

IOS ルータでの NAT を使用した IPSec/GRE の設定例

目次

[概要](#)

[はじめに](#)

[表記法](#)

[前提条件](#)

[使用するコンポーネント](#)

[設定](#)

[ネットワーク図](#)

[設定](#)

[確認](#)

[トラブルシューティング](#)

[トラブルシューティングのためのコマンド](#)

[セキュリティ アソシエーション \(SA \) の消去](#)

[関連情報](#)

概要

この設定例は、generic routing encapsulation (GRE) /IPsec トンネルがネットワークアドレス変換 (NAT)を稼働しているファイアウォールを通過する IPsec (IPSec)上に GRE を設定する方法を示しています。

はじめに

表記法

ドキュメント表記の詳細は、『[シスコ テクニカル ティップスの表記法](#)』を参照してください。

前提条件

このタイプの設定は、IPX (次の例を参照) やルーティング アップデートなど、通常はファイアウォールを通過しない、トラフィックのトンネル化や暗号化に使用できます。この例では、2621 と 3660 間のトンネルは、トラフィックが LAN セグメントのデバイス (IPSec ルータからの拡張 IP および IPX の ping ではなく) で生成された場合にのみ、動作します。注 :

注: これは、ポートアドレス変換 (PAT) では動作しません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco IOS® 12.4
- Cisco PIX Firewall 535
- Cisco PIX Firewall ソフトウェア リリース 7.x 以降

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。対象のネットワークが実稼働中である場合には、どのような作業についても、その潜在的な影響について確実に理解しておく必要があります。

設定

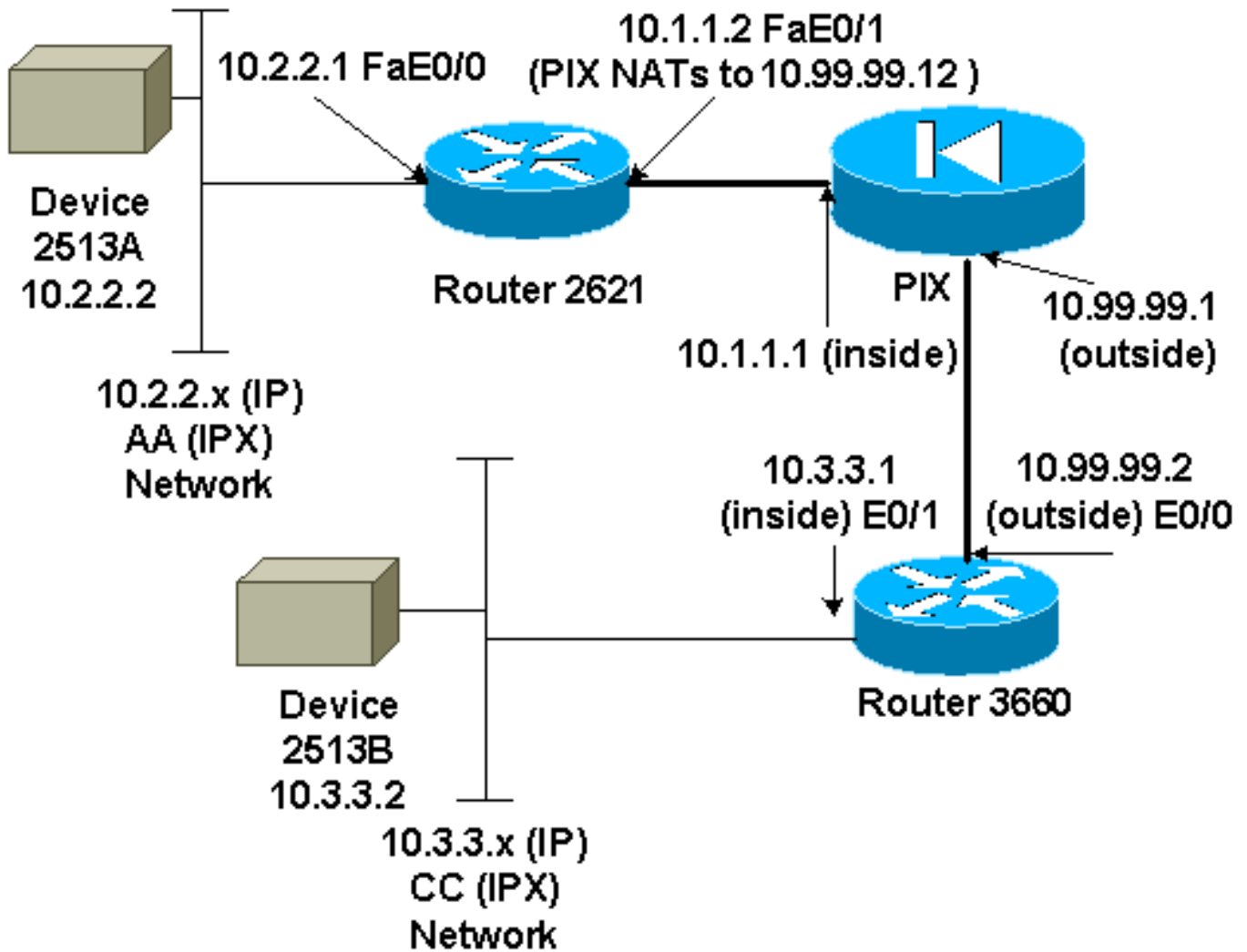
この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

注: このドキュメントで使用されているコマンドの詳細を調べるには、[Command Lookup Tool](#) ([登録ユーザ専用](#)) を使用してください。

IOS 設定に関する注意： Cisco IOS 12.2(13)T 以降のコード (より大きな番号が付けられた T-train コード、12.3 以降のコード) では、設定済みの IPSEC 「crypto マップ」を物理インターフェイスに適用するだけですみ、GRE トンネル インターフェイスに適用する必要はありません。12.2.(13)T 以降を使用している場合に、物理インターフェイスとトンネル インターフェイスの両方に「crypto マップ」を適用しても、正常に動作します。ただし、物理インターフェイスだけで適用することを強くお勧めします。

ネットワーク図

このドキュメントでは次の図に示すネットワーク



注: この設定で使用している IP アドレスは、インターネット上で正式にルーティング可能なものではありません。これらは [RFC 1918](https://www.rfc-editor.org/rfc/rfc1918) で、ラボ環境で使用されたアドレスです。

ネットワーク ダイアグラムに関する注記

- 10.2.2.1 から 10.3.3.1 (IPX ネットワーク BB) への GRE トンネル
- 10.1.1.2 (10.99.99.12) から 10.99.99.2 への IPSec トンネル

設定

デバイス 2513A
<pre> ipx routing 00e0.b064.20c1 ! interface Ethernet0 ip address 10.2.2.2 255.255.255.0 no ip directed-broadcast ipx network AA ! ip route 0.0.0.0 0.0.0.0 10.2.2.1 !--- Output Suppressed </pre>
2621
<pre> version 12.4 service timestamps debug uptime service timestamps log uptime no service password-encryption </pre>

```
!  
hostname 2621  
!  
ip subnet-zero  
!  
ip audit notify log  
ip audit po max-events 100  
ipx routing 0030.1977.8f80  
isdn voice-call-failure 0  
cns event-service server  
!  
crypto isakmp policy 10  
  hash md5  
  authentication pre-share  
crypto isakmp key cisco123 address 10.99.99.2  
!  
crypto ipsec transform-set myset esp-des esp-md5-hmac  
!  
crypto map mymap local-address FastEthernet0/1  
crypto map mymap 10 ipsec-isakmp  
  set peer 10.99.99.2  
  set transform-set myset  
  match address 101  
!  
controller T1 1/0  
!  
interface Tunnel0  
  ip address 192.168.100.1 255.255.255.0  
  no ip directed-broadcast  
  ipx network BB  
  tunnel source FastEthernet0/0  
  tunnel destination 10.3.3.1  
  crypto map mymap  
!  
interface FastEthernet0/0  
  ip address 10.2.2.1 255.255.255.0  
  no ip directed-broadcast  
  duplex auto  
  speed auto  
  ipx network AA  
!  
interface FastEthernet0/1  
  ip address 10.1.1.2 255.255.255.0  
  no ip directed-broadcast  
  duplex auto  
  speed auto  
  crypto map mymap  
!  
ip classless  
ip route 10.3.3.0 255.255.255.0 Tunnel0  
ip route 10.3.3.1 255.255.255.255 10.1.1.1  
ip route 10.99.99.0 255.255.255.0 10.1.1.1  
no ip http server  
!  
access-list 101 permit gre host 10.2.2.1 host 10.3.3.1  
!  
line con 0  
  transport input none  
line aux 0  
line vty 0 4  
!  
no scheduler allocate  
end
```

!--- Output Suppressed

PIX

```
pixfirewall# sh run
: Saved
:
PIX Version 7.0
!
hostname pixfirewall
enable password 2KFQnbNIdI.2KYOU encrypted
names
!
interface Ethernet0
 nameif outside
 security-level 0
 ip address 10.99.99.1 255.255.255.0
!
interface Ethernet1
 nameif inside
 security-level 100
 ip address 10.1.1.1 255.255.255.0
!
global (outside) 1 10.99.99.50-10.99.99.60
nat (inside) 1 0.0.0.0 0.0.0.0 0 0

static (inside,outside) 10.99.99.12 10.1.1.2 netmask
255.255.255.255 0 0
access-list 102 permit esp host 10.99.99.12 host
10.99.99.2
access-list 102 permit udp host 10.99.99.12 host
10.99.99.2 eq isakmp

route outside 0.0.0.0 0.0.0.0 10.99.99.2 1
route inside 10.2.2.0 255.255.255.0 10.1.1.2 1
```

!--- Output Suppressed

3660

```
version 12.4
service timestamps debug datetime
service timestamps log uptime
no service password-encryption
!
hostname 3660
!
memory-size iomem 30
ip subnet-zero
no ip domain-lookup
!
ipx routing 0030.80f2.2950
cns event-service server
!
crypto isakmp policy 10
 hash md5
 authentication pre-share
crypto isakmp key cisco123 address 10.99.99.12
!
crypto ipsec transform-set myset esp-des esp-md5-hmac
!
crypto map mymap local-address FastEthernet0/0
crypto map mymap 10 ipsec-isakmp
 set peer 10.99.99.12
 set transform-set myset
```

```
match address 101
!
interface Tunnel0
 ip address 192.168.100.2 255.255.255.0
 no ip directed-broadcast
 ipx network BB
 tunnel source FastEthernet0/1
 tunnel destination 10.2.2.1
 crypto map mymap
!
interface FastEthernet0/0
 ip address 10.99.99.2 255.255.255.0
 no ip directed-broadcast
 ip nat outside
 duplex auto
 speed auto
 crypto map mymap
!
interface FastEthernet0/1
 ip address 10.3.3.1 255.255.255.0
 no ip directed-broadcast
 ip nat inside
 duplex auto
 speed auto
 ipx network CC
!
ip nat pool 3660-nat 10.99.99.70 10.99.99.80 netmask
255.255.255.0
ip nat inside source list 1 pool 3660-nat
ip classless
ip route 0.0.0.0 0.0.0.0 Tunnel0
ip route 10.2.2.1 255.255.255.255 10.99.99.1
ip route 10.99.99.12 255.255.255.255 10.99.99.1
no ip http server
!
access-list 1 permit 10.3.3.0 0.0.0.255
access-list 101 permit gre host 10.3.3.1 host 10.2.2.1
!
line con 0
 transport input none
line aux 0
line vty 0 4
 login
!
end
!--- Output Suppressed
```

デバイス 2513B

```
ipx routing 00e0.b063.e811
!
interface Ethernet0
 ip address 10.3.3.2 255.255.255.0
 no ip directed-broadcast
 ipx network CC
!
ip route 0.0.0.0 0.0.0.0 10.3.3.1
!--- Output Suppressed
```

確認

このセクションでは、設定が正常に動作しているかどうかを確認する際に役立つ情報を提供して

います。

特定の **show** コマンドは、[Output Interpreter Tool](#) ([登録ユーザ専用](#)) によってサポートされています。このツールを使用すると、**show** コマンド出力の分析を表示できます。

- [show crypto ipsec sa](#) - フェーズ 2 のセキュリティ アソシエーションを表示します。
- [show crypto isakmp sa](#) - すべての暗号化エンジンで現在実行中の暗号化セッションの接続を表示します。
- オプション : [show interfaces tunnel number](#) - トンネル インタフェース情報を表示します。
- [show ip route](#) - すべてのスタティック IP ルート、または、認証、許可、およびアカウントリング (AAA) ルート ダウンロード機能を使用してインストールされたスタティック IP ルートを表示します。
- [show ipx route](#) - IPX ルーティング テーブルの内容を表示します。

[トラブルシューティング](#)

ここでは、設定のトラブルシューティングに役立つ情報について説明します。

[トラブルシューティングのためのコマンド](#)

特定の **show** コマンドは、[Output Interpreter Tool](#) ([登録ユーザ専用](#)) によってサポートされています。このツールを使用すると、**show** コマンド出力の分析を表示できます。

注: **debug** コマンドを使用する前に、『[debug コマンドに関する重要な情報](#)』を参照してください。

- [debug crypto engine](#) - 暗号化されたトラフィックを表示します。
- [debug crypto ipsec](#) - フェーズ 2 の IPSec ネゴシエーションを表示します。
- [debug crypto isakmp](#) - フェーズ 1 の Internet Security Association and Key Management Protocol (ISAKMP) ネゴシエーションを表示します。
- オプション : [debug ip routing](#) - ルーティング情報プロトコル (RIP) ルーティング テーブルの更新とルートキャッシュ更新に関する情報を表示します。
- [debug ipx routing {activity | events}](#) - `debug ipx routing {activity | events}` - ルータが送受信する IPX ルーティング パケットに関する情報を表示します。

[セキュリティ アソシエーション \(SA \) の消去](#)

- [clear crypto ipsec sa](#) - IPSec のすべてのセキュリティ アソシエーションを消去します。
- [clear crypto isakmp](#) - IKE セキュリティ アソシエーションを消去します。
- オプション : [clear ipx route *](#) - IPX ルーティング テーブルからすべてのルートを削除します。

[関連情報](#)

- [IP セキュリティ \(IPSec \) 製品に関するサポートページ](#)
- [サポート ページ : GRE](#)
- [テクニカルサポート - Cisco Systems](#)