
<td>A new unseen node starts to send packets in the network.</td>
</tr>
<tr>
<td>Built-in Checks</td>
<td>SIGN:PASSWORD:WEAK</td>
<td>Weak password used</td>
<td>Weak password used</td>
</tr>
<tr>
<td></td>
<td>SIGN:DDOS</td>
<td>DDOS attack</td>
<td>DDOS attack</td>
</tr>
<tr>
<td></td>
<td>SIGN:MULTIPLE-OT_DEVICE-RESERVATIONS</td>
<td>Multiple OT device reservations</td>
<td>Multiple OT device reservations</td>
</tr>
<tr>
<td>Learned Behavior</td>
<td>VI:NEW-NODE</td>
<td>New node appeared</td>
<td>A new unseen node starts to send packets in the network.</td>
</tr>
<tr>
<td>Built-in Checks</td>
<td>SIGN:PROGRAM:DOWNLOAD</td>
<td>Program downloaded from device</td>
<td>The program of the OT device has been downloaded from another host. This can be a legitimate operation during maintenance and upgrade of the software or an unauthorized tentative to read the program logic.</td>
</tr>
<tr>
<td>Learned Behavior</td>
<td>VI:PROC:NEW-VALUE</td>
<td>New SCADA variable value</td>
<td>A new variable value or behavior has been detected in a SCADA slave.</td>
</tr>
<tr>
<td>Learned Behavior/ Custom Checks</td>
<td>VI:PROC:CRITICAL-STATE-OFF</td>
<td>Critical state off</td>
<td>The system has exited from a Process Critical State.</td>
</tr>
<tr>
<td>Protocol Validation</td>
<td>SIGN:INVALID-IP</td>
<td>Invalid IP</td>
<td>A packet with invalid IP packets reserved for special purposes (e.g. loopback addresses). Packets with such addresses can originate from misconfiguration or spoofing/denial of service attacks.</td>
</tr>
<tr>
<td>Learned Behavior</td>
<td>VI:NEW-SCADA-NODE</td>
<td>New SCADA node appeared</td>
<td>A new unseen node speaking SCADA protocols starts to send packets in the network.</td>
</tr>
<tr>
<td>Learned Behavior</td>
<td>VI:NEW-MAC</td>
<td>New Mac address</td>
<td>A new unseen MAC address has appeared in the network.</td>
</tr>
</tbody>
</table>
Requesting Technical Support

Technical product support is available through the Pulse Secure Global Support Center (PSGSC). If you have a support contract, file a ticket with PSGSC.

- Product warranties—For product warranty information, visit https://support.pulsesecure.net/product-service-policies/

Self-Help Online Tools and Resources

For quick and easy problem resolution, Pulse Secure provides an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: https://support.pulsesecure.net
- Search for known bugs: https://support.pulsesecure.net
- Find product documentation: https://www.pulsesecure.net/techpubs
- Download the latest versions of software and review release notes: https://support.pulsesecure.net
- Open a case online in the CSC Case Management tool: https://support.pulsesecure.net
- To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: https://support.pulsesecure.net

For important product notices, technical articles, and to ask advice:

- Search the Pulse Secure Knowledge Center for technical bulletins and security advisories: https://kb.pulsesecure.net
- Ask questions and find solutions at the Pulse Community online forum: https://community.pulsesecure.net

Opening a Case with PSGSC

You can open a case with PSGSC on the Web or by telephone.

- Use the Case Management tool in the PSGSC at https://support.pulsesecure.net.
- Call 1-844 751 7629 (Toll Free, US).

For international or direct-dial options in countries without toll-free numbers, see https://support.pulsesecure.net/support/support-contacts/

---

<table>
<thead>
<tr>
<th>Category</th>
<th>Type ID</th>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Built-in Checks</td>
<td>SIGN:UNSUPPORTED</td>
<td>Unknown RTU ID requested</td>
<td>An unsupported function has been called on the remote peer. This may mean that a malfunctioning software is trying to perform an operation without success or that a malicious attacker is trying to understand the functionalities of the device.</td>
</tr>
</tbody>
</table>
Reporting Documentation Issues

To report any errors or inaccuracies in Pulse Secure technical documentation, or to make suggestions for future improvement, contact Pulse Secure Technical Support (https://support.pulsesecure.net). Include a full description of your issue or suggestion and the document(s) to which it relates.