目次

概要

この資料が収集装置に IPSecトンネルを通して AVC トラフィックを通過させるために必要な設定を説明したものです。 デフォルトで、AVC 情報は収集装置に IPSecトンネルを渡ってエクスポートすることができません

前提条件

Cisco はこれらのトピックの基本的な知識があることを推奨します:

- アプリケーションの可視性と制御（AVC）
- 容易なパフォーマンスモニタ（EzPM）

背景説明

複数のアプリケ– ションに認識し、分析し、制御するのに Cisco AVC 機能が使用されています。 よりよいエンドユーザ体験に終ってネットワークで、アプリケーション 帯域幅 使用の粒状制御のための AVC 有効アプリケーション単位のポリシー、動作するアプリケーションのパフォーマンスに表示とネットワークインフラストラクチャに、構築されてアプリケーション 対応が。 このテクノロジーについてのより多くの詳細を見つけることができます。

EzPM は従来のパフォーマンスの監視 設定を設定するより速く、簡単な方法です。 現在 EzPM は提供しません従来のパフォーマンスモニタ 設定 モデルの完全な柔軟性を。 EzPM についての

より多くの詳細を見つけることができます。

制限事項

現在 AVC はパススルー トンネリング プロトコルの数を、詳細ここに見つけることができますサポートしません。

インターネット プロトコル セキュリティによって（IPSec）は AVC およびこの資料のためのサポートされていないパススルー トンネリング プロトコルの 1 つ当たりますこの制限のための可能性のある回避策がです。

設定

このセクションはある特定の制限を模倣するのに使用される完全な設定を説明します。

ネットワーク図

このネットワークダイアグラムでルータ全員にスタティック・ ルートを使用して到達可能性が互いにあります。 R1 は EzPM 設定で設定され、R2 ルータによって確立される 1 つの IPSecトンネルがあります。 R3 はエクスポーターもの Cisco プライム記号またはパフォーマンスデータを収集することができる他のどの種類である可能性がある エクスポーターとしてここにはたらいています。

AVC トラフィックは R1 によって生成され、R2 によってエクスポーターに送信 されます。 R1 は IPSecトンネル インターフェイス上の R2 に AVC トラフィックを送信 します。

初期設定

このセクションは R1 によって R3 のための初期設定を説明します。

R1

```
!
interface Loopback0
ip address 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 ルート 0.0.0.0 0.0.0.0 172.16.1.2
```

!

R2

!

インターフェイス GigabitEthernet0/0/0

IP アドレス 172.16.2.2 255.255.255.0

ネゴシエーション自動

!

インターフェイス GigabitEthernet0/0/1

ip address 172.16.1.2 255.255.255.0

ネゴシエーション自動

!

R3

!

インターフェイス GigabitEthernet0/0

ip address 172.16.2.1 255.255.255.0

duplex auto

speed auto

!

IP ルート 0.0.0.0 0.0.0.0 172.16.2.2

!

IPSec の設定

このセクションは R1 および R2 ルータのための IPSec構成を説明します。

R1

!

IPアクセスリスト拡張 IPSec_Match

割り当て IP ホスト 172.16.2.1

```
!
crypto isakmp policy 1
 encr aes 256
 hash md5
 authentication pre-share
 グループ 2
暗号 isakmp key cisco123 アドレス 172.16.1.2
!
!
暗号 IPSec トランスフォーム セット set2 esp-aes 256 esp-sha-hmac
 モード トンネル
!
!
crypto map vpn 10 ipsec-isakmp
 一定ピア 172.16.1.2
 transform-set set2 を設定 して下さい
 アドレス IPSec_Match を一致する
!
interface GigabitEthernet0/1
 ip address 172.16.1.1 255.255.255.0
 duplex auto
 speed auto
 crypto map vpn
!
```

R2

```
!
```

```
IPアクセスリスト拡張 IPSec_Match
 割り当て IPホスト 172.16.2.1
!
crypto isakmp policy 1
 encr aes 256
 hash md5
 authentication pre-share
 グループ 2
暗号 isakmp key cisco123 アドレス 172.16.1.1
!
!
暗号 IPSec トランスフォーム セット set2 esp-aes 256 esp-sha-hmac
 モード トンネル
!
!
crypto map vpn 10 ipsec-isakmp
 一定ピア 172.16.1.1
 transform-set set2 を設定 して下さい
 アドレス IPSec_Match を一致する
 反転ルート
!
インターフェイス GigabitEthernet0/0/1
 ip address 172.16.1.2 255.255.255.0
 ネゴシエーション自動
 cdp enable
 crypto map vpn
!
```

IPSec 構成が予想通りはたらいているかどうか確かめるために、show crypto isakmp sa があるように出力を確認して下さい

```
R1#show  isakmp sa

IPv4  ISAKMP SA

dst  conn ID

IPv6  ISAKMP SA
```

セキュリティ結合を始動するために、エクスポーター (R1 からの R3 を、172.16.2.1) ping して下さい。

```
R1#ping 172.16.2.1

Type escape sequence to abort.

5 100-byte ICMP  172.16.2.1   2 :

!!!!!

 100% 5/5 /avg/ = 1/1/4 ms
```

この場合、ルータは R1 から起き、エクスポーターに向かうトラフィックはカプセル化される ESP であることを確認するアクティブ セキュリティ アソシエーションを備えています。

```
R1#show  isakmp sa

IPv4  ISAKMP SA

dst  conn ID

172.16.1.2 172.16.1.1 QM_IDLE 1002

IPv6  ISAKMP SA
```

EzPM 設定

このセクションは R1 ルータのための EzPM 設定を説明します。

R1

```
!

class-map match-all PERF 月曜日 ACL

 説明 PrimeAM によって生成されるエンティティ-このエンティティを修正しませんでしたり、または使用しないで下さい
```

protocol ip を一致する

!

パフォーマンスモニタ コンテキスト パフォーマンスモニタ プロファイル アプリケーション エクスペリエンス

エクスポーター宛先 172.16.2.1 ソース GigabitEthernet0/1 転送する UDP（ユーザ・データグラム・プロトコル）ポート 9991

トラフィック モニタ アプリケーション トラフィック統計

トラフィック モニタ メッセージ交換トラフィック統計 ipv4

トラフィック モニタ Application Response Time ipv4

トラフィック モニタ メディア ipv4 入力

トラフィック モニタ メディア ipv4 出力

トラフィック モニタ URL ipv4 は PERF 月曜日 ACL をクラス取り替えます

!

監視される必要インターフェイスの EzPM プロファイルを適用して下さい; ここにループバック 0 インターフェイスを監視しています。

R1

!

interface Loopback0

ip address 1.1.1.1 255.255.255.255

パフォーマンスモニタ コンテキスト パフォーマンスモニタ

!

回避策

上の設定によって、出力をのための**示しますパフォーマンスモニタ** contextcontext-name**exporter を奪取** して下さい。

出力 機能 オプションのステータスがあるように確認して下さい、デフォルトで予期された動作であり、そういうわけで AVC トラフィックがカプセル化されないし、ここに暗号化されていない**使用されなかった**状態にあるはずです。

AVC トラフィック パススルーがインターフェイスするようにするために IPSecトンネルは使用された状態に**出力 機能** オプションあります。 そしてそれをするために、それはフロー エクスポーター プロファイルで明示的に 有効に ならなければなりません。 このオプションを有効に する詳しいステップバイステップ手順は下記にあります。

Step-1

完全な出力をのための示し、**パフォーマンスモニタ コンテキスト** *コンテキストネーム* **設定コマンドを**テキスト工ディタで保存します奪取 して下さい。 この出力のためのスニップは下記にあります、

```
R1#show

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

!              !

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

!

! ==========

!

  Performance-Monitor-1



 172.16.2.1

 GigabitEthernet0/1

 UDP  9991

  ipfix

   300

    300

 VRF   300

 c3pl-class-table  300

 c3pl-policy-table  300

   300

   300

  300

  300
```

Step-2

フロー エクスポーター プロファイルの下で**出力 機能** オプションを明示的に追加して下さい。 出力 機能 オプションを追加した後フロー エクスポーター プロファイルはこのようになります、

フロー エクスポーター Performance-Monitor-1

説明パフォーマンスモニタ コンテキスト パフォーマンスモニタ エクスポーター

宛先 172.16.2.1

ソース GigabitEthernet0/1

転送する UDP（ユーザ・データグラム・プロトコル）9991

エクスポート プロトコル ipfix

テンプレート データ タイムアウト 300

出力 機能

オプション インターフェイス テーブル タイムアウト 300

オプション VRF 表 タイムアウト 300

オプション c3pl-class-table タイムアウト 300

オプション c3pl-policy-table タイムアウト 300

オプション リファレンス表 タイムアウト 300

オプション アプリケーション表 タイムアウト 300

オプション アプリケーション属性タイムアウト 300

オプション副アプリケーション表 タイムアウト 300

あるように出力の他を、変えません出力で何か他のもの残して下さい。

Step-3

この場合、インターフェイスとルータから EzPM プロファイルを同様に取除いて下さい。

!

Interface loopback 0

パフォーマンスモニタ コンテキスト パフォーマンスモニタ無し

exit

!

!

パフォーマンスモニタ コンテキスト パフォーマンスモニタ プロファイル アプリケーション エクスペリエンス無し

!

Step-4

R1 ルータの修正された構成を適用して下さい。 により予期せぬ動作を引き起こすかもしれないのでない単一 コマンドが抜けていることを確かめて下さい。

検証

このセクションはこの回避策がここに述べられる AVC パケットのための制限のどのように克服を助けたかチェックするのにこの資料で使用される確認 方式を記述し。

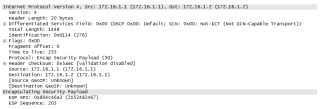
回避策を適用する前に、IPSec ピア ルータ（R2）によって受信されたパケットは廃棄されます。メッセージの下で同様に生成されます:

```
%IPSEC-3-RECVD_PKT_NOT_IPSEC: Rec'd  IPsecdest_addr= 172.16.2.1src_addr=
172.16.1.1prot= 17
```

ここに R2 は 172.16.2.1 に向かうが、受け取り パケットは明白な UDP パケット（prot=17）であり、ESP カプセル化されたパケットを期待していますそれはこれらのパケットを廃棄する予期された動作です。 パケットキャプチャの下で R2 で受信されるパケットがカプセル化される AVC のためのデフォルトの動作である ESP の代りに明白な UDP パケットであることを示します。

```
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)
```

回避策を適用した後、R2 で受信される AVC パケットがカプセル化される ESP であるおよび R2 で見られるこれ以上のエラーメッセージわかりませんことが下記のパケットキャプチャからはっきり。



トラブルシューティング

現在この設定に関する特定なトラブルシューティングの情報がありません。