目录

简介

本文描述为通过AVC流量要求的配置通过IPSec隧道对收集器。默认情况下， AVC信息不可能在对收集器的一个IPSec隧道间导出

先决条件

思科建议您有这些主题基础知识：

- 应用程序可见性和控制(AVC)
- 容易性能监控程序(EzPM)

背景信息

思科AVC功能用于在多个应用程序识别，分析和控制。当应用程序感知被建立到网络基础设施，加上可见性到运行在网络的申请性能， AVC enable (event)每个应用程序策略对应用程序带宽使用粒状控制，造成一个更加好的终端用户经验。您能找到关于此技术的更多详细信息。

EzPM是一个更加快速和更加简单的方法配置传统性能监控配置。目前EzPM不提供传统性能监控程序配置型号的全双工灵活性。您能找到关于EzPM的更多详细信息。

限制

目前AVC不支持转接隧道协议数量，详细信息可以找到此处。

Internet协议安全性(IPSec)是其中一AVC和本文的不支持的转接隧道协议寻址此限制的可能的应急方案。

配置

此部分描述用于的完整的配置模拟给的限制。

网络图

使用静态路由，在此网络图中所有路由器彼此有可接通性。R1配置与EzPM配置并且有用R2路由器设立的一个IPSec隧道。R3工作作为出口方此处，可能是思科最初或其他出口方能够收集性能数据。

AVC流量由R1生成，并且发送对出口方通过R2。R1发送AVC流量对在IPSec隧道接口的R2。

初始配置

此部分通过R3描述R1的初始配置。

R1

```
!
interface Loopback0
IP地址1.1.1.1 255.255.255.255
!

interface GigabitEthernet0/1

 ip address 172.16.1.1 255.255.255.0

 duplex auto

 speed auto

!

ip route 0.0.0.0 0.0.0.0 172.16.1.2

!
```

R2

```
!

接口GigabitEthernet0/0/0

 IP地址172.16.2.2 255.255.255.0
```

协商自动

!

接口GigabitEthernet0/0/1

ip address 172.16.1.2 255.255.255.0

协商自动

!

R3

!

接口GigabitEthernet0/0

IP地址172.16.2.1 255.255.255.0

duplex auto

speed auto

!

ip route 0.0.0.0 0.0.0.0 172.16.2.2

!

IPSec配置

此部分描述R1和R2路由器的IPSec配置。

R1

!

IP访问控制列表延长的IPSec_Match

permit ip其中任一主机172.16.2.1

!

crypto isakmp policy 1

encr aes 256

哈希md5

authentication pre-share

第2组

crypto isakmp key cisco123地址172.16.1.2

!

!

crypto ipsec transform-set set2 ESP aes 256 esp-sha-hmac

模式通道

!

!

加密映射VPN 10 ipsec-isakmp

集合对等体172.16.1.2

set transform-set set2

匹配地址IPSec_Match

!

interface GigabitEthernet0/1

ip address 172.16.1.1 255.255.255.0

duplex auto

speed auto

加密映射VPN

!

R2

!

IP访问控制列表延长的IPSec_Match

permit IP主机其中任一172.16.2.1

!

crypto isakmp policy 1

encr aes 256

哈希md5

authentication pre-share

第2组

crypto isakmp key cisco123地址172.16.1.1

!

!

crypto ipsec transform-set set2 ESP aes 256 esp-sha-hmac

模式通道

!

!

加密映射VPN 10 ipsec-isakmp

集合对等体172.16.1.1

set transform-set set2

匹配地址IPSec_Match

反向路由

!

接口GigabitEthernet0/0/1

ip address 172.16.1.2 255.255.255.0

协商自动

cdp enable (event)

加密映射VPN

!

要验证是否IPSec设置工作正如所料，请检查输出show crypto isakmp sa

```
R1#show crypto isakmp sa

IPv4 crypto ISAKMP SA

dst srcconn-id

IPv6 crypto ISAKMP SA
```

为了带动安全关联，请ping出口方(R3， 172.16.2.1)从R1。

```
R1-ping 172.16.2.1

Type escape sequence to abort.

5 100-byte ICMP172.16.2.12

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms

R1-
```

现在，路由器将有一个即时安全审核关联，确认流量起源于R1和被注定对出口方是被封装的ESP。

```
R1#show crypto isakmp sa

IPv4 crypto ISAKMP SA

dst srcconn-id

172.16.1.2 172.16.1.1 QM_IDLE 1002

IPv6 crypto ISAKMP SA
```

EzPM配置

此部分描述R1路由器的EzPM配置。

R1

```
!

class-map match-all穿孔机星期一ACL

 说明PrimeAM生成的实体-请勿修改也请勿请使用此实体

 match protocol ip

!

性能监控程序上下文性能监控程序配置文件应用程序体验

 出口方目的地172.16.2.1来源GigabitEthernet0/1传输udp端口9991

 流量监控应用程序流量统计

 流量监控会话流量统计ipv4

 流量监控应用响应时间ipv4
```

流量监控媒体ipv4入口

流量监控媒体ipv4出口

流量监控URL ipv4中集集团替换穿孔机星期一ACL

!

应用在需要是受监视的接口的EzPM配置文件;此处我们监控loopback0接口。

R1

!

interface Loopback0

IP地址1.1.1.1 255.255.255.255

性能监控程序上下文性能监控程序

!

解决方法

使用到位上述配置，请采取输出为**显示性能监控程序**contextcontext-nameexporter。

检查**输出功能**选项状况，默认情况下应该在没**使用的**状态，是预料之中的行为，并且所以AVC流量没有被封装也没有加密此处。

为了让AVC流量穿过IPSec隧道接口，**输出功能**选项在使用的状态。并且执行那，它在flow exporter配置文件必须明确地启用。下面启用此选项的详细的逐步程序。

Step-1

采取完整输出为**显示性能监控程序上下文***上下文名称***配置命令**并且保存它在记事本。下面此输出的截取，

```
R1#show

!
================================================================================
=======

!              !

!
================================================================================
=======

!

! ==========
```

```
!

flow exporter Performance-Monitor-1



172.16.2.1

GigabitEthernet0/1

udp 9991

ipfix

300

300

VRF300

c3pl-class-table300

c3pl-policy-table300

300

300

300

SUB300

-----------------------------------------------
```

Step-2

明确地添加**output-features**选项在flow exporter配置文件下。在添加output-features选项以后flow exporter配置文件将看上去象这个，

```
flow exporter Performance-Monitor-1

 说明性能监控程序上下文性能监控程序出口方

 目的地172.16.2.1

 来源GigabitEthernet0/1

 传输udp 9991

 出口协议ipfix

 模板数据超时300
```

output-features

选项接口塔布莱超时300

选项VRF塔布莱超时300

选项c3pl-class-table超时300

选项c3pl-policy-table超时300

选项抽样人员塔布莱超时300

选项应用程序塔布莱超时300

选项应用程序属性超时300

选项SUB应用程序塔布莱超时300

留下输出的其余，不修改别的在输出中。

Step-3

现在，请删除EzPM配置文件从接口和从路由器。

!

Interface loopback 0

没有性能监控程序上下文性能监控程序

退出

!

!

没有性能监控程序上下文性能监控程序配置文件应用程序体验

!

Step-4

运用在R1路由器的已修改设置。确保没有单个命令没有未命中，因为可能引起所有意外行为。

验证

此部分描述在本文的验证使用的方法检查，并且此应急方案如何帮助解决被提及的AVC数据包的限制此处。

在应用应急方案前， IPSec同位路由器接收的数据包(R2)将丢弃。在消息之下将生成：

```
%IPSEC-3-RECVD_PKT_NOT_IPSEC Rec'dIPSec dest_addr= 172.16.2.1 src_addr=
```

```
172.16.1.1 prot= 17
```

此处R2期待为172.16.2.1是注定的ESP封装数据包，但是收到的信息包是无格式UDP数据包(prot=17)，并且它是丢弃这些数据包的预料之中的行为。在数据包捕获之下显示数据包接收在R2是一无格式UDP数据包而不是被封装的ESP，是AVC的默认行为。

```
Internet Protocol Version 4, Src: 172.16.1.1 (172.16.1.1), Dst: 172.16.2.1 (172.16.2.1)
  Version: 4
  Header Length: 20 bytes
⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
  Total Length: 1348
  Identification: 0x961a (38426)
⊞ Flags: 0x00
  Fragment offset: 0
  Time to live: 255
  Protocol: UDP (17)
⊞ Header checksum: 0xc56b [validation disabled]
  Source: 172.16.1.1 (172.16.1.1)
  Destination: 172.16.2.1 (172.16.2.1)
  [Source GeoIP: Unknown]
  [Destination GeoIP: Unknown]
User Datagram Protocol, Src Port: 50208 (50208), Dst Port: 9991 (9991)
  Source Port: 50208 (50208)
  Destination Port: 9991 (9991)
  Length: 1328
⊞ Checksum: 0xb7ec [validation disabled]
  [Stream index: 0]
Data (1320 bytes)
```

在应用应急方案以后，没有从下面的数据包捕获AVC数据包接收在R2是被封装的ESP和在R2看到的没有其他错误消息清楚看见。

```
Internet Protocol Version 4, Src: 172.16.1.1 (172.16.1.1), Dst: 172.16.1.2 (172.16.1.2)
  Version: 4
  Header Length: 20 bytes
⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
  Total Length: 1448
  Identification: 0x0114 (276)
⊞ Flags: 0x00
  Fragment offset: 0
  Time to live: 255
  Protocol: Encap Security Payload (50)
⊞ Header checksum: 0x5aec [validation disabled]
  Source: 172.16.1.1 (172.16.1.1)
  Destination: 172.16.1.2 (172.16.1.2)
  [Source GeoIP: Unknown]
  [Destination GeoIP: Unknown]
Encapsulating Security Payload
  ESP SPI: 0x804c46a3 (2152482467)
  ESP Sequence: 203
```

排除故障

目前没有有该配置的具体故障排除信息。