NAT とスタティックを使用したルータ IPsec トンネルのプライベート間ネットワークの設定

目次

概要

この設定例では、次の方法を説明します。

- 2 つのプライベート ネットワーク (10.1.1.x と 172.16.1.x) 間でのトラフィックの暗号化。
- 10.1.1.3 のネットワーク デバイスへのスタティック IP アドレス (外部アドレス 200.1.1.25) の割り当て。

Access Control List (ACL; アクセス コントロール リスト) を使用して、プライベート間ネットワーク トラフィックに対して Network Address Translation (NAT; ネットワーク アドレス変換) を行わないようにルータに通知します。続いてこのトラフィックは暗号化され、ルータから発信される際にトンネル上に配置されます。 この設定例には、10.1.1.x ネットワーク上の内部サーバ用のスタティック NAT もあります。 この設定例では NAT コマンドで route-map オプションを使用して、ネットワーク アドレス変換されないようにしています (トラフィックに暗号化されたトンネル経由の宛先が設定されている場合) 。

前提条件

要件

このドキュメントに関する固有の要件はありません。

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(R) ソフトウェア リリース 12.3(14)T
- 2 台の Cisco ルータ

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。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

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。

ACL の deny 文で NAT トラフィックを指定する理由

Cisco IOS IPsec または VPN を使用する場合、概念上では、ネットワークをトンネルに置き換えることになります。 次の図では 200.1.1.1 から 100.1.1.1 に向かう Cisco IOS IPsec トンネルにより、インターネット クラウドを置き換えます。 このトンネルでリンクされている 2 つのプライベート LAN の視点からは、このネットワークを透過的にします。 このため、通常は、1 つのプライベート LAN からリモートのプライベート LAN へ向かうトラフィックには NAT を使用する必要はありません。 パケットが内部 Router 3 ネットワークに到達する場合、200.1.1.1 ではなく 10.1.1.0/24 ネットワークからの発信元 IP アドレスを持つ Router 2 ネットワークからのパケットを確認する必要があります。

NAT の設定方法の詳細は、『NAT の処理順序』を参照してください。 このドキュメントでは、パケットが内部から外部へ向かう際に、暗号化チェックの前に NAT が行われることが示されています。 設定でこの情報を指定する必要があるのはこのためです。

```
ip nat inside source list 122 interface Ethernet0/1 overload

access-list 122 deny ip 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255
access-list 122 permit ip 10.1.1.0 0.0.0.255 any
```

注: トンネルを構築したまま NAT を使用することも可能です。 この場合、NAT トラフィックを「IPsec の対象トラフィック」（このドキュメントの他のセクションでは ACL 101 と呼ばれる）として指定します。 NAT がアクティブである間にトンネルを構築する方法の詳細については、『LAN のサブネットが重複しているルータ間での IPSec トンネルの設定』を参照してください。

スタティック NAT の概要と、IPsec トンネル経由で当該アドレスに到達できない理由

この設定には、10.1.1.3 のサーバに関するスタティックな 1 対 1 の NAT も含まれます。 インターネット ユーザがアクセスできるように、これは 200.1.1.25 にネットワーク アドレス変換されます。 次のコマンドを発行します。

```
ip nat inside source static 10.1.1.3 200.1.1.25
```

このスタティック NAT により、172.16.1.x ネットワーク上のユーザは、暗号化されたトンネルを

経由しては 10.1.1.3 に到達できなくなります。 ACL 122 を使用して、暗号化されたトラフィックがネットワーク アドレス変換されないようにする必要があるのはこのためです。 ところが、スタティック NAT コマンドは、10.1.1.3 とのすべての接続に関する一般的な NAT 文よりも優先されます。 スタティック NAT 文では、暗号化されたトラフィック特定的に、ネットワーク アドレス変換されないようにしているのではありません。 172.16.1.x ネットワーク上のユーザが 10.1.1.3 に接続し、そのため暗号化されたトンネル経由では戻らない場合、10.1.1.3 からの応答は 200.1.1.25 にネットワーク アドレス変換されます (NAT は暗号化の前に行われます) 。

スタティック NAT 文で route-map コマンドを使用して、暗号化されたトラフィックがネットワーク アドレス変換 (スタティックな 1 対 1 の NAT であっても) されないようにする必要があります。

注: スタティック NAT に対する route-map オプションは、Cisco IOS ソフトウェア リリース 12.2(4)T 以降でのみサポートされています。 詳細については、『NAT：スタティック変換によりルート マップを使用する機能』を参照してください。

スタティックにネットワーク アドレス変換されるホストである 10.1.1.3 への暗号化されたアクセスを許可するには、次の追加コマンドを発行する必要があります。

```
ip nat inside source static 10.1.1.3 200.1.1.25 route-map nonat
!
access-list 150 deny   ip host 10.1.1.3 172.16.1.0 0.0.0.255
access-list 150 permit ip host 10.1.1.3 any
!
route-map nonat permit 10
 match ip address 150
```

これらの文により、ACL 150 に一致するトラフィックにのみスタティック NAT を適用するようにルータに通知されます。 ACL 150 では、発信元が 10.1.1.3 であり、宛先が暗号化されたトンネル経由の 172.16.1.x であるトラフィックには NAT を適用しないように指定されています。 ただし、発信元が 10.1.1.3 であるその他すべてのトラフィック (インターネットベースのトラフィック) には NAT が適用されます。

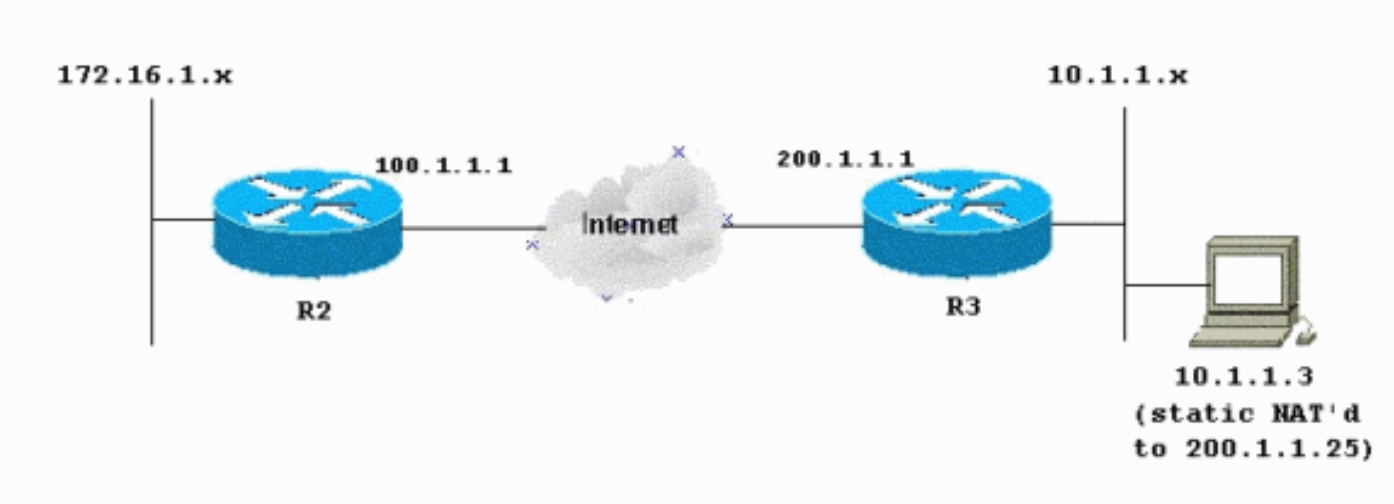
設定

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。

ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。



設定

このドキュメントでは、次の設定を使用します。

- ルータ 2
- ルータ 3

R2：ルータ設定

```
R2#write terminal
Building configuration...
Current configuration : 1412 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R2
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
clock timezone EST 0
ip subnet-zero
no ip domain lookup
!
!
crypto isakmp policy 10
 authentication pre-share
!
crypto isakmp key ciscokey address 200.1.1.1
!
!
crypto ipsec transform-set myset esp-3des esp-md5-hmac
!
crypto map myvpn 10 ipsec-isakmp
 set peer 200.1.1.1
 set transform-set myset
!--- Include the private-network-to-private-network
```

```
traffic !--- in the encryption process: match address
101
!
!
!
interface Ethernet0/0
 ip address 172.16.1.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
!
interface Ethernet1/0
 ip address 100.1.1.1 255.255.255.0
 ip nat outside
 ip virtual-reassembly
 crypto map myvpn
!
ip classless
ip route 0.0.0.0 0.0.0.0 100.1.1.254
!
ip http server
no ip http secure-server
!
!--- Except the private network from the NAT process: ip
nat inside source list 175 interface Ethernet1/0
overload
!
!--- Include the private-network-to-private-network
traffic !--- in the encryption process: access-list 101
permit ip 172.16.1.0 0.0.0.255 10.1.1.0 0.0.0.255
!--- Except the private network from the NAT process:
access-list 175 deny   ip 172.16.1.0 0.0.0.255 10.1.1.0
0.0.0.255
access-list 175 permit ip 172.16.1.0 0.0.0.255 any
!
!
!
control-plane
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 login
!
end
```

R3：ルータ設定

```
R3#write terminal
Building configuration...
Current configuration : 1630 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R3
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
```

```
!
resource policy
!
clock timezone EST 0
ip subnet-zero
no ip domain lookup
!
crypto isakmp policy 10
 authentication pre-share
crypto isakmp key ciscokey address 100.1.1.1
!
!
crypto ipsec transform-set myset esp-3des esp-md5-hmac
!
crypto map myvpn 10 ipsec-isakmp
 set peer 100.1.1.1
 set transform-set myset
!--- Include the private-network-to-private-network
traffic !--- in the encryption process: match address
101
!
!
!
interface Ethernet0/0
 ip address 10.1.1.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
!
interface Ethernet1/0
 ip address 200.1.1.1 255.255.255.0
 ip nat outside
 ip virtual-reassembly
 crypto map myvpn
!
!
ip classless
ip route 0.0.0.0 0.0.0.0 200.1.1.254
!
no ip http server
no ip http secure-server
!
!--- Except the private network from the NAT process: ip
nat inside source list 122 interface Ethernet1/0
overload
!--- Except the static-NAT traffic from the NAT process
if destined !--- over the encrypted tunnel: ip nat
inside source static 10.1.1.3 200.1.1.25 route-map nonat
!
access-list 101 permit ip 10.1.1.0 0.0.0.255 172.16.1.0
0.0.0.255
!--- Except the private network from the NAT process:
access-list 122 deny   ip 10.1.1.0 0.0.0.255 172.16.1.0
0.0.0.255
access-list 122 permit ip 10.1.1.0 0.0.0.255 any
!--- Except the static-NAT traffic from the NAT process
if destined !--- over the encrypted tunnel: access-list
150 deny   ip host 10.1.1.3 172.16.1.0 0.0.0.255
access-list 150 permit ip host 10.1.1.3 any
!
route-map nonat permit 10
 match ip address 150
!
!
!
```

```
control-plane
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 login
!
end
```

確認

現在、この設定に使用できる確認手順はありません。

トラブルシューティング

ここでは、設定に関するトラブルシューティングについて説明します。

詳細については、『IP Security のトラブルシューティング - debug コマンドの理解と使用』を参照してください。

トラブルシューティングのためのコマンド

Output Interpreter Tool（OIT）（登録ユーザ専用）では、特定の **show** コマンドがサポートされています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

注: debug コマンドを使用する前に、『**debug コマンドの重要な情報**』を参照してください。

- **debug crypto ipsec sa** —フェーズ2 の IPSec ネゴシエーションを表示する。
- **debug crypto isakmp sa** —フェーズ1 の ISAKMP ネゴシエーションを参照して下さい。
- **debug crypto engine** : —暗号化されたセッションを表示します。

関連情報

- IPSec ネゴシエーション/IKE プロトコル
- テクニカルサポートとドキュメント - Cisco Systems