Configuração dinâmica de FlexVPN com listas de atributos locais AAA

Índice

Introdução

Este exemplo de configuração demonstra como usar a autenticação local, a lista de atributos da autorização, e da contabilidade (AAA) a fim executar dinâmico e potencialmente a configuração avançada sem o uso do server externo do Remote Authentication Dial-In User Service (RADIUS).

Isto está desejado em determinadas encenações, especialmente quando a distribuição rápida ou o teste são exigidos. Tais disposições são tipicamente laboratórios do proof-of-concept, testes novos do desenvolvimento, ou Troubleshooting.

A configuração dinâmica é importante no concentrador/lado de hub onde as políticas ou os atributos diferentes devem ser aplicados em um usuário per., por-cliente, por sessão base.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

A informação neste documento é baseada sobre, mas não limitada a, este versão de software e hardware. Esta lista não esboça os requisitos mínimos, mas reflete o estado do dispositivo ao longo da fase de teste desta característica.

Hardware

- A agregação presta serviços de manutenção ao Roteadores (o ASR) - ASR 1001 - "bsns-asr1001-4" chamado
- Geração 2 do Roteadores dos Serviços integrados (ISR G2) - 3925e - "bsns-3925e-1" chamado
- Geração 2 do Roteadores dos Serviços integrados (ISR G2) - 3945e - "bsns-3945e-1" chamado

Software

- Liberação 3.8 do Cisco IOS XE - 15.3(1)S
- Software Release 15.2(4)M1 e 15.2(4)M2 de Cisco IOS®

Licenças

- Os roteadores ASR têm as licenças de recurso do **adventerprise** e do **IPsec** permitidas.
- O Roteadores ISR G2 tem as licenças de recurso **ipbasek9**, **securityk9**, e **hseck9** permitidas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

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 do spoke (ISR) são utilizados, que simulem clientes.

Configurações

As configurações neste documento são pretendidas mostrar tanto quanto possível uma instalação básica, com padrões espertos. Para recomendações da Cisco na criptografia, visite a página da criptografia da próxima geração em cisco.com.

Configuração de raio

Como mencionado previamente, a maioria das ações nesta documentação são executadas no hub. A configuração de raio está aqui para a referência. Nesta configuração, observe que somente a mudança é identidade entre o cliente1 e o Client2 (indicados em corajoso).

```
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 porções:

1. **A configuração da conectividade básica**, que esboça a configuração precisou para a conectividade básica.
2. **A configuração prolongada**, que esboça as alterações de configuração precisou a fim demonstrar como um administrador pode usar a lista de atributos AAA para executar por usuário ou por sessão alterações de configuração.

Configuração de conectividade básica

Esta configuração é para a referência somente e não é significada ser ótima, somente funcional.

A grande limitação desta configuração é uso da chave pré-compartilhada (PSK) como o método de autenticação. Cisco recomenda o uso dos 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 prolongada

Há algumas coisas necessárias atribuir atributos AAA a uma sessão particular. Este exemplo mostra o trabalho completo para o cliente1; então mostra como adicionar um outro cliente/usuário.

Configuração prolongada do hub para o 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` **Nota:** Recorde que a entidade atribuída através dos atributos deve existir localmente. Neste caso, o **mapa de política** foi configurado previamente.`policy-map TEST`
   `class class-default`
   `shape average 60000`
2. Atribua a lista de atributos AAA a uma **política da autorização.**`crypto ikev2 authorization policy` **`Client1`** `pool FlexSpokes aaa attribute list Client1 route set interface`
3. Assegure-se de que esta política nova usada pelos clientes que conectam. Neste caso, extraia a parcela **username da** identidade enviada pelos clientes. Os clientes devem usar um endereço email de ClientX@cisco.com (X é 1 ou 2, dependente do cliente). **O mangler** racha o endereço email na parcela username e de domínio e usa somente um deles (username neste caso) para escolher o nome da política da 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 é operacional, client2 pode ser relativamente fácil adicionado.

Configuração prolongada do hub para Client2

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

```
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, um Maximum Segment Size actualizado (MSS) que ajustam-se e uma lista de acessos de entrada para operar-se para este cliente são aplicados. Outros ajustes podem facilmente ser escolhidos. Uma configuração típica é atribuir o roteamento virtual e a transmissão diferentes (VRF) para clientes diferentes. Como mencionado mais cedo, toda a entidade atribuída à lista de atributos, tal como a lista de acesso 133 nesta encenação, deve já existir na configuração.

Vista geral do processo

Esta figura esboça o ordem de operação quando a autorização de AAA está processada através do perfil da versão 2 do intercâmbio de chave de Internet (IKEv2) e contém o específico da informação a este exemplo de configuração.

Verificação

Esta seção mostra como verificar que os ajustes atribuídos previamente estiveram aplicados aos clientes.

Cliente1

Estão aqui os comandos que verificam que os ajustes das unidades de transmissão máxima (MTU), assim como a política de serviços estiveram aplicados.

```
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

Estão aqui os comandos que verificam que os ajustes MSS estiveram empurrados e que a lista de acesso 133 esteve aplicada igualmente 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 a debugar. Isto é útil quando você precisa de abrir um caso de TAC e de obter coisas na trilha mais rápidas.

Debugar IKEv2

Comece com este comando debug principal:

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

Incorpore então estes comandos:

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

Debugar a atribuição do atributo AAA

Se você gostaria de debugar a atribuição AAA dos atributos, estes debugam podem ser úteis.

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

Conclusão

Este documento demonstra como usar a lista de atributos AAA a fim permitir a flexibilidade adicionada nas disposições de FlexVPN onde o servidor Radius não pôde estar disponível ou não é desejado. A lista de atributos AAA oferece opções de configuração adicionadas no por sessão, base por grupo, se se exige.

Informações Relacionadas

- FlexVPN e manual de configuração da versão 2 do intercâmbio de chave de Internet, Cisco IOS Release 15M&T
- Serviços de autenticação remotas de usuários discados (RAIO)
- Solicitações de Comentários (RFCs)
- Negociação IPsec/Protocolos IKE
- Suporte Técnico e Documentação - Cisco Systems