Configurazione di una rete tunnel IPsec del router da privata a privata con NAT e una porta

Sommario

Introduzione

In questa configurazione di esempio viene illustrato come:

- Cripta il traffico tra due reti private (10.1.1.x e 172.16.1.x).
- Assegnare un indirizzo IP statico (indirizzo esterno 200.1.1.25) a un dispositivo di rete in 10.1.1.3.

Gli elenchi di controllo di accesso (ACL) vengono usati per dire al router di non eseguire Network Address Translation (NAT) sul traffico di rete da privato a privato, che viene quindi crittografato e posizionato sul tunnel mentre esce dal router. In questa configurazione di esempio è presente anche un NAT statico per un server interno sulla rete 10.1.1.x. In questa configurazione di esempio viene utilizzata l'opzione route-map del comando NAT per impedire che il traffico venga ignorato se anche il traffico relativo è destinato al tunnel crittografato.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Software Cisco IOS® versione 12.3(14)T
- Due router Cisco

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Perché l'istruzione Deny nell'ACL specifica il traffico NAT?

Concettualmente, una rete viene sostituita con un tunnel quando si utilizza Cisco IOS IPsec o una VPN. In questo diagramma, il cloud Internet viene sostituito da un tunnel IPsec Cisco IOS con lunghezza compresa tra 200.1.1.1 e 100.1.1.1. Rendere trasparente la rete dal punto di vista delle due LAN private collegate tra loro dal tunnel. Per questo motivo, in genere non si desidera utilizzare NAT per il traffico che va da una LAN privata alla LAN privata remota. Quando i pacchetti raggiungono la rete interna del router 3, si desidera visualizzare i pacchetti provenienti dalla rete del router 2 con un indirizzo IP di origine proveniente dalla rete 10.1.1.0/24 anziché 200.1.1.1.

Per ulteriori informazioni su come configurare un NAT, fare riferimento a Ordine di funzionamento NAT. Questo documento mostra che il NAT ha luogo prima del controllo crittografico quando il pacchetto va dall'interno all'esterno. Per questo motivo, è necessario specificare queste informazioni nella configurazione.

```
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
```

Nota: è anche possibile costruire il tunnel e continuare a usare NAT. In questo scenario, il traffico NAT viene specificato come "traffico interessante per IPsec" (indicato come ACL 101 in altre sezioni del presente documento). Per ulteriori informazioni su come creare un tunnel mentre NAT è attivo, fare riferimento a Configurazione di un tunnel IPsec tra router con subnet LAN duplicate.

E per quanto riguarda il protocollo NAT statico, perché non è possibile raggiungere l'indirizzo tramite il tunnel IPsec?

Questa configurazione include anche un NAT uno a uno statico per un server alla versione 10.1.1.3. Si tratta di un NAT alla versione 200.1.1.25 in modo che gli utenti Internet possano accedervi. Immettere questo comando

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

Questo NAT statico impedisce agli utenti della rete 172.16.1.x di raggiungere la versione 10.1.1.3 tramite il tunnel crittografato. Infatti, è necessario negare che il traffico crittografato sia stato identificato da NAT con ACL 122. Tuttavia, il comando NAT statico ha la precedenza sull'istruzione NAT generica per tutte le connessioni da e per la versione 10.1.1.3. L'istruzione NAT statica non impedisce esplicitamente che il traffico crittografato sia identificato anche da NAT. Le risposte da 10.1.1.3 sono NAT'd a 200.1.1.25 quando un utente sulla rete 172.16.1.x si connette a 10.1.1.3 e quindi non torna indietro sul tunnel crittografato (il NAT si verifica prima della crittografia).

Ènecessario impedire al traffico crittografato di essere di tipo NAT (anche in modo statico, un dispositivo NAT per uno) con un comando **route-map** sull'istruzione NAT statica.

Nota: l'opzione **route-map** su un NAT statico è supportata solo dal software Cisco IOS versione 12.2(4)T e successive. Per ulteriori informazioni, fare riferimento a NAT - Possibilità di utilizzare mappe percorsi con traduzioni statiche.

Ènecessario usare questi comandi aggiuntivi per consentire l'accesso crittografato alla versione 10.1.1.3, l'host NAT con stato statico:

```
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
```

Queste istruzioni indicano al router di applicare il NAT statico solo al traffico che corrisponde all'ACL 150. L'ACL 150 dice di non applicare il NAT al traffico proveniente dalla versione 10.1.1.3 e destinato al tunnel crittografato fino alla versione 172.16.1.x. Tuttavia, applicarlo a tutto il traffico originato dalla versione 10.1.1.3 (traffico basato su Internet).

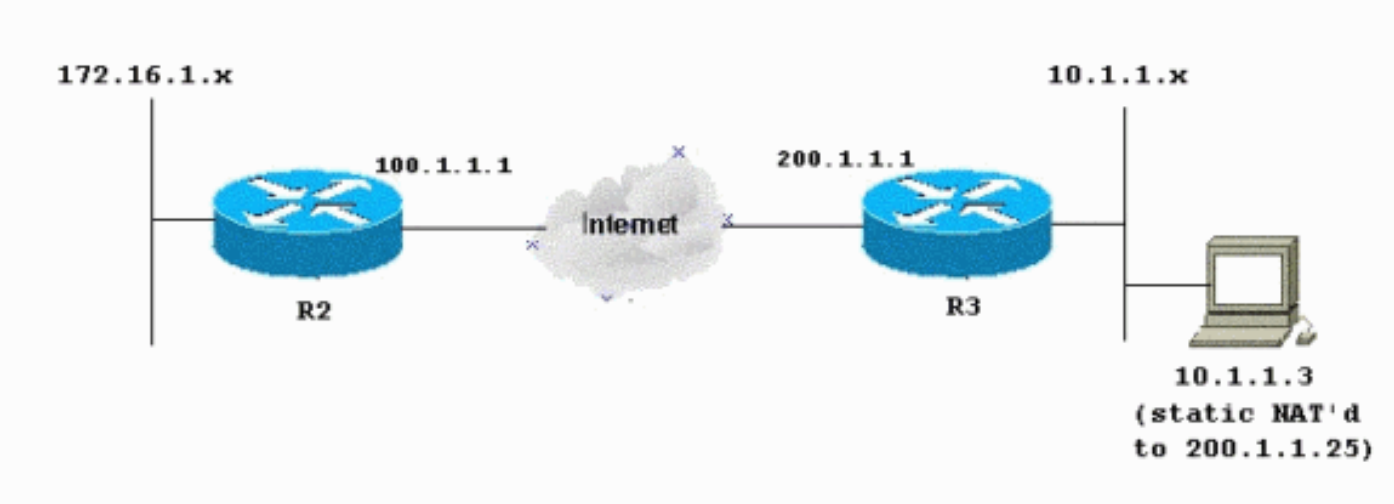
Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questo documento, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Configurazioni

Nel documento vengono usate queste configurazioni:

- Router 2
- Router 3

R2 - Configurazione router

```
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 - Configurazione router

```
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
```

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Utilizzare questa sezione per risolvere i problemi relativi alla configurazione.

Per ulteriori informazioni, fare riferimento a Risoluzione dei problemi di sicurezza IP - Comprensione e uso dei comandi di debug.

Comandi per la risoluzione dei problemi

Lo strumento Output Interpreter (solo utenti registrati) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

Nota: consultare le informazioni importanti sui comandi di debug prima di usare i comandi di **debug**.

- **debug crypto ipsec sa**: visualizza le negoziazioni IPsec della fase 2.
- **debug crypto isakmp sa**: vedere le negoziazioni ISAKMP della fase 1.
- **debug crypto engine**: visualizza le sessioni crittografate.

Informazioni correlate

- Negoziazione IPsec/protocolli IKE - Cisco Systems
- Documentazione e supporto tecnico – Cisco Systems