Pulse Policy Secure

802.1X Authentication with Cisco Switch on Windows

Configuration Guide
Pulse Secure, LLC
2700 Zanker Road, Suite 200 San Jose, CA 95134
www.pulsesecure.net

Pulse Secure and the Pulse Secure logo are trademarks of Pulse Secure, LLC in the United States. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Pulse Secure, LLC assumes no responsibility for any inaccuracies in this document. Pulse Secure, LLC reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

802.1X Authentication with Cisco Switch

The information in this document is current as of the date on the title page.

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 www.pulsesecure.net. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.”
Introduction

This example describes a phased approach to deploy IEEE 802.1x port-based authentication with Cisco Switch on Windows platform to provide secure and role based access control using Pulse Policy Secure.

Figure: Overview

Configuration

The goal is to provide secure and role based access control using ACLs on Cisco Switch through PPS.

- Configuring Authentication Server
- Updating Default Realm
- Updating Default Sign-in Policy
- Creating a Host Checker Policy
- Creating User Role
- Creating a new RADIUS Client
- Configuring RADIUS Return Attribute Policies
- Configuring 802.1X Connections
- Configuring Cisco Switch
Configuring Authentication Server

Create a new AD Authentication server, select Authentication > Auth.Servers. For example, Select AD server from the drop down and Click New Server.

Figure 1: Authentication Server

The AD configuration page is shown below.
Updating Default Realm

1. Select **User Realms > User > General**.
2. Under Authentication, select the AD as the authentication server.
3. Click **Save Changes**.

**Figure 2: Realm**
Updating Default Sign-in Policy

1. Select Authentication > Signing In > Sign-in Policies.
2. Add Available Realms as Users, Authentication protocol set as 802.1X.
3. Click Save Changes.

Figure 3: Sign-in Policy
Creating a Host Checker Policy

2. Under Policies, Click New and enter a policy name and click Continue.

3. Under Rule Settings, select the rule type as Predefined Firewall and click Add.

4. Enter the rule name and specify the criteria for compliance and click Save Changes.
Creating User Roles

1. Select Users > User Roles > New User Role.
2. Enter a name. For example, Full Access Role, Limited Access Role.
3. Click Save Changes.

Figure 4: User Role

For Limited Access Role, ensure that the Host Checker not required option is not selected.

5. Set Role Mapping rules. Select User Realms > Users > Role Mapping > New Rule
Figure 5: Role Mapping Rule

Once the role mapping roles are configured the following screen is displayed.

Figure 6: Completed Role Mapping Rules
Creating a new RADIUS Client

Add the Switch as RADIUS client
1. Select **Endpoint Policy > Network Access > RADIUS Client**.
2. Enter the name.
3. Enter the IP address of the Switch.
4. Select the make/model as Cisco Systems.
5. Select the default location group.
6. Click **Save Changes**.
   Shared Secret will be used in the Cisco/RADIUS configuration.

**Figure 7: RADIUS client**
Configuring RADIUS Return Attribute Policies

Define RADIUS Return Attribute policy based on ACL for different roles.

1. Set RADIUS return attributes. Select **Endpoint Policy > Network Access > RADIUS Return Attribute Policies**. Click **New Policy**.

2. Under RADIUS Attributes tab, select the check box for **Return Attribute**. Select appropriate Vendor Specific Attribute as Return Attribute. In the Value field, define the ACL/Firewall Filter. For example, Return Attribute is **Filter-Id** and Value as **compliant.in**.

Figure 8: RADIUS Return Attribute Policy
Similarly define a remediation policy with Return Attribute as *Filter-Id* and Value as *noncompliant.in*.

**Figure 9: RADIUS Return Attribute Policy**

![RADIUS Return Attribute Policy](image)
The following example shows the Filter-Id radius attribute policy for Cisco Switches.

Figure 10: RADIUS Return Attributes: Filter-Id

The following example shows RADIUS return attribute used to send the VLAN ID. In the below example, VLAN 65 is sent for Full Access Role and VLAN 60 for Limited Access Role.

The following example shows the Cisco-AVPair radius attribute policy for Cisco Switches.

Note:
- When using VSAs there is no need to configure ACL/Firewall filters in the switches. These are managed by PPS and access control entries (ACEs) will be applied on the switches after User Authentication.
- VLAN change using CoA is not supported with Cisco Switches. It is recommended to use RADIUS disconnect for VLAN change.
Figure 11: RADIUS Return Attributes: Cisco-AVPair

<table>
<thead>
<tr>
<th>Policies</th>
<th>Attributes</th>
<th>Location Group</th>
<th>Interface</th>
<th>Applies to role</th>
</tr>
</thead>
<tbody>
<tr>
<td>1: full_access_with_AVP_A</td>
<td>Cisco AVPair: avpair#161:permit:ip any any</td>
<td>Default</td>
<td>N/A</td>
<td>Full Access Role</td>
</tr>
</tbody>
</table>

A RADIUS return attributes policy specifies the return list attributes to send to an 802.1X network access device, such as which VLAN endpoints must use to access the network. If no policy applies, Open Port is the default action.
Configuring 802.1X Connections


Figure 12: Connections
2. Under Connections, Click **New** to create a **New Pulse Secure Connection**. Ensure that you have the valid device certificate to avoid certificate warnings at Pulse Client.

Note: The configuration mentioned is only for User mode connections.

**Figure 13:** Pulse Secure Connection

3. Enter name and select Type as Pulse Secure (802.1X).
4. Click **Save Changes**.
Configuring Cisco Switch

CLI command to configure 802.1X on Cisco 3850. The switch configuration varies for each switch type. Run the show run command on your switch to ensure that your access interface connections are set up.

```
# Interface configuration.
interface GigabitEthernet1/0/7
switchport access vlan 60
switchport mode access
authentication periodic
authentication timer reauthenticate server
authentication event server dead action authorize
access-session port-control auto
dot1x pae authenticator
spanning-tree portfast
end

# Specify the server group for authentication, authorization and accounting.
aaa authentication dot1x default group <group-name>
aaa authorization network default group <group-name>
aaa accounting dot1x default start-stop group <group-name>

# Configure the PPS as radius server.
radius server <PPS-Server-name>
    address ipv4 <PPS-IP Address> auth-port 1812 acct-port 1813
    key psecure
    radius-server attribute 44 extend-with-addr
    radius-server attribute 6 on-for-login-auth
    radius-server attribute 8 include-in-access-req
    radius-server attribute 25 access-request include
    radius-server retransmit 1

# Create the server group which will be used for AAA.
# Add PPS as server in the server group.
aaa group server radius <group-name>
    server name <PPS-Server-name>

# ACL configuration
ip access-list extended compliant
    permit ip any any
ip access-list extended uncompliant
    deny ip any host <Resource-IP-Address1>
    deny ip any host <Resource-IP-Address2>
    permit ip any any
```
Results

Authenticate devices using 802.1X using Pulse Client. For example, in the above configuration scenario, users will be assigned Limited access role if the Host Checker compliance fails. A sample screenshot of users trying to access the network using Pulse Client on windows platform is shown below.

![Screenshot of Pulse Secure client with limited access role]

You can verify the active users table to view the session details of the user. The user gets a limited access role.

![Screenshot of active users table with limited access role]

© 2019 by Pulse Secure, LLC. All rights reserved
For troubleshooting you can verify the user access logs.

Verify the Switch for the applied Filter-id. In the below example, Filter-id applied is noncompliant.

```
Interface:  GigabitEthernet1/0/13
  IIF-ID:  0x19C91A80
  MAC Address:  0050.56bf.554f
  IPv6 Address:  Unknown
  IPv4 Address:  Unknown
  User-Name:  anonymous
  Status:  Authorized
  Domain:  DATA
  Oper host mode:  multi-host
  Oper control dir:  both
  Session timeout:  N/A
  Common Session ID:  0A190FCA0000029B7A2669E1
  Acct Session ID:  0x0000000f
  Handle:  0x6d00000f
  Current Policy:  POLICY_Gi1/0/3

Local Policies:
  Service Template:  DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
  Security Policy:  Should Secure
  Security Status:  Link Unsecured

Server Policies:
  Filter-ID:  noncompliant

Method status list:
  Method  State
  dot1x   Authc Success
```
The user turns ON the Windows Firewall and the Host Checker policy passes and the user connection is successfully established.

You can verify the active users table to view the session details of the user.

**Figure 14: Active Users- Full Access Role**
For troubleshooting you can verify the user access logs.

**Figure 15: User Access Logs for compliant role.**

Verify the Switch for change of Filter-ID to compliant.

<table>
<thead>
<tr>
<th>Interface: GigabitEthernet1/0/13</th>
</tr>
</thead>
<tbody>
<tr>
<td>IIF-ID: 0x11BB48C9</td>
</tr>
<tr>
<td>MAC Address: 0050.56bf.554f</td>
</tr>
<tr>
<td>IPv6 Address: Unknown</td>
</tr>
<tr>
<td>IPv4 Address: Unknown</td>
</tr>
<tr>
<td>User-Name: anonymous</td>
</tr>
<tr>
<td>Status: Authorized</td>
</tr>
<tr>
<td>Domain: DATA</td>
</tr>
<tr>
<td>Oper host mode: multi-host</td>
</tr>
<tr>
<td>Oper control dir: both</td>
</tr>
<tr>
<td>Session timeout: N/A</td>
</tr>
<tr>
<td>Common Session ID: 0A190FCA0000029C7A2CAD96</td>
</tr>
<tr>
<td>Acct Session ID: 0x00000010</td>
</tr>
<tr>
<td>Handle: 0x1a000010</td>
</tr>
<tr>
<td>Current Policy: POLICY_Gi1/0/3</td>
</tr>
<tr>
<td>Local Policies:</td>
</tr>
<tr>
<td>Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)</td>
</tr>
<tr>
<td>Security Policy: Should Secure</td>
</tr>
<tr>
<td>Security Status: Link Unsecured</td>
</tr>
<tr>
<td>Server Policies:</td>
</tr>
<tr>
<td>Filter-ID: compliant</td>
</tr>
<tr>
<td>Method status list:</td>
</tr>
<tr>
<td>Method</td>
</tr>
<tr>
<td>dot1x</td>
</tr>
</tbody>
</table>
Appendix

CLI commands on Cisco Switch running 15.2.

```bash
#show configuration
version 15.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname myswitch
boot-start-marker
boot-end-marker
enable password Cisco
username admin privilege 15 secret 5 $1$mUVx$5INk8ibYzrj4fyRtVPhb91
aaa new-model
aaa group server radius radiusgroup
  server name radiusserver
aaa authentication login default local
aaa authentication enable default enable
aaa authentication dot1x default group radiusgroup
aaa authorization network default group radiusgroup
aaa authorization auth-proxy default group radiusgroup
aaa accounting send stop-record authentication failure
aaa accounting update newinfo
aaa accounting identity default start-stop broadcast group radiusgroup
aaa accounting network default start-stop group radiusgroup
aaa server radius dynamic-author
  client 10.209.126.152 server-key 12345
  port 3799
  auth-type all
  ignore session-key
  ignore server-key
aaa session-id common
clock timezone IST 5 30
switch 1 provision ws-c2960x-24pd-l
ip dhcp snooping
ip domain-name pps.local
crypto pki trustpoint TP-self-signed-3051400704
```
enrollment selfsigned
subject-name cn=IOS-Self-Signed-Certificate-3051400704
revocation-check none
rsakeypair TP-self-signed-3051400704
crypto pki certificate chain TP-self-signed-3051400704
certificate self-signed 01 nvram:IOS-Self-Sig#1.cer
dot1x system-auth-control
dot1x test timeout 30
service-template webauth-global-inactive
inactivity-timer 3600
service-template DEFAULT_LINKSEC_POLICY_MUST_SECURE
service-template DEFAULT_LINKSEC_POLICY_SHOULD_SECURE
service-template DEFAULT_CRITICAL_VOICE_TEMPLATE
voice vlan
spanning-tree mode pvst
spanning-tree extend system-id
vlan internal allocation policy ascending
class-map type control subscriber match-all AAA_SVR_DOWN_AUTHD_HOST
match result-type aaa-timeout
match authorization-status authorized
class-map type control subscriber match-all AAA_SVR_DOWN_UNAUTHD_HOST
match result-type aaa-timeout
match authorization-status unauthorized
class-map type control subscriber match-all DOT1X
match method dot1x
class-map type control subscriber match-all DOT1X_FAILED
match method dot1x
match result-type method dot1x authoritative
class-map type control subscriber match-all DOT1X_MEDIUM_PRIO
match authorizing-method-priority gt 20
class-map type control subscriber match-all DOT1X_NO_RESP
match method dot1x
match result-type method dot1x agent-not-found
class-map type control subscriber match-all DOT1X_TIMEOUT
match method dot1x
match result-type method dot1x method-timeout
class-map type control subscriber match-all MAB
match method mab
class-map type control subscriber match-all MAB_FAILED
match method mab
match result-type method mab authoritative

policy-map type control subscriber POLICY_Gi1/0/2
event session-started match-all
10 class always do-until-failure
10 authenticate using dot1x priority 10
event authentication-failure match-first
5 class DOT1X_FAILED do-until-failure
10 terminate dot1x
20 authenticate using mab priority 20
10 class DOT1X_NO_RESP do-until-failure
10 terminate dot1x
20 authenticate using mab priority 20
20 class MAB_FAILED do-until-failure
10 terminate mab
20 authentication-restart 60
40 class always do-until-failure
10 terminate dot1x
20 terminate mab
30 authentication-restart 60
event agent-found match-all
10 class always do-until-failure
10 terminate mab
20 authenticate using dot1x priority 10
event authentication-success match-all
10 class always do-until-failure
10 activate service-template DEFAULT_LINKSEC_POLICY_SHOULD_SECURE

policy-map type control subscriber POLICY_Gi1/0/3
event session-started match-all
10 class always do-until-failure
10 authenticate using dot1x priority 10
event authentication-failure match-first
5 class DOT1X_FAILED do-until-failure
10 terminate dot1x
20 authenticate using mab priority 20
10 class DOT1X_NO_RESP do-until-failure
10 terminate dot1x
authenticate using mab priority 20
20 class MAB_FAILED do-until-failure
10 terminate mab
20 authentication-restart 60
40 class always do-until-failure
10 terminate dot1x
20 terminate mab
30 authentication-restart 60
event agent-found match-all
10 class always do-until-failure
10 terminate mab
20 authenticate using dot1x priority 10
event authentication-success match-all
10 class always do-until-failure
10 activate service-template DEFAULT_LINKSEC_POLICY_SHOULD_SECURE
interface FastEthernet0
no ip address
interface GigabitEthernet1/0/1
interface GigabitEthernet1/0/2
description ################GUEST_ACCESS################
switchport mode access
switchport port-security
authentication periodic
access-session host-mode single-host
access-session port-control auto
mab
dot1x pae authenticator
dot1x timeout tx-period 10
service-policy type control subscriber POLICY_Gi1/0/2
interface GigabitEthernet1/0/3
description #############802.1x#############
switchport mode access
switchport port-security
authentication periodic
authentication timer reauthenticate 43200
access-session host-mode single-host
access-session port-control auto
mab
dot1x pae authenticator
dot1x timeout tx-period 10
service-policy type control subscriber POLICY_Gi1/0/3
interface GigabitEthernet1/0/4
  switchport access vlan 60
  switchport mode access
  authentication periodic
  authentication timer reauthenticate server
  access-session port-control auto
dot1x pae authenticator
  spanning-tree portfast
interface GigabitEthernet1/0/5
interface Vlan1
  ip address 10.209.216.96 255.255.255.0
  ip default-gateway 10.209.126.254
  ip http server
  ip http secure-server
  ip access-list extended PERMIT-ALL
    permit ip any any
  ip access-list extended RESTRICT-ALL
    deny udp any any eq domain
    deny ip any host 10.209.126.152
    permit ip any any
  ip radius source-interface Vlan1
!
  snmp-server community public RO
  snmp-server community private RW
!
  radius-server attribute 6 on-for-login-auth
  radius-server attribute 8 include-in-access-req
  radius-server attribute 25 access-request include
  radius-server dead-criteria time 30 tries 3
!
  radius server radiusserver
    address ipv4 10.209.226.152 auth-port 1812 acct-port 1813
    key 12345
no vstack
line con 0
line vty 0 4
  transport input ssh
line vty 5 15
  transport input ssh
end