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

内容

概要

この設定例では、以下の実行方法について説明します。

- 2 つのプライベート ネットワーク（10.1.1.x と 172.16.1.x）間のトラフィックを暗号化する。
- 10.1.1.3 のネットワーク デバイスにスタティック IP アドレス（外部アドレス 200.1.1.25）を割り当てる。

プライベート間ネットワーク トラフィックに対してネットワーク アドレス変換（NAT）を行わないように、アクセス コントロール リスト（ACL）を使用してルータに指示します。これにより、それらのトラフィックは暗号化され、ルータから出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 も含まれています。この設定例では、トラフィックが暗号化トンネル経由で宛先に向かう場合にもネットワーク アドレス変換されないように、NAT コマンドで route-map オプションを使用しています。

前提条件

要件

このドキュメントに特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いています。

- Cisco IOS® Software 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ました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、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。

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下記の図のように、インターネット クラウドを 200.1.1.1 から 100.1.1.1 に向かう Cisco IOS IPsec トンネルに置き換えます。トンネルでリンクされている 2 つのプライベート LAN から見た場合に、このネットワークが透過的になるようにします。したがって、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 NAT を使用する必要はありません。これにより、パケットが内部 Router 3 ネットワークに到達したときに、200.1.1.1 ではなく 10.1.1.0/24 ネットワークを発信元 IP アドレスとする、Router 2 ネットワークからのパケットを確認できます。

NAT の設定方法の詳細については、「NAT の処理順序」を参照してください。この参照ドキュメントには、パケットが内部から外部に向かう場合に、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：トンネルを構築しても、NATを使用できます。その場合は、NAT トラフィックを「IPsec の対象トラフィック」として指定します（本ドキュメントの他の項では ACL 101 として言及）。NAT がアクティブなときにトンネルを構築する方法については、「LAN 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 について、および 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のサーバに対するスタティック1対1のNATも含まれています。これは、インターネットユーザが200.1.1.25にアクセスできるようにNATを使用したものです。次のコマンドを実行します。

```
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トンネルを介して 10.1.1.3 に到達できなくなります。これは、暗号化されたトラフィックがACL 122でNATされることを拒否する必要があるためです。ただし、スタティックNATコマンドは、10.1.1.3とのすべての接続で一般的なNATステートメントよりも優先されます。スタティックNATステートメントでは、暗号化されたトラフィックもNAT化されません。172.16.1.x ネットワーク上のユーザが 10.1.1.3 に接続し、それによって暗号化トンネル経由で戻らない場合、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、暗号化トラフィックが（スタティックな 1 対 1 の NAT 変換であっても）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ります。**

注：スタティックNATの**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：スタティック変換でルート 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 に暗号化アクセスできるようにするには、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
```

これらの文は、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指示します。ACL 150は、10.1.1.3を送信元とし、暗号化されたトンネルを経由して172.16.1.xに送信されるトラフィックにはNATを適用しないようにします。ただし、発信元が 10.1.1.3 のその他のトラフィック（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。

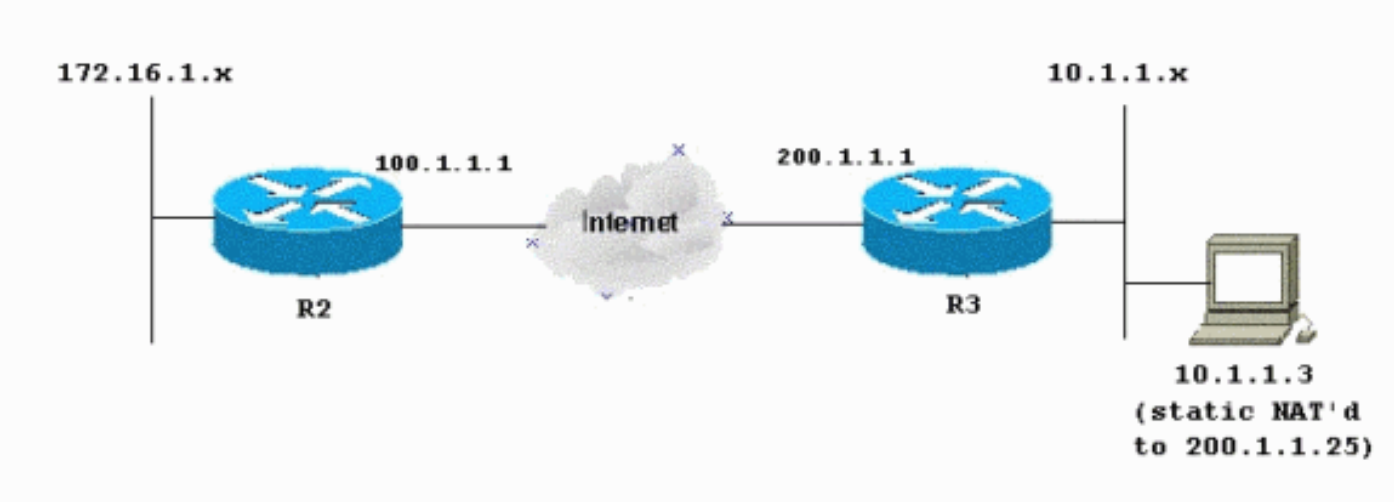
設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

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 セットアップを使用します。



設定

このドキュメントでは、次の構成を使用します。

- ルータ 2
- Router 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。

トラブルシュート

このセクションは、設定のトラブルシューティングを行う際に参照してください。

その他のトラブルシューティング情報については、「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

アウトプット インタープリタ ツール（登録ユーザ専用）（OIT）は、特定の show コマンドをサポートします。OIT を使用して、show コマンドの出力の分析を表示します。

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します。**
- **debug crypto isakmp sa：フェーズ 1 の ISAKMP ネゴシエーションを表示します。**
- **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 - Cisco Systems
- テクニカル サポートとドキュメント – Cisco Systems