PIX/ASA 7.x/FWSM 3.x : Traduire plusieurs adresses IP globales en adresse IP locale unique à l'aide de la traduction d'adresses réseau (NAT) à stratégie statique

Contenu

Introduction

Ce document fournit une configuration d'échantillon pour tracer une adresse IP locale des adresses IP deux ou plus globaux par la traduction d'adresses de réseau statique basée sur la politique (NAT) sur le logiciel 7.x des dispositifs de sécurité PIX/Adaptive (ASA).

Conditions préalables

Conditions requises

Assurez-vous que vous répondez aux exigences suivantes avant d'essayer cette configuration :

- Assurez-vous que vous avez des connaissances pratiques du PIX/ASA 7.x CLI et expérience préalable configurant des Listes d'accès et NAT statique.

Composants utilisés

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

- Cet exemple spécifique utilise une ASA 5520. Cependant les configurations NAT de stratégie

travaillent à n'importe quelle appliance PIX ou ASA qui exécute 7.x.

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

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Configurez

Cet exemple de configuration a un web server interne chez 192.168.100.50, situé derrière l'ASA. La condition requise est que le serveur doit être accessible à l'interface réseau extérieure par son adresse IP interne de 192.168.100.50 et son adresse externe de 172.16.171.125. Il y a également une condition de stratégie de sécurité que l'adresse IP privée de 192.168.100.50 peut seulement être accédée à par le réseau 172.16.171.0/24. Supplémentaire, le Protocole ICMP (Internet Control Message Protocol) et le trafic du port 80 sont les seuls protocoles ont permis d'arrivée au web server interne. Puisqu'il y a deux adresses IP globales tracées à une adresse IP locale, vous devez utiliser la stratégie NAT. Autrement, le PIX/ASA rejette la statique deux linéaire avec une erreur d'adresse superposante.

Remarque: Utilisez l'outil Command Lookup Tool (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Ce document utilise cette configuration réseau

Configuration

Ce document utilise cette configuration.

```
ciscoasa(config)#show run : Saved : ASA Version 7.2(2) !
hostname ciscoasa enable password 8Ry2YjIyt7RRXU24
encrypted names ! interface GigabitEthernet0/0 nameif
outside security-level 0 ip address 172.16.171.124
255.255.255.0 ! interface GigabitEthernet0/1 nameif
inside security-level 100 ip address 192.168.100.1
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 nameif
management security-level 100 ip address 192.168.1.1
255.255.255.0 management-only ! passwd 2KFQnbNIdI.2KYOU
encrypted ftp mode passive !--- policy_nat_web1 and
policy_nat_web2 are two access-lists that match the
source !--- address we want to translate on. Two access-
lists are required, though they !--- can be exactly the
same. access-list policy_nat_web1 extended permit ip
host 192.168.100.50 any access-list policy_nat_web2
extended permit ip host 192.168.100.50 any !--- The
```

```
inbound_outside access-list defines the security policy,
as previously described. !--- This access-list is
applied inbound to the outside interface. access-list
inbound_outside extended permit tcp 172.16.171.0
255.255.255.0 host 192.168.100.50 eq www access-list
inbound_outside extended permit icmp 172.16.171.0
255.255.255.0 host 192.168.100.50 echo-reply access-list
inbound_outside extended permit icmp 172.16.171.0
255.255.255.0 host 192.168.100.50 echo access-list
inbound_outside extended permit tcp any host
172.16.171.125 eq www access-list inbound_outside
extended permit icmp any host 172.16.171.125 echo-reply
access-list inbound_outside extended permit icmp any
host 172.16.171.125 echo pager lines 24 logging asdm
informational mtu management 1500 mtu inside 1500 mtu
outside 1500 no failover icmp unreachable rate-limit 1
burst-size 1 no asdm history enable arp timeout 14400 !-
-- This first static allows users to reach the
translated global IP address of the !--- web server.
Since this static appears first in the configuration,
for connections !--- initiated outbound from the
internal web server, the ASA translates the source !---
address to 172.16.171.125. static (inside,outside)
172.16.171.125 access-list policy_nat_web1 !--- The
second static allows networks to access the web server
by its private !--- IP address of 192.168.100.50. static
(inside,outside) 192.168.100.50 access-list
policy_nat_web2 !--- Apply the inbound_outside access-
list to the outside interface. access-group
inbound_outside in interface outside route outside
0.0.0.0 0.0.0.0 172.16.171.1 1 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 uauth 0:05:00 absolute http
server enable http 192.168.1.0 255.255.255.0 management
no snmp-server location no snmp-server contact snmp-
server enable traps snmp authentication linkup linkdown
coldstart telnet timeout 5 ssh timeout 5 console timeout
0 ! class-map inspection_default match default-
inspection-traffic ! ! policy-map type inspect dns
preset_dns_map parameters 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 !
service-policy global_policy global prompt hostname
context
```

Vérifiez

Cette section fournit des informations qui vous permettront de vérifier que votre configuration fonctionne correctement.

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** .

1. Sur le routeur en amont 172.16.171.1 IOS®, vérifiez-vous peut atteindre les deux adresses

IP globales du web server par l'intermédiaire de la **commande ping**.router#**ping 172.16.171.125** Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 172.16.171.125, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms router#**ping 192.168.100.50** Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.100.50, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms

2. Sur l'ASA, vérifiez que vous voyez les traductions qui sont établies dans la table de traduction (xlate).ciscoasa(config)#**show xlate global 192.168.100.50** 2 in use, 28 most used **Global 192.168.100.50 Local 192.168.100.50** ciscoasa(config)#**show xlate global 172.16.171.125** 2 in use, 28 most used **Global 172.16.171.125 Local 192.168.100.50**

Dépannez

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Si votre ping ou connexion est infructueuse, tentative d'employer des Syslog pour déterminer s'il y a des problèmes avec la configuration de traduction. Sur un réseau légèrement utilisé (tel qu'un environnement de travaux pratiques), la taille de tampon de journalisation est habituellement suffisante pour dépanner le problème. Autrement, vous devez envoyer les Syslog à un serveur externe de Syslog. Activez se connecter à la mémoire tampon au niveau 6 afin de voir si la configuration est correcte dans ces entrées de Syslog.

ciscoasa(config)#**logging buffered 6** ciscoasa(config)#**logging on** *!--- From 172.16.171.120, initiate a TCP connection to port 80 to both the external !--- (172.16.171.125) and internal addresses (192.168.100.50).* ciscoasa(config)#**show log** Syslog logging: enabled Facility: 20 Timestamp logging: disabled Standby logging: disabled Deny Conn when Queue Full: disabled Console logging: disabled Monitor logging: disabled Buffer logging: level debugging, 4223 messages logged Trap logging: disabled History logging: disabled Device ID: disabled Mail logging: disabled ASDM logging: level informational, 4032 messages logged %ASA-5-111008: User 'enable_15' executed the 'clear logging buffer' command. %ASA-7-609001: Built local-host outside:172.16.171.120 %ASA-7-609001: Built local-host inside:192.168.100.50 **%ASA-6-302013: Built inbound TCP connection 67 for outside:172.16.171.120/33687 (172.16.171.120/33687) to** inside:192.168.100.50/80 (172.16.171.125/80) **%ASA-6-302013: Built inbound TCP connection 72 for outside:172.16.171.120/33689 (172.16.171.120/33689) to inside:192.168.100.50/80 (192.168.100.50/80)**

Si vous voyez des erreurs de traduction dans le log, vérifiez une deuxième fois vos configurations NAT. Si vous n'observez aucun Syslog, employez la fonction de **capture** sur l'ASA pour tenter de capturer le trafic sur l'interface. Afin d'installer une capture, vous devez d'abord spécifier une liste d'accès pour être assortie sur un type de trafic ou un écoulement spécifique de TCP. Ensuite, vous devez appliquer cette capture à un ou plusieurs interfaces afin de commencer à capturer des paquets.

*!--- Create a capture access-list to match on port 80 traffic to !--- the external IP address of 172.16.171.125. !--- **Note:** These commands are over two lines due to spatial reasons.*
ciscoasa(config)#**access-list acl_capout permit tcp host 172.16.171.120 host 172.16.171.125 eq 80**
ciscoasa(config)#**access-list acl_capout permit tcp host 172.16.171.125 eq 80 host 172.16.171.120**
ciscoasa(config)# *!--- Apply the **capture** to the outside interface.* ciscoasa(config)#**capture capout access-list acl_capout interface outside** *!--- After you initiate the traffic, you see output similar to this when you view !--- the capture. Note that packet 1 is the SYN packet from the client, while packet !--- 2 is the SYN-ACK reply packet from the internal server. If you apply a **capture** !--- on the inside interface, in packet 2 you should see the server reply with !--- 192.168.100.50 as its source address.* ciscoasa(config)#**show capture capout** 4 packets captured 1: 13:17:59.157859 **172.16.171.120.21505 > 172.16.171.125.80: S** 2696120951:2696120951(0) win 4128 <mss 1460> 2: 13:17:59.159446 **172.16.171.125.80 > 172.16.171.120.21505: S** 1512093091:1512093091(0) **ack** 2696120952 win 4128 <mss 536> 3: 13:17:59.159629 172.16.171.120.21505 > 172.16.171.125.80: . ack 1512093092 win 4128 4: 13:17:59.159873 172.16.171.120.21505 > 172.16.171.125.80: . ack 1512093092 win 4128

Informations connexes

- Référence de commandes ASA 7.2
- Logiciels pare-feu Cisco PIX
- Références des commandes du pare-feu Cisco Secure PIX
- Notices de champs relatives aux produits de sécurité (y compris PIX)
- Demandes de commentaires (RFC)
- Support et documentation techniques - Cisco Systems