了解基于策略的VPN隧道内的加密ACL计数器

目录

简介

本文档介绍基于策略的VPN隧道中的加密访问控制列表(ACL)计数器的行为。

先决条件

要求

建议掌握下列主题的相关知识：

- Cisco IOS® /Cisco IOS® XE平台上的基于策略的站点到站点VPN
- Cisco IOS/Cisco IOS XE平台上的访问控制列表

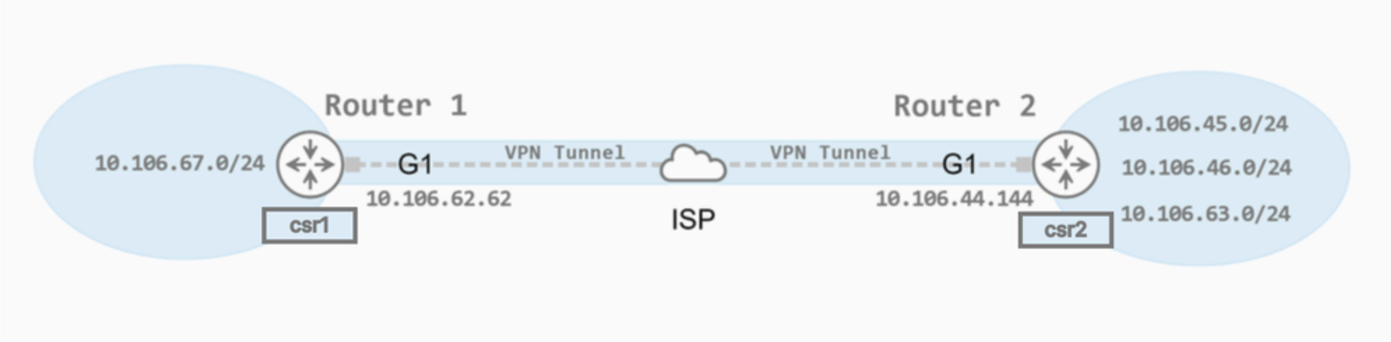
使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科C8kv，版本17.12.04(MD)

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

拓扑



拓扑

场景

通过研究两个不同的场景，我们希望了解从不同对等体发起流量和重置隧道时如何影响ACL命中计数。

1. 场景一：在VPN隧道处于非活动状态时从Router1发起的流量

   在此方案中，当VPN隧道最初关闭且流量从Router1发起时，将分析ACL命中计数的更改。此分析有助于了解初始设置以及加密ACL计数器如何对第一次流量尝试做出反应。

2. 场景二：当VPN隧道处于活动状态时从Router2发起的流量

   在此场景中，已建立VPN隧道，并探索从Router2发起的流量。此场景提供了有关ACL计数器在隧道处于活动状态且流量从其他对等设备引入时的行为方式的见解。

通过比较这些场景，我们可以全面了解VPN隧道中ACL计数器在不同条件下的动态。

配置

我们已经在两台Cisco C8kv路由器（指定为对等体）之间配置了一个基于策略的站点到站点VPN隧道。Router1命名为“csr1”，Router2命名为“csr2”。

Router1上的加密配置

```
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
```

Router2上的加密配置

```
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
```

VPN隧道内加密访问控制列表计数器的行为分析

最初，两台设备各自加密访问列表上的ACL命中计数均为零。

```
csr1#sh 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#
```

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

两个对等设备上的各自加密访问列表上的访问控制列表命中计数为零。

场景一：在VPN隧道处于非活动状态时从Router1发起的流量

初始状态：

连接Router1的VPN隧道(IP:10.106.67.27)和Router2(IP:10.106.45.145)当前处于非活动状态。

执行的操作:

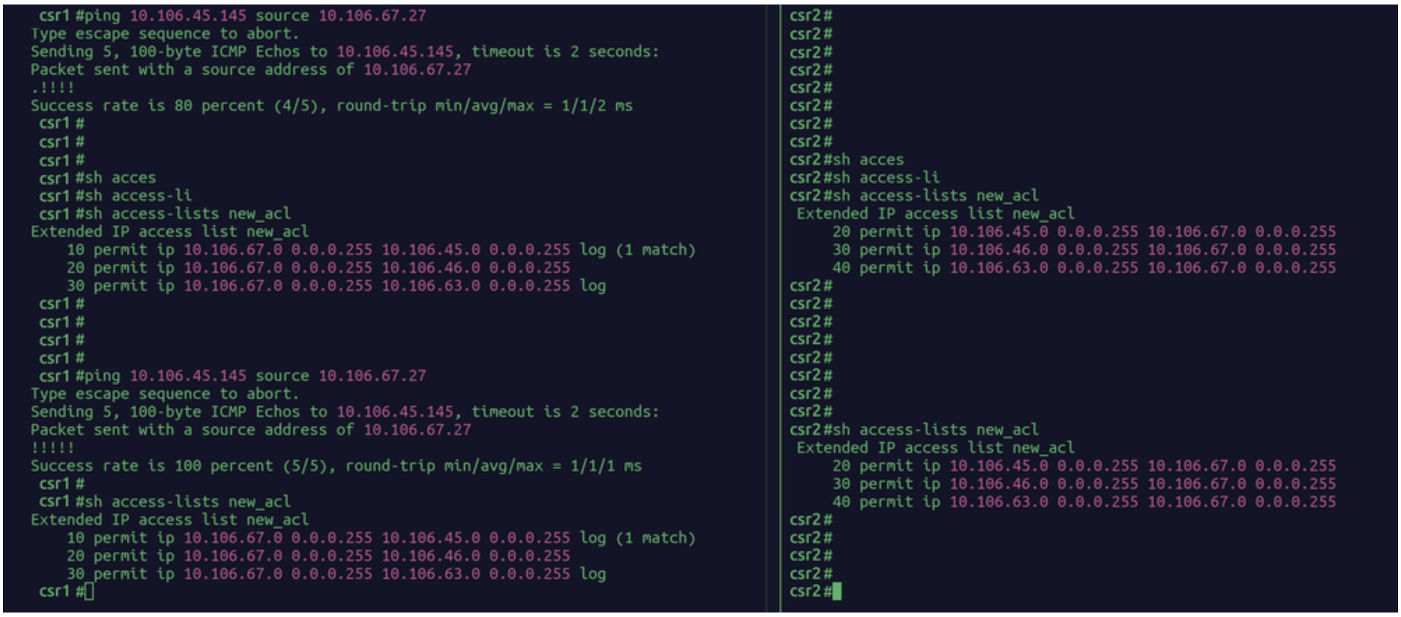
流量从Router1发起，旨在与Router2建立通信。

观察结果:

1. ACL计数器行为：
   a.从Router1发起流量时，Router1上的访问控制列表(ACL)计数器中会出现明显的增加。此增加仅在隧道尝试建立时出现一次。
   b.ACL计数器的增加只发生在发起路由器（本场景中为Router1）上。Router2在此阶段不反映其ACL计数器的任何更改。
2. 隧道建立：
   a.在与流量启动对应的初始增量之后，成功建立第一个和Router2之间的隧道。
   b.建立隧道后，Router1上的ACL计数器会稳定下来，并且没有进一步增加，这表明ACL规则已经匹配，并且现在始终允许流量通过已建立的隧道。

3. 隧道重新初始化：
   只有当隧道丢弃并需要重新建立时，Router1上的ACL计数器才会再次增加。这表明ACL规则由尝试建立隧道的初始流量启动触发，而不是在隧道处于活动状态后通过持续的数据传输触发。

总之，此场景表明，Router1上的ACL计数器对用于创建隧道的初始流量尝试非常敏感，但是在VPN隧道启动并运行后，该计数器仍保持静态。



Scenaria 1

场景2:VPN隧道处于活动状态时从Router2发起的流量

初始状态：

连接Router1的VPN隧道(IP:10.106.67.27)和Router2(IP:10.106.45.145)当前处于活动状态且运行正常。

执行的操作:

1. 隧道启动时，流量从Router2发往Router1。
2. 随后，隧道被有意清除（或重置）。
3. 清除隧道后，Router2再次发起流量以重新建立连接。

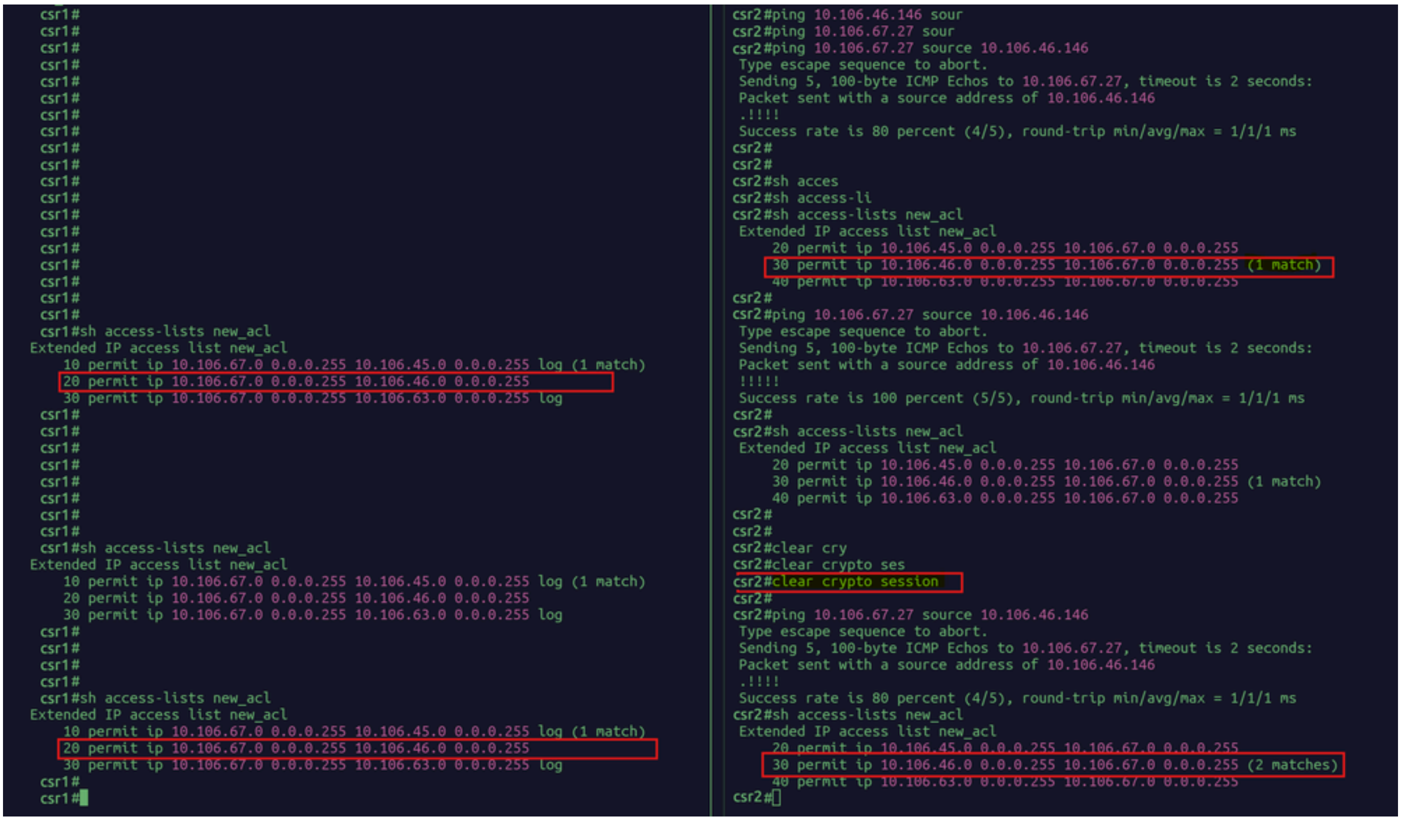
观察结果:

1. 初始流量发起：
   a.当流量首次从Router2发起而隧道已经建立时，访问控制列表(ACL)计数器不会立即发生更改。
   b.这表示已建立的隧道中的持续流量不会触发ACL计数器增量。
2. 隧道清除和重新启动：
   a.清除隧道后，第一个路由器与Router2之间建立的连接会暂时中断。这就需要针对任何后续流量重新建立过程。
   b.当隧道清除后，从Router2重新发起流量时，Router2的ACL计数器会出现一个可观测的增量

。此增量表示ACL规则再次被使用，以方便隧道的创建。

3. ACL计数器特异性：
   ACL计数器的增量仅出现在发起流量的端（在本例中为Router2）。此行为突出显示ACL在监控发起端上的流量发起过程方面的作用，而Router1的ACL计数器在此阶段不受影响。

总之，此场景说明在重新建立VPN隧道时，Router2上的ACL计数器对流量的启动作出响应。计数器不会随活动隧道内的常规流量而增加，但会响应隧道重建的需要，确保精确跟踪隧道启动事件。



场景 2

结论:

加密ACL计数器的行为显示它们在VPN隧道的启动阶段专门注册命中计数。

特定于启动器的增量：从Router1启动隧道时，只在Router1上观察到命中计数增加。同样，如果从Router2启动，则命中计数仅在Router2上增加。这突出说明了ACL在监控源上的流量启动过程方面所起的作用。

建立后的稳定性：成功建立隧道后，两个对等体上的ACL计数器保持不变，表示没有进一步的命中。此稳定性将一直持续到隧道被清除或重置，然后再次尝试流量发起。
此行为强调了访问控制列表在跟踪和控制隧道创建的初始阶段中的功能，从而确保已建立的隧道内的后续数据流不会影响命中计数。

主要讯息：

ACL计数器行为：在隧道启动过程中，ACL计数器仅在发起方一侧注册增量。这表示计数器旨在监控触发隧道建立的初始流量。

静态计数器建立后：一旦隧道处于活动状态并建立，ACL计数器将保持不变。它们不会反映任何进一步的活动，除非隧道重置且需要重新启动，突出表明关注初始流量事件。

流量启动特异性：ACL命中计数特定于启动隧道的对等设备。这种专用性可确保精确跟踪哪一端负责启动VPN连接，从而实现准确的监控和控制。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。