Configuração dinâmica FlexVPN com listas de atributos AAA locais

Contents

Introduction

Este exemplo de configuração demonstra como usar a lista de atributos AAA (Authentication, Authorization, and Accounting) local para executar uma configuração dinâmica e potencialmente avançada sem o uso do servidor RADIUS (Remote Authentication Dial-In User Service) externo.

Isso é desejado em determinados cenários, especialmente quando a implantação ou o teste rápidos são necessários. Essas implantações são geralmente laboratórios de prova conceitual, novos testes de implantação ou solução de problemas.

A configuração dinâmica é importante no lado do concentrador/hub, onde diferentes políticas ou atributos devem ser aplicados por usuário, por cliente e por sessão.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas, mas não se limitam a, nessas versões de software e hardware. Essa lista não descreve os requisitos mínimos, mas reflete o estado do dispositivo durante toda a fase de teste desse recurso.

Hardware

- Roteadores de serviços de agregação (ASR) - ASR 1001 - chamados de "bsns-asr1001-4"
- Integrated Services Routers Generation 2 (ISR G2) - 3925e - chamado "bsns-3925e-1"
- Integrated Services Routers Generation 2 (ISR G2) - 3945e - chamado "bsns-3945e-1"

Software

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

Licenças

- Os roteadores ASR têm as licenças de recursos **adventerprise** e **ipsec** habilitadas.
- Os roteadores ISR G2 têm as licenças de recursos **ipbasek9**, **securityk9** e **hseck9** habilitadas.

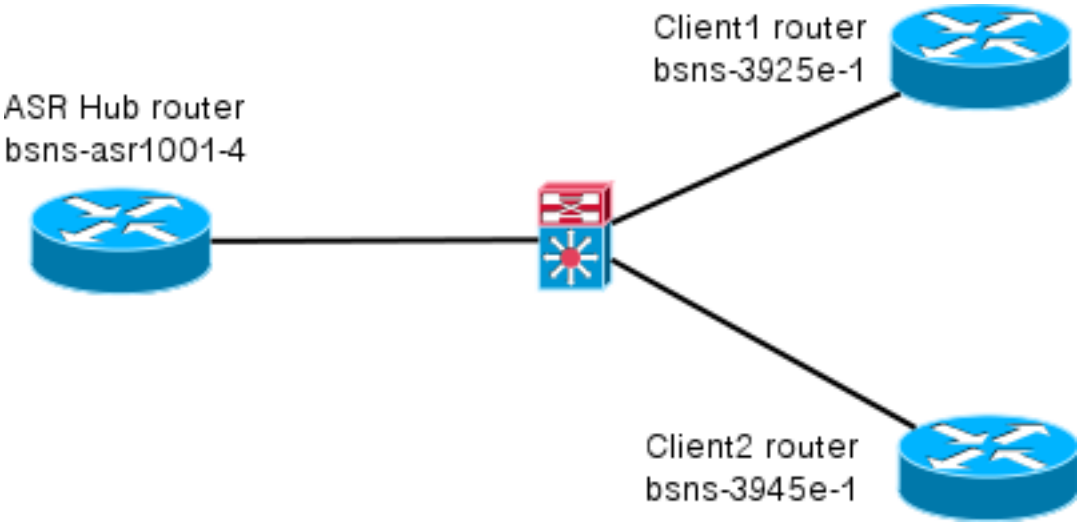
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Topologia

A topologia usada neste exercício é básica. Um roteador de hub (ASR) e dois roteadores spoke (ISR) são utilizados, o que simula clientes.



Configurações

As configurações neste documento destinam-se a mostrar uma configuração básica, com padrões inteligentes o máximo possível. Para obter recomendações da Cisco sobre criptografia, visite a página Criptografia de última geração em cisco.com.

Configuração de Spoke

Como mencionado anteriormente, a maioria das ações nesta documentação são executadas no hub. A configuração do spoke está aqui para referência. Nesta configuração, observe que somente a alteração é a identidade entre Cliente1 e Cliente2 (exibida em negrito).

```
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
```

Configuração do hub

A configuração do hub é dividida em duas partes:

1. **Configuração de conectividade básica**, que descreve a configuração necessária para a conectividade básica.
2. **Configuração estendida**, que descreve as alterações de configuração necessárias para demonstrar como um administrador pode usar a lista de atributos AAA para executar alterações de configuração por usuário ou por sessão.

Configuração de conectividade básica

Essa configuração é apenas para referência e não deve ser ideal, apenas funcional.

A maior limitação dessa configuração é o uso da chave pré-compartilhada (PSK) como método de autenticação. A Cisco recomenda o uso de certificados sempre que aplicável.

```
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
```

Configuração estendida

Há algumas coisas necessárias para atribuir atributos AAA a uma sessão específica. Este exemplo mostra o trabalho completo para o cliente1; em seguida, mostra como adicionar outro cliente/usuário.

Configuração de Hub Estendido para Cliente1

1. Defina uma lista de atributos AAA.
   ```
   aaa attribute list Client1
    attribute type interface-config "ip mtu 1300" protocol ip
    attribute type interface-config "service-policy output TEST" protocol ip
   ```
   Observação: lembre-se de que a entidade atribuída por atributos deve existir localmente. Nesse caso, o **mapa de políticas** foi configurado anteriormente.
   ```
   policy-map TEST
    class class-default
    shape average 60000
   ```
2. Atribuir uma lista de atributos AAA a uma **política de autorização.**
   ```
   crypto ikev2 authorization policy Client1
    pool FlexSpokes
    aaa attribute list Client1
    route set interface
   ```
3. Assegure-se de que essa nova política seja usada pelos clientes que se conectam. Nesse caso, extraia a parte do **nome de usuário** da identidade enviada pelos clientes. Os clientes devem usar um endereço de e-mail ClientX@cisco.com (X é 1 ou 2, dependendo do cliente). O **gerente** divide o endereço de email em nome de usuário e parte de domínio e usa apenas um deles (nome de usuário, nesse caso) para escolher o nome da política de autorização.
   ```
   crypto ikev2 name-mangler GET_NAME
    email username

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

Quando o cliente1 está operacional, o cliente2 pode ser adicionado relativamente fácil.

Configuração de Hub Estendido para Cliente2

Assegure a existência de uma política e um conjunto separado de atributos, se necessário.

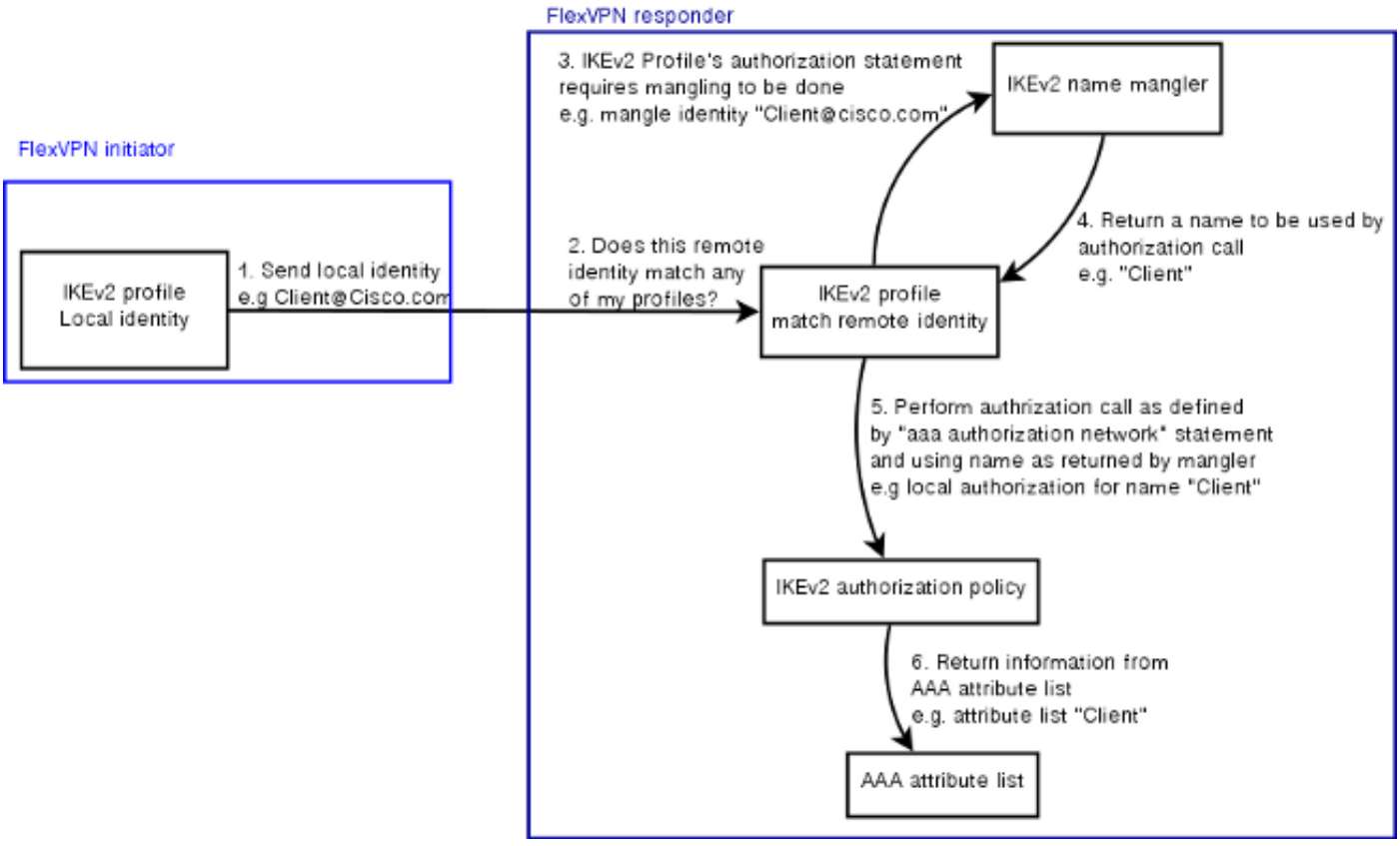
```
aaa attribute list Client2
 attribute type interface-config "ip tcp adjust-mss 1200" protocol ip
 attribute type interface-config "ip access-group 133 in" protocol ip

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

Neste exemplo, é aplicada uma configuração de tamanho máximo de segmento (MSS) atualizada e uma lista de acesso de entrada para operar para este cliente. Outras configurações podem ser facilmente escolhidas. Uma configuração típica é atribuir roteamento e encaminhamento virtual (VRF) diferentes para clientes diferentes. Como mencionado anteriormente, qualquer entidade atribuída à lista de atributos, como access-list 133 neste cenário, já deve existir na configuração.

Visão geral do processo

Esta figura descreve a ordem de operação quando a autorização AAA é processada através do perfil do Internet Key Exchange versão 2 (IKEv2) e contém informações específicas para este exemplo de configuração.



Verificação

Esta seção mostra como verificar se as configurações atribuídas anteriormente foram aplicadas aos clientes.

Cliente1

Aqui estão os comandos que verificam se as configurações de MTU (Maximum Transmission Units, Unidades Máximas de Transmissão), bem como a política de serviço foram aplicadas.

```
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

Aqui estão os comandos que verificam se as configurações de MSS foram enviadas e se a lista de acesso 133 também foi aplicada como um filtro de entrada na interface de acesso virtual 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

Há dois blocos principais para depuração. Isso é útil quando você precisa abrir um caso do TAC e fazer as coisas funcionarem mais rapidamente.

Depurar IKEv2

Comece com este comando de depuração principal:

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

Em seguida, insira estes comandos:

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

Depurar atribuição de atributo AAA

Se você quiser depurar a atribuição AAA de atributos, essas depurações podem ser úteis.

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

Conclusão

Este documento demonstra como usar a lista de atributos AAA para permitir maior flexibilidade em implantações FlexVPN em que o servidor RADIUS pode não estar disponível ou não é desejado. A lista de atributos AAA oferece opções de configuração adicionais por sessão, por grupo, se necessário.

Informações Relacionadas

- Guia de configuração do FlexVPN e Internet Key Exchange versão 2, Cisco IOS versão 15M&T
- Serviços de Usuário de Discagem de Autenticação Remota (RADIUS - Remote Authentication Dial-In User Services)
- Solicitações de Comentários (RFCs)

- Negociação IPsec/Protocolos IKE
- Suporte Técnico e Documentação - Cisco Systems