

Configurazione di un tunnel IPSec tra router con subnet LAN duplicate

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Premesse](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazioni](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Comandi per la risoluzione dei problemi](#)

[Informazioni correlate](#)

Introduzione

Questo documento offre un esempio di rete che simula l'unione di due società con lo stesso schema di indirizzamento IP. Due router sono connessi con un tunnel VPN e le reti dietro ciascun router sono le stesse. Affinché un sito possa accedere agli host dell'altro, sui router viene utilizzato Network Address Translation (NAT) per modificare gli indirizzi di origine e di destinazione in subnet diverse.

Nota: questa configurazione non è consigliata come configurazione permanente in quanto potrebbe creare confusione dal punto di vista della gestione della rete.

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:

- Router A: Router Cisco 3640 con software Cisco IOS® versione 12.3(4)T

- Router B: Router Cisco 2621 con software Cisco IOS® versione 12.3(5)

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](#).

Premesse

In questo esempio, quando l'host 172.16.1.2 del Sito A accede allo stesso host con indirizzo IP del Sito B, si connette a un indirizzo 172.19.1.2 anziché all'indirizzo 172.16.1.2 effettivo. Quando l'host sul Sito B accede al Sito A, si connette a un indirizzo 172.18.1.2. NAT sul router A converte qualsiasi indirizzo 172.16.x.x in un indirizzo simile alla voce corrispondente 172.18.x.x dell'host. Il formato NAT sul router B cambia da 172.16.x.x a 172.19.x.x.

La funzione crypto su ciascun router cripta il traffico convertito attraverso le interfacce seriali. Notare che il protocollo NAT *precede* la crittografia su un router.

Nota: questa configurazione consente solo la comunicazione tra le due reti. Non consente la connettività Internet. Sono necessari percorsi aggiuntivi a Internet per la connettività a percorsi diversi dai due siti. In altre parole, è necessario aggiungere un altro router o firewall su ciascun lato, con più route configurate sugli host.

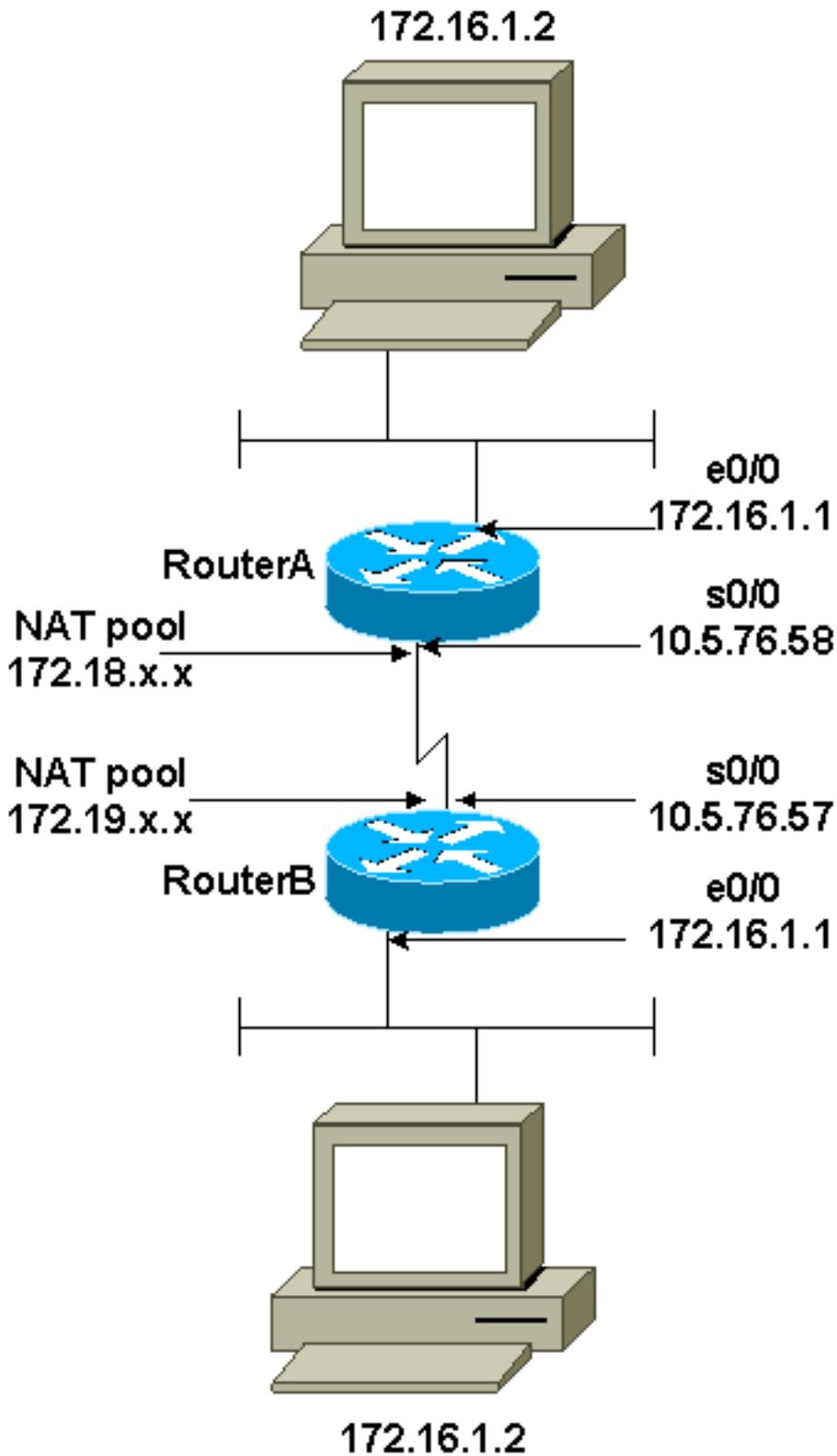
Configurazione

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 A](#)
- [Router B](#)

Router A

```
Current configuration : 1404 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname SV3-2
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
ip subnet-zero
!
!
!
ip audit notify log
ip audit po max-events 100
ip ssh break-string
no ftp-server write-enable
!
!
!--- These are the Internet Key Exchange (IKE)
parameters. crypto isakmp policy 10
  encr 3des
  hash md5
  authentication pre-share
crypto isakmp key cisco123 address 10.5.76.57
!
!--- These are the IPSec parameters. crypto ipsec
transform-set myset1 esp-3des esp-md5-hmac
!
!
crypto map mymap 10 ipsec-isakmp
  set peer 10.5.76.57
  set transform-set myset1
  !--- Encrypt traffic to the other side. match address
100
!
!
!
interface Serial0/0
  description Interface to Internet
  ip address 10.5.76.58 255.255.0.0
  ip nat outside
  clockrate 128000
  crypto map mymap
!
interface Ethernet0/0
  ip address 172.16.1.1 255.255.255.0
  no ip directed-broadcast
  ip nat inside
  half-duplex
!
!
!--- This is the NAT traffic. ip nat inside source
static network 172.16.0.0 172.18.0.0 /16 no-alias
ip http server
no ip http secure-server
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/0
```

```
!  
!--- Encrypt traffic to the other side. access-list 100  
permit ip 172.18.0.0 0.0.255.255 172.19.0.0 0.0.255.255  
!  
control-plane  
!  
!  
line con 0  
line aux 0  
line vty 0 4  
!  
!  
end
```

Router B

```
Current configuration : 1255 bytes  
!  
version 12.3  
service timestamps debug datetime msec  
service timestamps log datetime msec  
no service password-encryption  
!  
hostname SV3-15  
!  
boot-start-marker  
boot-end-marker  
!  
!  
memory-size iomem 15  
no aaa new-model  
ip subnet-zero  
!  
!  
!  
ip audit notify log  
ip audit po max-events 100  
!  
!--- These are the IKE parameters. crypto isakmp policy  
10  
  encr 3des  
  hash md5  
  authentication pre-share  
crypto isakmp key cisco123 address 10.5.76.58  
!  
!--- These are the IPSec parameters. crypto ipsec  
transform-set myset1 esp-3des esp-md5-hmac  
!  
crypto map mymap 10 ipsec-isakmp  
  set peer 10.5.76.58  
  set transform-set myset1  
!--- Encrypt traffic to the other side. match address  
100  
!  
!  
interface FastEthernet0/0  
  ip address 172.16.1.1 255.255.255.0  
  ip nat inside  
  duplex auto  
  speed auto  
!  
interface Serial0/0  
  description Interface to Internet
```

```
ip address 10.5.76.57 255.255.0.0
ip nat outside
crypto map mymap
!
!--- This is the NAT traffic. ip nat inside source
static network 172.16.0.0 172.19.0.0 /16 no-alias
ip http server
no ip http secure-server
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/0
!
!--- Encrypt traffic to the other side. access-list 100
permit ip 172.19.0.0 0.0.255.255 172.18.0.0 0.0.255.255
!
!
line con 0
line aux 0
line vty 0 4
!
!
!
end
```

Verifica

Le informazioni contenute in questa sezione permettono di verificare che la configurazione funzioni correttamente.

Alcuni comandi **show** sono supportati dallo [strumento Output Interpreter \(solo utenti registrati\)](#); lo strumento permette di visualizzare un'analisi dell'output del comando **show**.

- **show crypto ipsec sa**: visualizza le associazioni di sicurezza della fase 2.
- **show crypto isakmp sa**: visualizza le associazioni di sicurezza della fase 1.
- **show ip nat translation**: visualizza le traduzioni NAT correnti in uso.

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Comandi per la risoluzione dei problemi

Alcuni comandi **show** sono supportati dallo [strumento Output Interpreter \(solo utenti registrati\)](#); lo strumento permette di visualizzare un'analisi dell'output del comando **show**.

Nota: prima di usare i comandi di **debug**, consultare le [informazioni importanti sui comandi di debug](#).

- **debug crypto ipsec**: visualizza le negoziazioni IPsec della fase 2.
- **debug crypto isakmp**: visualizza le negoziazioni ISAKMP (Internet Security Association and Key Management Protocol) della fase 1.
- **debug crypto engine**: visualizza il traffico crittografato.

Informazioni correlate

- [Pagina di supporto per IPSec](#)
- [Configurazione di IPSec Network Security](#)
- [Configurazione del protocollo di protezione di Internet Key Exchange](#)
- [Supporto tecnico – Cisco Systems](#)