

Differenziazione dei tipi di autenticazione sulle piattaforme ASA per le decisioni sulle policy ISE

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Attributo tipo client RADIUS VSA 3076/150](#)

[Configurazione](#)

[Passaggio 1](#)

[Passaggio 2](#)

[Verifica](#)

[Informazioni correlate](#)

[Introduzione](#)

In questo documento viene descritto come configurare Cisco Identity Services Engine (ISE) in modo che utilizzi l'attributo specifico del fornitore RADIUS (VSA) del tipo client per differenziare più tipi di autenticazione utilizzati sulle appliance Cisco Adaptive Security (ASA). Le organizzazioni spesso richiedono decisioni sulle policy basate sul modo in cui l'utente viene autenticato sull'appliance ASA. Ciò permette anche di applicare la policy alle connessioni di gestione ricevute sull'appliance ASA, in modo da poter usare RADIUS al posto di TACACS+, quando necessario.

[Prerequisiti](#)

[Requisiti](#)

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Autenticazione e autorizzazione ISE.
- Metodi di autenticazione ASA e configurazione RADIUS.

[Componenti usati](#)

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Adaptive Security Appliance release 8.4.3.1
- Cisco Identity Services Engine release 1.1.1

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento [Cisco sulle convenzioni nei suggerimenti tecnici](#).

Attributo tipo client RADIUS VSA 3076/150

L'attributo Client-Type è stato aggiunto in ASA versione 8.4.3, che consente all'ASA di inviare il tipo di client che si autentica all'ISE nei pacchetti Access-Request (e Accounting-Request), e all'ISE di prendere decisioni sui criteri basati su tale attributo. Questo attributo non richiede alcuna configurazione sull'appliance ASA e viene inviato automaticamente.

L'attributo Client-Type è attualmente definito con i seguenti valori interi:

1. Cisco VPN Client (Internet Key Exchange versione (IKEv1))
2. AnyConnect Client e SSL VPN
3. VPN SSL senza client
4. Cut-through-proxy
5. VPN SSL L2TP/IPsec
6. VPN IPsec client AnyConnect (IKEv2)

Configurazione

In questa sezione vengono fornite le informazioni necessarie per configurare ISE in modo che utilizzi l'attributo Client-Type descritto nel presente documento.

Passaggio 1

Creare l'attributo personalizzato




Per aggiungere i valori dell'attributo Client-Type a ISE, creare l'attributo e inserirne i valori come dizionario personalizzato.

1. Ad ISE, selezionare **Policy > Policy Elements > Dictionaries > System**.
2. Nei dizionari del **sistema**, selezionare **RADIUS > RADIUS Vendors > Cisco-VPN3000**.
3. L'ID fornitore visualizzato sullo schermo dovrebbe essere 3076. Fare clic sulla scheda **Attributi dizionario**. Fare clic su **Add** (vedere la Figura 1). **Figura 1: Attributi dizionario**

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

Popolare i campi nel modulo degli attributi dei fornitori RADIUS personalizzato, come mostrato nella Figura 2. **Figura 2: Attributo fornitore RADIUS**

▼ 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	⊗

Fare clic sul pulsante **Salva** nella parte inferiore della schermata.

Passaggio 2

Aggiungi attributo di tipo client

Per utilizzare il nuovo attributo per le decisioni relative ai criteri, aggiungerlo a una regola di autorizzazione nella sezione Condizioni.

1. Ad ISE, selezionare **Policy > Authorization** (Policy > Autorizzazione).
2. Creare una nuova regola o modificare un criterio esistente.
3. Nella sezione Condizioni della regola, espandere il riquadro Condizioni e selezionare **Crea una nuova condizione** (per una nuova regola) o **Aggiungi attributo/valore** (per una regola preesistente).
4. Nel campo **Select Attribute** (Seleziona attributo), selezionare **Cisco-VPN3000 > Cisco-VPN3000:CVPN3000/ASA/PIX7x-Client-Type**.
5. Scegliere l'operatore appropriato (**Uguale** o **Diverso da**) per l'ambiente.
6. Scegliere il **tipo di autenticazione** che si desidera associare.
7. Assegnare un **risultato di autorizzazione** appropriato al criterio.
8. Selezionate **Fatto (Done)**.
9. Fare clic su **Salva**.

Dopo la creazione della regola, la condizione di autorizzazione dovrebbe essere simile a quella illustrata nella Figura 3.

Figura 3: Esempio di condizione di autorizzazione

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

Verifica

Per verificare che l'attributo Client-Type sia in uso, esaminare le autenticazioni dell'ASA in ISE.

1. Passare a **Operazioni > Autenticazioni**
2. Fare clic sul pulsante **Details** (Dettagli) per autenticare l'appliance ASA.
3. Scorrere fino ad **Altri attributi** e cercare **CVPN3000/ASA/PIX7x-Client-Type=** (vedere Figura 4)**Figura 4: Dettagli altri attributi**

```
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. Il campo **Altri attributi** deve indicare il valore ricevuto per l'autenticazione. La regola deve corrispondere al criterio definito nel passaggio 2 della sezione di configurazione.

Informazioni correlate

- [Cisco Identity Services Engine](#)
- [Cisco Adaptive Security Appliance serie 5500 Next-Generation Firewall](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)