

Differentiate Authentication Types on ASA Platforms for Policy Decisions on ISE



Document ID: 115962

Contributed by Beau Wallace, Cisco TAC Engineer.
Mar 03, 2013

Contents

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

RADIUS VSA 3076/150 Client-Type Attribute

Configure

- Step 1
- Step 2

Verify

Related Information

Introduction

This document describes how to configure Cisco Identity Services Engine (ISE) to utilize the Client-Type RADIUS Vendor-Specific Attribute (VSA) in order to differentiate multiple types of authentication used on the Cisco Adaptive Security Appliance (ASA). Organizations often require policy decisions based on the way the user is authenticated to the ASA. This also allows you to apply policy to received management connections on the ASA, which allows us to use RADIUS in place of TACACS+, when prudent.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- ISE authentication and authorization.
- ASA authentication methods and RADIUS configuration.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Adaptive Security Appliance Release 8.4.3.
- Cisco Identity Services Engine Release 1.1.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

RADIUS VSA 3076/150 Client-Type Attribute

The Client-Type attribute was added in ASA Release 8.4.3, which allows the ASA to send the type of client that authenticates to the ISE in Access-Request (and Accounting-Request) packets, and allows ISE to make policy decisions based on that attribute. This attribute requires no configuration on the ASA, and is sent automatically.

The Client-Type attribute is currently defined with these integer values:

1. Cisco VPN Client (Internet Key Exchange Version (IKEv1))
2. AnyConnect Client SSL VPN
3. Clientless SSL VPN
4. Cut-Through-Proxy
5. L2TP/IPsec SSL VPN
6. AnyConnect Client IPsec VPN (IKEv2)

Configure

In this section, you are provided the information you need in order to configure ISE to utilize the Client-Type attribute described in this document.

Step 1

Create the Custom Attribute

To add the Client-Type attribute values to ISE, create the attribute and populate its values as a custom dictionary.




1. On ISE, navigate to **Policy > Policy Elements > Dictionaries > System**.
2. Within the **System** dictionaries, navigate to **RADIUS > RADIUS Vendors > Cisco-VPN3000**.
3. The Vendor ID on the screen should be 3076. Click on the **Dictionary Attributes** tab.
 - a. Click **Add** (See Figure 1).

Figure 1: Dictionary Attributes

RADIUS Vendors List > Cisco-VPN3000

Dictionary Dictionary Attributes

Dictionary Attributes

 Add  Edit  Delete

<input type="checkbox"/>	Name	Attribute Numb... ▲	Type	Direction
<input type="checkbox"/>	CVPN3000/ASA/PIX7.x...	1	STRING	BOTH
<input type="checkbox"/>	CVPN3000/ASA/PIX7.x...	10	UINT32	BOTH
<input type="checkbox"/>	CVPN3000/ASA/PIX7.x...	11	UINT32	BOTH
<input type="checkbox"/>	CVPN3000/ASA/PIX7.x...	12	STRING	BOTH
<input type="checkbox"/>	CVPN3000/ASA/PIX7.x...	128	IPV4	BOTH
<input type="checkbox"/>	CVPN3000/ASA/PIX7.x...	129	IPV4	BOTH
<input type="checkbox"/>	CVPN3000/ASA/PIX7.x...	13	UINT32	BOTH
<input type="checkbox"/>	CVPN3000/ASA/PIX7.x...	131	IPV4	BOTH
<input type="checkbox"/>	CVPN3000/ASA/PIX7.x...	132	UINT32	BOTH
<input type="checkbox"/>	CVPN3000/ASA/PIX7.x...	133	STRING	BOTH
<input type="checkbox"/>	CVPN3000/ASA/PIX7.x...	134	IPV4	BOTH
<input type="checkbox"/>	CVPN3000/ASA/PIX7.x...	135	UINT32	BOTH
<input type="checkbox"/>	CVPN3000/ASA/PIX7.x...	136	UINT32	BOTH
<input type="checkbox"/>	CVPN3000/ASA/PIX7.x...	137	UINT32	BOTH
<input type="checkbox"/>	CVPN3000/ASA/PIX7.x...	15	STRING	BOTH
<input type="checkbox"/>	CVPN3000/ASA/PIX7x-...	150	UINT32	BOTH

b. Populate the fields in the custom RADIUS Vendor Attribute form as seen in Figure 2.

Figure 2: RADIUS Vendor Attribute

▼ RADIUS Vendor Attribute

* Attribute Name

Description

* Internal Name

* Data Type

* Direction

* ID (0-255)

Does this attribute support Tagging

Is this a attribute allowed multiple times in Authz Profile

Allowed Values

+ Add - Delete

<input type="checkbox"/>	Name	Value	isDefault
<input type="checkbox"/>	Cisco VPN Client (IKEv1)	1	⊗
<input type="checkbox"/>	AnyConnect Client SSL...	2	⊗
<input type="checkbox"/>	Clientless SSL VPN	3	⊗
<input type="checkbox"/>	Cut-Through-Proxy	4	⊗
<input type="checkbox"/>	L2TP/IPsec SSL VPN	5	⊗
<input type="checkbox"/>	AnyConnect Client IPse...	6	⊗

c. Click the **Save** button at the bottom of the screen.

Step 2

Add Client-Type Attribute

In order to utilize the new attribute for policy decisions, add the attribute to an authorization rule in the conditions section.

1. In ISE, navigate to **Policy > Authorization**.
2. Create a new rule or modify an existing policy.
3. In the conditions section of the rule, expand the conditions pane and select either **Create a New Condition** (for a new rule) or **Add Attribute/Value** (for a pre-existing rule).
4. In the **Select Attribute** field, navigate to **Cisco-VPN3000 > Cisco-VPN3000:CVPN3000/ASA/PIX7x-Client-Type**.
5. Choose the appropriate operator (**Equals** or **Not Equals**) for your environment.
6. Choose the **Authentication type** you wish to match.
7. Assign an **Authorization Result** appropriate to your policy.
8. Click **Done**.
9. Click **Save**.

After the rule is created, the Authorization Condition should look similar to the example in Figure 3.

Figure 3: Authorization Condition Example

```
if Cisco-VPN3000:CVPN3000/ASA/PIX7x-Client-Type EQUALS Cut-Through-Proxy
```

Verify

In order to verify the Client-Type attribute is in use, examine the authentications from the ASA in ISE.

1. Navigate to **Operations > Authentications**
2. Click the **Details** button for the authentication from the ASA.
3. Scroll down to **Other Attributes** and look for **CVPN3000/ASA/PIX7x-Client-Type=** (See Figure 4)

Figure 4: Other Attributes Details

```
ConfigVersionId=4, DestinationPort=1812, Protocol=Radius, CVPN3000/ASA/PIX7x-Client-  
Type=4, CPMSessionID=0e24970b0000000051000B89, EndPointMACAddress=00-55-44-33-22-11, Device Type=Device  
Type#All Device Types, Location=Location#All Locations, Device IP Address=172.18.254.150
```

4. The **Other Attributes** field should indicate the received value for the authentication. The rule should match the policy defined in step 2 of the configuration section.

Related Information

- [Cisco Identity Services Engine](#)
- [Cisco Adaptive Security Appliance 5500 Series Next Generation Firewalls](#)
- [Technical Support & Documentation – Cisco Systems](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2014 – 2015 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Mar 03, 2013

Document ID: 115962
