IPSec を介した TACACS+

マニュアルの変更履歴

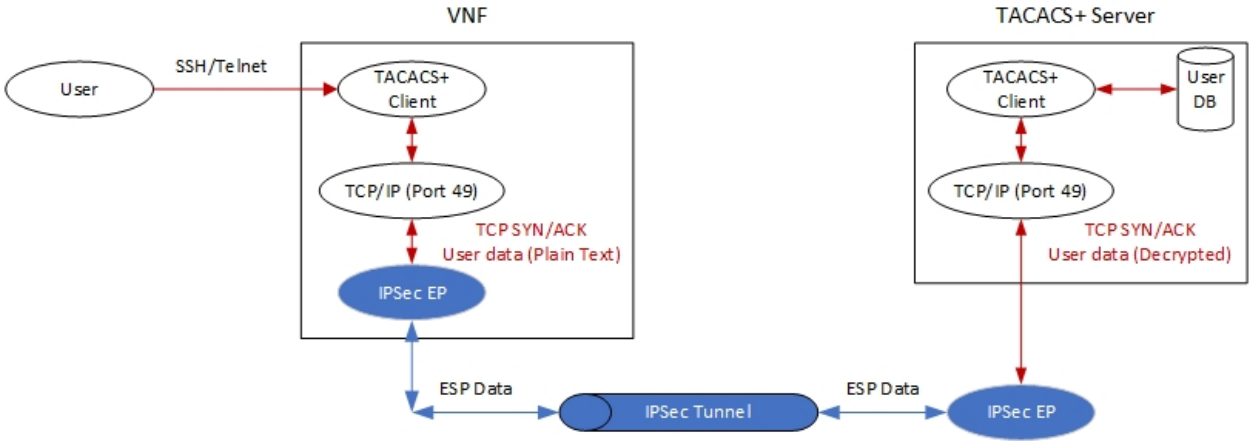
改訂の詳細	リリース
初版	21.24

機能説明

Terminal Access Controller Access Control Server Plus（TACACS+）は、StarOS でのユーザーアクセス権限の認証に使用されるセキュリティプロトコルです。TACACS+ クライアントおよびサーバーを介して送信される認証データを保護するために、CUPS VNF は認証データの暗号化に関して TACACS+ over IPSec をサポートしています。

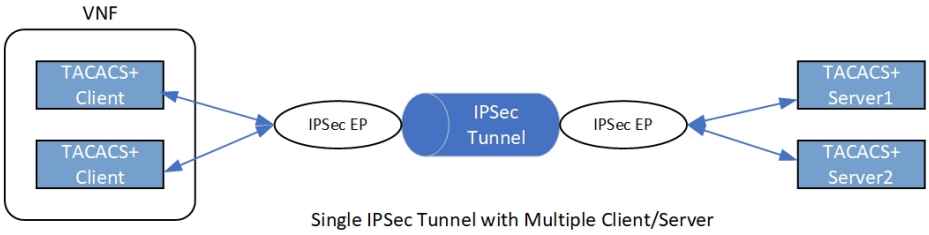
アーキテクチャ

次の図は、セキュアな TACACS+ アーキテクチャを示しています。

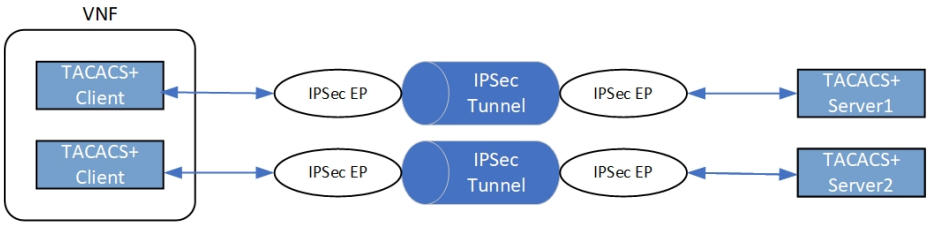


導入アーキテクチャ

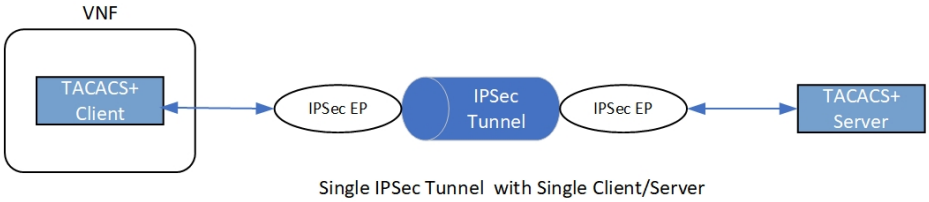
TACACS+クライアント/サーバーをセキュアな方法で使用する方法は複数あります。単一または複数の TACACS+ サーバーを使用できます。単一の VNF で単一または複数のクライアントをホストできます。TACACS+ over IPSec ソリューションは、単一の VNF で複数のクライアントを処理できます。



Single IPSec Tunnel with Multiple Client/Server



Multiple IPSec Tunnel with Multiple Client/Server



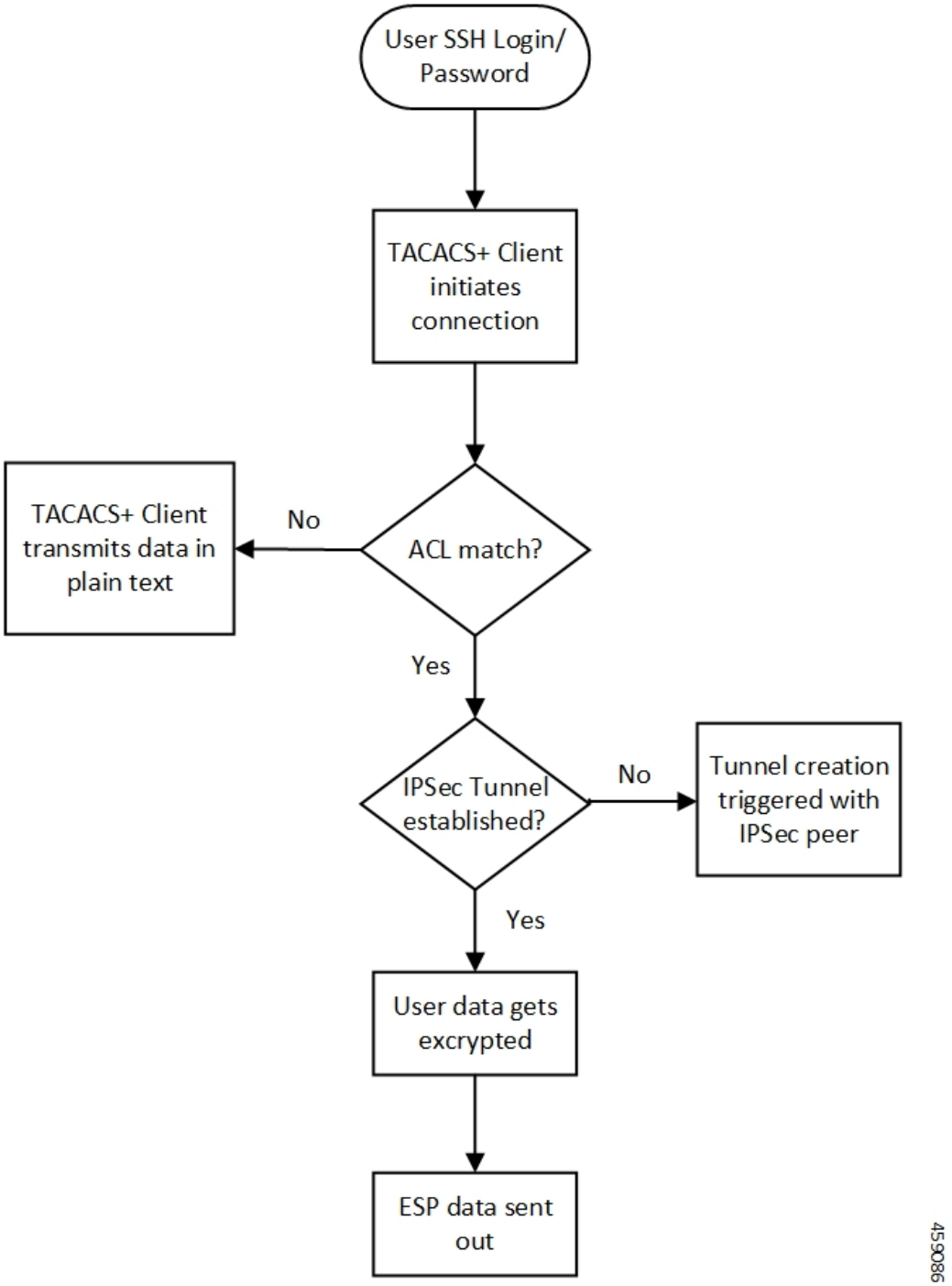
Single IPSec Tunnel with Single Client/Server

機能の仕組み

展開要件に応じて、保護する必要がある複数のアプリケーションには、独立した ACL ルールがあります。これらの ACL ルールは、単一の暗号マップまたは個別の暗号マップの一部として設定されます。どちらの場合も、複数の TUN インターフェイスが作成され、暗号化を必要とする各アプリケーションに接続されます。

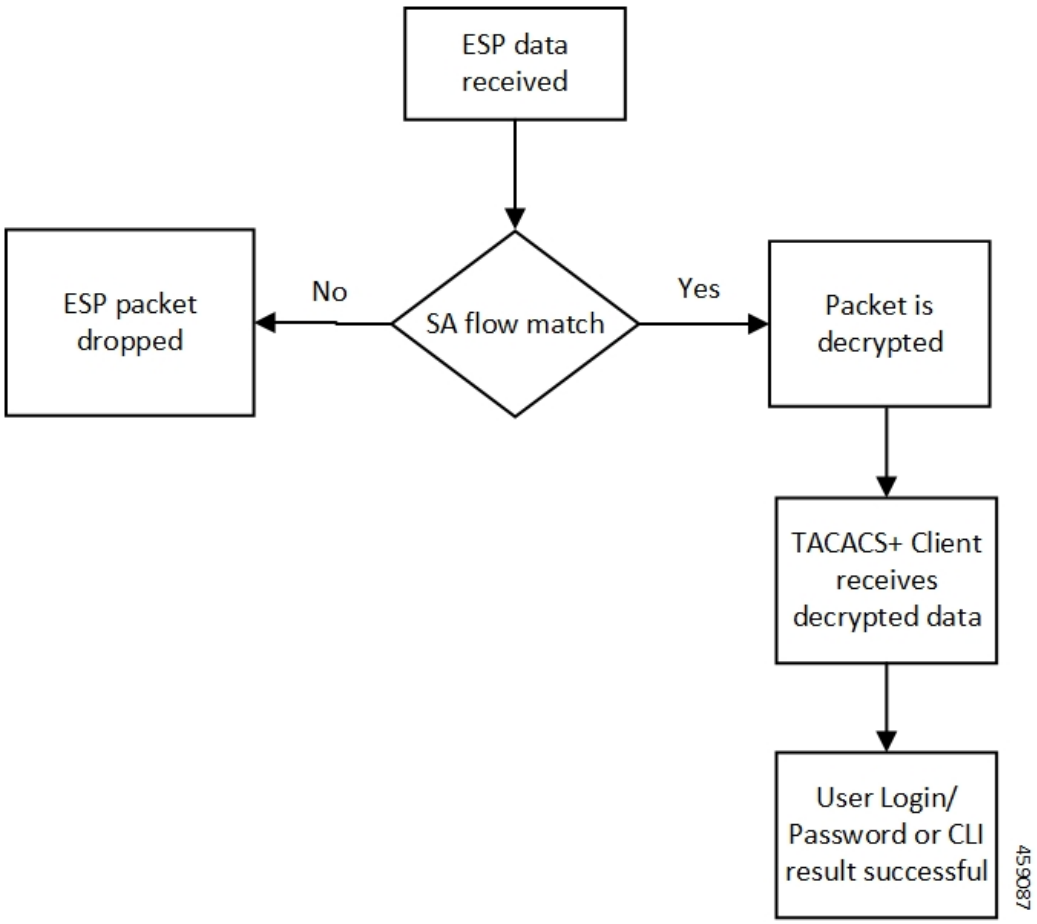
TACACS+ クライアントデータの暗号化

次の図は、トンネルの確立とパケット暗号化を表したものです。



TACACS+ サーバーデータの復号

次の図は、パケットの復号について説明したものです。



次の手順では、IPSec を介して TACACS+ データセキュリティを実現するためのパケットフローについて説明します。

1. TACACS+/アプリケーションは、最初の TCP-SYN パケットの形式で TACACS+ サーバーとの TCP 接続を開始します。
2. SYN パケットは TUN インターフェイスにルーティングされ、ローカルコンテキストで IpsecMgr によって直接読み取られます。
3. IpsecMgr は、ACL と照合するために TCP-SYN パケットを NPUSIM の最初のインスタンスに送信します。
    1. ACL エントリが TCP-SYN パケットと一致する場合、パケットを IpsecMgr またはローカルに送り返します。
    2. パケットが ACL エントリと一致しない場合、NPUSIM はパケットの暗号化を回避して、ローカル管理インターフェイスにパケットを送信します。
4. IpsecMgr またはローカルコンテキストは、ACL との照合の後に NPUSIM からパケットを受信します。ローカルコンテキストで作成されたローカル raw ソケットを使用して IKE-INIT/IKE-AUTH パケットを交換することで、ピアとの IPSec トンネルの形成をトリガーします。

5. 最初の TCP-SYN パケットは、IPSec トンネルの作成をトリガーした後、IpsecMgr またはローカルでドロップされます。
6. TACACS+ やアプリケーションが別の TCP-SYN パケットを送信し、ステップ 2 ～ 3b が繰り返されます。
7. IpsecMgr は ACL との照合の後に NPUSIM から 2 番目の TCP-SYN パケットを受信すると、トンネルはすでに確立されているため、TCP-SYN パケットを暗号化し、IpsecMgr やローカルによってローカルコンテキストで作成された ESP raw ソケットを介してパケットを送信します。
8. IpsecMgr は、管理ポートを介してローカルコンテキストの ESP raw ソケットから送られてきた ESP パケットもリッスンします。
9. IpsecMgr やローカルで ESP パケットを受信すると、SA フロー処理のために ESP パケットを NPUSIM に送信します。
10. SA フローが NPUSIM で一致する場合、ESP パケットはパケットの復号を行う IpsecMgr またはローカルに送信されます。
11. このパケットは、TACACS+ クライアントから TACACS+ サーバーに送信された 2 番目の TCP-SYN パケットの応答である TCP-SYN-ACK の可能性があります。
12. 復号されたパケットは、TACACS+ またはアプリケーションに返送されたときの送信元の TUN インターフェイスに返送されます。
13. 双方向通信は、TCP-ACK パケットを送信する TACACS+ またはアプリケーションによって確立されます。上記の手順は、後続のすべてのパケットのデータセキュリティを実現するために繰り返されます。

リカバリ

IPsec トンネルは、アクティブの TACACS+ クライアントと TACACS+ サーバーアプリケーションの間で確立されます。スタンバイと TACACS+ サーバー間には IPsec トンネルは確立されません。通常のシナリオでは、IPsec エンドポイントが情報（ハートビート）メッセージを交換して、IPsec トンネルの正常性を確認します。アクティブ VNF がダウンした場合、TACACS+ サーバーの IPSec エンドポイントは、アクティブ VNF の IPSec エンドポイントのデッドピア検出（DPD）によりそれを検出します。DPD タイムアウトも設定可能です。DPD は、TACACS+ サーバー側でトンネルのクリアをトリガーします。スタンバイ VNF がアクティブに戻り、TACACS+ アプリケーションが TACACS+ サーバーアプリケーションとのデータ交換を開始すると、新しいアクティブ VNF と TACACS+ サーバー間に新しい IPsec トンネルが確立されます。

制限事項

この機能には次の既知の制限事項があります。

- IPv6 を使用する TACACS+ は、IPv6 トンネルエンドポイントを使用する IPSec ではサポートされません。ただし、IPSec を使用しない場合は、IPv6 を使用する TACACS+ がサポートされます。また、IPv4 を使用する TACACS+ は、IPv4 トンネルエンドポイントを使用する IPSec の有無にかかわらずサポートされます。
- ローカルコンテキストの暗号マップは、Day-0/Day-1 設定の一部として事前設定する必要があります。つまり、ローカルコンテキストの暗号マップがある場合は、他のコンテキストで暗号マップを設定する前に、ローカルコンテキストで暗号マップを設定する必要があります。

TACACS+ over IPSec の設定

ここでは、TACACS+ over IPSec 機能の設定方法について説明します。

この設定には、次の手順が含まれます。

1. TACACS+ コンフィギュレーション モードの設定。
2. IPSec を使用した TACACS+ のプロビジョニング。
3. トンネルモードでの IPSec を使用した TACACS+ のプロビジョニング。
4. トランスポートモードでの IPSec を使用した TACACS+ のプロビジョニング

TACACS+ コンフィギュレーション モードの設定

StarOS/VNF で TACACS+ をプロビジョニングするための設定は、非 CUPS アーキテクチャでの設定と同じです。ただし、「IPSec トンネルモード」でトンネルを確立するには、**src-ip** をプロビジョニングする必要があります。TACACS+通信用に追加の送信元IPアドレス（*src_ip*）を 1 つ予約し、その通信を保護する必要があります。

「IPSec トランスポートモード」でトンネルを確立する場合、追加の **src-ip** をプロビジョニングする必要はありません。管理インターフェイス IP アドレスは **src-ip** として選択されます。

以下に設定例を示します。

```
configure
  context context_name
    tacacs mode
      server priority priority_number ip-address server_ip_address password
text_password src_ip
      accounting command
      authorization prompt
    #exit
  aaa tacacs+
end
```

IPSec を使用した TACACS+ のプロビジョニング

次の設定により、すべての IKE/ESP パケットがユーザースペースの IPSec マネージャまたはローカルで処理されます。非ローカルコンテキストや VPP、IFtask、NPU などの基盤となるデータプレーンの IPSec マネージャでは処理されません。

```
configure
  require crypto ikev1-acl software context context
  require crypto ikev2-acl software context context
end
```

トンネルモードでの IPSec を使用した TACACS+ のプロビジョニング

次の設定例では、トンネルモードのローカルコンテキストでクリプトマップを作成します。**209.165.201.1** と **209.165.200.225** は、それぞれ TACACS+ サーバーとクラアントの IP アドレスと見なされます。

（注） 現在、トンネルモードは IKEv2 でのみサポートされています。

```
configure
  context local
    ip access-list foo
      permit ip 209.165.200.225 1 0.0.0.0 209.165.201.1 0.0.0.0
    #exit
    ipsec transform-set B-foo
      group 14
    #exit
    ikev2-ikesa transform-set ikesa-foo
      group 14
    #exit
    crypto map foo ikev2-ipv4
      match address foo
      authentication local pre-shared-key encrypted key EncryptedKey1
      authentication remote pre-shared-key encrypted key EncryptedKey2
      ikev2-ikesa max-retransmission 3
      ikev2-ikesa retransmission-timeout 2000
      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 209.165.200.226
      ikev2-ikesa policy error-notification
    #exit
    interface local1
      ip address 209.165.200.227 255.255.255.224
      ipv6 address 2001:420:2c7f:f620::83/64 secondary
      crypto-map foo
    #exit
```

トランスポートモードでの IPSec を使用した TACACS+ のプロビジョニング

次の設定例では、**209.165.200.229** が TACACS+ サーバーの IP アドレスと見なされるトランスポートモードのローカルコンテキストでクリプトマップを作成します。

（注） 現在、トランスポートモードは IKEv1 でのみサポートされています。

```
configure
  context local
    ip access-list foo
      permit tcp 209.165.200.228 0.0.0.0 209.165.200.229 0.0.0.0
    #exit
    ip routing shared-subnet
    ikev1 keepalive dpd interval 3600 timeout 10 num-retry 3
    crypto ipsec transform-set A-foo esp hmac sha1-96 cipher aes-cbc-128
      mode transport
    #exit
    ikev1 policy 1
    #exit
    crypto map foo ipsec-ikev1
      match address foo
      set peer 209.165.200.229
      set ikev1 encrypted preshared-key EncryptedKey1
      set pfs group2
      set transform-set A-foo
    #exit
    interface local1
      ip address 209.165.200.228 255.255.255.224
      ipv6 address 2001:420:2c7f:f620::84/64 secondary
      crypto-map foo
    #exit
```

モニタリングおよびトラブルシューティング

コマンドと出力の表示

この機能をサポートするために、次の show CLI コマンドを使用できます。

- **show crypto map**
- **show crypto ikev2-ikesa security-associations** *summary*
- **show crypto ikev1 security-associations** *summary*
- **show crypto statistics**
- **show crypto ipsec security-associations** *summary*

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。