

ローカル AAA の属性リストを使った FlexVPN の動的設定

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[トポロジ](#)

[設定](#)

[スポーク設定](#)

[ハブの設定](#)

[基本的な接続設定](#)

[拡張設定](#)

[プロセスの概要](#)

[確認](#)

[Client1](#)

[Client2](#)

[デバッグ](#)

[IKEv2 のデバッグ](#)

[AAA 属性割り当てのデバッグ](#)

[結論](#)

[関連情報](#)

概要

この設定例では、外部の Remote Authentication Dial-In User Service (RADIUS) サーバを使用せずにローカルの認証、許可、およびアカウントリング (AAA) 属性リストを使用して動的設定を、場合によっては高度な設定を行う方法を示します。

これは、特定のシナリオ、特に迅速な導入またはテストが必要なシナリオで求められる設定です。このような導入は、通常、概念実証ラボ、新規の導入テスト、またはトラブルシューティングで使用されます。

動的設定は、ユーザごと、顧客ごと、セッションごとにさまざまなポリシーや属性を適用する必要があるコンセントレータ/ハブ側で重要です。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものですが、必ずしもこれらのバージョンに限定されません。このリストには最小要件は記載されていませんが、この機能のテスト フェーズ全体にわたってのデバイスの状態を示しています。

ハードウェア

- アグリゲーション サービス ルータ (ASR) - ASR 1001 - 「bsns-asr1001-4」と呼びます。
- Integrated Services Router Generation 2 (ISR G2) - 3925e - 「bsns-3925e-1」と呼びます。
- Integrated Services Router Generation 2 (ISR G2) - 3945e - 「bsns-3945e-1」と呼びます。

ソフトウェア

- Cisco IOS XE Release 3.8 - 15.3(1)S
- Cisco IOS® ソフトウェア リリース 15.2(4)M1 および 15.2(4)M2

ライセンス

- ASR ルータでは、adventerprise および ipsec の機能ライセンスがイネーブルになっています。
- ISR G2 ルータでは、ipbasek9、securityk9、および hseck9 の機能ライセンスがイネーブルになっています。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始しています。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『[シスコ テクニカル ティップスの表記法](#)』を参照してください。

トポロジ

この演習で使用するトポロジは基本トポロジです。1 台のハブ ルータ (ASR) と、クライアントをシミュレートする 2 台のスポーク ルータ (ISR) を使用します。

設定

このドキュメントに記載した設定の目的は、スマートなデフォルト値をできる限り多く使用した基本設定を示すことです。暗号化に関するシスコの推奨事項については、cisco.com の「[次世代暗号化](#)」ページを参照してください。

スポーク設定

すでに述べたように、このドキュメントのほとんどの操作はハブで実行します。スポーク設定は参考のために記載しています。この設定では、唯一の変更箇所は Client1 と Client2 の間の ID (太字で表示) であることに注意してください。

```
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 Tunnell 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 Tunnell 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
```

ハブの設定

ハブ設定は、次の2つの部分に分かれています。

1. **基本的な接続設定**：基本的な接続に必要な設定です。
2. **拡張設定**：管理者が AAA 属性リストを使用してユーザごとまたはセッションごとの設定変更を行う方法を示すために必要な設定変更です。

基本的な接続設定

この設定は、参照目的でのみ使用されるもので、必ずしも最適な設定ではありません。単に動作するというだけです。

この設定の最も大きな制限は、事前共有キー (PSK) を認証方式として使用することです。シスコでは、できる限り証明書を使用することを推奨しています。

```
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

```

拡張設定

AAA 属性を特定のセッションに割り当てるには、いくつか必要な操作があります。この例では、まず client1 についての全作業を示し、次に、別のクライアントまたはユーザを追加する方法を示します。

Client1 の拡張ハブ設定

1. AAA 属性リストを定義します。aaa attribute list Client1

```

attribute type interface-config "ip mtu 1300" protocol ip
attribute type interface-config "service-policy output TEST" protocol ip

```

注: 属性によって割り当てられるエンティティは、ローカルに存在しなければならない点に注意してください。この場合、**policy-map** は事前に設定されています。policy-map TEST

```

class class-default
shape average 60000

```
2. **authorization policy** に AAA 属性リストを割り当てます。crypto ikev2 authorization policy Client1 pool FlexSpokes aaa attribute list Client1 route set interface
3. 接続するクライアントが必ずこの新しいポリシーを使用するようにします。この場合、クライアントから送信された ID の **username** 部分を抽出します。クライアントは、電子メールアドレス ClientX@cisco.com を使用する必要があります (X は 1 または 2 のいずれかで、クライアントに応じて決まります)。mangler は、電子メールアドレスをユーザ名部分とドメイン部分に分割し、そのうちの一方のみ (この場合はユーザ名) を使用して許可ポリシーの名前を選択します。crypto ikev2 name-mangler GET_NAME

```
email username
```

```
crypto ikev2 profile Flex_IKEv2
```

```
aaa authorization group psk list default name-mangler GET_NAMEclient1 が動作している場合、client2 は比較的簡単に追加できます。
```

Client2 の拡張ハブ設定

必要に応じて、ポリシーと個別の属性セットが存在していることを確認します。

```
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
```

この例では、このクライアントに対して作用する、最新の最大セグメント サイズ (MSS) 設定とインバウンド アクセス リストが適用されます。他の設定は簡単に選択できます。一般的な設定では、クライアントごとに異なる Virtual Routing and Forwarding (VRF) を割り当てます。先に述べたように、属性リストに割り当てられるエンティティ (このシナリオのアクセス リスト 133 など) は、あらかじめ設定に存在している必要があります。

プロセスの概要

次の図は、AAA 許可が Internet Key Exchange Version 2 (IKEv2) プロファイルで処理されるときの操作の順序を示しており、この設定例に固有の情報を含んでいます。

確認

この項では、以前に割り当てた設定がクライアントに適用されていることを検証する方法を示します。

Client1

最大伝送ユニット (MTU) 設定とサービス ポリシーが適用されたことを検証するコマンドを以下に示します。

```
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

以下に、MSS 設定がプッシュされたこと、およびアクセス リスト 133 も同等の仮想アクセス イ

インターフェイスにインバウンド フィルタとして適用されたことを検証するコマンドを示します。

```
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 (...)
```

デバッグ

デバッグが必要な主要ブロックが 2 つあります。これは、TAC ケースをオープンして、問題をすばやく解決する必要がある場合に役立ちます。

IKEv2 のデバッグ

まず、次の主要なデバッグ コマンドを入力します。

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

続いて、次のコマンドを入力します。

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

AAA 属性割り当てのデバッグ

AAA 属性の割り当てをデバッグする場合は、次のデバッグが役立ちます。

```
debug aaa authorization
```

```
debug aaa attr
```

```
debug aaa proto local
```

結論

このドキュメントでは、RADIUS サーバが使用できない、または使用しない方がよい FlexVPN 環境で、AAA 属性リストを使用して柔軟性を高める方法を示します。AAA 属性リストを使用すると、必要に応じてセッションごと、グループごとに設定を拡張することができます。

関連情報

- [FlexVPN およびインターネット キー エクスチェンジ \(IKE\) バージョン 2 コンフィギュレーション ガイド、Cisco IOS リリース 15M&T](#)
- [Remote Authentication Dial-In User Services \(RADIUS\)](#)
- [Requests for Comments \(RFC\)](#)
- [IPSec ネゴシエーション/IKE プロトコル](#)
- [テクニカルサポートとドキュメント - Cisco Systems](#)