Configurazione dinamica FlexVPN con elenchi di attributi AAA locali

Sommario

Introduzione

In questo esempio di configurazione viene illustrato come utilizzare l'elenco degli attributi Autenticazione, Autorizzazione e Accounting (AAA) locale per eseguire una configurazione dinamica e potenzialmente avanzata senza utilizzare il server RADIUS (Remote Authentication Dial-In User Service) esterno.

Ciò è auspicabile in alcuni scenari, in particolare quando è necessario eseguire un test o una distribuzione rapida. Tali implementazioni sono in genere laboratori di prova, nuovi test di installazione o risoluzione dei problemi.

La configurazione dinamica è importante sul lato concentratore/hub, in cui è necessario applicare criteri o attributi diversi per utente, cliente e sessione.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano, tra l'altro, su queste versioni software e hardware. L'elenco non descrive i requisiti minimi, ma riflette lo stato del dispositivo durante la fase di prova di questa funzione.

Hardware

- Aggregation Services Router (ASR) - ASR 1001 - chiamato "bsns-asr1001-4"
- Integrated Services Router Generation 2 (ISR G2) - 3925e - chiamato "bsns-3925e-1"
- Integrated Services Router Generation 2 (ISR G2) - 3945e - chiamato "bsns-3945e-1"

Software

- Cisco IOS XE release 3.8 - 15.3(1)S
- Software Cisco IOS® versione 15.2(4)M1 e 15.2(4)M2

Licenze

- Sui router ASR le licenze **adventure** e **ipsec** sono abilitate.
- Sui router ISR G2 sono abilitate le licenze delle funzionalità **ipbasek9**, **securityk9** e **hseck9**.

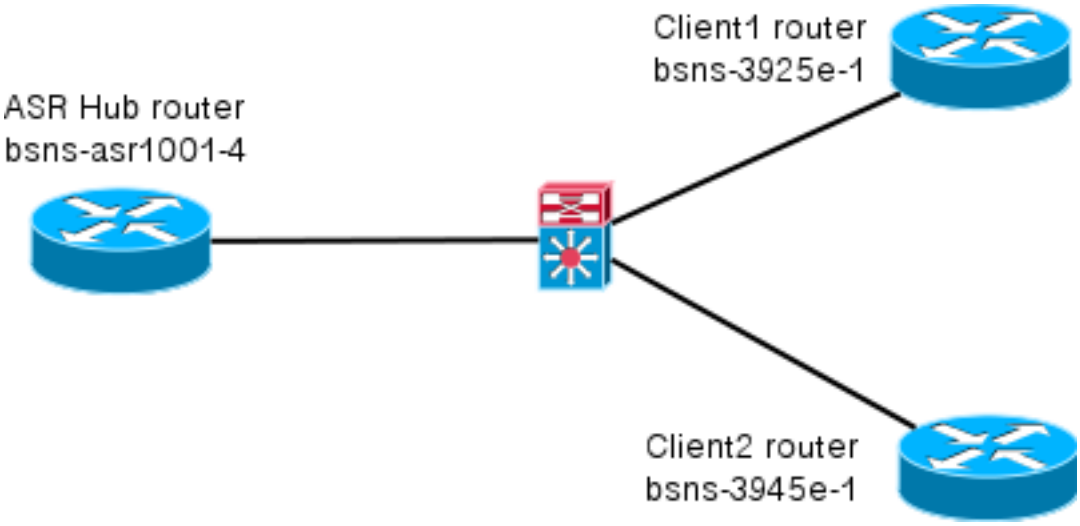
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Topologia

La topologia utilizzata in questo esercizio è di base. Vengono utilizzati un router hub (ASR) e due router spoke (ISR), che simulano i client.



Configurazioni

Le configurazioni di questo documento hanno lo scopo di mostrare un'impostazione di base, con i valori predefiniti più intelligenti possibili. Per i consigli di Cisco sulla crittografia, visitare la pagina Next-Generation Encryption su cisco.com.

Configurazione spoke

Come accennato in precedenza, la maggior parte delle operazioni descritte in questa documentazione vengono eseguite sull'hub. La configurazione dello spoke è qui per riferimento. In questa configurazione, l'identità tra Client1 e Client2 è l'unica modifica (visualizzata in grassetto).

```
aaa new-model
aaa authorization network default local
aaa session-id common

crypto ikev2 keyring Flex_key
 peer Spokes
 address 0.0.0.0 0.0.0.0
 pre-shared-key local cisco
 pre-shared-key remote cisco
 !!
crypto ikev2 profile Flex_IKEv2
 match identity remote address 0.0.0.0
 identity local email Client1@cisco.com
 authentication remote pre-share
 authentication local pre-share
 keyring local Flex_key
 aaa authorization group psk list default default
 virtual-template 1

crypto logging session

crypto ipsec profile default
 set ikev2-profile Flex_IKEv2

interface Tunnel1
 ip address negotiated
 ip mtu 1400
 ip nhrp network-id 2
 ip nhrp shortcut virtual-template 1
```

```
 ip nhrp redirect
 ip tcp adjust-mss 1360
 tunnel source GigabitEthernet0/0
 tunnel destination 172.25.1.1
 tunnel path-mtu-discovery
 tunnel protection ipsec profile default

interface Virtual-Template1 type tunnel
 ip unnumbered Tunnel1
 ip mtu 1400
 ip nhrp network-id 2
 ip nhrp shortcut virtual-template 1
 ip nhrp redirect
 ip tcp adjust-mss 1360
 tunnel path-mtu-discovery
 tunnel protection ipsec profile default
```

Configurazione hub

La configurazione dell'hub è divisa in due parti:

1. **Configurazione della connettività di base**, che indica la configurazione necessaria per la connettività di base.
2. **Configurazione estesa**, che descrive le modifiche alla configurazione necessarie per dimostrare come un amministratore può utilizzare l'elenco degli attributi AAA per eseguire modifiche alla configurazione per utente o per sessione.

Configurazione connettività di base

Questa configurazione è solo a scopo di riferimento e non deve essere ottimale, ma solo funzionale.

Il limite massimo di questa configurazione è l'utilizzo della chiave già condivisa (PSK) come metodo di autenticazione. Cisco consiglia di utilizzare i certificati quando applicabile.

```
aaa new-model
aaa authorization network default local

aaa session-id common
crypto ikev2 authorization policy default
 pool FlexSpokes
 route set interface

crypto ikev2 keyring Flex_key
 peer Spokes
 address 0.0.0.0 0.0.0.0
 pre-shared-key local cisco
 pre-shared-key remote cisco
 !!
 peer Client1
 identity email Client1@cisco.com
 pre-shared-key cisco
 !!
 peer Client2
 identity email Client2@cisco.com
 pre-shared-key cisco

crypto ikev2 profile Flex_IKEv2
```

```
 match fvrf any
 match identity remote address 0.0.0.0
 match identity remote email domain cisco.com
 authentication remote pre-share
 authentication local pre-share
 keyring local Flex_key
 aaa authorization group psk list default default
 virtual-template 1

no crypto ikev2 http-url cert

crypto logging session

crypto ipsec profile default
 set ikev2-profile Flex_IKEv2

interface Virtual-Template1 type tunnel
 vrf forwarding IVRF
 ip unnumbered Loopback100
 ip mtu 1400
 ip nhrp network-id 2
 ip nhrp redirect
 ip tcp adjust-mss 1360
 tunnel path-mtu-discovery
 tunnel vrf INTERNET
 tunnel protection ipsec profile default
```

Configurazione estesa

Per assegnare gli attributi AAA a una determinata sessione, è necessario eseguire alcune operazioni. Nell'esempio viene mostrato il lavoro completo per client1; viene quindi illustrato come aggiungere un altro client/utente.

Configurazione hub esteso per Client1

1. Definire un elenco di attributi AAA.
   ```
   aaa attribute list Client1
    attribute type interface-config "ip mtu 1300" protocol ip
    attribute type interface-config "service-policy output TEST" protocol ip
   ```
   Nota: l'entità assegnata tramite gli attributi deve esistere localmente. In questo caso, la **mappa dei criteri** è stata configurata in precedenza.
   ```
   policy-map TEST
    class class-default
    shape average 60000
   ```
2. Assegnare un elenco di attributi AAA a un **criterio di autorizzazione.**
   ```
   crypto ikev2 authorization policy Client1
    pool FlexSpokes
    aaa attribute list Client1
    route set interface
   ```
3. Verificare che il nuovo criterio sia utilizzato dai client che si connettono. In questo caso, estrarre la parte relativa al **nome utente** dell'identità inviata dai client. I client devono utilizzare un indirizzo e-mail di ClientX@cisco.com (X è 1 o 2, a seconda del client). Il **gestore** suddivide l'indirizzo di posta elettronica in nome utente e dominio e ne utilizza solo uno (in questo caso nome utente) per scegliere il nome del criterio di autorizzazione.
   ```
   crypto ikev2 name-mangler GET_NAME
    email username

   crypto ikev2 profile Flex_IKEv2
   ```

```
aaa authorization group psk list default name-mangler GET_NAME
```

Quando il client1 è operativo, l'aggiunta del client2 è relativamente semplice.

Configurazione hub esteso per Client2

Assicurarsi che esistano un criterio e, se necessario, una serie separata di attributi.

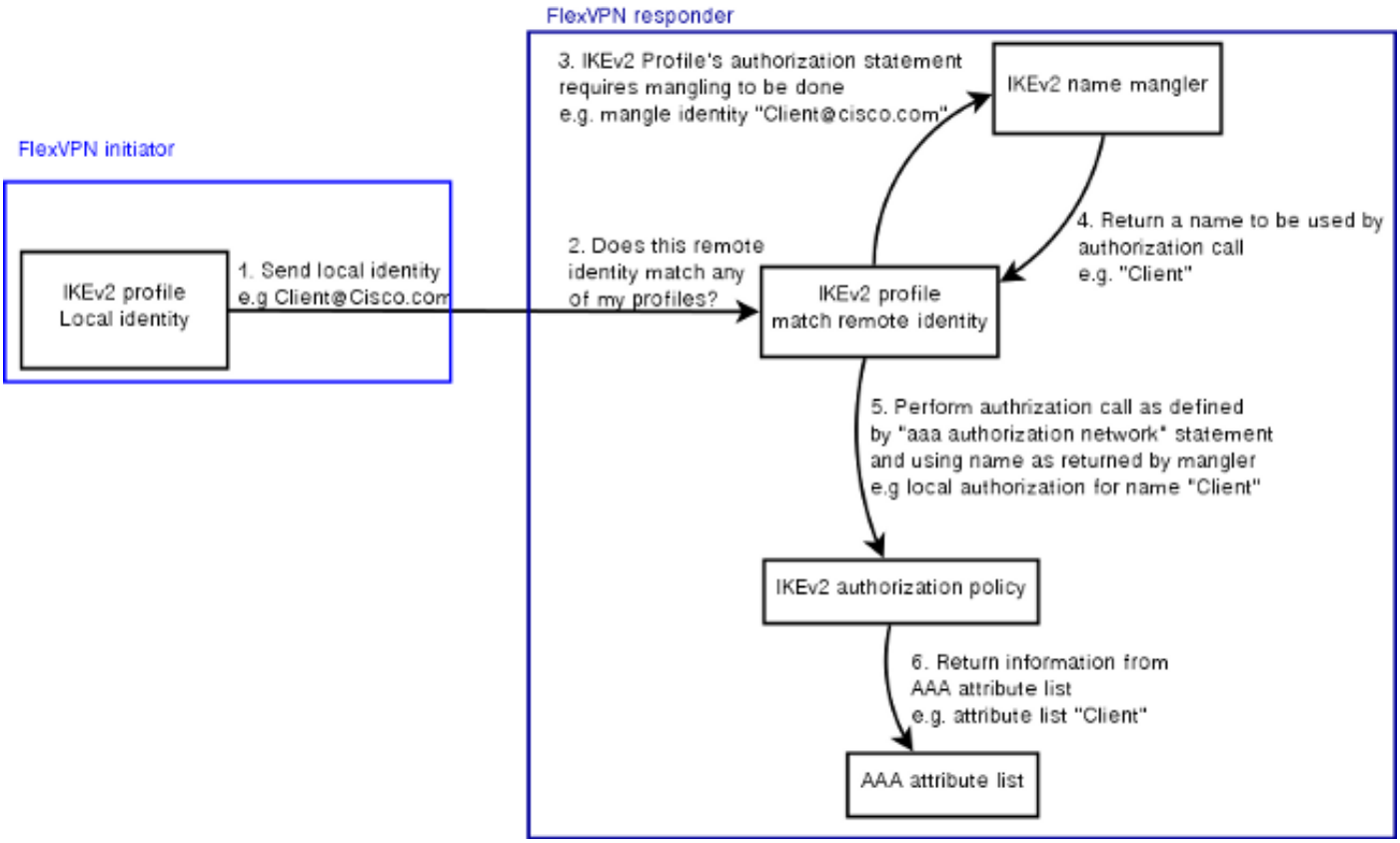
```
aaa attribute list Client2
 attribute type interface-config "ip tcp adjust-mss 1200" protocol ip
 attribute type interface-config "ip access-group 133 in" protocol ip

crypto ikev2 authorization policy Client2
 pool FlexSpokes
 aaa attribute list Client2
 route set interface
```

Nell'esempio, vengono applicate un'impostazione aggiornata relativa alle dimensioni massime del segmento (MSS) e un elenco degli accessi in entrata da utilizzare per il client. Altre impostazioni possono essere scelte facilmente. Una tipica impostazione consiste nell'assegnare VRF (Virtual Routing and Forwarding) differenti per client diversi. Come accennato in precedenza, qualsiasi entità assegnata all'elenco attributi, ad esempio l'elenco degli accessi 133 in questo scenario, deve esistere già nella configurazione.

Panoramica del processo

Nella figura viene illustrato l'ordine delle operazioni quando l'autorizzazione AAA viene elaborata tramite il profilo Internet Key Exchange versione 2 (IKEv2) e vengono fornite informazioni specifiche per questo esempio di configurazione.



Verifica

Questa sezione illustra come verificare che le impostazioni precedentemente assegnate siano state applicate ai client.

Cliente1

Di seguito sono riportati i comandi che verificano che le impostazioni MTU (Maximum Transmission Units) e i criteri del servizio siano stati applicati.

```
bsns-asr1001-4#show cef int virtual-access 1
(...)
 Hardware idb is Virtual-Access1
 Fast switching type 14, interface type 21
 IP CEF switching enabled
 IP CEF switching turbo vector
 IP Null turbo vector
 VPN Forwarding table "IVRF"
 IP prefix lookup IPv4 mtrie 8-8-8-8 optimized
 Tunnel VPN Forwarding table "INTERNET" (tableid 2)
 Input fast flags 0x0, Output fast flags 0x4000
 ifindex 16(16)
 Slot unknown (4294967295) Slot unit 1 VC -1
 IP MTU 1300
 Real output interface is GigabitEthernet0/0/0

bsns-asr1001-4#show policy-map interface virtual-access1
 Virtual-Access1

Service-policy output: TEST

Class-map: class-default (match-any)
 5 packets, 620 bytes
 5 minute offered rate 0000 bps, drop rate 0000 bps
 Match: any
 Queueing
 queue limit 64 packets
 (queue depth/total drops/no-buffer drops) 0/0/0
 (pkts output/bytes output) 5/910
 shape (average) cir 60000, bc 240, be 240
 target shape rate 60000
```

Cliente2

Di seguito sono riportati i comandi che verificano che le impostazioni MSS siano state push e che l'elenco degli accessi 133 sia stato applicato anche come filtro in entrata sull'interfaccia di accesso virtuale equivalente.

```
bsns-asr1001-4#show cef int virtual-access 2
Virtual-Access2 is up (if_number 18)
 Corresponding hwidb fast_if_number 18
 Corresponding hwidb firstsw->if_number 18
 Internet address is 0.0.0.0/0
 Unnumbered interface. Using address of Loopback100 (192.168.1.1)
 ICMP redirects are never sent
```

```
 Per packet load-sharing is disabled
 IP unicast RPF check is disabled
 Input features: Access List, TCP Adjust MSS
 (...)

bsns-asr1001-4#show ip interface virtual-access2
Virtual-Access2 is up, line protocol is up
 Interface is unnumbered. Using address of Loopback100 (192.168.1.1)
 Broadcast address is 255.255.255.255
 MTU is 1400 bytes
 Helper address is not set
 Directed broadcast forwarding is disabled
 Outgoing access list is not set
 Inbound access list is 133, default is not set
(...)
```

Debug

Il debug deve essere eseguito su due blocchi principali. Questa funzione è utile quando è necessario aprire una richiesta TAC e iniziare a lavorare più rapidamente.

Debug IKEv2

Iniziare con questo comando di debug principale:

```
debug crypto ikev2 [internal|packet]
```

Immettere quindi i seguenti comandi:

```
show crypto ikev2 sa
show crypto ipsec sa peer a.b.c.d
```

Assegnazione attributi debug AAA

Se si desidera eseguire il debug dell'assegnazione degli attributi AAA, questi debug possono essere utili.

```
debug aaa authorization
debug aaa attr
debug aaa proto local
```

Conclusioni

In questo documento viene illustrato come utilizzare l'elenco degli attributi AAA per consentire una maggiore flessibilità nelle distribuzioni FlexVPN in cui il server RADIUS potrebbe non essere disponibile o non essere desiderato. L'elenco degli attributi AAA offre opzioni di configurazione aggiunte per sessione e per gruppo, se necessario.

Informazioni correlate

- Guida alla configurazione di FlexVPN e Internet Key Exchange versione 2, Cisco IOS release

15M&T

- RADIUS (Remote Authentication Dial-In User Services)
- RFC (Requests for Comments)
- Negoziazione IPSec/protocolli IKE
- Documentazione e supporto tecnico – Cisco Systems