Exemple de configuration ASA 8.3(x) Dynamic PAT avec deux réseaux internes et Internet

Contenu

Introduction

Ce document fournit une configuration d'échantillon pour le TAPOTEMENT dynamique sur une appliance de sécurité adaptable Cisco (ASA) cette version de logiciel de passages 8.3(1). PAT dynamique traduit de plusieurs vraies adresses à une adresse IP tracée simple en traduisant vraie le port d'adresse source et de source à l'adresse tracée et au seul port tracé. Chaque connexion exige une session de traduction distincte, parce que le port éphémère diffère pour chacune d'entre elles.

Conditions préalables

Conditions requises

Assurez-vous que vous répondez à ces exigences avant d'essayer cette configuration :

- Assurez-vous que le réseau interne a deux réseaux situés sur l'intérieur de l'ASA :192.168.0.0/24 — Réseau directement connecté à l'ASA.192.168.1.0/24 — Réseau sur l'intérieur de l'ASA, mais derrière un autre périphérique (par exemple, un routeur).
- Veillez les utilisateurs internes pour obtenir PAT comme suit :Les hôtes sur le sous-réseau 192.168.1.0/24 obtiendront PAT à une adresse IP supplémentaire donnée par l'ISP (10.1.5.5).N'importe quel autre hôte derrière l'intérieur de l'ASA obtiendra PAT à l'adresse IP extérieure d'interface de l'ASA (10.1.5.1).

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Appliance de sécurité adaptable Cisco (ASA) avec la version 8.3(1)
- Version 6.3(1) ASDM

Remarque: Référez-vous à Permettre l'accès HTTPS pour l'ASDM afin de permettre l'ASA d'être configuré par l'ASDM.

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.

Conventions

Référez-vous au Conventions relatives aux conseils techniques Cisco pour les informations sur des conventions de document.

Configuration

Diagramme du réseau

Ce document utilise la configuration réseau suivante :

Remarque: Les schémas d'adressage d'IP utilisés dans cette configuration ne sont pas légalement routables sur Internet. Ce sont des adresses RFC 1918 qui ont été utilisées dans un environnement de laboratoire.

- Configuration de l'interface de ligne de commande ASA
- Configuration ASDM

Configuration de l'interface de ligne de commande ASA

Ce document utilise les configurations présentées ci-dessous.

Configuration PAT dynamique ASA

```
ASA#configure terminal Enter configuration commands, one per line. End with CNTL/Z. !--- Creates an object called OBJ_GENERIC_ALL. !--- Any host IP not already matching another configured !--- object will get PAT to the outside interface IP !--- on the ASA (or 10.1.5.1), for internet bound traffic. ASA(config)#object network OBJ_GENERIC_ALL ASA(config-obj)#subnet 0.0.0.0 0.0.0.0 ASA(config-obj)#exit ASA(config)#nat (inside,outside) source dynamic OBJ_GENERIC_ALL interface !--- The above statements are the equivalent of the !--- nat/global combination (as shown below) in v7.0(x), !--- v7.1(x), v7.2(x), v8.0(x), v8.1(x) and v8.2(x) ASA code: nat (inside) 1 0.0.0.0 0.0.0.0 global (outside) 1 interface !--- Creates an object called OBJ_SPECIFIC_192-168-1-0.
```

```
!--- Any host IP facing the the 'inside' interface of
the ASA !--- with an address in the 192.168.1.0/24
subnet will get PAT !--- to the 10.1.5.5 address, for
internet bound traffic. ASA(config)#object network
OBJ_SPECIFIC_192-168-1-0 ASA(config-obj)#subnet
192.168.1.0 255.255.255.0 ASA(config-obj)#exit
ASA(config)#nat (inside,outside) source dynamic
OBJ_SPECIFIC_192-168-1-0 10.1.5.5 !--- The above
statements are the equivalent of the nat/global !---
combination (as shown below) in v7.0(x), v7.1(x),
v7.2(x), v8.0(x), !--- v8.1(x) and v8.2(x) ASA code: nat
(inside) 2 192.168.1.0 255.255.255.0 global (outside) 2
10.1.5.5
```

Configuration en cours ASA 8.3(1)

```
ASA#show run : Saved : ASA Version 8.3(1) ! hostname ASA
enable password 8Ry2YjIyt7RRXU24 encrypted passwd
2KFQnbNIdI.2KYOU encrypted names ! !--- Configure the
outside interface. ! interface GigabitEthernet0/0 nameif
outside security-level 0 ip address 10.1.5.1
255.255.255.0 !--- Configure the inside interface. !
interface GigabitEthernet0/1 nameif inside security-
level 100 ip address 192.168.0.1 255.255.255.0 !
interface GigabitEthernet0/2 shutdown no nameif no
security-level no ip address ! interface
GigabitEthernet0/3 shutdown no nameif no security-level
no ip address ! interface Management0/0 shutdown no
nameif no security-level no ip address management-only !
boot system disk0:/asa831-k8.bin ftp mode passive object
network OBJ_SPECIFIC_192-168-1-0 subnet 192.168.1.0
255.255.255.0 object network OBJ_GENERIC_ALL subnet
0.0.0.0 0.0.0.0 pager lines 24 no failover icmp
unreachable rate-limit 1 burst-size 1 asdm image
disk0:/asdm-631.bin no asdm history enable arp timeout
14400 nat (inside,outside) source dynamic
OBJ_GENERIC_ALL interface nat (inside,outside) source
dynamic OBJ_SPECIFIC_192-168-1-0 10.1.5.5 route inside
192.168.1.0 255.255.255.0 192.168.0.254 1 route outside
0.0.0.0 0.0.0.0 10.1.5.2 timeout xlate 3:00:00 timeout
conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp
0:00:02 timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00
mgcp 0:05:00 mgcp-pat 0:05:00 timeout sip 0:30:00
sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect
0:02:00 timeout sip-provisional-media 0:02:00 uauth
0:05:00 absolute timeout tcp-proxy-reassembly 0:01:00
dynamic-access-policy-record DfltAccessPolicy http
server enable http 192.168.0.0 255.255.254.0 inside no
snmp-server location no snmp-server contact snmp-server
enable traps snmp authentication linkup linkdown
coldstart crypto ipsec security-association lifetime
seconds 28800 crypto ipsec security-association lifetime
kilobytes 4608000 telnet timeout 5 ssh timeout 5 console
timeout 0 threat-detection basic-threat threat-detection
statistics access-list no threat-detection statistics
tcp-intercept ! class-map inspection_default match
default-inspection-traffic ! ! policy-map type inspect
dns preset_dns_map parameters message-length maximum
client auto message-length maximum 512 policy-map
global_policy class inspection_default inspect dns
preset_dns_map inspect ftp inspect h323 h225 inspect
h323 ras inspect rsh inspect rtsp inspect esmtp inspect
sqlnet inspect skinny inspect sunrpc inspect xdmcp
inspect sip inspect netbios inspect tftp inspect ip-
options ! service-policy global_policy global prompt
```

```
hostname context
Cryptochecksum:6fffbd3dc9cb863fd71c71244a0ecc5f : end
```

Configuration ASDM

Afin de se terminer cette configuration par l'interface ASDM, vous devez :

1. Ajoutez trois objets de réseau ; ce les exemples ajoute ces objets de réseau :OBJ_GENERIC_ALLOBJ_SPECIFIC_192-168-1-010.1.5.5
2. Créez deux règles NAT/PAT ; ce les exemples crée des règles NAT pour ces objets de réseau :OBJ_GENERIC_ALLOBJ_SPECIFIC_192-168-1-0

Ajoutez les objets de réseau

Terminez-vous ces étapes afin d'ajouter des objets de réseau :

1. Ouvrez une session à l'ASDM, et choisissez la **configuration > le Pare-feu > les objets > les objets de réseau/groupes**.
2. Choisissez **ajoutent > objet de réseau** afin d'ajouter un objet de réseau.La boîte de dialogue d'objet de réseau d'ajouter apparaît.
3. Écrivez ces informations dans la boîte de dialogue d'objet de réseau d'ajouter :Nom de l'objet de réseau. (Cet exemple utilise *OBJ_GENERIC_ALL*.)Type d'objet de réseau. (Cet exemple utilise le *réseau*.)Adresse IP pour l'objet de réseau. (Cet exemple utilise *0.0.0.0*.)Netmask pour l'objet de réseau. (Cet exemple utilise *0.0.0.0*.)
4. Cliquez sur **OK**.L'objet de réseau est créé et apparaît dans les objets de réseau/groupes les répertorient, suivant les indications de cette image :
5. Répétez les étapes précédentes afin d'ajouter un deuxième objet de réseau, et cliquez sur OK.Cet exemple utilise ces valeurs :Nom : *OBJ_SPECIFIC_192-168-1-0*Type : *Réseau*Adresse IP : *192.168.1.0*Netmask : *255.255.255.0*Le deuxième objet est créé et apparaît dans les objets de réseau/groupes les répertorient, suivant les indications de cette image :
6. Répétez les étapes précédentes afin d'ajouter un troisième objet de réseau, et cliquez sur OK.Cet exemple utilise ces valeurs :Nom : *10.1.5.5*Type : *Hôte*Adresse IP : *10.1.5.5*Les troisième objets de réseau est créés et apparaît dans les objets de réseau/groupes les répertorient.Les objets de réseau/groupes que la liste devrait maintenant inclure les trois ont exigé des objets nécessaires pour que les règles NAT mettent en référence.

Créez les règles NAT/PAT

Terminez-vous ces étapes afin de créer des règles NAT/PAT :

1. Créez la première règle NAT/PAT :Dans l'ASDM, choisissez la **configuration > le Pare-feu > les règles NAT**, et cliquez sur Add.La boîte de dialogue de règle NAT d'ajouter apparaît.Dans le critère de correspondance : La région de paquet d'origine de la boîte de dialogue de règle NAT d'ajouter, choisissent **à l'intérieur de la** liste déroulante d'interface de source.Cliquez sur le furetage (…) bouton situé à la droite du champ texte d'adresse source.La boîte de dialogue d'origine d'adresse source de furetage apparaît.Dans la boîte de dialogue d'origine d'adresse source de furetage, choisissez le premier objet de réseau que vous avez créé. (Pour cet exemple, choisissez **OBJ_GENERIC_ALL**.)Cliquez sur l'**adresse source d'origine**, et cliquez sur OK.L'objet de réseau *OBJ_GENERIC_ALL* apparaît maintenant dans la zone adresse d'adresse source dans le critère de correspondance : Région de paquet d'origine de

la boîte de dialogue de règle NAT d'ajouter.Dans l'action : La région traduite de paquet de la boîte de dialogue de règle NAT d'ajouter, choisissent **PAT dynamique (peau) de la** case NAT de dialogue Type de source.Cliquez sur le furetage (**…**) bouton situé à la droite de la zone adresse d'adresse source.La boîte de dialogue d'adresse source traduite par furetage apparaît.Dans le furetage la boîte de dialogue traduite d'adresse source, choisissent l'objet **extérieur d'**interface. (Cette interface a été déjà créée parce que ce fait partie de la configuration d'origine.)Cliquez sur l'**adresse source traduite**, et cliquez sur OK.L'interface extérieure apparaît maintenant dans la zone adresse d'adresse source dans l'action : Région traduite de paquet sur la boîte de dialogue de règle NAT d'ajouter.**Remarque:** Le champ d'*interface de destination* change également en l'interface extérieure.Vérifiez que la règle d'abord terminée de PAT apparaît comme suit :Dans le critère de correspondance : La région de paquet d'origine, vérifient ces valeurs :Interface de source = à l'intérieurAdresse source = OBJ_GENERIC_ALLAdresse de destination = quelsService = quelsDans l'action : La région traduite de paquet, vérifient ces valeurs :Type NAT de source = PAT dynamique (peau)Adresse source = dehorsAdresse de destination = originalService = originalCliquez sur **OK**.La première règle NAT apparaît dans l'ASDM, suivant les indications de cette image :

2. Créez la deuxième règle NAT/PAT :Dans l'ASDM, choisissez la **configuration > le Pare-feu > les règles NAT**, et cliquez sur Add.Dans le critère de correspondance : La région de paquet d'origine de la boîte de dialogue de règle NAT d'ajouter, choisissent **à l'intérieur de la** liste déroulante d'interface de source.Cliquez sur le furetage (**…**) bouton situé à la droite de la zone adresse d'adresse source.La boîte de dialogue d'origine d'adresse source de furetage apparaît.Dans la boîte de dialogue d'origine d'adresse source de furetage, choisissez le deuxième objet que vous avez créé. (Pour cet exemple, choisissez **OBJ_SPECIFIC_192-168-1-0**.)Cliquez sur l'**adresse source d'origine**, et cliquez sur OK.L'objet de réseau *OBJ_SPECIFIC_192-168-1-0* apparaît dans la zone adresse d'adresse source dans le critère de correspondance : Région de paquet d'origine de la boîte de dialogue de règle NAT d'ajouter.Dans l'action : La région traduite de paquet de la boîte de dialogue de règle NAT d'ajouter, choisissent **PAT dynamique (peau) de la** case NAT de dialogue Type de source.Cliquez sur**… le** bouton situé à la droite de la zone adresse d'adresse source.La boîte de dialogue d'adresse source traduite par furetage apparaît.Dans le furetage la boîte de dialogue traduite d'adresse source, choisissent l'objet de **10.1.5.5**. (Cette interface a été déjà créée parce que ce fait partie de la configuration d'origine).Cliquez sur l'**adresse source traduite**, et puis cliquez sur OK.L'objet de réseau de **10.1.5.5** apparaît dans la zone adresse d'adresse source dans l'action : Région traduite de paquet de la boîte de dialogue de règle NAT d'ajouter.Dans le critère de correspondance : La région de paquet d'origine, choisissent **dehors de la** liste déroulante d'interface de destination.**Remarque:** Si vous ne choisissez pas *dehors* pour cette option, l'interface de destination en mettra en référence.Vérifiez que le deuxième s'est terminé la règle NAT/PAT apparaît comme suit :Dans le critère de correspondance : La région de paquet d'origine, vérifient ces valeurs :Interface de source = à l'intérieurAdresse source = OBJ_SPECIFIC_192-168-1-0Adresse de destination = dehorsService = quelsDans l'action : La région traduite de paquet, vérifient ces valeurs :Type NAT de source = PAT dynamique (peau)Adresse source = 10.1.5.5Adresse de destination = originalService = originalCliquez sur **OK**.La configuration NAT terminée apparaît dans l'ASDM, suivant les indications de cette image :
3. Cliquez sur le **bouton Apply** afin d'appliquer les modifications à la configuration en cours.

Ceci se termine la configuration de PAT dynamique sur une appliance de sécurité adaptable Cisco (ASA).

Vérifiez

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes **show**. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show** .

Vérifier la règle générique de PAT

- hôte local d'exposition — Affiche les états de réseau d'hôtes locaux.ASA#**show local-host**
  Interface outside: 1 active, 2 maximum active, 0 denied local host: <125.252.196.170>, TCP flow count/limit = 2/unlimited TCP embryonic count to host = 0 TCP intercept watermark = unlimited UDP flow count/limit = 0/unlimited *!--- The TCP connection outside address corresponds !--- to the actual destination of 125.255.196.170:80* Conn: **TCP outside 125.252.196.170:80 inside 192.168.0.5:1051**, idle 0:00:03, bytes 13758, flags UIO TCP outside 125.252.196.170:80 inside 192.168.0.5:1050, idle 0:00:04, bytes 11896, flags UIO Interface inside: 1 active, 1 maximum active, 0 denied local host: <192.168.0.5>, TCP flow count/limit = 2/unlimited TCP embryonic count to host = 0 TCP intercept watermark = unlimited UDP flow count/limit = 0/unlimited *!--- The TCP PAT outside address corresponds to the !--- outside IP address of the ASA – 10.1.5.1.* Xlate: TCP **PAT from inside:192.168.0.5/1051 to outside:10.1.5.1/32988** flags ri idle 0:00:17 timeout 0:00:30 TCP PAT from inside:192.168.0.5/1050 to outside:10.1.5.1/17058 flags ri idle 0:00:17 timeout 0:00:30 Conn: TCP outside 125.252.196.170:80 inside 192.168.0.5:1051, idle 0:00:03, bytes 13758, flags UIO TCP outside 125.252.196.170:80 inside 192.168.0.5:1050, idle 0:00:04, bytes 11896, flags UIO
- show conn — Affiche l'état de connexion pour le type de connexion indiqué.ASA#**show conn** 2 in use, 3 most used TCP outside 125.252.196.170:80 inside 192.168.0.5:1051, idle 0:00:06, bytes 13758, flags UIO TCP outside 125.252.196.170:80 inside 192.168.0.5:1050, idle 0:00:01, bytes 13526, flags UIO
- show xlate — Affiche les informations sur les emplacements de traduction.ASA#**show xlate** 4 in use, 7 most used Flags: D - DNS, I - dynamic, r - portmap, s - static, I - identity, T - twice TCP PAT from inside:192.168.0.5/1051 to outside:10.1.5.1/32988 flags ri idle 0:00:23 timeout 0:00:30 TCP PAT from inside:192.168.0.5/1050 to outside:10.1.5.1/17058 flags ri idle 0:00:23 timeout 0:00:30

Vérifier la règle spécifique de PAT

- hôte local d'exposition — Affiche les états de réseau d'hôtes locaux.ASA#**show local-host**
  Interface outside: 1 active, 2 maximum active, 0 denied local host: <125.252.196.170>, TCP flow count/limit = 2/unlimited TCP embryonic count to host = 0 TCP intercept watermark = unlimited UDP flow count/limit = 0/unlimited *!--- The TCP connection outside address corresponds to !--- the actual destination of 125.255.196.170:80.* Conn: **TCP outside 125.252.196.170:80 inside 192.168.1.5:1067**, idle 0:00:07, bytes 13758, flags UIO TCP outside 125.252.196.170:80 inside 192.168.1.5:1066, idle 0:00:03, bytes 11896, flags UIO Interface inside: 1 active, 1 maximum active, 0 denied local host: <192.168.0.5>, TCP flow count/limit = 2/unlimited TCP embryonic count to host = 0 TCP intercept watermark = unlimited UDP flow count/limit = 0/unlimited *!--- The TCP PAT outside address corresponds to an !--- outside IP address of 10.1.5.5.* Xlate: **TCP PAT from inside:192.168.1.5/1067 to outside:10.1.5.5/35961** flags ri idle 0:00:17 timeout 0:00:30 TCP PAT from inside:192.168.1.5/1066 to outside:10.1.5.5/23673 flags ri idle 0:00:17 timeout 0:00:30 Conn: TCP outside 125.252.196.170:80 inside 192.168.1.5:1067, idle 0:00:07, bytes 13758, flags UIO TCP outside 125.252.196.170:80 inside 192.168.1.5:1066, idle 0:00:03, bytes 11896, flags UIO
- show conn — Affiche l'état de connexion pour le type de connexion indiqué.ASA#**show conn** 2 in use, 3 most used TCP outside 125.252.196.170:80 inside 192.168.1.5:1067, idle 0:00:07, bytes 13653, flags UIO TCP outside 125.252.196.170:80 inside 192.168.1.5:1066, idle 0:00:03, bytes 13349, flags UIO
- show xlate — Affiche les informations sur les emplacements de traduction.ASA#**show xlate** 3 in

```
use, 9 most used Flags: D - DNS, I - dynamic, r - portmap, s - static, I - identity, T -
twice TCP PAT from inside:192.168.1.5/1067 to outside:10.1.5.5/35961 flags ri idle 0:00:23
timeout 0:00:30 TCP PAT from inside:192.168.1.5/1066 to outside:10.1.5.5/29673 flags ri idle
0:00:23 timeout 0:00:30
```

Dépannez

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

Informations connexes

- Cisco Adaptive Security Device Manager
- Dispositifs de sécurité adaptatifs de la gamme Cisco ASA 5500
- Demandes de commentaires (RFC)
- Support et documentation techniques - Cisco Systems