Entender os contadores de criptografia ACL dentro de túneis VPN baseados em política

Contents

Introdução

Este documento descreve o comportamento dos contadores da lista de controle de acesso (ACL - Access Control List) criptografados dentro de túneis VPN baseados em política.

Pré-requisitos

Requisitos

A Cisco recomenda o conhecimento destes tópicos:

- VPN site a site com base em políticas na plataforma Cisco IOS® /Cisco IOS® XE
- Listas de controle de acesso na plataforma Cisco IOS/Cisco IOS XE

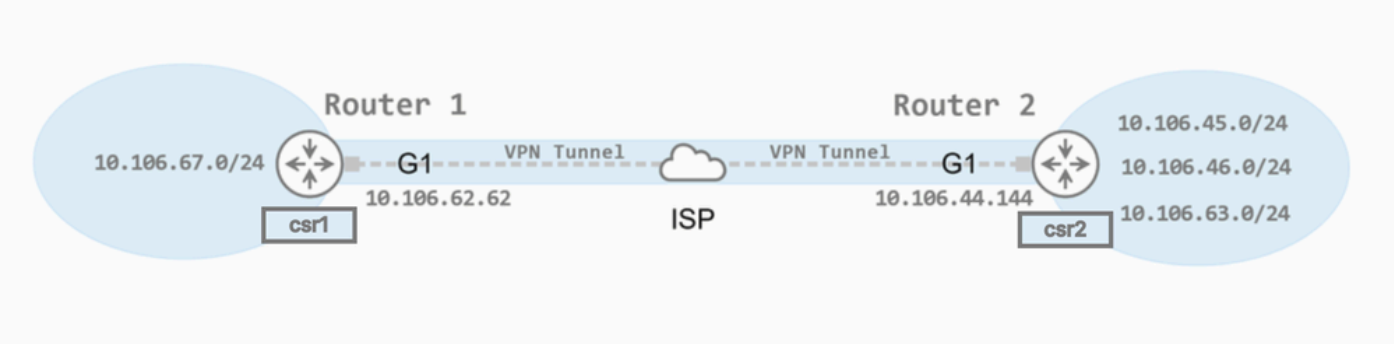
Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco C8kv, versão 17.12.04(MD)

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 rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Topologia



Topologia

Cenários

Examinando dois cenários distintos, pretendemos entender como as contagens de acertos da ACL são afetadas quando o tráfego é iniciado de diferentes peers e quando os túneis são redefinidos.

1. Cenário Um: Tráfego iniciado do Router1 enquanto o túnel VPN está inativo

   Neste cenário, as alterações nas contagens de ocorrências de ACL são analisadas quando o túnel VPN é inicialmente desativado e o tráfego é iniciado do Roteador 1. Essa análise ajuda a entender a configuração inicial e como os contadores de ACL criptografados reagem à primeira tentativa de fluxo de tráfego.

2. Cenário dois: Tráfego iniciado do Roteador 2 enquanto o túnel VPN está ativo

   Neste cenário, o túnel VPN já está estabelecido e o tráfego é iniciado do Roteador 2 é explorado. Este cenário fornece insights sobre como os contadores de ACL se comportam quando o túnel está ativo e o tráfego é introduzido a partir de um peer diferente.

Comparando esses cenários, podemos obter uma compreensão abrangente da dinâmica dos contadores de ACL em túneis VPN sob condições variadas.

Configuração

Configuramos um túnel VPN site a site baseado em política entre dois roteadores Cisco C8kv, designados como pares. Router1 é chamado de "csr1" e Router2 é chamado de "csr2".

Configuração criptografada no Roteador 1

```
csr1#sh ip int br
Interface              IP-Address      OK?   Method   Status  Protocol
GigabitEthernet1       10.106.62.62    YES   NVRAM    up      up
GigabitEthernet2       10.106.67.27    YES   NVRAM    up      up
```

```
csr1#sh run | sec crypto map
crypto map nigarapa_map 100 ipsec-isakmp
   set peer 10.106.44.144
   set transform-set new_ts
   set ikev2-profile new_profile
   match address new_acl
```

```
csr1#sh ip access-lists new_acl
Extended IP access list new_acl
   10 permit ip 10.106.67.0 0.0.0.255 10.106.45.0 0.0.0.255 log
   20 permit ip 10.106.67.0 0.0.0.255 10.106.46.0 0.0.0.255
   30 permit ip 10.106.67.0 0.0.0.255 10.106.63.0 0.0.0.255 log
```

```
csr1#sh run int GigabitEthernet1
Building configuration...

Current configuration : 162 bytes
!
interface GigabitEthernet1
ip address 10.106.62.62 255.255.255.0
ip nat outside
negotiation auto
no mop enabled
no mop sysid
crypto map nigarapa_map
end
```

Configuração criptografada no roteador 2

```
csr2#sh ip int br
Interface              IP-Address        OK?     Method       Status     Protocol
GigabitEthernet1       10.106.44.144     YES     NVRAM        up         up
GigabitEthernet2       10.106.45.145     YES     NVRAM        up         up
GigabitEthernet3       10.106.46.146     YES     NVRAM        up         up
GigabitEthernet4       10.106.63.13      YES     NVRAM        up         up
```

```
csr2#sh run | sec crypto map
crypto map nigarapa_map 100 ipsec-isakmp
   set peer 10.106.62.62
   set transform-set new_ts
   set ikev2-profile new_profile
   match address new_acl
```

```
csr2#sh ip access-lists new_acl
Extended IP access list new_acl
   10 permit ip 10.106.45.0 0.0.0.255 10.106.67.0 0.0.0.255
   20 permit ip 10.106.46.0 0.0.0.255 10.106.67.0 0.0.0.255
   30 permit ip 10.106.63.0 0.0.0.255 10.106.67.0 0.0.0.255
```

```
csr2#sh run int GigabitEthernet1
Building configuration...

Current configuration : 163 bytes
!
interface GigabitEthernet1
ip address 10.106.44.144 255.255.255.0
ip nat outside
negotiation auto
no mop enabled
no mop sysid
crypto map nigarapa_map
end
```

Análise Comportamental dos Contadores da Lista de Controle de Acesso de Criptografia em Túneis VPN

Inicialmente, ambos os dispositivos têm uma contagem de acertos de ACL igual a zero em suas respectivas listas de acesso de criptografia.

A contagem de ocorrências de Lista de Controle de Acesso de zero em suas respectivas listas de acesso de criptografia em ambos os dispositivos pares.

Cenário Um: Tráfego iniciado do Router1 enquanto o túnel VPN está inativo

Estado inicial:

O túnel VPN que conecta o Roteador 1 (IP: 10.106.67.27) e Roteador2 (IP: 10.106.45.145) está inativo no momento.

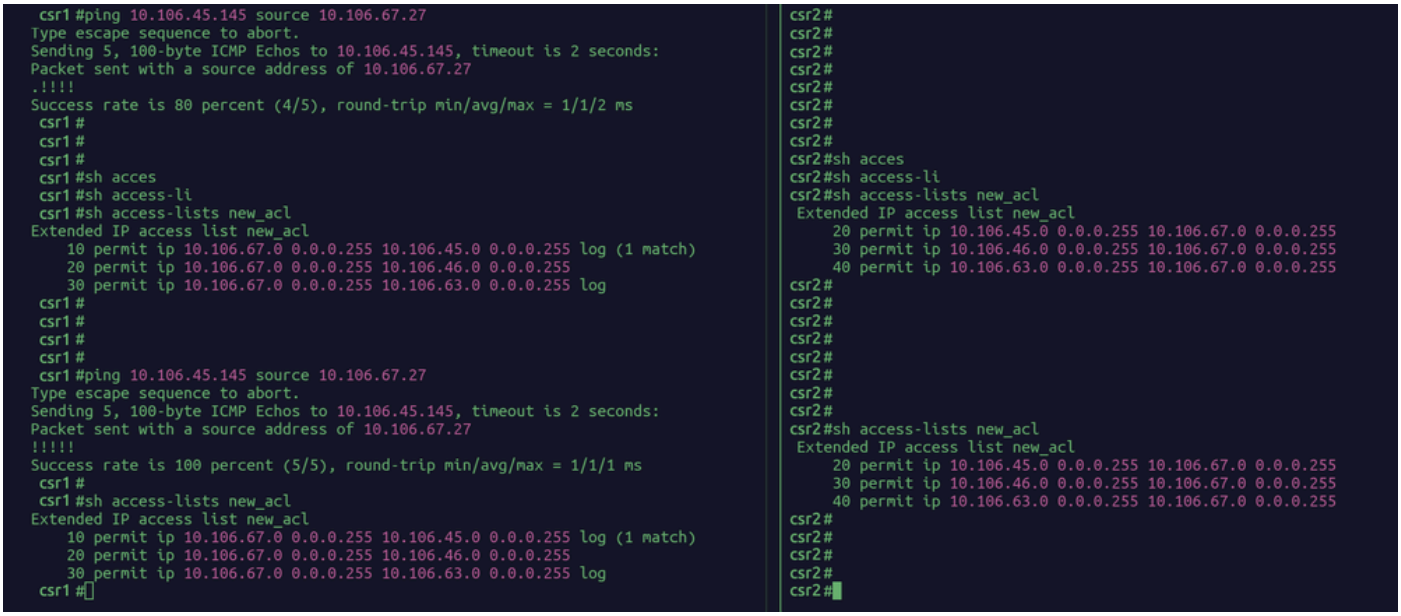
Ação realizada:

O tráfego é iniciado do Roteador 1, destinado a estabelecer comunicação com o Roteador 2.

Observações:

1. Comportamento do contador de ACL:
   a. Ao iniciar o tráfego do Roteador 1, há um aumento notável no contador da Lista de Controle de Acesso (ACL) no Roteador 1. Esse aumento ocorre apenas uma vez no momento em que o túnel tenta estabelecer.
   b. O aumento no contador de ACL é observado exclusivamente no roteador iniciador, que é o Roteador 1 neste cenário. O Roteador2 não reflete nenhuma alteração em seu contador de ACL nesse estágio.
2. Estabelecimento de túnel:
   a. Após o incremento inicial correspondente ao início do tráfego, o túnel entre o primeiro e o Roteador2 é estabelecido com êxito.
   b. Após o estabelecimento do túnel, o contador de ACL no Router1 estabiliza e não exibe mais incrementos, indicando que a regra de ACL foi correspondida e agora está permitindo consistentemente o tráfego através do túnel estabelecido.
3. Reinicialização do túnel:
   O contador de ACL no Router1 experimentará outro incremento somente se o túnel cair e exigir restabelecimento. Isso sugere que a regra da ACL é acionada pela iniciação do tráfego inicial, que tenta estabelecer o túnel, em vez de pela transferência de dados contínua quando o túnel está ativo.

Em resumo, esse cenário demonstra que o contador de ACL no Router1 é sensível às tentativas iniciais de tráfego para a criação do túnel, mas permanece estático quando o túnel VPN está ativo e operacional.



Cenário 1

Cenário dois:Tráfego iniciado do Roteador 2 enquanto o túnel VPN está ativo

Estado inicial:

O túnel VPN que conecta o Roteador 1 (IP: 10.106.67.27) e Roteador2 (IP: 10.106.45.145) está ativo e operacional no momento.

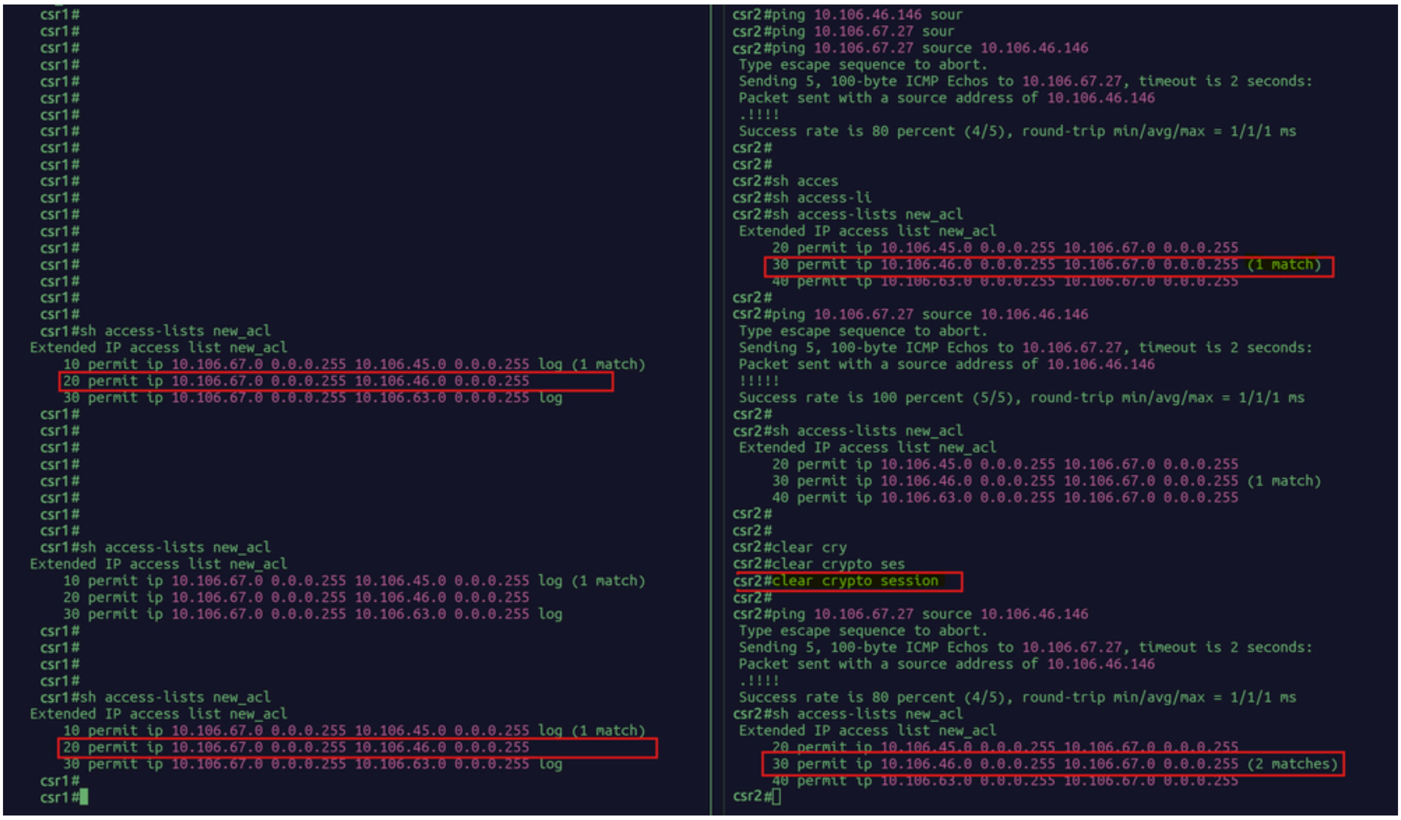
Ação realizada:

1. O tráfego é iniciado do Roteador 2 em direção ao Roteador 1 enquanto o túnel está ativo.
2. Posteriormente, o túnel é deliberadamente removido (ou redefinido).
3. Após a limpeza do túnel, o Roteador2 inicia o tráfego novamente para restabelecer a conexão.

Observações:

1. Início inicial do tráfego:
   a. Quando o tráfego é iniciado pela primeira vez a partir do Roteador2 enquanto o túnel já está estabelecido, não há nenhuma alteração imediata no contador da Lista de Controle de Acesso (ACL).
   b. Isso indica que o tráfego em andamento em um túnel já estabelecido não dispara o incremento do contador de ACL.
2. Limpeza e reinicialização do túnel:
   a. Ao limpar o túnel, a conexão estabelecida entre o primeiro e o Roteador2 é temporariamente interrompida. Isso exige um processo de restabelecimento para qualquer tráfego subsequente.
   b. Quando o tráfego é reiniciado do Roteador2 após a limpeza do túnel, há um incremento observável no contador de ACL no Roteador2. Esse incremento significa que as regras de ACL estão sendo envolvidas mais uma vez para facilitar a criação do túnel.
3. Especificidade do contador de ACL:
   O incremento no contador de ACL ocorre somente no lado que inicia o tráfego, que, nesse caso, é o Roteador 2. Esse comportamento destaca a função da ACL no monitoramento e controle dos processos de iniciação de tráfego no lado de origem, enquanto o contador de ACL do Roteador 1 permanece inalterado durante essa fase.

Em resumo, este cenário ilustra que o contador de ACL no Roteador 2 responde ao início do tráfego ao restabelecer um túnel VPN. O contador não aumenta com o fluxo de tráfego regular dentro de um túnel ativo, mas reage à necessidade de restabelecimento do túnel, garantindo o rastreamento preciso dos eventos de início do túnel.



Cenário 2

Conclusão:

O comportamento dos contadores de criptografia ACL revela que eles registram contagens de ocorrências exclusivamente durante a fase de início do túnel VPN.

Incremento específico do iniciador: Quando o túnel é iniciado a partir do Roteador 1, o aumento na contagem de ocorrências é observado somente no Roteador 1. Da mesma forma, se a iniciação ocorrer a partir do Roteador 2, a contagem de ocorrências aumenta apenas no Roteador 2. Isso destaca a função da ACL no monitoramento do processo de iniciação do tráfego na origem.

Pós-estabelecimento da estabilidade: Uma vez que o túnel é estabelecido com êxito, os contadores de ACL em ambos os peers permanecem inalterados, indicando que não há mais acessos. Essa estabilidade persiste até que o túnel seja limpo ou reinicializado, e a iniciação do tráfego seja tentada novamente.
Esse comportamento enfatiza a funcionalidade das Listas de controle de acesso no rastreamento e controle da fase inicial de criação do túnel, garantindo que o fluxo de dados subsequente dentro do túnel estabelecido não afete as contagens de ocorrências.

Pontos principais:

Comportamento do contador de ACL: Os registros dos contadores de ACL são incrementados exclusivamente no lado do iniciador durante o processo de início do túnel. Isso indica que os contadores foram projetados para monitorar o tráfego inicial que dispara o estabelecimento do

túnel.

Contadores estáticos após o estabelecimento: Quando o túnel estiver ativo e estabelecido, os contadores da ACL permanecerão inalterados. Eles não refletem nenhuma outra atividade a menos que o túnel seja reinicializado e precise ser reiniciado, enfatizando o foco nos eventos de tráfego iniciais.

Especificidade de início de tráfego: As contagens de acertos da ACL são específicas para o peer que inicia o túnel. Essa especificidade garante o rastreamento preciso de qual lado é responsável por iniciar a conexão VPN, permitindo o monitoramento e o controle precisos.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.