IKEV2 VRF サポート

機能の概要と変更履歴

要約データ

該当製品または機能エリア	StarOS
該当プラットフォーム	• ASR 5500 • VPC-DI
機能のデフォルト	該当なし
このリリースでの関連する変更点	N/A
関連資料	該当なし

マニュアルの変更履歴

改訂の詳細	リリース
最初の導入。	• 21.28.m6 • 21.28.F3

機能説明

StarOS では、IKEv2 VRF 機能がない場合、IPSec IKEv1 トンネルのみが VRF 認識であり、IKEv1 は任意の VRF から発信される暗号化トラフィックをトンネルします。一方、IPSec IKEv2 トンネルは、デフォルトの VRF でのみトラフィックを確立して暗号化します。IKEv2 VRF 機能は、任意の VRF で IPSec IKEv2 トンネルの確立とトラフィックの暗号化をサポートします。

仕組み

ASR5500 および VPC-DI 環境で IKEv2 の VRF をサポートするには、復号されたパケットが破棄されないように、適切な VRF で処理する必要があります。次の機能が発生します。

- ACL は、制御パケットとトリガーパケットに対して初めてヒットします。
- IPSec にパケットを送信し、トンネルを作成します。
- キーの交換を開始し、キーペアによってトンネルを確立します。
- トンネルが確立されると、その特定の ipsecmgr フロー DB エントリが削除され、新しいエントリが作成されます。これにより、次のパケットが暗号エンジンに渡され、転送されます。これは、IPv4 と IPv6 に共通です。

。

制限事項

次の制限事項があります。

- キー交換とトンネルの確立は、トラフィックを暗号化する必要がある VRF ではなく、デフォルト VRF で行われます。
- 暗号マップごとの IPSec ACL の最大数は 7 です。APN で複数の IP チャンクをサポートするには、複数のアクセスリストを設定する必要があります。これにより、エンタープライズ VRF ごとの IPSec トンネルが複数になる可能性があります。
- 暗号マップに対応する ACL ルールを再設定するには、既存のトンネルを再確立する必要があります。この操作により、アップリンクおよびダウンリンクのサブスクライバトラフィックが中断します。

VRF を使用した IKEv2 IPSec の設定

VRF を使用して IKEv2 IPSec を設定するには、次の設定コマンド例を使用します。次の設定例は、エンタープライズ VRF と デフォルト VRF でループバック IP がオーバーラップして、デ

フォルト VRF からのキーの交換を可能にすると同時に、暗号マップを VRF インターフェイスに適用できるようにする方法を示しています。

```
context ipsec-s
    ip vrf i-s
    #exit
    ip access-list boo
      permit ip host 2.1.1.1 host 2.2.1.1
    #exit
    crypto ipsec transform-set A-foo esp hmac sha1-96 cipher aes-cbc-128
      mode tunnel
    #exit
    ipsec transform-set B-foo
      hmac sha2-256-128
      group 14
    #exit
    ikev1 policy 1
    #exit
    ikev2-ikesa transform-set ikesa-foo
      group 14
      hmac sha2-256-128
      prf sha2-256
    #exit
    crypto map foo ikev2-ipv4
      match address boo
      authentication local pre-shared-key encrypted key
+B0bqvzhrkkwujr2kt37b0yxo4631silym4g2zn9r2rs0o7xrn3r4i09aexdk701t8d0cqt2ivg039da1267r6tcurpyk3qhdjbfwo7t6s

      authentication remote pre-shared-key encrypted key
+B0975tvzeoi0lg2zl78a17mnhv20yw3cesh97zi436qvsyoadulmh2pbgcnndjxchq0c3fn5p2i3y7b12uqc4bwsmi5x324ikw0wfzus8

      ikev2-ikesa transform-set list ikesa-foo
      ikev2-ikesa rekey
      payload foo-sa0 match ipv4
        ipsec transform-set list B-foo
        rekey keepalive
      #exit
      peer 5.2.1.1
    #exit
    interface ike
      ip address 192.168.110.120 255.255.255.0
    #exit
    interface iv1 loopback
      ip vrf forwarding i-s
      ip address 2.1.1.1 255.255.255.255
    #exit
    interface iv2 loopback
      ip vrf forwarding i-s
      ip address 5.1.1.1 255.255.255.255
      crypto-map foo
    #exit
    interface iv3 loopback
      ip address 5.1.1.1 255.255.255.255
    #exit
    subscriber default
    exit
    aaa group default
    #exit
    gtpp limit-secondary-rat-usage 32
    ip route 5.2.1.1 255.255.255.255 192.168.110.89 ike
  #exit
  port ethernet 1/10
    no shutdown
    vlan 110
```

```
    no shutdown
    bind interface ike ipsec-s
  #exit
#exit
```

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。