Istruzione NAT e PAT utilizzate nell'esempio di configurazione di Cisco Secure ASA Firewall

Sommario

Introduzione

In questo documento vengono forniti esempi di configurazioni di base NAT (Network Address Translation) e PAT (Port Address Translation) sul firewall Cisco Secure Adaptive Security Appliance (ASA). Questo documento fornisce anche diagrammi di rete semplificati. Per informazioni più dettagliate, consultare la documentazione della versione software dell'ASA in uso.

Questo documento offre un'analisi personalizzata del dispositivo Cisco.

Per ulteriori informazioni, fare riferimento alla configurazione NAT sulle appliance di sicurezza ASA serie 5500/5500-X.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza di Cisco Secure ASA Firewall.

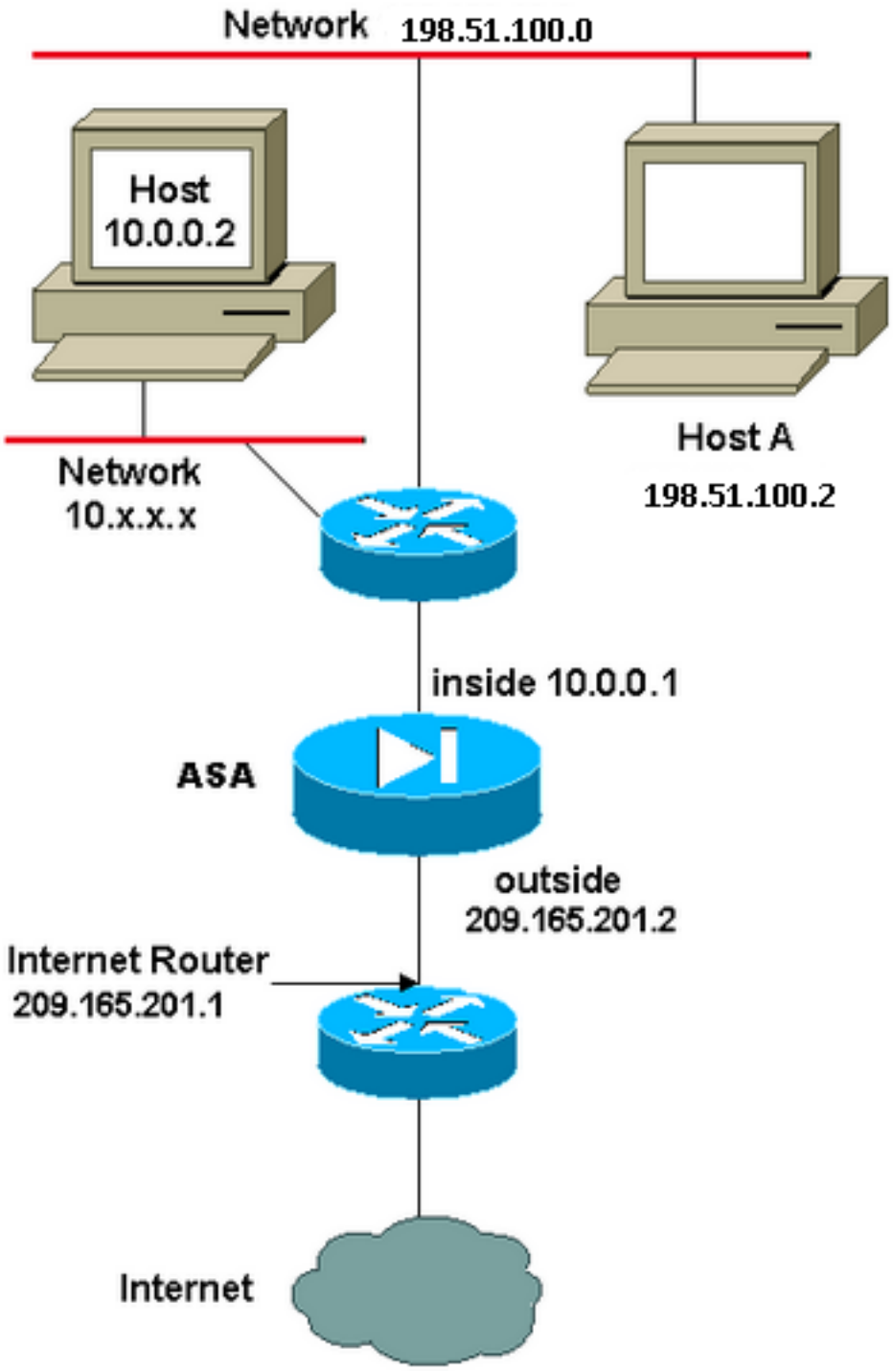
Componenti usati

Per la stesura del documento, è stato usato il software Cisco Secure ASA Firewall versione 8.4.2 e successive.

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.

Configurazione - Più istruzioni NAT con NAT manuale e automatica

Esempio di rete



Nell'esempio, l'ISP fornisce al gestore della rete un blocco di indirizzi IP compreso tra 209.165.201.0/27 e 209.165.201.1. Il gestore della rete decide di assegnare 209.165.201.1 all'interfaccia interna del router Internet e 209.165.201.2 all'interfaccia esterna dell'ASA.

L'amministratore di rete dispone già di un indirizzo di classe C assegnato alla rete, 198.51.100.0/24, e di alcune workstation che utilizzano tali indirizzi per accedere a Internet. Queste workstation non richiedono alcuna traduzione degli indirizzi perché dispongono già di indirizzi validi. Tuttavia, alle nuove workstation vengono assegnati indirizzi nella rete 10.0.0.0/8 e devono essere tradotti (poiché 10.x.x.x è uno degli spazi di indirizzi non instradabili secondo la RFC 1918 .

Per supportare questo progetto di rete, l'amministratore di rete deve utilizzare due istruzioni NAT e un pool globale nella configurazione ASA:

```
global (outside) 1 209.165.201.3-209.165.201.30 netmask 255.255.255.224
nat (inside) 1 10.0.0.0 255.0.0.0 0 0
```

Questa configurazione non converte l'indirizzo di origine di alcun traffico in uscita dalla rete 198.51.100.0/24. Converte un indirizzo di origine nella rete 10.0.0.0/8 in un indirizzo compreso nell'intervallo tra 209.165.201.3 e 209.165.201.30.

> **Nota:** Quando si dispone di un'interfaccia con un criterio NAT e non esiste un pool globale per un'altra interfaccia, è necessario utilizzare nat 0 per impostare l'eccezione NAT.

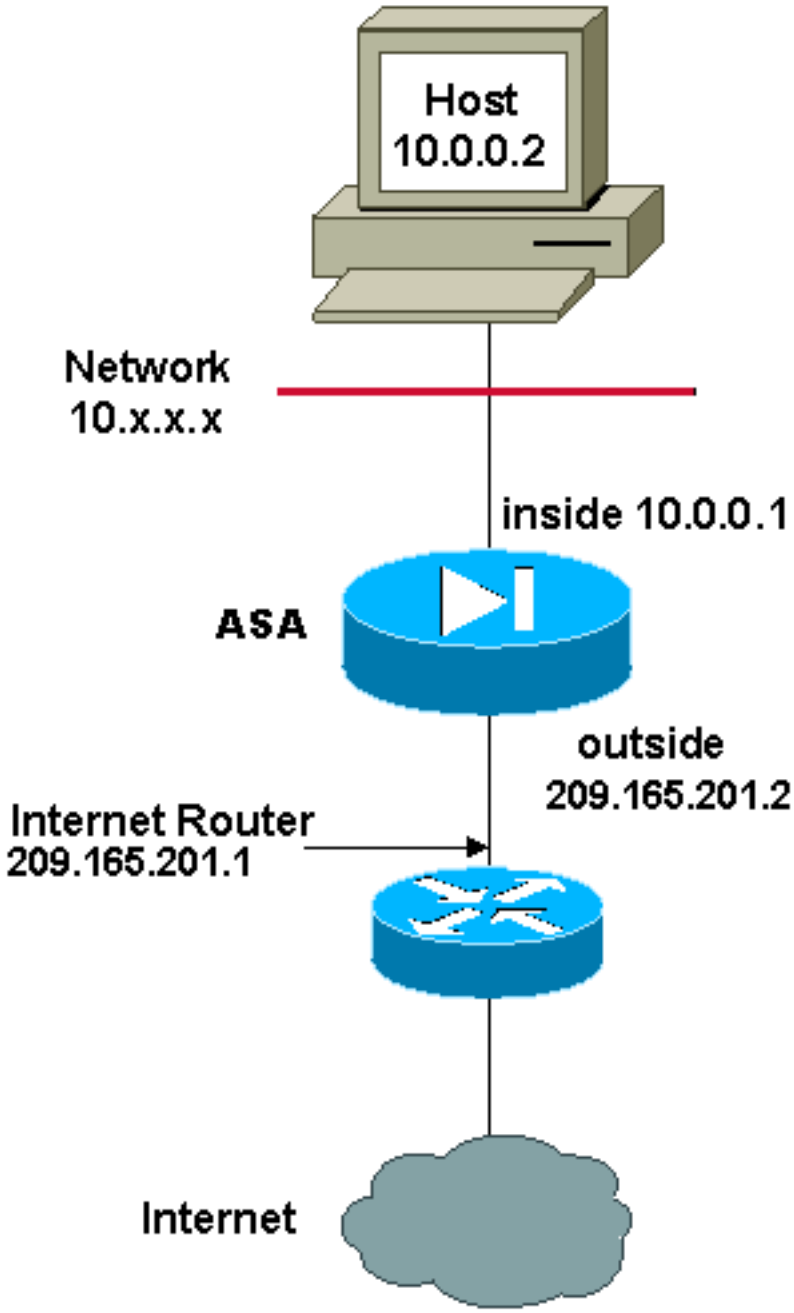
ASA versione 8.3 e successive

Ecco la configurazione.

```
object network obj-10.0.0.0/8
subnet 10.0.0.0 255.0.0.0

object network obj-198.51.100.0/24
subnet 198.51.100.0 255.255.255.0

object network obj-natted
range 209.165.201.3 209.165.201.30

object network any-1
subnet 0.0.0.0 0.0.0.0

Using the Manual Nat statements:

nat (inside,outside) source static obj-198.51.100.0/24 obj-198.51.100.0/24
destination static any-1 any-1

nat (inside,outside) source dynamic obj-10.0.0.0/8 obj-natted

Using the Auto Nat statements:

object network obj-10.0.0.0/8
subnet 10.0.0.0 255.0.0.0
nat (inside,outside) dynamic obj-natted

object network obj-198.51.100.0/24
subnet 198.51.100.0 255.255.255.0
nat (inside,outside) static obj-198.51.100.0/24
```

Configurazione - Più pool globali

Esempio di rete



Nell'esempio, il gestore della rete dispone di due intervalli di indirizzi IP registrati su Internet. Il gestore della rete deve convertire tutti gli indirizzi interni compresi nell'intervallo 10.0.0.0/8 in indirizzi registrati. Gli intervalli di indirizzi IP che il gestore della rete deve utilizzare sono compresi tra 209.165.201.1 e 209.165.201.30 e tra 209.165.200.225 e 209.165.200.254. Il gestore della rete può eseguire questa operazione con:

```
global (outside) 1 209.165.201.3-209.165.201.30 netmask 255.255.255.224
global (outside) 1 209.165.200.225-209.165.200.254 netmask 255.255.255.224
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
```

> **Nota:** Nell'istruzione NAT viene utilizzato uno schema di indirizzamento con caratteri jolly. Questa istruzione indica all'appliance ASA di tradurre tutti gli indirizzi di origine interni quando vengono trasmessi a Internet. Se lo si desidera, l'indirizzo specificato in questo comando può essere più specifico.

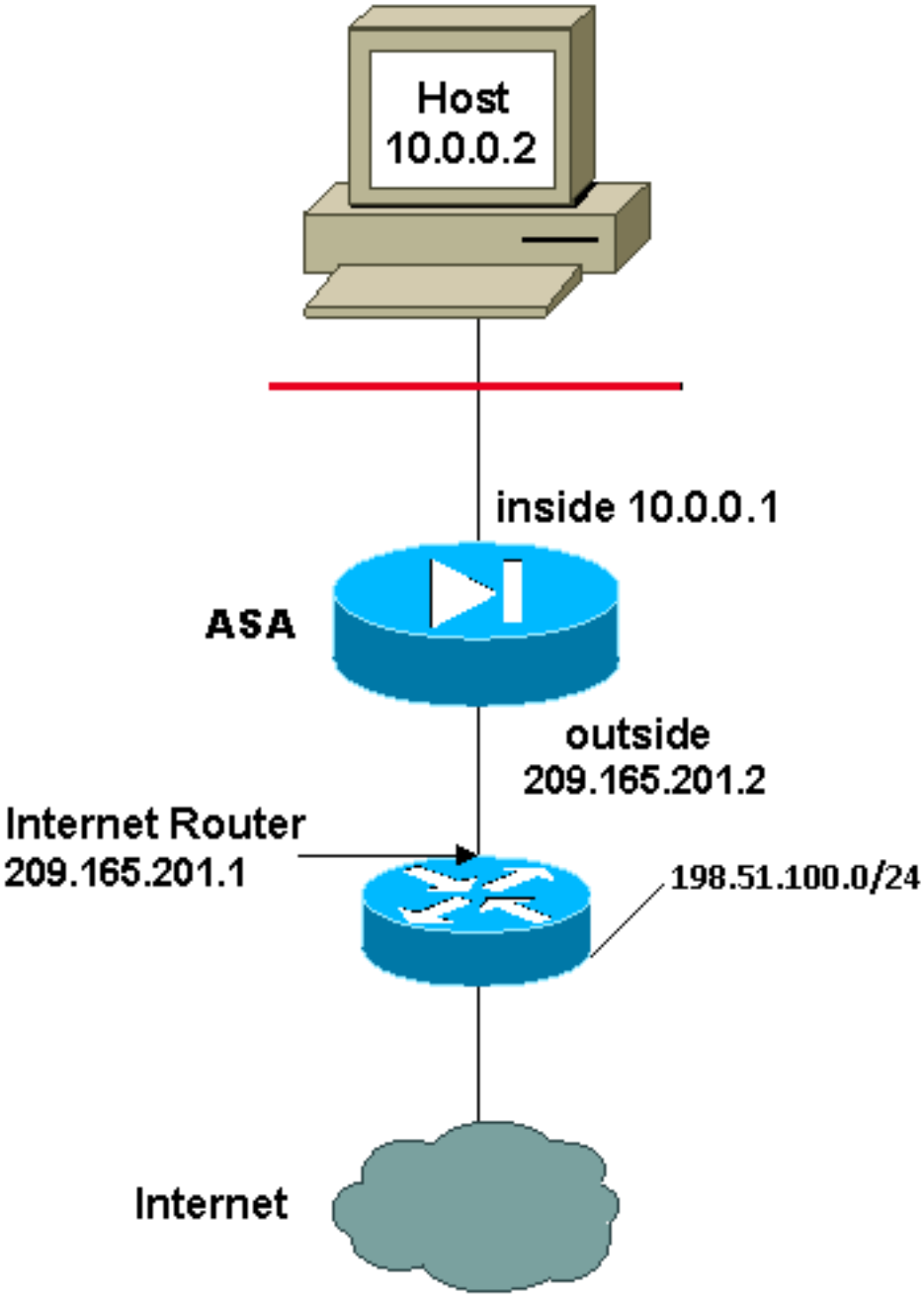
ASA versione 8.3 e successive

Ecco la configurazione.

```
object network obj-natted
range 209.165.201.3 209.165.201.30

object network obj-natted-2
range 209.165.200.225 209.165.200.254

object network any-1
subnet 0.0.0.0 0.0.0.0

Using the Manual Nat statements:

nat (inside,outside) source dynamic any-1 obj-natted
nat (inside,outside) source dynamic any-1 obj-natted-2

Using the Auto Nat statements:

object network any-1
subnet 0.0.0.0 0.0.0.0
nat (inside,outside) dynamic obj-natted

object network any-2
subnet 0.0.0.0 0.0.0.0
nat (inside,outside) dynamic obj-natted-2
```

Configurazione - Combinazione di istruzioni NAT e PAT

Esempio di rete



Nell'esempio, l'ISP fornisce al gestore della rete un intervallo di indirizzi compreso tra 209.165.201.1 e 209.165.201.30, che la società potrà utilizzare. Il gestore della rete ha deciso di usare 209.165.201.1 per l'interfaccia interna sul router Internet e 209.165.201.2 per l'interfaccia esterna sull'appliance ASA. Viene quindi lasciato con 209.165.201.3 fino a 209.165.201.30 da utilizzare per il pool NAT. Tuttavia, il gestore della rete sa che, in qualsiasi momento, possono essere più di 28 le persone che tentano di uscire dall'appliance ASA. Il gestore della rete ha deciso di selezionare 209.165.201.30 e impostarlo come indirizzo PAT in modo che più utenti possano condividere un indirizzo contemporaneamente.

Questi comandi istruiscono l'ASA a convertire l'indirizzo di origine in 209.165.201.3 in 209.165.201.29 per i primi 27 utenti interni a passare attraverso l'ASA. Dopo aver esaurito questi indirizzi, l'ASA converte tutti gli indirizzi di origine successivi in 209.165.201.30 finché uno degli indirizzi nel pool NAT non diventa libero.

> **Nota:** Nell'istruzione NAT viene utilizzato uno schema di indirizzamento con caratteri jolly. Questa istruzione indica all'appliance ASA di tradurre tutti gli indirizzi di origine interni

quando vengono trasmessi a Internet. Se lo si desidera, l'indirizzo specificato in questo comando può essere più specifico.

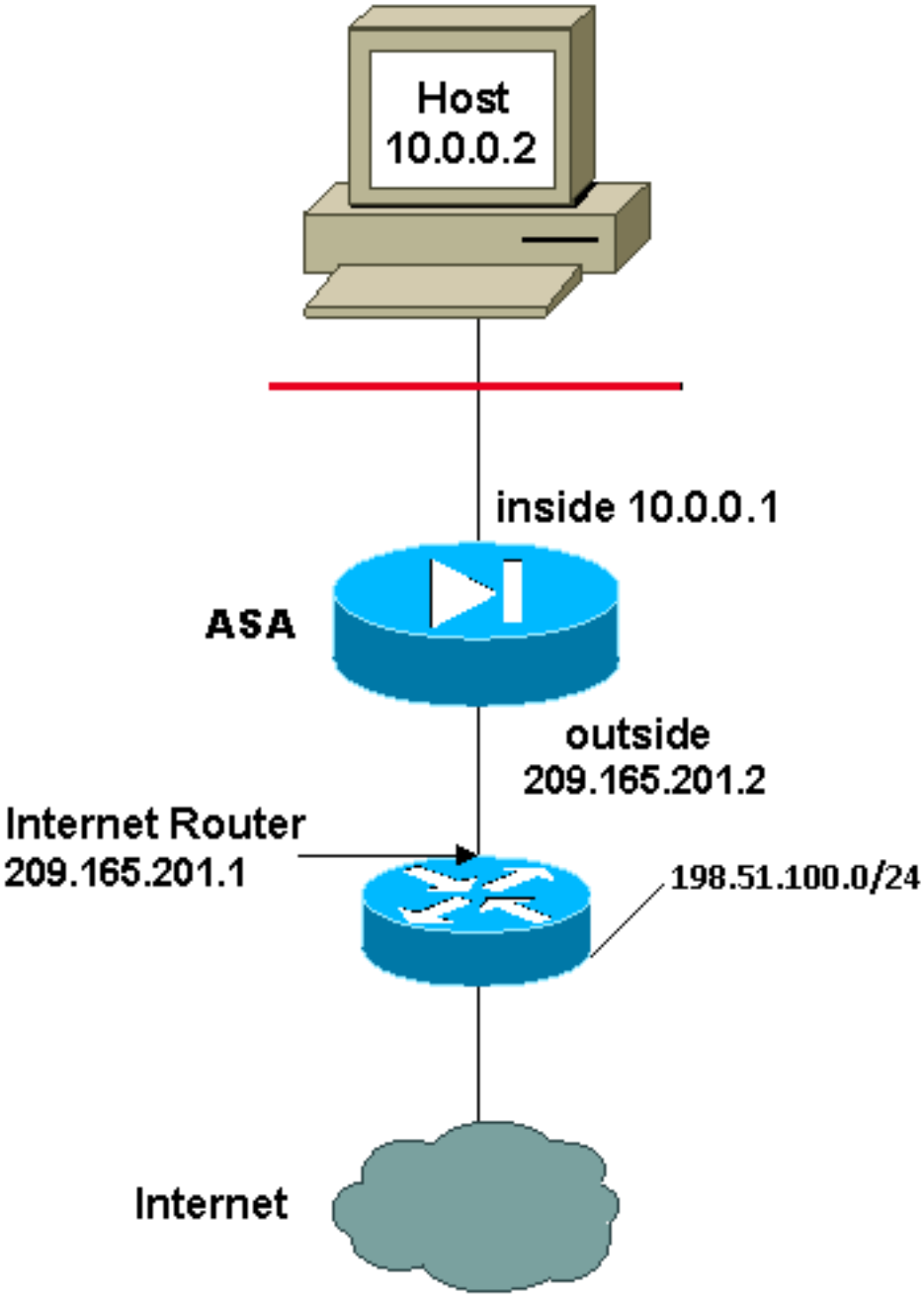
ASA versione 8.3 e successive

Ecco la configurazione.

```
Using the Manual Nat statements:
object network any-1
subnet 0.0.0.0 0.0.0.0

object network obj-natted
range 209.165.201.3 209.165.201.30

object network obj-natted-2
subnet 209.165.201.30 255.255.255.224

nat (inside,outside) source dynamic 0.0.0.0/0 obj-natted
nat (inside,outside) source dynamic 0.0.0.0/0 obj-natted-2

Using the Auto Nat statements:

object network any-1
subnet 0.0.0.0 0.0.0.0
nat (inside,outside) dynamic obj-natted

object network any-2
subnet 0.0.0.0 0.0.0.0
nat (inside,outside) dynamic obj-natted-2
```

Configurazione - Più istruzioni NAT con istruzioni manuali

Esempio di rete



Nell'esempio, l'ISP fornisce al gestore della rete un intervallo di indirizzi compreso tra 209.165.201.1 e 209.165.201.30. Il gestore della rete decide di assegnare 209.165.201.1 all'interfaccia interna del router Internet e 209.165.201.2 all'interfaccia esterna dell'ASA.

Tuttavia, in questo scenario, un altro segmento della LAN privata viene posizionato fuori dal router Internet. Il gestore della rete preferisce non sprecare gli indirizzi dal pool globale quando gli host di queste due reti comunicano tra loro. Il gestore della rete deve ancora tradurre l'indirizzo di origine di tutti gli utenti interni (10.0.0.0/8) quando si accede a Internet.

Questa configurazione non converte gli indirizzi con indirizzo di origine 10.0.0.0/8 e indirizzo di destinazione 198.51.100.0/24. Converte l'indirizzo di origine da qualsiasi traffico avviato dalla rete 10.0.0.0/8 e destinato a un percorso diverso da 198.51.100.0/24 in un indirizzo compreso tra l'intervallo 209.165.201.3 e 209.165.201.30.

se il dispositivo Cisco restituisce i risultati di un comando **write terminal**, è possibile usare lo strumento Output Interpreter (solo utenti registrati).

ASA versione 8.3 e successive

Ecco la configurazione.

Using the Manual Nat statements:

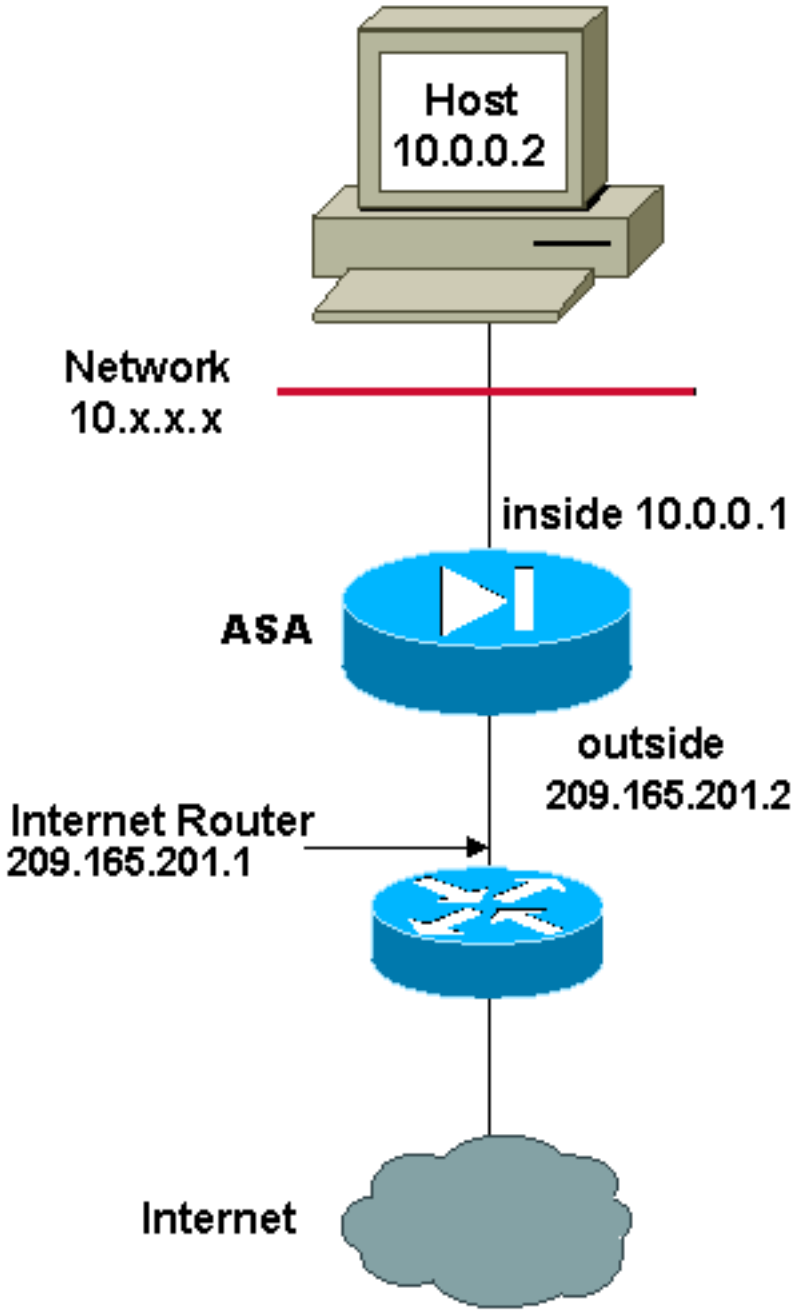
```
object network obj-10.0.0.0/8
subnet 10.0.0.0 255.0.0.0

object network obj-198.51.100.0/24
subnet 198.51.100.0 255.255.255.0

object network obj-natted
range 209.165.201.3 209.165.201.30

nat (inside,outside) source static obj-10.0.0.0/8 obj-10.0.0.0/8 destination
static obj-198.51.100.0/24 obj-198.51.100.0/24

nat (inside,outside) source dynamic obj-10.0.0.0/8 obj-natted
```

Using the Auto Nat statements:

```
object network obj-natted
range 209.165.201.3 209.165.201.30
nat (inside,outside) source static obj-10.0.0.0/8 obj-10.0.0.0/8 destination
static obj-198.51.100.0/24 obj-198.51.100.0/24

object network obj-10.0.0.0/8
subnet 10.0.0.0 255.0.0.0
nat (inside,outside) dynamic obj-natted
```

Configura - Usa criterio NAT

Esempio di rete



Quando si utilizza un elenco degli accessi con il comando **nat** per qualsiasi ID NAT diverso da 0, viene abilitato il criterio NAT.

Il criterio NAT consente di identificare il traffico locale per la traduzione degli indirizzi in base alla specifica degli indirizzi di origine e di destinazione (o porte) in un elenco degli accessi. NAT normale utilizza solo indirizzi/porte di origine. Il criterio NAT utilizza indirizzi/porte di origine e di destinazione.

> **Nota:** Tutti i tipi di NAT supportano i criteri NAT ad eccezione dell'esenzione NAT (elenco accessi NAT 0). L'esenzione NAT utilizza un Access Control List (ACL) per identificare gli indirizzi locali, ma differisce dal criterio NAT in quanto le porte non vengono considerate.

Con il criterio NAT, è possibile creare più istruzioni NAT o statiche che identificano lo stesso indirizzo locale purché la combinazione di origine/porta e destinazione/porta sia univoca per ogni istruzione. È quindi possibile far corrispondere diversi indirizzi globali a ciascuna coppia origine/porta e destinazione/porta.

Nell'esempio, il gestore della rete deve fornire l'accesso per l'indirizzo IP di destinazione 172.30.1.11 per la porta 80 (Web) e la porta 23 (Telnet), ma deve utilizzare due indirizzi IP diversi come indirizzo di origine. 209.165.201.3 viene utilizzato come indirizzo di origine per il Web e 209.165.201.4 viene utilizzato per Telnet e deve convertire tutti gli indirizzi interni compresi nell'intervallo 10.0.0.0/8. Il gestore della rete può eseguire questa operazione con:

```
access-list WEB permit tcp 10.0.0.0 255.0.0.0
172.30.1.11 255.255.255.255 eq 80
access-list TELNET permit tcp 10.0.0.0 255.0.0.0 172.30.1.11
255.255.255.255 eq 23

nat (inside) 1 access-list WEB
nat (inside) 2 access-list TELNET
global (outside) 1 209.165.201.3 255.255.255.224
global (outside) 2 209.165.201.4 255.255.255.224
```

ASA versione 8.3 e successive

Ecco la configurazione.

```
Using the Manual Nat statements:

object network obj-10.0.0.0/8
subnet 10.0.0.0 255.0.0.0

object network obj-172.30.1.11
host 172.30.1.11

object network obj-209.165.201.3
host 209.165.201.3

object network obj-209.165.201.4
host 209.165.201.4

object service obj-23
service tcp destination eq telnet

object service obj-80
service tcp destination eq telnet

nat (inside,outside) source dynamic obj-10.0.0.0/8 obj-209.165.201.3 destination
static obj-172.30.1.11 obj-172.30.1.11 service obj-80 obj-80
nat (inside,outside) source dynamic obj-10.0.0.0/8 obj-209.165.201.4 destination
static obj-172.30.1.11 obj-172.30.1.11 service obj-23 obj-23
```

> **Nota:** Per ulteriori informazioni sulla configurazione di NAT e PAT sull'appliance ASA versione 8.4, fare riferimento alle informazioni su NAT.
>
> Per ulteriori informazioni sulla configurazione degli elenchi degli accessi sull'appliance ASA versione 8.4, fare riferimento alle informazioni sugli elenchi degli accessi.

Verifica

Provare ad accedere a un sito Web tramite HTTP con un browser Web. In questo esempio viene

usato un sito ospitato all'indirizzo 198.51.100.100. Se la connessione ha esito positivo, l'output della sezione successiva può essere visualizzato sulla CLI di ASA.

Connessione

```
ASA(config)# show connection address 10.0.0.2
16 in use, 19 most used
TCP outside 198.51.100.100:80 inside 10.0.0.2:57431, idle 0:00:06, bytes 9137,
flags UIO
```

L'ASA è un firewall con stato e il traffico di ritorno dal server Web può attraversare nuovamente il firewall perché corrisponde a una ***connessione*** nella tabella delle connessioni del firewall. Il traffico che corrisponde a una connessione preesistente può passare attraverso il firewall senza essere bloccato da un ACL di interfaccia.

Nell'output precedente, il client sull'interfaccia interna ha stabilito una connessione con l'host 198.51.100.100 dall'interfaccia esterna. Questa connessione viene effettuata con il protocollo TCP ed è rimasta inattiva per sei secondi. I flag di connessione indicano lo stato corrente della connessione. Per ulteriori informazioni sui flag di connessione, consultare Flag di connessione TCP ASA.

Syslog

```
ASA(config)# show log | in 10.0.0.2

Jun 28 2014 11:31:23: %ASA-6-305011: Built dynamic TCP translation from inside:
10.0.0.2/57431 to outside:209.165.201.3/57431

Jun 28 2014 11:31:23: %ASA-6-302013: Built outbound TCP connection 2921 for outside:
198.51.100.100/80 (198.51.100.100/80) to inside:10.0.0.2/57431 (209.165.201.3/57431)
```

Il firewall ASA genera syslog durante il normale funzionamento. L'intervallo dei syslog è espresso in dettaglio in base alla configurazione di registrazione. L'output mostra due syslog visualizzati al livello sei, o livello **"informativo"**.

In questo esempio vengono generati due syslog. Il primo è un messaggio di registro che indica che il firewall ha creato una **traduzione**, in particolare una traduzione TCP dinamica (PAT). Indica l'indirizzo IP e la porta di origine, nonché l'indirizzo IP e la porta convertiti, quando il traffico attraversa le interfacce interna ed esterna.

Il secondo syslog indica che il firewall ha creato una **connessione** nella relativa tabella di connessione per il traffico specifico tra il client e il server. Se il firewall è stato configurato per bloccare questo tentativo di connessione o altri fattori hanno impedito la creazione della connessione (vincoli di risorse o una possibile configurazione errata), il firewall non genererà un registro che indichi che la connessione è stata creata. Viene invece registrato un motivo per cui la connessione viene negata o un'indicazione relativa al fattore che ha impedito la creazione della connessione.

Traduzioni NAT (Xlate)

```
ASA(config)# show xlate local 10.0.0.2
3 1in use, 810 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
s - static, T - twice, N - net-to-net
TCP PAT from inside:10.0.0.2/58799 to outside:209.165.201.3/57431 flags ri idle
0:12:22 timeout 0:00:30
```

Nell'ambito di questa configurazione, PAT è configurato in modo da convertire gli indirizzi IP degli host interni in indirizzi instradabili su Internet. Per confermare la creazione delle traduzioni, è possibile controllare la tabella xlate (translation). Il comando **show xlate,** se combinato con la parola chiave **local** e l'indirizzo IP dell'host interno, mostra tutte le voci presenti nella tabella di conversione per quell'host. L'output precedente mostra che è attualmente presente una traduzione per questo host tra le interfacce interna ed esterna. L'indirizzo IP e la porta dell'host interno vengono convertiti nell'indirizzo 10.165.200.226 per ciascuna configurazione.

I flag elencati, **r i** , indicano che la traduzione è **dinamica** e una **portmap**. Per ulteriori informazioni sulle diverse configurazioni NAT, vedere Informazioni su NAT.

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.