Diferenciación de tipos de autenticación en plataformas ASA para decisiones de políticas en ISE

Contenido

Introducción

Este documento describe cómo configurar Cisco Identity Services Engine (ISE) para utilizar el atributo específico del proveedor RADIUS (VSA) de tipo de cliente para diferenciar varios tipos de autenticación utilizados en Cisco Adaptive Security Appliance (ASA). Las organizaciones a menudo requieren decisiones de políticas basadas en la forma en que el usuario se autentica en el ASA. Esto también le permite aplicar políticas a las conexiones de administración recibidas en el ASA, lo que nos permite utilizar RADIUS en lugar de TACACS+, cuando sea prudente.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Autenticación y autorización ISE.
- Métodos de autenticación ASA y configuración RADIUS.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

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

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Atributo RADIUS VSA 3076/150 Client-Type

El atributo Client-Type se agregó en la versión 8.4.3 de ASA, que permite al ASA enviar el tipo de cliente que se autentica a ISE en los paquetes Access-Request (y Accounting-Request), y permite a ISE tomar decisiones de políticas basadas en ese atributo. Este atributo no requiere configuración en el ASA y se envía automáticamente.

El atributo Client-Type se define actualmente con estos valores enteros:

1. Cliente VPN de Cisco (versión de intercambio de claves de Internet (IKEv1)
2. VPN SSL de AnyConnect Client
3. VPN SSL sin cliente
4. Cut-Through-Proxy
5. VPN SSL L2TP/IPsec
6. VPN IPsec de AnyConnect Client (IKEv2)

Configurar

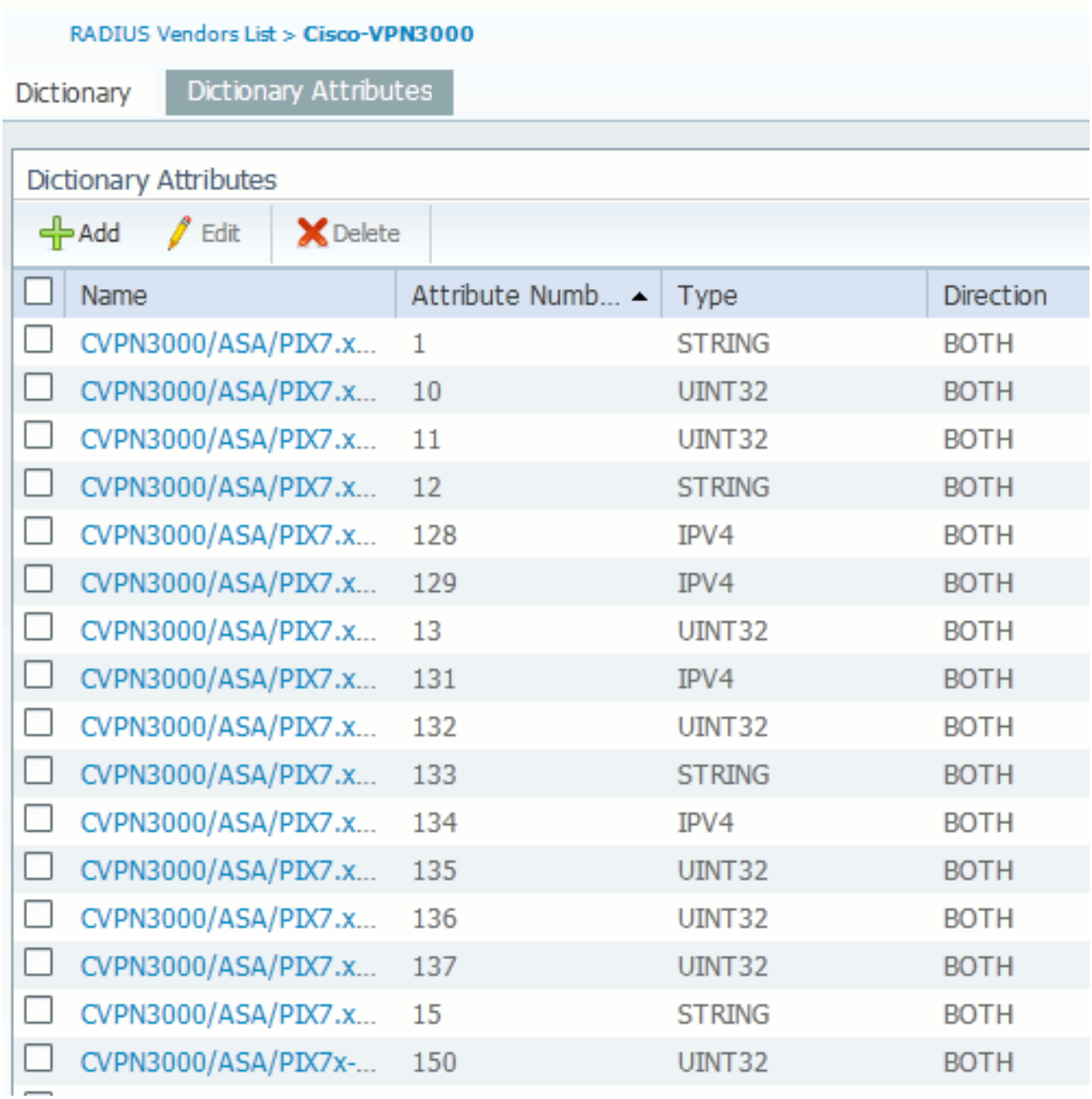
En esta sección, se le proporciona la información que necesita para configurar ISE para utilizar el atributo Client-Type descrito en este documento.

Paso 1

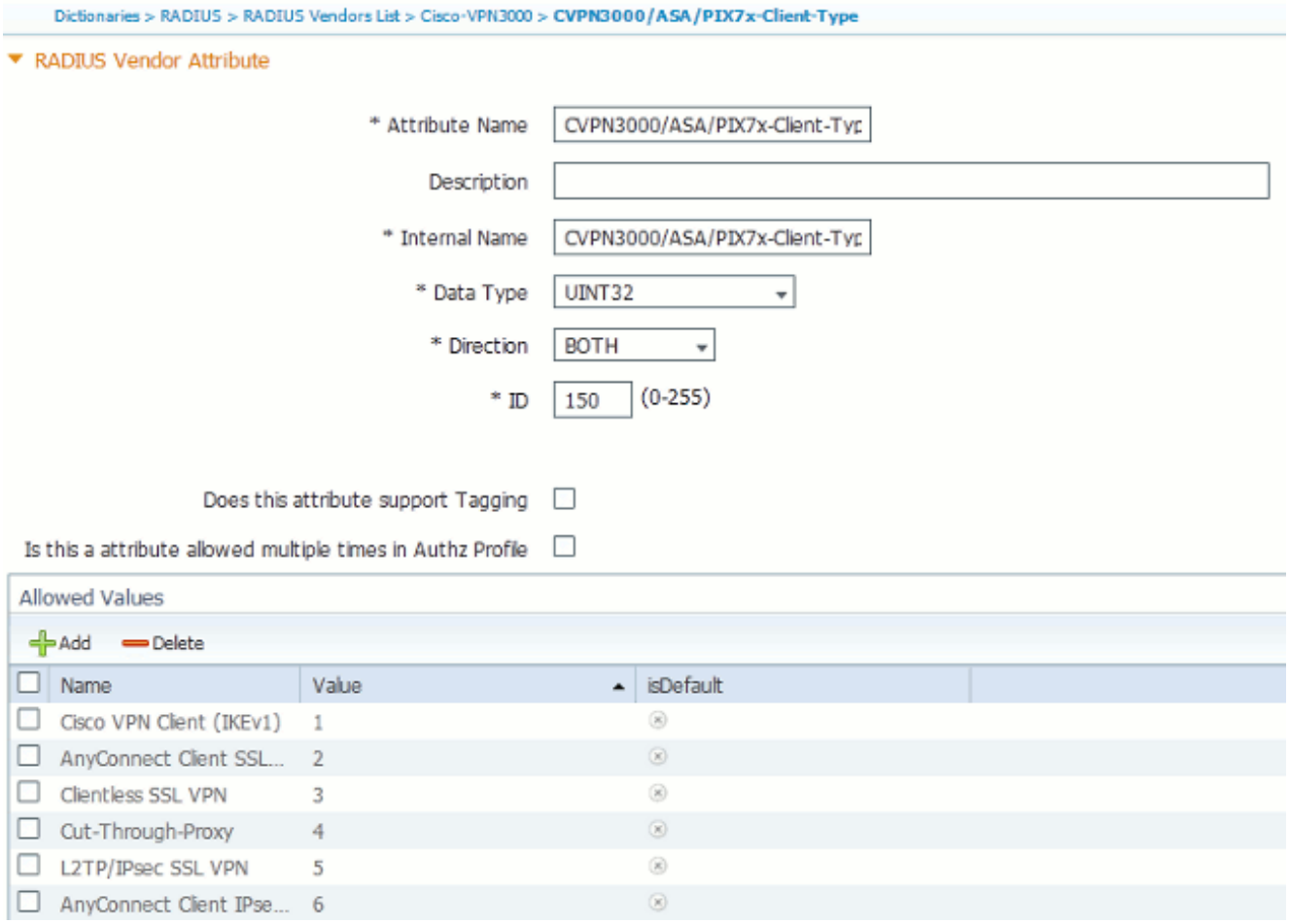
Crear el atributo personalizado

Para agregar los valores de atributo Client-Type a ISE, cree el atributo y rellene sus valores como diccionario personalizado.

1. En ISE, navegue hasta **Policy** > **Policy Elements** > **Dictionaries** > **System**.
2. Dentro de los diccionarios **del sistema**, navegue hasta **RADIUS** > **RADIUS** Vendors **>** Cisco-VPN3000.
3. La ID del proveedor en la pantalla debe ser 3076. Haga clic en la pestaña **Atributos del diccionario**.Haga clic en **Agregar** (consulte la Figura 1).**Figura 1: Atributos del diccionario**



Rellene los campos del formulario RADIUS Vendor Attribute personalizado, como se muestra en la Figura 2.**Figura 2: Atributo del proveedor RADIUS**



Haga clic en el botón **Guardar** de la parte inferior de la pantalla.

Paso 2

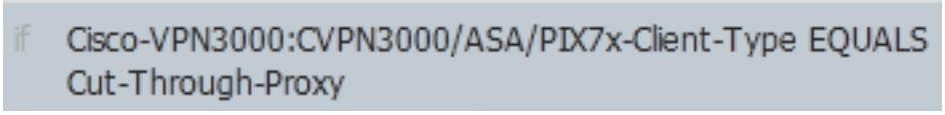
Agregar atributo Client-Type

Para utilizar el nuevo atributo para las decisiones de política, agregue el atributo a una regla de autorización en la sección de condiciones.

1. En ISE, navegue hasta **Policy > Authorization**.
2. Cree una nueva regla o modifique una política existente.
3. En la sección Condiciones de la regla, expanda el panel Condiciones y seleccione **Crear una nueva condición** (para una nueva regla) o **Agregar atributo/valor** (para una regla anterior).
4. En el campo **Select Attribute**, navegue hasta **Cisco-VPN3000 > Cisco-VPN3000:CVPN3000/ASA/PIX7x-Client-Type**.
5. Elija el operador adecuado (**Igual** o **No igual**) para su entorno.
6. Elija el **tipo de autenticación** que desea que coincida.
7. Asigne un **resultado de autorización** adecuado a su política.
8. Haga clic en Done (Listo).
9. Click **Save.**

Después de crear la regla, la condición de autorización debe ser similar al ejemplo de la figura 3.

Figura 3: Ejemplo de Condición de Autorización



Verificación

Para verificar que el atributo Client-Type está en uso, examine las autenticaciones del ASA en ISE.

1. Vaya a **Operaciones > Autenticaciones**
2. Haga clic en el botón **Detalles** para la autenticación desde el ASA.
3. Desplácese hacia abajo hasta **Otros atributos** y busque **CVPN3000/ASA/PIX7x-Client-Type=** (consulte la figura 4)**Figura 4: Detalles de otros atributos**

   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. El campo **Otros atributos** debe indicar el valor recibido para la autenticación. La regla debe coincidir con la política definida en el paso 2 de la sección de configuración.

Información Relacionada

- Cisco Identity Services Engine
- Firewalls de última generación Cisco Adaptive Security Appliance serie 5500
- Soporte Técnico y Documentación - Cisco Systems