Configurazione di Network Address Translation e degli ACL su un firewall ASA

Sommario

Introduzione

In questo documento viene descritto come configurare Network Address Translation (NAT) e Access Control Lists (ACL) su un firewall ASA.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Per questo documento, è stato usato un firewall ASA 5510 con codice ASA versione 9.1(1).

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.

Premesse

Questo documento descrive un esempio semplice e diretto di come configurare NAT e ACL su un firewall ASA per consentire la connettività in entrata e in uscita. È stato scritto con un firewall ASA (Adaptive Security Appliance) 5510 piuttosto che con il codice ASA versione 9.1(1), ma può essere applicato facilmente a qualsiasi altra piattaforma firewall ASA. Se si usa una piattaforma come ASA 5505, che usa VLAN invece di un'interfaccia fisica, è necessario modificare i tipi di interfaccia in base alle esigenze.

Panoramica

Obiettivi

In questa configurazione di esempio, è possibile esaminare le configurazioni NAT e ACL necessarie per consentire l'accesso in entrata a un server Web nella zona DMZ di un firewall ASA e la connettività in uscita dagli host interni e dalla zona DMZ. Questo può essere riassunto in due obiettivi:

1. Consenti agli host interni e connettività DMZ in uscita verso Internet.
2. Consentire agli host su Internet di accedere a un server Web sulla DMZ con indirizzo IP 192.168.1.100.

Prima di eseguire la procedura necessaria per raggiungere questi due obiettivi, questo documento esamina brevemente il modo in cui gli ACL e i NAT lavorano sulle versioni più recenti del codice ASA (versione 8.3 e successive).

Panoramica della lista di controllo dell'accesso

Le Access Control Lists (Access-lists o ACLs for short) sono il metodo con cui il firewall ASA determina se il traffico è autorizzato o rifiutato. Per impostazione predefinita, il traffico che passa da un livello di protezione inferiore a quello superiore viene rifiutato. ma può essere ignorato da un ACL applicato all'interfaccia di protezione inferiore. Per impostazione predefinita, anche l'ASA consente il traffico dalle interfacce di sicurezza più alte a quelle più basse. Questo comportamento può essere ignorato anche con un ACL.

Nelle versioni precedenti del codice ASA (8.2 e precedenti), l'ASA ha confrontato una connessione o un pacchetto in arrivo con l'ACL di un'interfaccia senza prima annullare la conversione del pacchetto. In altre parole, l'ACL doveva autorizzare il pacchetto come se si trattasse di acquisire il pacchetto sull'interfaccia. Nella versione 8.3 e successive, l'ASA annulla la conversione del pacchetto prima di controllare gli ACL dell'interfaccia. Ciò significa che per il codice versione 8.3 e successive e per questo documento, è consentito il traffico verso l'IP reale dell'host e non verso l'IP tradotto dell'host.

Per ulteriori informazioni sugli ACL, vedere la sezione Configurazione delle regole di accesso della Guida alla configurazione della CLI del firewall Cisco ASA serie 9.1.

Panoramica NAT

Il protocollo NAT sull'appliance ASA nella versione 8.3 e successive è suddiviso in due tipi noti come Auto NAT (Object NAT) e Manual NAT (Twice NAT). Il primo dei due, Object NAT, è configurato nella definizione di un oggetto di rete. Un esempio è illustrato più avanti in questo documento. Uno dei vantaggi principali di questo metodo NAT è che l'ASA ordina automaticamente le regole da elaborare per evitare conflitti. Questa è la forma più semplice di NAT, ma con essa si ha un limite nella granularità della configurazione. Ad esempio, non è possibile prendere una decisione sulla traduzione in base alla destinazione nel pacchetto, come è possibile fare con il secondo tipo di NAT, Manual Nat. Il NAT manuale è più solido nella sua granularità, ma richiede che le linee siano configurate nell'ordine corretto in modo da poter raggiungere il comportamento corretto. Ciò complica questo tipo NAT e, di conseguenza, non può essere utilizzato in questo esempio di configurazione.

Per ulteriori informazioni su NAT, vedere la sezione Informazioni su NAT della guida alla configurazione della CLI del firewall Cisco ASA Series, 9.1.

Configurazione

Per iniziare

L'impostazione di configurazione base dell'ASA è costituita da tre interfacce connesse a tre segmenti di rete. Il segmento di rete dell'ISP è collegato all'interfaccia Ethernet0/0 ed è etichettato all'esterno con un livello di protezione pari a 0. La rete interna è stata collegata a Ethernet0/1 e contrassegnata come interna con un livello di protezione di 100. Il segmento DMZ, in cui risiede il server Web, è collegato a Ethernet 0/2 ed etichettato come DMZ con un livello di protezione di 50.

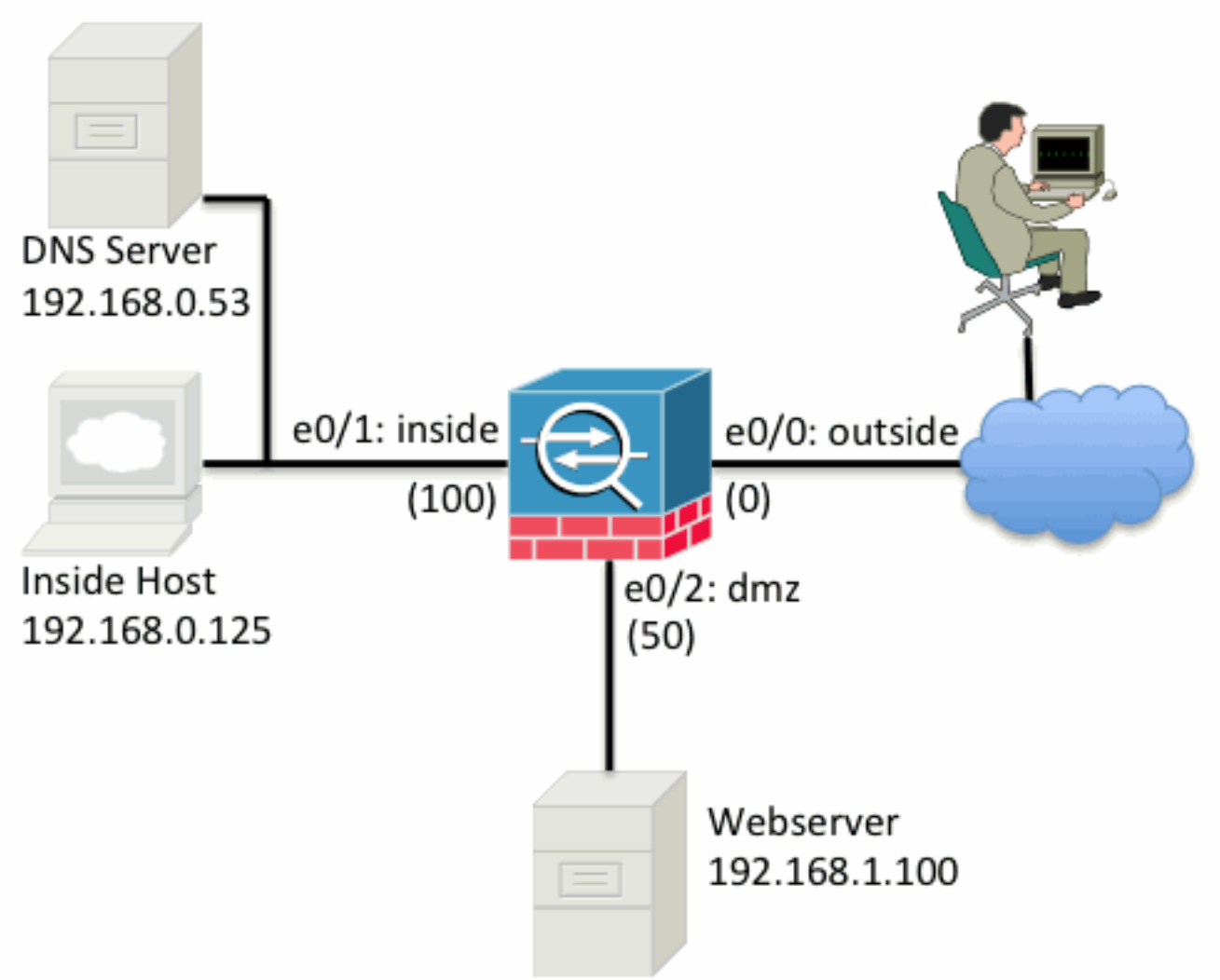
Di seguito vengono riportati la configurazione dell'interfaccia e gli indirizzi IP dell'esempio:

```
interface Ethernet0/0
nameif outside
security-level 0
ip address 198.51.100.100 255.255.255.0
!
interface Ethernet0/1
nameif inside
security-level 100
ip address 192.168.0.1 255.255.255.0
!
interface Ethernet0/2
nameif dmz
security-level 50
ip address 192.168.1.1 255.255.255.0
!
route outside 0.0.0.0 0.0.0.0 198.51.100.1
```

Qui è possibile vedere come l'interfaccia interna dell'ASA sia impostata sull'indirizzo IP 192.168.0.1 e sia il gateway predefinito per gli host interni. L'interfaccia esterna dell'ASA è configurata con un indirizzo IP ottenuto dall'ISP. È presente un percorso predefinito che imposta l'hop successivo come gateway ISP. Se si utilizza DHCP, il valore viene fornito automaticamente. L'interfaccia DMZ è configurata con l'indirizzo IP 192.168.1.1 ed è il gateway predefinito per gli host sul segmento della rete DMZ.

Topologia

Di seguito è riportata una descrizione visiva di come questa operazione è cablata e configurata:



Passaggio 1. Configurare NAT per consentire agli host di uscire da Internet

Nell'esempio viene utilizzato l'oggetto NAT, noto anche come AutoNAT. La prima cosa da configurare sono le regole NAT che permettono agli host sui segmenti interni e DMZ di connettersi a Internet. Poiché questi host utilizzano indirizzi IP privati, è necessario tradurli in un percorso instradabile su Internet. In questo caso, tradurre gli indirizzi in modo che assomiglino all'indirizzo IP dell'interfaccia esterna dell'ASA. Se l'indirizzo IP esterno cambia frequentemente (forse a causa di DHCP), questo è il modo più semplice per configurare il sistema.

Per configurare questa NAT, è necessario creare un oggetto di rete che rappresenti la subnet interna e uno che rappresenti la subnet DMZ. In ognuno di questi oggetti configurare una regola NAT dinamica in grado di trasferire i client PAT (Port Address Translation) man mano che passano dalle rispettive interfacce all'interfaccia esterna.

La configurazione è simile alla seguente:

```
object network inside-subnet
subnet 192.168.0.0 255.255.255.0
nat (inside,outside) dynamic interface
!
object network dmz-subnet
subnet 192.168.1.0 255.255.255.0
nat (dmz,outside) dynamic interface
```

Se si controlla la configurazione corrente a questo punto (con l'output del comando show run), si

osserverà che la definizione dell'oggetto è suddivisa in due parti dell'output. La prima parte indica solo ciò che è presente nell'oggetto (host/subnet, indirizzo IP e così via), mentre la seconda sezione mostra che la regola NAT è associata a tale oggetto. Se si considera la prima voce dell'output precedente:

Quando gli host che corrispondono alla subnet 192.168.0.0/24 attraversano l'interfaccia interna fino all'interfaccia esterna, si desidera convertirli dinamicamente nell'interfaccia esterna.

Passaggio 2. Configurare NAT per accedere al server Web da Internet

Ora che gli host all'interno e le interfacce DMZ possono accedere a Internet, è necessario modificare la configurazione in modo che gli utenti su Internet possano accedere al nostro server Web sulla porta TCP 80. In questo esempio, la configurazione consente agli utenti di Internet di connettersi a un altro indirizzo IP fornito dall'ISP, un indirizzo IP aggiuntivo di *nostra proprietà*. Per questo esempio, utilizzare 198.51.100.101. Con questa configurazione, gli utenti di Internet possono raggiungere il server Web DMZ accedendo alla porta TCP 80 198.51.100.101. Usare l'oggetto NAT per questa attività. L'ASA può convertire la porta TCP 80 sul server Web (192.168.1.100) in una porta TCP 80 all'esterno (198.51.100.101). Analogamente a quanto fatto in precedenza, definite un oggetto e definite le regole di traslazione per tale oggetto. Inoltre, definire un secondo oggetto che rappresenti l'indirizzo IP a cui è possibile tradurre questo host.

La configurazione è simile alla seguente:

```
object network webserver-external-ip
host 198.51.100.101
!
object network webserver
host 192.168.1.100
nat (dmz,outside) static webserver-external-ip service tcp www www
```

Solo per riepilogare il significato della regola NAT in questo esempio:

Quando un host che corrisponde all'indirizzo IP 192.168.1.100 sui segmenti DMZ stabilisce una connessione originata dalla porta TCP 80 (www) e tale connessione esce dall'interfaccia esterna, si desidera convertirla nella porta TCP 80 (www) sull'interfaccia esterna e convertire tale indirizzo IP in 198.51.100.101.

Sembra un po' strano... "originato dalla porta TCP 80 (www)", ma il traffico web è destinato alla porta 80. È importante capire che queste norme NAT sono per loro natura bidirezionali. Di conseguenza, potete capovolgere il testo per riformulare questa frase. Il risultato ha molto più senso:

Quando gli host esterni stabiliscono una connessione con la porta TCP 198.51.100.101 sulla porta TCP di destinazione 80 (www), è possibile convertire l'indirizzo IP di destinazione in 192.168.1.100 e la porta di destinazione in 192.168.1.100 e la porta di destinazione in www (TCP port 80) e inviarla alla DMZ.

Ciò ha più senso se formulato in questo modo. Quindi, occorre configurare gli ACL.

Passaggio 3. Configurazione degli ACL

NAT è configurato e la fine di questa configurazione è vicina. Tenere presente che gli ACL sull'appliance ASA consentono di ignorare il comportamento di sicurezza predefinito, che è il

seguente:

- Il traffico proveniente da un'interfaccia di sicurezza inferiore viene rifiutato quando raggiunge un'interfaccia di sicurezza superiore.
- Il traffico che proviene da un'interfaccia di sicurezza più alta è consentito quando raggiunge un'interfaccia di sicurezza più bassa.

Pertanto, senza aggiungere alcun ACL alla configurazione, il traffico riportato nell'esempio funziona:

- Gli host all'interno (livello di protezione 100) possono connettersi agli host sulla DMZ (livello di protezione 50).
- Gli host interni (livello di protezione 100) possono connettersi agli host esterni (livello di protezione 0).
- Gli host sulla DMZ (livello di protezione 50) possono connettersi agli host esterni (livello di protezione 0).

Tuttavia, il traffico viene rifiutato:

- Gli host esterni (livello di protezione 0) non possono connettersi agli host interni (livello di protezione 100).
- Gli host all'esterno (livello di protezione 0) non possono connettersi agli host sulla DMZ (livello di protezione 50).
- Gli host sulla DMZ (livello di protezione 50) non possono connettersi agli host all'interno (livello di protezione 100).

Poiché il traffico dall'esterno alla rete DMZ viene rifiutato dall'ASA con la sua configurazione corrente, gli utenti su Internet non possono raggiungere il server Web nonostante la configurazione NAT nel passaggio 2. È necessario autorizzare esplicitamente questo traffico. Nel codice della versione 8.3 e successive, è necessario usare l'indirizzo IP reale dell'host nell'ACL e non l'indirizzo IP tradotto. Ciò significa che la configurazione deve autorizzare il traffico destinato a 192.168.1.100 e NON il traffico destinato a 198.51.100.101 sulla porta 80. Per semplicità, gli oggetti definiti nel passaggio 2 possono essere usati anche per questo ACL. Dopo aver creato l'ACL, occorre applicarlo in entrata sull'interfaccia esterna.

Di seguito è riportato l'aspetto dei comandi di configurazione:

```
access-list outside_acl extended permit tcp any object webserver eq www
!
access-group outside_acl in interface outside
```

La riga access-list riporta:

Autorizzare il traffico da qualsiasi punto all'host rappresentato dal server Web dell'oggetto (192.168.1.100) sulla porta 80.

Èimportante che la configurazione utilizzi la parola chiave any. Poiché l'indirizzo IP di origine dei client non è noto in quanto raggiunge il sito Web, specificare il significato 'Qualsiasi indirizzo IP'.

E il traffico proveniente dal segmento DMZ e destinato agli host sul segmento di rete interno? Ad esempio, un server della rete interna a cui devono connettersi gli host della DMZ. Come può l'ASA autorizzare solo il traffico specifico destinato al server interno e bloccare tutto il resto destinato al segmento interno dalla DMZ?

Nell'esempio si presume che nella rete interna sia presente un server DNS all'indirizzo IP 192.168.0.53 a cui gli host nella zona demilitarizzata devono accedere per la risoluzione DNS. È possibile creare l'ACL richiesto e applicarlo all'interfaccia DMZ in modo che l'ASA possa ignorare il comportamento di sicurezza predefinito, menzionato in precedenza, per il traffico che entra nell'interfaccia.

Di seguito è riportato l'aspetto dei comandi di configurazione:

```
object network dns-server
host 192.168.0.53
!
access-list dmz_acl extended permit udp any object dns-server eq domain
access-list dmz_acl extended deny ip any object inside-subnet
access-list dmz_acl extended permit ip any any
!
access-group dmz_acl in interface dmz
```

L'ACL è più complesso del semplice traffico verso il server DNS sulla porta UDP 53. Se l'unica cosa che abbiamo fatto è stata quella prima linea di collegamento, tutto il traffico sarebbe stato bloccato dalla zona demilitarizzata verso gli host su Internet. Alla fine dell'ACL, gli ACL contengono un'istruzione implicita di rifiuto, ossia 'deny ip any any'. Di conseguenza, gli host DMZ non sarebbero in grado di accedere a Internet. Anche se il traffico tra la zona DMZ e l'esterno è autorizzato per impostazione predefinita, quando si applica un ACL all'interfaccia della zona DMZ, i comportamenti di sicurezza predefiniti per l'interfaccia della zona DMZ non sono più attivi e il traffico deve essere autorizzato esplicitamente nell'ACL dell'interfaccia.

Passaggio 4. Configurazione di test con la funzionalità Packet Tracer

Una volta completata la configurazione, è necessario verificarla per accertarsi che funzioni. Il metodo più semplice consiste nell'utilizzare gli host effettivi (se si tratta della rete). Tuttavia, nell'interesse di testarlo dalla CLI e di esplorare ulteriormente alcuni degli strumenti dell'ASA, usare il packet tracer per verificare e potenzialmente eseguire il debug di eventuali problemi incontrati.

Il tracciatore dei pacchetti simula un pacchetto basato su una serie di parametri e inietta il pacchetto sul percorso dati dell'interfaccia, in modo simile a come farebbe un pacchetto reale se venisse prelevato dalla rete. Questo pacchetto viene seguito attraverso la miriade di controlli e processi che vengono eseguiti mentre passa attraverso il firewall, e packet tracer nota il risultato. Simulare l'uscita dell'host interno da un host su Internet. Questo comando indica al firewall di:

Simulare un pacchetto TCP in entrata nell'interfaccia interna dall'indirizzo IP 192.168.0.125 sulla porta di origine 12345 destinato a un indirizzo IP di 203.0.113.1 sulla porta 80.

```
ciscoasa# packet-tracer input inside tcp 192.168.0.125 12345 203.0.113.1 80

Phase: 1
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 2
```

```
Type: ROUTE-LOOKUP
Subtype: input
Result: ALLOW
Config: Additional Information:
in 0.0.0.0 0.0.0.0 outside Phase: 3
Type: NAT
Subtype:
Result: ALLOW
Config:
object network inside-subnet
nat (inside,outside) dynamic interface
Additional Information:
Dynamic translate 192.168.0.125/12345 to 198.51.100.100/12345

Phase: 4
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 5
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 6
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 8
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 1, packet dispatched to next module

Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: allow
```

Il risultato finale è che il traffico è autorizzato, ossia ha superato tutti i controlli NAT e ACL nella configurazione e è stato inviato all'interfaccia di uscita, all'esterno. Notare che il pacchetto è stato tradotto nella Fase 3 e i dettagli di quella Fase mostrano la regola con cui è stata trovata una corrispondenza. L'host 192.168.0.125 viene convertito dinamicamente in 198.51.100.100 in base alla configurazione.

Ora, eseguirlo per una connessione da Internet al server Web. Tenere presente che gli host su Internet possono accedere al server Web connettendosi a 198.51.100.101 sull'interfaccia esterna. Anche in questo caso, il comando seguente si traduce in:

Simulare un pacchetto TCP in entrata nell'interfaccia esterna dall'indirizzo IP 192.0.2.123 sulla porta di origine 12345 destinato a un indirizzo IP 198.51.100.101 sulla porta 80.

```
ciscoasa# packet-tracer input outside tcp 192.0.2.123 12345 198.51.100.101 80

Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
object network webserver
nat (dmz,outside) static webserver-external-ip service tcp www www
Additional Information:
NAT divert to egress interface dmz
Untranslate 198.51.100.101/80 to 192.168.1.100/80

Phase: 2
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group outside_acl in interface outside
access-list outside_acl extended permit tcp any object webserver eq www
Additional Information:

Phase: 3
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 4
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 5
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
object network webserver
nat (dmz,outside) static webserver-external-ip service tcp www www
Additional Information:

Phase: 6
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 7
Type: IP-OPTIONS
Subtype:
```

```
Result: ALLOW
Config:
Additional Information:

Phase: 8
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 3, packet dispatched to next module

Result:
input-interface: outside
input-status: up
input-line-status: up
output-interface: dmz
output-status: up
output-line-status: up
Action: allow
```

Di nuovo, il risultato è che il pacchetto è autorizzato. Gli ACL vengono estratti, la configurazione è corretta e gli utenti di Internet (esterni) possono accedere al server Web tramite l'indirizzo IP esterno.

Verifica

Le procedure di verifica sono incluse nella Fase 4 - Test della configurazione con la funzione Packet Tracer.

Risoluzione dei problemi

Non sono attualmente disponibili informazioni specifiche su come risolvere i problemi relativi a questa configurazione.

Conclusioni

La configurazione di un'appliance ASA per eseguire un NAT di base non è così difficile. L'esempio riportato in questo documento può essere adattato allo scenario specifico se si modificano gli indirizzi IP e le porte utilizzati nelle configurazioni di esempio. La configurazione finale dell'ASA, se combinata, è simile a quella di un'appliance ASA 5510:

```
ASA Version 9.1(1)
!
interface Ethernet0/0
nameif outside
security-level 0
ip address 198.51.100.100 255.255.255.0
!
interface Ethernet0/1
nameif inside
security-level 100
ip address 192.168.0.1 255.255.255.0
!
interface Ethernet0/2
```

```
nameif dmz
security-level 50
ip address 192.168.1.1 255.255.255.0
!
object network inside-subnet
subnet 192.168.0.0 255.255.255.0
object network dmz-subnet
subnet 192.168.1.0 255.255.255.0
object network webserver
host 192.168.1.100
object network webserver-external-ip
host 198.51.100.101
object network dns-server
host 192.168.0.53

!
access-list outside_acl extended permit tcp any object webserver eq www
access-list dmz_acl extended permit udp any object dns-server eq domain
access-list dmz_acl extended deny ip any object inside-subnet
access-list dmz_acl extended permit ip any any
!
object network inside-subnet
nat (inside,outside) dynamic interface
object network dmz-subnet
nat (dmz,outside) dynamic interface
object network webserver
nat (dmz,outside) static webserver-external-ip service tcp www www
access-group outside_acl in interface outside
access-group dmz_acl in interface dmz
!
route outside 0.0.0.0 0.0.0.0 198.51.100.1 1
```

Ad esempio, su un'ASA 5505 con le interfacce connesse come mostrato sopra (all'esterno collegato a Ethernet0/0, all'interno collegato a Ethernet0/1 e la DMZ collegata a Ethernet0/2):

```
ASA Version 9.1(1)
!
interface Ethernet0/0
description Connected to Outside Segment
switchport access vlan 2
!
interface Ethernet0/1
description Connected to Inside Segment
switchport access vlan 1
!
interface Ethernet0/2
description Connected to DMZ Segment
switchport access vlan 3
!
interface Vlan2
nameif outside
security-level 0
ip address 198.51.100.100 255.255.255.0
!
interface Vlan1
nameif inside
security-level 100
ip address 192.168.0.1 255.255.255.0
!
interface Vlan3
nameif dmz
security-level 50
ip address 192.168.1.1 255.255.255.0
```

```
!
object network inside-subnet
subnet 192.168.0.0 255.255.255.0
object network dmz-subnet
subnet 192.168.1.0 255.255.255.0
object network webserver
host 192.168.1.100
object network webserver-external-ip
host 198.51.100.101
object network dns-server
host 192.168.0.53



!
access-list outside_acl extended permit tcp any object webserver eq www
access-list dmz_acl extended permit udp any object dns-server eq domain
access-list dmz_acl extended deny ip any object inside-subnet
access-list dmz_acl extended permit ip any any
!
object network inside-subnet
nat (inside,outside) dynamic interface
object network dmz-subnet
nat (dmz,outside) dynamic interface
object network webserver
nat (dmz,outside) static webserver-external-ip service tcp www www
access-group outside_acl in interface outside
access-group dmz_acl in interface dmz
!
route outside 0.0.0.0 0.0.0.0 198.51.100.1 1
```

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).