Dynamische FlexVPN-Konfiguration mit lokalen AAA-Attributlisten

Inhalt

Einführung

In diesem Konfigurationsbeispiel wird veranschaulicht, wie die Attributliste für lokale Authentifizierung, Autorisierung und Abrechnung (AAA) verwendet wird, um eine dynamische und möglicherweise erweiterte Konfiguration ohne Verwendung eines RADIUS-Servers (Remote Authentication Dial-In User Service) durchzuführen.

Dies ist in bestimmten Szenarien erwünscht, insbesondere wenn eine schnelle Bereitstellung oder ein schneller Test erforderlich ist. Bei solchen Bereitstellungen handelt es sich in der Regel um Proof-of-Concept-Labs, neue Bereitstellungstests oder die Fehlerbehebung.

Dynamische Konfiguration ist wichtig auf der Konzentrator-/Hub-Seite, auf der unterschiedliche Richtlinien oder Attribute pro Benutzer, pro Kunde und pro Sitzung angewendet werden sollten.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf, aber nicht beschränkt auf diese Software- und Hardwareversionen. In dieser Liste werden die Mindestanforderungen nicht beschrieben, sondern der Status des Geräts während der gesamten Testphase dieser Funktion wiedergegeben.

Hardware

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

Software

- Cisco IOS XE Version 3.8 - 15.3(1)S
- Cisco IOS® Softwareversion 15.2(4)M1 und 15.2(4)M2

Lizenzen

- Auf ASR-Routern sind die Funktionslizenzen **für** Unternehmen und **IPSec** aktiviert.
- Für ISR G2-Router sind die Funktionslizenzen **ipbasek9**, **securityk9** und **hseck9** aktiviert.

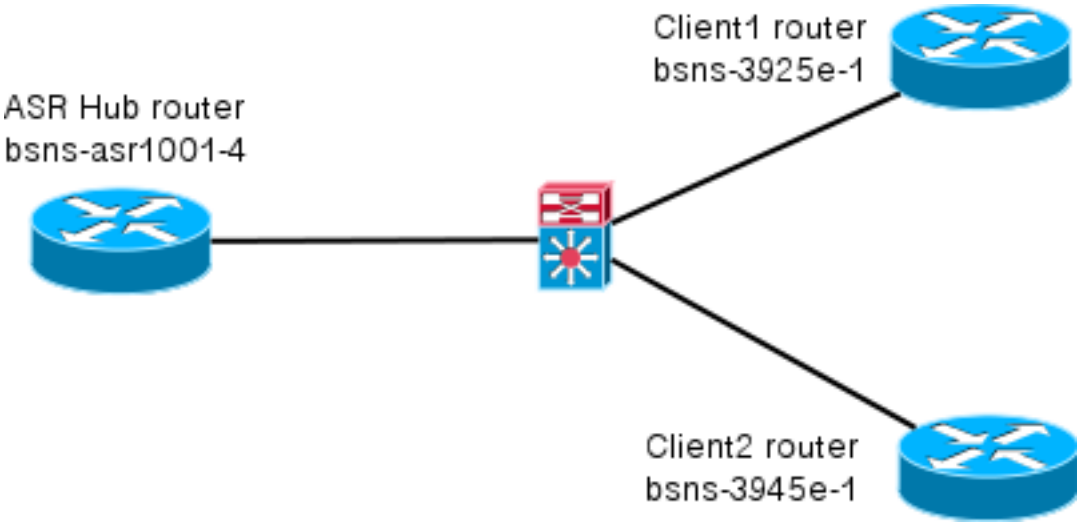
Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Topologie

Die in dieser Übung verwendete Topologie ist einfach. Es werden ein Hub-Router (ASR) und zwei Spoke-Router (ISR) verwendet, die Clients simulieren.



Konfigurationen

Die Konfigurationen in diesem Dokument sollen eine grundlegende Konfiguration mit möglichst intelligenten Standardeinstellungen anzeigen. Empfehlungen von Cisco zur Verschlüsselung finden Sie auf der Seite Verschlüsselung der nächsten Generation auf cisco.com.

Spoke-Konfiguration

Wie bereits erwähnt, werden die meisten Aktionen in dieser Dokumentation auf dem Hub ausgeführt. Die Spoke-Konfiguration dient als Referenz. Beachten Sie in dieser Konfiguration, dass nur die Identität zwischen Client1 und Client2 (fett dargestellt) geändert wird.

```
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
```

Hub-Konfiguration

Die Hub-Konfiguration ist in zwei Teile unterteilt:

1. **Grundlegende Konnektivitätskonfiguration**, in der die für die grundlegende Konnektivität erforderliche Konfiguration beschrieben wird.
2. **Erweiterte Konfiguration**, in der die erforderlichen Konfigurationsänderungen erläutert werden, um zu veranschaulichen, wie ein Administrator mithilfe der AAA-Attributliste Konfigurationsänderungen pro Benutzer oder pro Sitzung vornehmen kann.

Grundlegende Verbindungskonfiguration

Diese Konfiguration dient nur als Referenz und ist nicht optimal, sondern nur funktional.

Die größte Einschränkung dieser Konfiguration ist die Verwendung von Pre-Shared Key (PSK) als Authentifizierungsmethode. Cisco empfiehlt die Verwendung von Zertifikaten, sofern zutreffend.

```
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
```

Erweiterte Konfiguration

Es sind einige Dinge erforderlich, um AAA-Attribute einer bestimmten Sitzung zuzuweisen. Dieses Beispiel zeigt die vollständige Arbeit für client1. zeigt dann, wie ein anderer Client/Benutzer hinzugefügt wird.

Erweiterte Hub-Konfiguration für Client1

1. Definieren einer AAA-Attributliste.
   ```
   aaa attribute list Client1
    attribute type interface-config "ip mtu 1300" protocol ip
    attribute type interface-config "service-policy output TEST" protocol ip
   ```
   Hinweis: Beachten Sie, dass die mithilfe von Attributen zugewiesene Entität lokal vorhanden sein muss. In diesem Fall wurde **die Richtlinienzuweisung** zuvor konfiguriert.
   ```
   policy-map TEST
    class class-default
    shape average 60000
   ```
2. Weisen Sie einer **Autorisierungsrichtlinie** eine AAA-Attributliste zu.
   ```
   crypto ikev2 authorization policy Client1
    pool FlexSpokes
    aaa attribute list Client1
    route set interface
   ```
3. Stellen Sie sicher, dass diese neue Richtlinie von den Clients verwendet wird, die eine Verbindung herstellen. In diesem Fall extrahieren Sie den **Benutzernamen** Teil der Identität, die von den Clients gesendet wird. Die Clients sollten eine E-Mail-Adresse von ClientX@cisco.com verwenden (X ist 1 oder 2, abhängig vom Client). Der **Mangler** teilt die E-Mail-Adresse in den Benutzernamen und den Domänennamen auf und verwendet nur einen davon (in diesem Fall den Benutzernamen), um den Namen der Autorisierungsrichtlinie auszuwählen.
   ```
   crypto ikev2 name-mangler GET_NAME
    email username
   ```

```
crypto ikev2 profile Flex_IKEv2
 aaa authorization group psk list default name-mangler GET_NAME
```

Wenn client1 betriebsbereit ist, kann Client2 relativ einfach hinzugefügt werden.

Erweiterte Hub-Konfiguration für Client2

Stellen Sie sicher, dass eine Richtlinie und ggf. ein separater Satz von Attributen vorhanden sind.

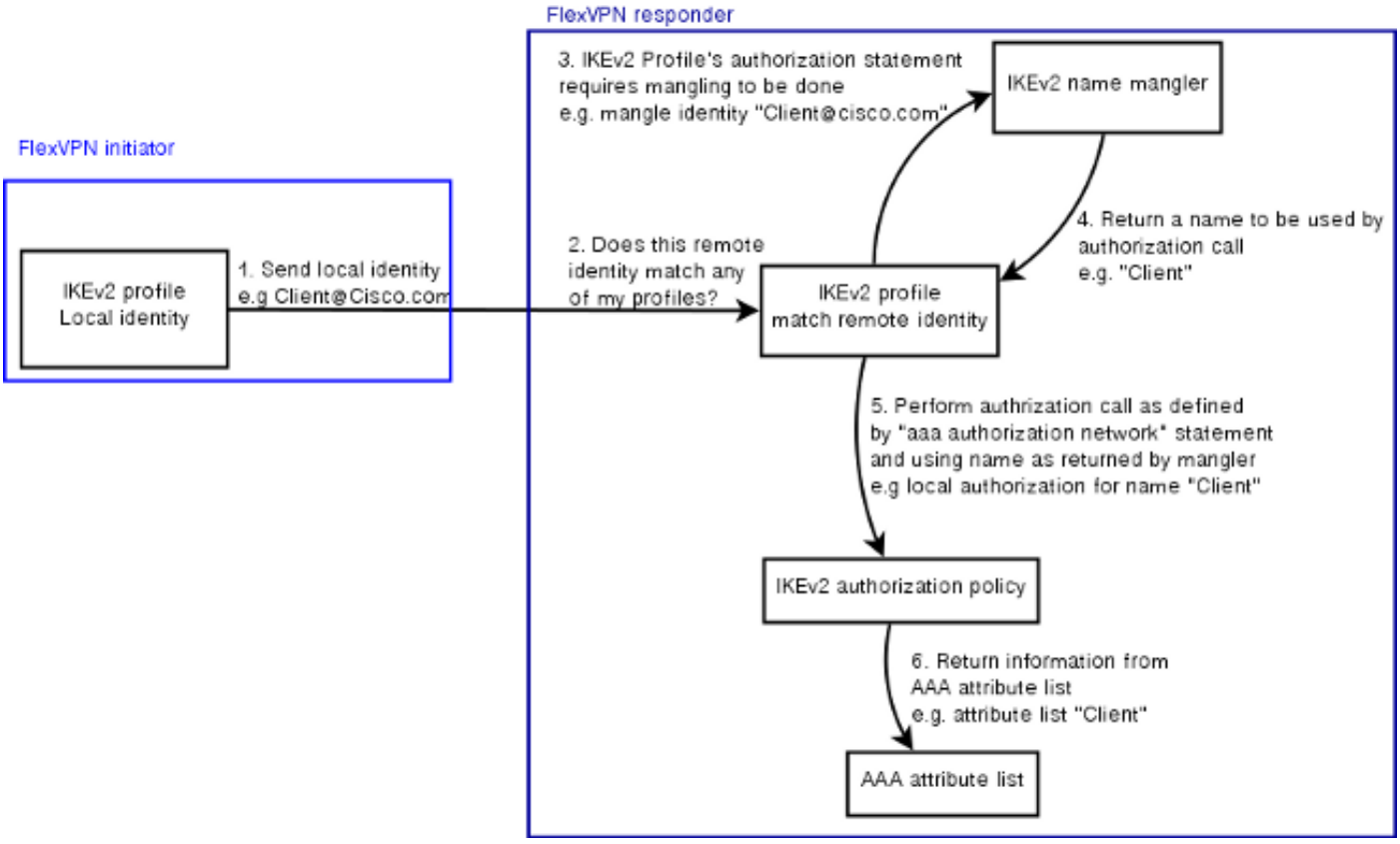
```
aaa attribute list Client2
 attribute type interface-config "ip tcp adjust-mss 1200" protocol ip
 attribute type interface-config "ip access-group 133 in" protocol ip

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

In diesem Beispiel werden eine aktualisierte MSS-Einstellung (Maximum Segment Size) und eine eingehende Zugriffsliste für diesen Client angewendet. Andere Einstellungen können problemlos ausgewählt werden. Eine typische Einstellung ist die Zuweisung unterschiedlicher VRF-Instanzen (Virtual Routing and Forwarding) für verschiedene Clients. Wie bereits erwähnt, muss jede der Attributliste zugewiesene Entität, z. B. die Zugriffsliste 133 in diesem Szenario, bereits in der Konfiguration vorhanden sein.

Prozessübersicht

Diese Abbildung zeigt die Reihenfolge der Vorgänge, in denen die AAA-Autorisierung über das IKEv2-Profil (Internet Key Exchange Version 2) verarbeitet wird, und enthält Informationen speziell für dieses Konfigurationsbeispiel.



Überprüfung

In diesem Abschnitt wird veranschaulicht, wie überprüft wird, ob die zuvor zugewiesenen Einstellungen auf die Clients angewendet wurden.

Client1

Mit den folgenden Befehlen wird überprüft, ob die Einstellungen für die maximale Übertragungseinheit (Maximum Transmission Units, MTU) sowie die Service-Richtlinie angewendet wurden.

```
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
```

Client2

Nachfolgend sind die Befehle aufgeführt, mit denen überprüft wird, ob die MSS-Einstellungen gedrückt wurden und ob die Zugriffsliste 133 auch als eingehender Filter auf die entsprechende virtuelle Zugriffsschnittstelle angewendet wurde.

```
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
(...)
```

Debuggen

Es gibt zwei Hauptblöcke, die gedebuggt werden müssen. Dies ist hilfreich, wenn Sie ein TAC-Ticket öffnen und die Bearbeitung beschleunigen müssen.

Debuggen von IKEv2

Beginnen Sie mit diesem wichtigen Debugbefehl:

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

Geben Sie dann die folgenden Befehle ein:

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

AAA-Attributzuweisung debuggen

Wenn Sie die AAA-Zuweisung von Attributen debuggen möchten, können diese Debuggen hilfreich sein.

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

Schlussfolgerung

In diesem Dokument wird veranschaulicht, wie die AAA-Attributliste verwendet wird, um in FlexVPN-Bereitstellungen, in denen der RADIUS-Server möglicherweise nicht verfügbar oder nicht erwünscht ist, mehr Flexibilität zu ermöglichen. Die AAA-Attributliste bietet zusätzliche Konfigurationsoptionen auf Sitzungs- und Gruppenbasis, falls erforderlich.

Zugehörige Informationen

- FlexVPN und Internet Key Exchange Version 2 Konfigurationsleitfaden, Cisco IOS Version 15M&T
- Remote Authentication Dial-In User Services (RADIUS)
- Anforderungen für Kommentare (RFCs)
- IPsec-Aushandlung/IKE-Protokolle
- Technischer Support und Dokumentation - Cisco Systems