Configurer la traduction d'adresses réseau et les ACL sur un pare-feu ASA

Table des matières

Introduction

Ce document décrit comment configurer la traduction d'adresses de réseau (NAT) et les listes de contrôle d'accès (ACL) sur un pare-feu ASA.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Les renseignements présentés dans ce document portent sur un pare-feu ASA 5510 qui exécute la version 9.1(1) du code ASA.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

Ce document décrit un exemple simple et direct de la façon de configurer la NAT et les ACL sur un pare-feu ASA afin d'autoriser la connectivité sortante et entrante. Il a été écrit avec un pare-feu ASA 5510 qui exécute le code ASA version 9.1(1), mais cela peut facilement s'appliquer à toute autre plate-forme de pare-feu ASA. Si vous utilisez une plateforme comme un pare-feu ASA 5505, qui utilise les VLAN au lieu d’une interface physique, vous devez modifier les types d’interface, selon le cas.

Aperçu

Objectifs

Dans cet exemple de configuration, vous pouvez examiner les configurations NAT et ACL nécessaires pour permettre l'accès entrant à un serveur Web dans la DMZ d'un pare-feu ASA, et autoriser la connectivité sortante à partir des hôtes internes et DMZ. Cela peut se résumer en deux objectifs :

1. Accorder aux hôtes internes et DMZ une connectivité sortante à Internet.
2. Accorder aux hôtes sur Internet un accès à un serveur Web dans la zone DMZ avec l’adresse IP 192.168.1.100.

Avant d'effectuer les étapes qui doivent être effectuées afin d'atteindre ces deux objectifs, ce document passe brièvement en revue la façon dont les ACL et NAT fonctionnent sur les versions plus récentes du code ASA (versions 8.3 et ultérieures).

Aperçu de la liste de contrôle d’accès

Le pare-feu ASA utilise les listes de contrôle d’accès (ACL) pour déterminer si le trafic est autorisé ou refusé. Par défaut, le trafic qui passe d’un niveau de sécurité inférieur à un niveau de sécurité supérieur est refusé. Cette règle peut être contournée par une ACL appliquée à l’interface de sécurité inférieure. L’ASA, par défaut, autorise également le trafic d’interfaces de sécurité supérieure vers des interface de sécurité inférieure. Ce comportement peut également être outrepassé par une ACL.

Dans les versions antérieures du code ASA (versions 8.2 et antérieures), l’ASA comparait une connexion ou un paquet entrant à l’ACL sur une interface, et ce, sans annuler la traduction du paquet au préalable. En d’autres termes, l’ACL devait autoriser le paquet, comme si vous alliez le capter sur l’interface. Dans la version 8.3 et les versions ultérieures du code, l’ASA annule la traduction du paquet avant de vérifier les ACL de l’interface. Cela signifie que dans ces versions du code et conformément au présent document, le trafic vers l’adresse IP réelle de l’hôte est autorisé, mais pas vers l’adresse IP traduite de l’hôte.

Reportez-vous à la section Configuration des règles d'accès du Guide de configuration de l'interface de ligne de commande du pare-feu de la gamme Cisco ASA 9.1 du Book 2 pour plus d'informations sur les ACL.

Présentation de NAT

La NAT sur l'ASA dans les versions 8.3 et ultérieures est divisée en deux types : NAT automatique (NAT d'objet) et NAT manuelle (NAT double). La première des deux, la NAT d'objet, est configurée dans la définition d'un objet réseau. Un exemple de ce type de NAT est fourni plus loin dans ce document. Un des principaux avantages de cette méthode est que l'ASA définit automatiquement l'ordre des règles de traitement afin d'éviter les conflits. C'est la forme plus simple de NAT, mais cette facilité est accompagnée d'une limitation de la granularité de la configuration. Par exemple, vous ne pouvez pas prendre une décision de traduction basée sur la destination dans le paquet, comme vous le pourriez avec le deuxième type de NAT, la NAT manuelle. La NAT manuelle est plus robuste sur le plan de la granularité, mais elle exige que les lignes soient configurées dans le bon ordre afin qu'elle puisse obtenir le bon comportement. Cela complique ce type de NAT, et par conséquent, il ne peut pas être utilisé dans cet exemple de configuration.

Reportez-vous à la section Information About NAT du Book 2 : Cisco ASA Series Firewall CLI Configuration Guide, 9.1 pour plus d'informations sur NAT.

Configurer

Pour commencer

La configuration de base d'un ASA consiste en trois interfaces connectées à trois segments de réseau. Le segment de réseau du fournisseur d'accès Internet (FAI) est connecté à l'interface Ethernet0/0 et étiqueté comme externe avec un niveau de sécurité de 0. Le réseau interne est connecté à l'interface Ethernet0/1 et est étiqueté comme interne, avec un niveau de sécurité de 100. Le segment DMZ, où réside le serveur Web, est connecté à l'interface Ethernet0/2 et est étiqueté comme DMZ, avec un niveau de sécurité de 50.

Voici la configuration de l'interface et les adresses IP de l'exemple :

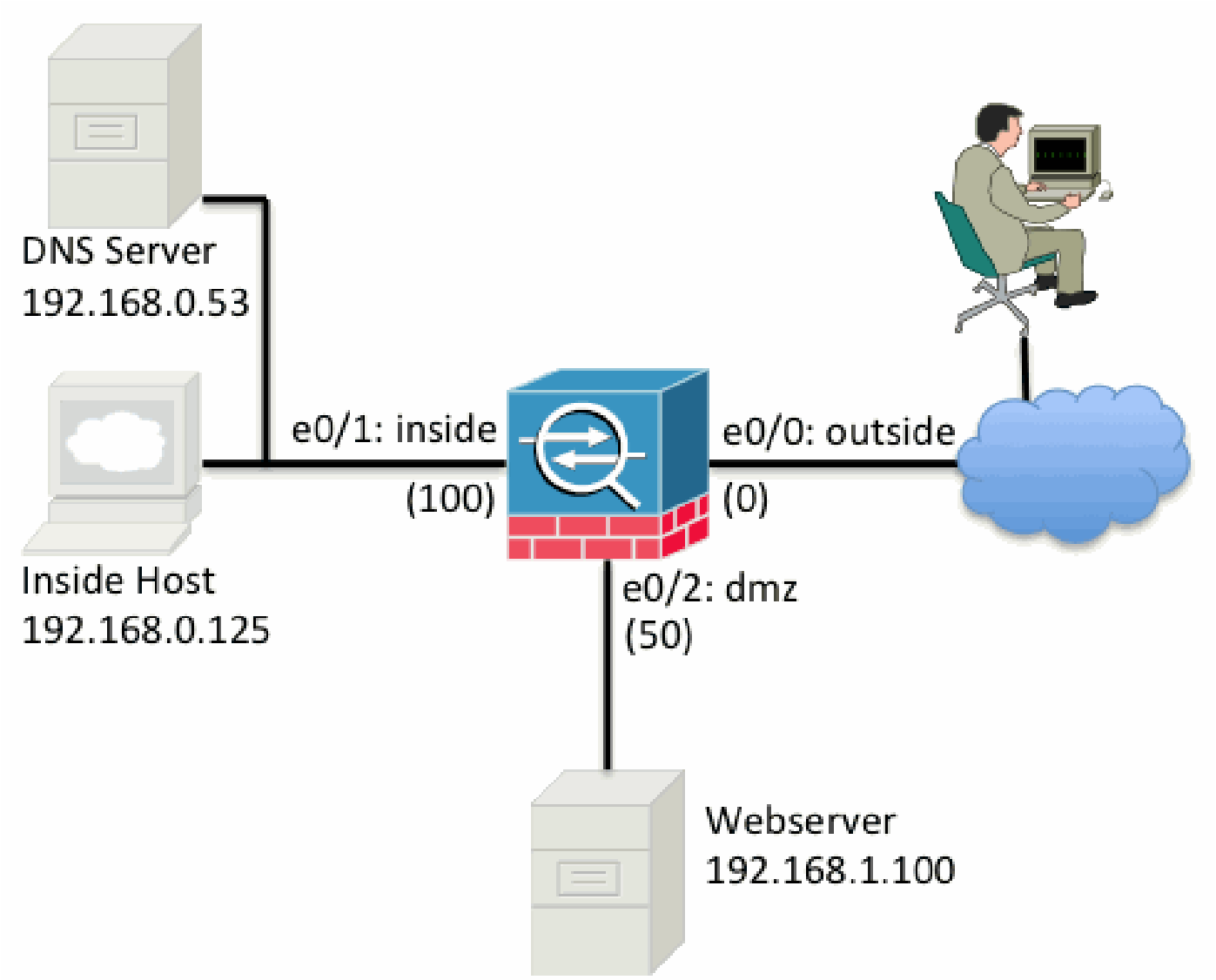
```
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 198.51.100.100 255.255.255.0
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 192.168.0.1 255.255.255.0
!
interface Ethernet0/2
 nameif dmz
 security-level 50
 ip address 192.168.1.1 255.255.255.0
```

```
!
route outside 0.0.0.0 0.0.0.0 198.51.100.1
```

Vous pouvez voir ici que l'interface interne de l'ASA est associée à l'adresse IP 192.168.0.1; il s'agit de la passerelle par défaut pour les hôtes internes. L'interface externe de l'ASA est configurée avec une adresse IP obtenue à partir du FAI. Une route par défaut définissant la passerelle du FAI comme le prochain nœud est en place. Si vous utilisez DHCP, cet itinéraire est fourni automatiquement. L'interface DMZ est configurée avec l'adresse IP 192.168.1.1; il s'agit de la passerelle par défaut pour les hôtes du segment réseau DMZ.

Topologie

Voici un aperçu visuel du câblage et de la configuration :



Étape 1. Configurer NAT pour autoriser les hôtes à accéder à Internet

Dans cet exemple, la fonction NAT d'objet, également appelée AutoNAT, est utilisée. En premier lieu, il faut configurer les règles NAT pour autoriser les hôtes des segments internes et DMZ à se

connecter à Internet. Étant donné que ces hôtes utilisent des adresses IP privées, vous avez besoin de les traduire en adresses pouvant être acheminées sur Internet. Dans ce cas, traduisez les adresses afin qu'elles ressemblent à l'adresse IP de l'interface externe de l'ASA. Si votre adresse IP externe change souvent (peut-être à cause de DHCP), il s'agit de la configuration la plus simple.

Afin de configurer cette NAT, vous devez créer un objet réseau qui représente le sous-réseau interne, et un autre qui représente le sous-réseau DMZ. Dans chacun de ces objets, configurez une règle NAT dynamique qui peut appliquer la traduction d'adresses de port (PAT) à ces clients lorsqu'ils passent de leurs interfaces respectives à l'interface externe.

Cette configuration ressemble à ceci :

```
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
```

Si vous examinez la configuration en cours à ce stade (avec le résultat de la commande show run), vous pouvez voir que la définition d'objet est divisée en deux parties du résultat. La première partie indique seulement ce qui est dans l'objet (hôte/sous-réseau, adresse IP et ainsi de suite), tandis que la seconde montre cette règle de NAT liée à cet objet. Si vous prenez la première entrée dans la sortie précédente :

Quand les hôtes qui correspondent au sous-réseau 192.168.0.0/24 passent de l'interface interne à l'interface externe, vous voulez les traduire dynamiquement vers l'interface externe.

Étape 2. Configurer la fonction NAT pour accéder au serveur Web à partir d'Internet

Maintenant que les hôtes sur les interfaces interne et DMZ peuvent accéder à Internet, vous devez modifier la configuration afin que les utilisateurs sur Internet puissent accéder à notre serveur Web sur le port TCP 80. Dans cet exemple, la configuration fait en sorte que les gens sur Internet peuvent se connecter à une autre adresse IP fournie par le FAI, une adresse IP supplémentaire que nous possédons. Aux fins de cet exemple, utilisez l'adresse IP 198.51.100.101. Avec cette configuration, les utilisateurs sur Internet peuvent accéder au serveur Web DMZ en accédant à 198.51.100.101 sur le port TCP 80. Utilisez la fonction NAT d'objet pour cette tâche, et l'ASA peut traduire le port TCP 80 sur le serveur Web (192.168.1.100) pour ressembler à 198.51.100.101 sur le port TCP 80 à l'extérieur. Comme ce qui a été fait précédemment, définissez un objet et les règles de traduction applicables. Définissez également un deuxième objet pour représenter l'adresse IP vers laquelle vous pouvez traduire cet hôte.

Cette configuration ressemble à ceci :

```
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
```

Voici un résumé de la signification de la règle de NAT dans cet exemple :

Lorsqu'un hôte qui correspond à l'adresse IP 192.168.1.100 sur les segments DMZ établit une connexion à partir du port TCP 80 (www) et que cette connexion va vers l'interface externe, vous voulez la traduire afin qu'elle corresponde au port TCP 80 (www) sur l'interface externe, et vous voulez traduire cette adresse IP vers 198.51.100.101.

Cela semble un peu étrange... « provient du port TCP 80 (www) », mais le trafic Web est destiné au port 80. Il est important de comprendre que ces règles de NAT sont bidirectionnelles par nature. Ainsi, vous pouvez retourner le libellé afin de reformuler cette phrase. Le résultat est beaucoup plus logique :

Lorsque des hôtes externes établissent une connexion à 198.51.100.101 sur le port TCP de destination 80 (www), vous pouvez traduire l'adresse IP de destination en 192.168.1.100 et le port de destination en port TCP 80 (www) et l'envoyer à la DMZ.

Cette phrase reformulée a plus de sens. Ensuite, vous devez configurer les ACL.

Étape 3. Configurer les ACL

La NAT est configurée, et nous approchons la fin de cette configuration. N'oubliez pas, les ACL sur l'ASA permettent d'outrepasser le comportement de sécurité par défaut, qui se présente comme suit :

- Le trafic d'une interface de sécurité inférieure est refusé lorsqu'il va vers une interface de sécurité supérieure.
- Le trafic d'une interface de sécurité supérieure est autorisé lorsqu'il va vers une interface de sécurité inférieure.

Ainsi, sans aucun ajout d'ACL à la configuration, le trafic dans l'exemple fonctionne dans les cas suivants :

- Les hôtes sur le réseau interne (niveau de sécurité 100) peuvent se connecter à des hôtes sur le réseau DMZ (niveau de sécurité 50).
- Les hôtes sur le réseau interne (niveau de sécurité 100) peuvent se connecter à des hôtes sur le réseau externe (niveau de sécurité 0).
- Les hôtes sur le réseau DMZ (niveau de sécurité 50) peuvent se connecter à des hôtes sur le réseau externe (niveau de sécurité 0).

Toutefois, ce trafic est refusé dans les cas suivants :

- Les hôtes sur le réseau externe (niveau de sécurité 0) ne peuvent se connecter à des hôtes

sur le réseau interne (niveau de sécurité 100).
- Les hôtes sur le réseau externe (niveau de sécurité 0) ne peuvent se connecter à des hôtes sur le réseau DMZ (niveau de sécurité 50).
- Les hôtes sur le réseau DMZ (niveau de sécurité 50) ne peuvent se connecter à des hôtes sur le réseau interne (niveau de sécurité 100).

Puisque le trafic du réseau externe vers le réseau DMZ est refusé par l'ASA dans sa configuration actuelle, les utilisateurs sur Internet ne peuvent pas atteindre le serveur Web malgré la configuration de la NAT à l'étape 2. Vous devez explicitement autoriser ce trafic. Dans les versions 8.3 et ultérieures du code, vous devez utiliser l'adresse IP réelle de l'hôte dans l'ACL, et non pas l'adresse IP traduite. Cela signifie que la configuration doit autoriser le trafic vers l'adresse 192.168.1.100, mais PAS celui vers l'adresse 198.51.100.101 sur le port 80. Pour des raisons de simplicité, les objets définis à l'étape 2 peuvent également être utilisés pour cette liste de contrôle d'accès. Une fois l'ACL créée, vous devez l'appliquer comme ACL entrante à l'interface externe.

Voici à quoi ressemblent ces commandes de configuration :

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

La ligne de l'ACL indique ce qui suit :

Autoriser le trafic de n'importe où (any) vers l'hôte représenté par le serveur Web (192.168.1.100) sur le port 80.

Il est important ici que la configuration utilise le mot-clé any. Étant donné que l'adresse IP source des clients n'est pas connue car elle atteint votre site Web, spécifiez une signification quelconque, « Toute adresse IP ».

Qu'en est-il du trafic provenant du segment DMZ vers les hôtes sur le segment réseau interne? Par exemple, un serveur sur le réseau interne auquel les hôtes sur le réseau DMZ doivent se connecter. Comment l'ASA peut-il autoriser uniquement ce trafic précis vers le serveur interne et bloquer tout autre trafic vers le segment interne en provenance du segment DMZ?

Dans cet exemple, on présume qu'un serveur DNS réside sur le réseau interne sous l'adresse IP 192.168.0.53 et que les hôtes du réseau DMZ doivent y accéder aux fins de résolution DNS. Vous créez l'ACL nécessaire et l'appliquez à l'interface DMZ de façon à ce que l'ASA puisse outrepasser le comportement de sécurité par défaut susmentionné pour le trafic entrant de l'interface.

Voici à quoi ressemblent ces commandes de configuration :

```
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 sert plus qu’à simplement autoriser le trafic vers le serveur DNS sur le port UDP 53. Si nous nous contentons de cette première ligne d’autorisation, tout le trafic serait bloqué de la DMZ vers les hôtes sur Internet. Les listes de contrôle d’accès comportent une instruction implicite deny IP any any à la fin de la liste. Ainsi, vos hôtes DMZ ne seraient pas en mesure d’accéder à Internet. Même si le trafic de l’interface DMZ vers l’interface externe est autorisé par défaut, si l’on applique une ACL à l’interface DMZ, les comportements de sécurité par défaut relatifs à cette dernière ne sont plus en vigueur, et vous devez autoriser explicitement le trafic dans l’ACL de l’interface.

Étape 4. Tester la configuration avec la fonctionnalité Packet Tracer

Maintenant que la configuration est terminée, vous devez la tester pour vous assurer qu’elle fonctionne. La méthode la plus simple consiste à utiliser des hôtes réels (s’il s’agit de votre réseau). Cependant, dans l'intérêt de tester cela à partir de l'interface de ligne de commande et d'explorer plus en détail certains des outils de l'ASA, utilisez le traceur de paquets afin de tester et potentiellement déboguer tous les problèmes rencontrés.

Cette fonction simule un paquet en fonction d’une série de paramètres et l’injecte dans le chemin de données de l’interface, comme s’il était véritablement capté par l’interface. Ce paquet est soumis à la myriade de contrôles et de processus lorsqu’il passe par le pare-feu, et le traceur de paquet consigne le résultat. Simuler l’hôte interne accédant à un hôte sur Internet. Cette commande indique au pare-feu :

Simuler un paquet TCP arrivant dans l’interface interne à partir de l’adresse IP 192.168.0.125 sur le port source 12345 vers l’adresse IP 203.0.113.1 sur le port 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
```

Ceci a pour résultat que le trafic est autorisé, ce qui signifie qu'il a réussi tous les contrôles de la

NAT et de l'ACL prévus par la configuration et a été envoyé à l'interface de sortie, à l'extérieur. Notez que le paquet a été traduit à la phase 3 et que les détails de cette phase indiquent quelle règle est touchée. L'hôte 192.168.0.125 est traduit dynamiquement vers 198.51.100.100 conformément à la configuration.

Maintenant, exécutez-le pour lancer une connexion entre Internet et le serveur Web. N'oubliez pas que les hôtes sur Internet peuvent accéder au serveur Web en se connectant à 198.51.100.101 sur l'interface externe. Encore une fois, cette commande demande au pare-feu d'exécuter ce qui suit :

Simuler un paquet TCP arrivant dans l'interface externe à partir de l'adresse IP 192.0.2.123 sur le port source 12345 vers l'adresse IP 198.51.100.101 sur le port 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
```

Encore une fois, le paquet est autorisé. Les listes de contrôle d’accès sont extraites, la configuration semble correcte et les utilisateurs sur Internet (à l’extérieur) peuvent accéder à ce serveur Web avec l’adresse IP externe.

Vérifier

Les procédures de vérification sont décrites à l’étape 4 – Mettre une configuration à l’essai avec la fonction de traceur de paquet.

Dépannage

Aucune information spécifique n'est actuellement disponible sur la façon de dépanner cette configuration.

Conclusion

La configuration d'un ASA pour effectuer la NAT de base n'est pas si difficile qu'une tâche. Vous pouvez adapter l’exemple du présent document à votre propre scénario en modifiant les adresses IP et les ports utilisés dans les configurations de l’exemple. Cette dernière configuration, lorsque combinée, ressemble à ceci sur un 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
```

Sur un ASA 5505, par exemple, avec les interfaces connectées comme indiqué précédemment (interface externe connectée à Ethernet0/0, interface interne connectée à Ethernet0/1 et interface DMZ connectée à 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
```

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.