Configuration NAT de base ASA : Web server dans le DMZ dans la version 8.3 et ultérieures ASA

Contenu

Introduction

Ce document fournit un exemple simple et direct de comment à la traduction d'adresses de configure network (NAT) et au Listes de contrôle d'accès (ACL) sur un Pare-feu ASA afin de permettre la Connectivité sortante aussi bien que d'arrivée. Ce document a été écrit avec un Pare-feu 5510 de l'appliance de sécurité adaptable (ASA) que la version 9.1(1) de code des passages ASA, mais ceci peut facilement appliquer à n'importe quelle autre plate-forme de Pare-feu ASA. Si vous utilisez une plate-forme telle qu'une ASA 5505, qui utilise des VLAN au lieu d'une interface physique, vous devez changer les types d'interface comme appropriés.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations dans ce document sont basées sur un Pare-feu ASA 5510 qui exécute la version 9.1(1) de code ASA.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Aperçu

Buts

En cet exemple de configuration, vous pouvez regarder quelle configuration NAT et d'ACL sera nécessaire afin de permettre l'accès entrant à un web server dans le DMZ d'un Pare-feu ASA, et permettez la Connectivité sortante d'interne et des hôtes DMZ. Ceci peut être récapitulé en tant que deux buts :

1. Permettez les hôtes sur l'intérieur et la Connectivité sortante DMZ à l'Internet.
2. Permettez aux hôtes sur l'Internet pour accéder à un web server sur le DMZ avec une adresse IP de 192.168.1.100.

Avant d'obtenir aux étapes qui doivent être terminées afin d'accomplir ces deux buts, ce document va brièvement au-dessus de la manière ACLs et du travail NAT sur les versions plus nouvelles du code ASA (version 8.3 et ultérieures).

Aperçu de liste de contrôle d'accès

Les listes de contrôle d'accès (Listes d'accès ou ACLs pour faire court) sont la méthode par laquelle le Pare-feu ASA détermine si le trafic est permis ou refusé. Par défaut, le trafic qui passe d'un **inférieur au niveau de sécurité plus élevé** est refusé. Ceci peut être ignoré par un ACL appliqué à cette interface à niveau de sécurité inférieur. Également l'ASA, par défaut, permet le trafic de **plus élevé aux interfaces à niveau de sécurité inférieur**. Ce comportement peut également être ignoré avec un ACL.

Dans les versions antérieures du code ASA (8.2 et plus tôt), l'ASA a comparé une connexion entrante ou un paquet contre l'ACL sur une interface sans untranslating le paquet d'abord. En d'autres termes, l'ACL a dû permettre le paquet comme si vous deviez capturer ce paquet sur l'interface. En code de version 8.3 et ultérieures, les untranslates ASA que paquet avant qu'il vérifie l'interface ACLs. Ceci signifie cela pour 8.3 et le code postérieur, et ce document, le trafic au vrai IP de l'hôte n'est permis et pas l'IP traduit de l'hôte.

Voyez la section de règles d'accès de l'ouvrage configurante 2 : Guide de configuration CLI de Pare-feu de gamme de Cisco ASA, 9.1 pour plus d'informations sur ACLs.

Présentation de NAT

NAT sur l'ASA dans la version 8.3 et ultérieures est divisé en deux types connus sous le nom de **NAT NAT (objet NAT)** et **manuel automatique (deux fois NAT)**. Les premiers des deux, **objectent NAT**, sont configurés dans la définition d'un objet de réseau. Un exemple de ceci est fourni plus tard dans ce document. Un avantage principal de cette méthode NAT est que l'ASA commande automatiquement les règles pour traiter afin d'éviter des conflits. C'est la forme la plus facile de

NAT, mais avec cette facilité est livré une limite dans la finesse de configuration. Par exemple, vous ne pouvez pas faire à une décision fondée de traduction sur le destination in le paquet car vous pourriez avec le deuxième type de NAT, **manuel nat**. **NAT manuel** est plus robuste dans sa finesse, mais elle exige que les lignes soient configurées dans l'ordre approprié de sorte qu'il puisse réaliser le comportement correct. Ceci complique ce type NAT, et en conséquence il ne sera pas utilisé dans cet exemple de configuration.

Voyez les informations sur la section de l'ouvrage NAT 2 : Guide de configuration CLI de Pare-feu de gamme de Cisco ASA, 9.1 pour plus d'informations sur NAT.

Configurez

Obtenez commencé

L'installation de base de configuration ASA est trois interfaces connectées à trois segments de réseau. Le segment de réseau ISP est connecté à l'interface Ethernet0/0 et **dehors** étiqueté avec un niveau de Sécurité de 0. Le réseau interne a été connecté à Ethernet0/1 et étiqueté en tant qu'**à l'intérieur** avec un niveau de Sécurité de 100. Le segment DMZ, où le web server réside, est connecté à Ethernet0/2 et étiqueté comme **DMZ** avec un niveau de Sécurité de 50.

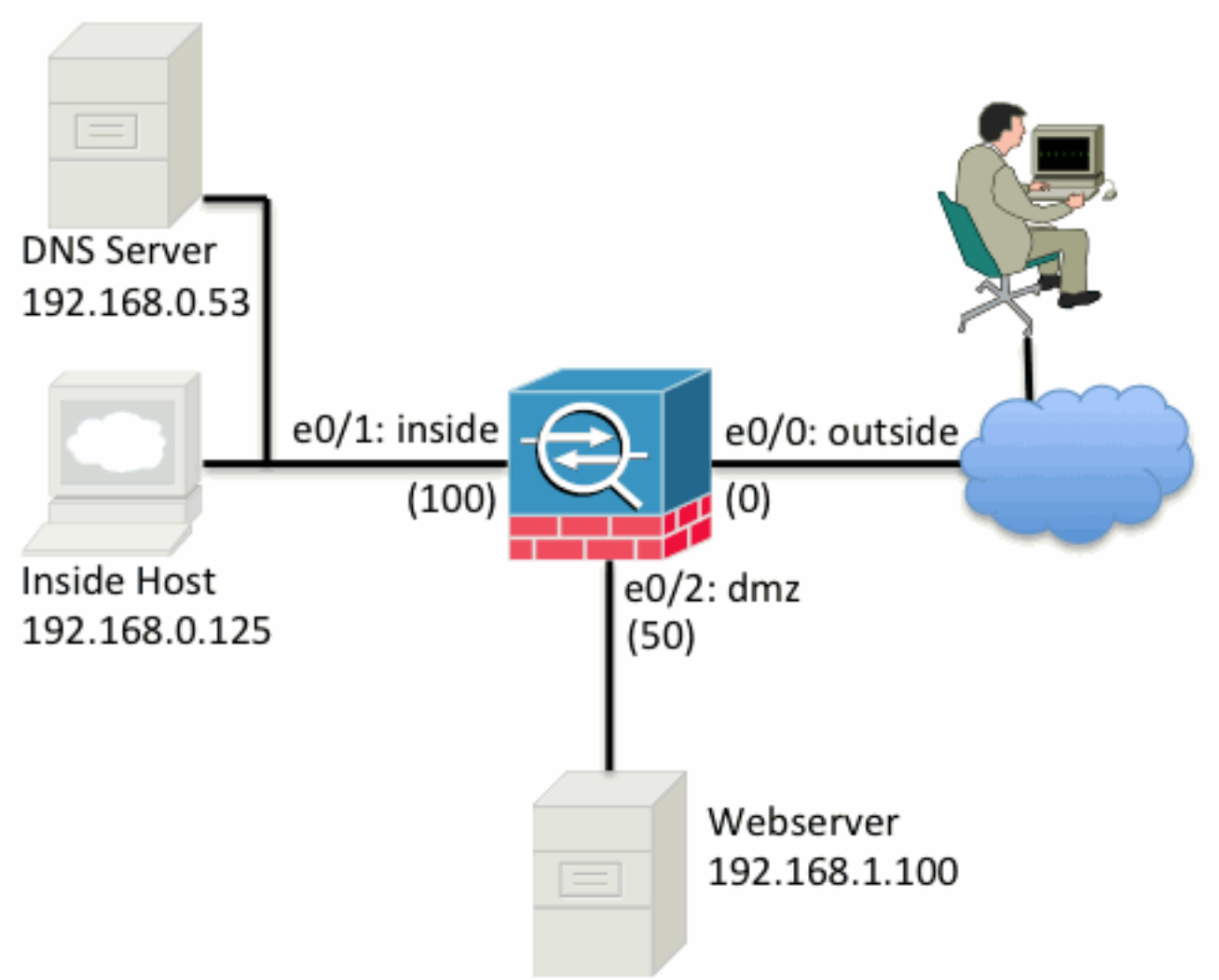
La configuration d'interface et les adresses IP pour l'exemple sont vues ici :

```
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
```

Voici que vous pouvez voir que l'**interface interne de l'**ASA est placée avec l'adresse IP de 192.168.0.1, et c'est la passerelle par défaut pour les hôtes internes. Les ASA **en dehors de l'**interface est configurées avec une adresse IP obtenue de l'ISP. Il y a un default route en place, qui place le prochain-saut pour être la passerelle ISP. Si vous utilisez le DHCP ceci est fourni automatiquement. L'interface **DMZ** est configurée avec l'adresse IP de 192.168.1.1, et c'est la passerelle par défaut pour des hôtes sur le segment de réseau DMZ.

Topologie

Voici un visuel les regardent comment ceci est câblé et configuré :



Étape 1 - Configurez NAT pour permettre à des hôtes pour sortir à l'Internet

Pour cet **objet d'**exemple **NAT**, également connu comme **AutoNAT**, est utilisé. La première chose à configurer est les règles NAT qui permettent les hôtes sur l'**intérieur** et des segments **DMZ** de se connecter à l'Internet. Puisque ces hôtes utilisent des adresses IP privées, vous devez les traduire à quelque chose qui est routable sur l'Internet. Dans ce cas, traduisez les adresses de sorte qu'ils ressemblent aux ASA **en dehors de l'**adresse IP d'interface. Si votre IP externe change fréquemment (peut-être en raison du DHCP) c'est la manière la plus simple d'établir ceci.

Afin de configurer ce NAT, vous devez créer un objet de réseau qui représente le sous-réseau **intérieur** aussi bien qu'un qui représentent le sous-réseau **DMZ**. Dans chacun de ces objets, configurez une règle **nat dynamique** qui translation d'adresses d'adresse du port (PAT) ces clients pendant qu'ils passent de leurs interfaces respectives à l'interface **extérieure**.

Cette configuration semble semblable 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 regardez la configuration en cours en ce moment (avec la sortie de l'**exposition exécutez la** commande), vous verrez que la définition d'objet est coupée en deux parts de la sortie. La

première partie indique seulement ce qui est dans l'objet (hôte/sous-réseau, adresse IP, et ainsi de suite), alors que la deuxième section prouve que règle NAT attachée à cet objet. Si vous prenez la première entrée dans la sortie précédente :

*Quand les hôtes qui apparient la traversée de 192.168.0.0/24 sous-réseaux de l'**interface interne à l'**interface **extérieure**, vous veulent les traduire dynamiquement à l'**interface extérieure**.*

Étape 2 - Configurez NAT pour accéder au serveur Web de l'Internet

Maintenant que les hôtes sur les interfaces **intérieures** et **DMZ** peuvent sortir à l'Internet, vous devez modifier la configuration de sorte que les utilisateurs sur l'Internet puissent accéder à notre web server sur le port TCP 80. Dans cet exemple, l'installation est de sorte que les gens sur l'Internet puissent se connecter à une autre adresse IP que l'ISP a fourni, une adresse IP supplémentaire nous *possédons*. Pour cet exemple, utilisation 198.51.100.101. Avec cette configuration, les utilisateurs sur l'Internet pourront atteindre le web server **DMZ** en accédant à 198.51.100.101 sur le port TCP 80. Utilisez l'**objet NAT** pour cette tâche, et l'ASA le port 80 de translate tcp sur le web server (192.168.1.100) ressemblera à 198.51.100.101 sur le port TCP 80 sur l'**extérieur**. De même à ce qui a été fait précédemment, définit un objet et définit des Règles de traduction pour cet objet. En outre, définissez un deuxième objet pour représenter l'IP que vous traduirez cet hôte à.

Cette configuration semble semblable 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
```

Récapituler juste ce que signifie cette règle NAT dans cet exemple :

*Quand un hôte qui apparie l'adresse IP **192.168.1.100** sur les segments **DMZ** établit une connexion originaire du **port TCP 80 (WWW)** et qui la connexion sort l'interface **extérieure**, vous voulez traduire cela pour être le **port TCP 80 (WWW)** sur l'interface **extérieure** et pour traduire cette adresse IP pour être **198.51.100.101**.*

Cela semble peu un impair… « originaire du port TCP 80 (WWW) », mais du trafic web *est destiné au* port 80. Il est important de comprendre que ces règles NAT sont bidirectionnelles en nature. En conséquence, vous pouvez inverser les formulations autour afin de reformuler cette phrase. Le résultat semble beaucoup plus raisonnable :

*Quand les hôtes sur l'**extérieur** établissent une connexion à **198.51.100.101** sur le **port TCP 80 (WWW) de** destination, vous traduirez l'adresse IP de destination pour être **192.168.1.100** et la destination port sera le **port TCP 80 (WWW)** et lui enverra le **DMZ**.*

Ceci semble plus de raisonnable une fois exprimé de cette façon. Ensuite, vous devez installer l'ACLs.

Étape 3 - Configurez ACLs

NAT est configuré et la fin de cette configuration est près. Souvenez-vous, ACLs sur l'ASA te permettent pour ignorer le comportement par défaut de Sécurité qui est comme suit :

- Trafiquez qui va d'une **interface à niveau de sécurité inférieur est refusé** quand elle va à une **interface à sécurité plus élevée**.
- Trafiquez qui va d'une **interface à sécurité plus élevée est laissé** quand elle va à une **interface à niveau de sécurité inférieur**.

Ainsi sans ajout de n'importe quel ACLs à la configuration, ce trafic dans l'exemple fonctionne :

- Les hôtes sur l'**intérieur** (niveau de Sécurité 100) peuvent se connecter aux hôtes sur le **DMZ** (niveau de Sécurité 50).
- Les hôtes sur l'**intérieur** (niveau de Sécurité 100) peuvent se connecter aux hôtes sur l'**extérieur** (niveau de Sécurité 0).
- Les hôtes sur le **DMZ** (niveau de Sécurité 50) peuvent se connecter aux hôtes sur l'**extérieur** (niveau de Sécurité 0).

Cependant, ce trafic est refusé :

- Les hôtes sur l'**extérieur** (niveau de Sécurité 0) ne peuvent pas se connecter aux hôtes sur l'**intérieur** (niveau de Sécurité 100).
- Les hôtes sur l'**extérieur** (niveau de Sécurité 0) ne peuvent pas se connecter aux hôtes sur le **DMZ** (niveau de Sécurité 50).
- Les hôtes sur le **DMZ** (niveau de Sécurité 50) ne peuvent pas se connecter aux hôtes sur l'**intérieur** (niveau de Sécurité 100).

Puisque le trafic de l'**extérieur au réseau DMZ** est refusé par l'ASA avec sa configuration en cours, les utilisateurs sur l'Internet ne peuvent pas atteindre le web server en dépit de la configuration NAT dans l'étape 2. Vous devez permettre explicitement ce trafic. En 8.3 et code postérieur vous devez utiliser le **vrai IP de l'**hôte dans l'ACL et pas l'**IP traduit**. Ceci signifie que la configuration doit permettre le trafic destiné à 192.168.1.100 et ne pas trafiquer destiné à 198.51.100.101 sur le port 80. Dans l'intéret de la simplicité, les objets définis dans l'étape 2 seront aussi bien utilisés pour cet ACL. Une fois que l'ACL est créé, vous devez l'appliquer d'arrivée sur l'interface extérieure.

Voici ce qui ressemblent à ces commandes de configuration :

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

Les états de la ligne de liste d'accès :

*Permettez le trafic de l'**any(where) à l'**hôte représenté par le **web server d'**objet **(192.168.1.100)** sur le port 80.*

Il est important la configuration utilise le **n'importe quel** mot clé ici. Puisque l'adresse IP source des clients n'est pas connue en tant que lui atteint votre site Web, spécifiez toutes les la signification « n'importe quelles adresses IP.

Que diriez-vous du trafic du segment **DMZ** a destiné aux hôtes sur le segment **intérieur de** réseau ? Par exemple, un serveur sur le réseau **intérieur au le**quel les hôtes sur le **DMZ** doivent se connecter. Comment l'ASA peut-elle laisser seulement que spécifique trafiquez destiné au serveur **intérieur** et bloquez tout autrement destiné au segment **intérieur du DMZ** ?

Dans cet exemple on le suppose qu'il y a un serveur DNS sur le réseau intérieur à l'adresse IP 192.168.0.53 qui les hôtes sur la nécessité **DMZ** d'accéder à pour la résolution de DN. Vous créez l'ACL requis et vous appliquez l'à l'interface **DMZ** ainsi l'ASA peut ignorer ce comportement par

défaut de Sécurité, cité précédemment, pour le trafic qui écrit cette interface.

Voici ce qui ressemblent à 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 est plus complexe que simplement permettant ce trafic au serveur DNS sur le port UDP 53. Si tout que nous avons fait est que d'abord ligne de « autorisation », alors tout le trafic serait bloqué du **DMZ aux** hôtes sur l'Internet. ACLs font refuser un implicite « l'IP tout » à la fin de l'ACL. En conséquence, vos **hôtes DMZ** ne pourraient pas sortir à l'Internet. Quoiqu'on permette le trafic du **DMZ à l'extérieur** par défaut, avec l'application d'un ACL à l'interface **DMZ**, ceux transfèrent des comportements de Sécurité pour l'interface **DMZ** ne sont plus en effet et vous devez explicitement permettre le trafic dans l'ACL d'interface.

Étape 4 - Configuration de test avec la configuration de Packet Tracer

Maintenant que la configuration est terminée, vous devez la tester afin de s'assurer que cela fonctionne. La méthode facile est d'utiliser les hôtes réels (si c'est votre réseau). Cependant, dans l'intérêt de tester ceci du CLI et autre en explorant certains des outils de l'ASA, employez le traceur de paquet afin de tester et mettre au point potentiellement tous les problèmes produits.

Le traceur de paquet fonctionne à côté de simuler un paquet basé sur une gamme de paramètres et injectant ce paquet au chemin de données d'interface, semblable à la manière qu'un paquet de vie réelle s'il était pris outre du fil. Ce paquet est suivi par la myriade des contrôles et des processus qui sont faits pendant qu'ils traversent le Pare-feu, et traceur de paquet note les résultats. Simulez l'hôte interne sortant à un hôte sur l'Internet. La commande ci-dessous instruit le Pare-feu à :

*Simulez un **paquet TCP** étant livré dans l'**interface interne de l'**IP address **192.168.0.125** sur le port **12345 de** source destiné à un IP address de **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
```

Le résultat final est qu'**on permet le** trafic, les whichmeans qu'il a passés à tout le NAT et l'ACL signe la configuration et a été envoyé l'interface de sortie, **dehors**. Notez que le paquet a été traduit dans le Phase 3 et les détails de cette phase affichent quelle règle est frappée. L'hôte 192.168.0.125 est traduit dynamiquement à 198.51.100.100 selon la configuration.

Maintenant, exécutez-le pour une connexion de l'Internet au web server. Souvenez-vous, des hôtes sur l'Internet accédera au web server en se connectant à 198.51.100.101 sur l'interface **extérieure**. De nouveau, cette prochaine commande se traduit à :

*Simulez un **paquet TCP** étant livré dans l'interface **extérieure de l'**IP address **192.0.2.123** sur le port **12345 de** source destiné à un IP address de **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
```

De nouveau, le résultat est qu'on permet le paquet. Le contrôle d'ACLs, la configuration semble correct, et les utilisateurs sur l'Internet (**dehors**) devraient pouvoir accéder à ce web server avec l'IP externe.

Vérifiez

Des procédures de vérification sont incluses dans l'étape 4 - configuration de test avec la configuration de Packet Tracer.

Dépannez

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Conclusion

La configuration d'une ASA pour faire NAT de base n'est pas celle décourager d'une tâche. L'exemple dans ce document peut être adapté à votre scénario spécifique si vous changez les adresses IP et les ports utilisés en exemples de configuration. La configuration de la finale ASA pour ceci, une fois combiné, regarde semblable à ceci pour une 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 une ASA 5505, par exemple, avec les interfaces connectées comme affiché précédemment (**extérieur** connecté à Ethernet0/0, **à l'intérieur de** connecté à Ethernet0/1 et au **DMZ** connecté 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
```