ASA 8.3(x) Dynamic PAT met twee interne netwerken en Internet Configuration Voorbeeld

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Conventies Configuratie Netwerkdiagram ASA CLI-configuratie ASDM-configuratie Verifiëren Verificatie van generieke PAT-regel Specifieke PAT-regel controleren Problemen oplossen Gerelateerde informatie

Inleiding

Dit document biedt een voorbeeldconfiguratie voor dynamisch PAT op een Cisco adaptieve security applicatie (ASA) die softwareversie 8.3(1) uitvoert. <u>Dynamisch PAT</u> vertaalt meerdere echte adressen naar één toegewezen IP-adres door het adres en de bronpoort naar het in kaart gebrachte adres en de unieke in kaart gebrachte poort te vertalen. Elke verbinding vereist een afzonderlijke vertaalsessie omdat de bronpoort verschilt voor elke verbinding.

Voorwaarden

Vereisten

Zorg ervoor dat u aan deze vereisten voldoet voordat u deze configuratie probeert:

- Zorg ervoor dat het interne netwerk twee netwerken binnen de ASA heeft:192.168.0.0/24—Netwerk rechtstreeks verbonden met de ASA.192.168.1.0/24—Netwerk binnen de ASA, maar achter een ander apparaat (bijvoorbeeld, een router).
- Zorg ervoor dat de interne gebruikers als volgt PAT krijgen:Hosts op 192.168.1.0/24 zal PAT aan een reservekopie IP adres krijgen dat door de ISP wordt gegeven (10.1.5.5).Elke andere host achter de binnenkant van de ASA krijgt PAT op het externe interface-IP-adres van de

ASA (10.1.5.1).

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco adaptieve security applicatie (ASA) met versie 8.3(1)
- ASDM versie 6.3(1)

Opmerking: Raadpleeg <u>HTTPS-toegang voor ASDM</u> om de ASA te kunnen configureren door de ASDM.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg de Cisco Technical Tips Convention voor informatie over documentconventies.

Configuratie

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



Opmerking: de IP-adresseringsschema's die in deze configuratie worden gebruikt, zijn niet wettelijk routeerbaar op het internet. Ze zijn <u>RFC 1918</u> adressen, die in een labomgeving gebruikt zijn.

- ASA CLI-configuratie
- <u>ASDM-configuratie</u>

ASA CLI-configuratie

Dit document maakt gebruik van de onderstaande configuraties.

ASA Dynamic PAT-configuratie	
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 ASA 8.3(1) actieve configuratie 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
1
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
```

ASDM-configuratie

Om deze configuratie via de ASDM-interface te voltooien, moet u:

- 1. Voeg drie netwerkobjecten toe; deze voorbeelden voegen deze netwerkobjecten toe :OBJ_GENERIC_ALLOBJ_SPECIFIC_192-168-1-010.1.5.5
- 2. Twee NAT/PAT-regels maken; deze voorbeelden maken NAT-regels voor deze netwerkobjecten:OBJ_GENERIC_ALLOBJ_SPECIFIC_192-168-1-0

Netwerkobjecten toevoegen

Voltooi deze stappen om netwerkobjecten toe te voegen:

1. Meld u aan bij ASDM en kies Configuration > Firewall > Objects > Network Objects/Group

Firewall AAA Rules Filewall > Quincts > Network Objects / Groups Ada Rules Public Servers URL Fibering Servers Dublic Servers URL Fibering Servers Dublic Servers Dublic Servers Dublic Servers Dublic Servers Name / 1 IP Address Netmask Description Object NAI Servers Objects/// Coss Maps Servers Dublic Servers Name / 1 IP Address Netmask Description Object NAI Dublic Servers Name / 1 IP Address Netmask Description Object NAI Dublic Servers Name / 1 IP Address Netmask Description Object NAI Dublic Servers Name / 1 IP Address Netmask Description Object NAI Dublic Servers Name / 1 IP Address Netmask Description Object NAI Dublic Servers Name / 1 IP Address Netmask Description Object NAI Dublic Servers Name / 1 IP Address Netmask Description Object NAI Dublic Servers Name / 1 IP Address Netmask Description Object NAI Dublic Servers Name / 1 IP Address Netmask Description Object NAI Dublic Servers Name / 1 IP Address Netmask Description Object NAI Dublic Servers Name / 1 IP Address Netmask Description Object NAI Dublic Servers Name / 1 IP Address Netmask Description Object NAI Dublic Servers Name / 1 IP Address Netmask Description Object NAI Dublic Servers Name / 1 IP Address Netmask Description Object NAI Dublic Servers Name / 1 IP Address Netmask Description Object NAI Dublic Servers Name / 1 IP Address Netmask Description Object NAI Dublic Servers Name / 1 IP Address Netmask Description Object NAI Dublic Servers Name / 1 IP Address Netmask Description Object NAI Dublic Servers Name / 1 IP Address Netmask Description Object NAI Dublic Servers Name / 1 IP Address Name / 1 IP	Home of Configuration S Mont	oring 🔲 Save 🔇 Refr	esh 🔇 Back 🕥	Forward 🌮 Help		CISCO
Public Servers Public Servers Three /1 IP-4 Network Objects/Sroups Objects Service Objects/Sroups Object Maps Object Naps IP-4 Network Objects/Sroups IP-4 Network Objects IP-4 Network Objects IP-4 Network Objects IP-5	AAA Rules	Configuration > Firewal ◆ Add ・ ■ Edit 1	> Objects > Netwo	rk Objects/Groups		
Introduct Detection Introduct Detection Unit work Objects Output Network Objects Image: Service Objects/Groups Image: Service Objects/Groups Image: Service Objects/Groups Image: Service Objects/Groups Image: Service Objects/Groups Image: Service Objects/Groups Image: Service Objects/Groups Image: Service Objects/Groups Image: Service Objects/Groups Image: Service Objects/Groups Image: Service Objects/Groups Image: Service Objects/Groups Image: Service Objects/Groups Image: Service Objects/Groups Image: Service Objects/Groups Image: Service Objects/Groups Image: Service Objects/Groups Image: Service Objects/Groups Image: Service Objects/Groups Image: Service Objects/Groups Image: Service Objects/Groups Image: Service Objects/Groups Image: Service Objects/Groups Image: Service Objects/Groups Image: Service Objects/Groups Image: Service Objects/Groups Image: Service Objects/Groups Image: Service Objects/Groups Image: Service Objects/Groups Image: Service Objects/Groups Image: Service Objects/Groups Image: Service Objects/Groups Image: Service Objects/Groups Image: Service Objects/Groups Image: Service Objects/Groups Image: Service Objects/Groups Image: Service Objects/Groups Image: Service Obje	URL Filtering Servers	Filter:	10 Adhess	- Material	Parrieties	Elteric
Image: Service Objects/Groups 0.0.0 0.0.0 0.0.0 Image: Service Objects/Groups 0.0.0 0.0.0 255.255.255.0 Image: Service Objects/Groups Image: Service Objects/Groups Image: Service Objects/Groups Image: Service Objects/Groups Image: Service Objects/Groups Image: Service Objects/Groups Image: Service Objects/Groups Image: Service Objects/Groups Image: Service Objects/Groups Image: Service Objects/Groups Image: Service Objects/Groups Image: Service Objects/Groups Image: Service Objects/Groups Image: Service Objects/Groups Image: Service Objects/Groups Image: Service Objects/Groups Image: Service Objects/Groups Image: Service Objects/Groups Image: Service Objects/Groups Image: Service Objects/Service Objects Image: Service Objects/Service Objects Image: Device Setup Image: Service Setup Image: Service Objects/Service Objects Image: Service Objects/Service Objects Image: Service Objects/Service Objects Image: Device Setup Image: Service Objects/Service Image: Service Objects/Service Image: Service Objects/Service Image: Service Objects/Service Image: Device Setup Image: Service Service Image: Service Service Image: Service Service Image: Service Service <td< td=""><td>Threat Detection</td><td>That Native / 4</td><td>IP A0gress</td><td>Necmase,</td><td>Description</td><td>Object NAT Addre</td></td<>	Threat Detection	That Native / 4	IP A0gress	Necmase,	Description	Object NAT Addre
W Service Objects/Groups Class Maps Dispect Maps Dispect Maps TCP Maps TCP Maps TCP Maps Device Setup Preval Ste-to-Site VPN Ste-to-Site VPN	Hatwork Objects	E) IPVY NOCHOR CODECC	0.0.0.0	0.0.0.0		
Class Maps Image: Cl	Service Objects/Groups	- all inside-network	192,168,0.0	255,255,255,0		
Inspect Maps Image: Construct Maps Image: Construct Maps Image: Construct Maps <td>Class Maps</td> <td>- ad outside-net</td> <td>10.1.5.0</td> <td>255.255.255.0</td> <td></td> <td></td>	Class Maps	- ad outside-net	10.1.5.0	255.255.255.0		
Regular Expressions IPv6 Network Objects Time Ranges IPv6 Network Objects Device Setup IPv6 Network Objects Remote Access VPN IPs Ste-to-Ste VPN IPs	Inspect Maps	- 3 192,168.0.233	192.168.0.233	255.255.255.255		
Time Ranges Image: Comparison of the Ranges Dervice Satup Frewall Remote Access VPN Ste-to-Ste VPN IPS	Regular Expressions	- IPv6 Network Objects				
Dervice Setup Errewal Remote Access VPN Ste-to-Ste VPN IP5	The Report VI	- any	11	0		
3 P2	Device Setup Firewal Remote Access VPN Sto-to-Site VPN					
, Device Management	Device Management					

2. Kies Add > Network Object om een netwerkobject toe te voegen.

🚰 Cisco ASDM 6.3 for ASA - 192.168.0	4				_ 0 ×
File View Tools Wizards Window	Help toring 🔛 Save 🔇 Refresh 🔇	Back 🕐 Fo	Look rward 💡 Help	k For:	CISCO
Firewall O P ×	Configuration > Firewall > Object	ts > Network	Objects/Groups and		Etter Gearl
URL Filtering Servers	Network Object Group	tress	Netmask	Description	Object NAT Address
□-La objects	E IPv4 Network Objects				
Network Objects/Groups	- 🥥 any 0.0.0.0		0.0.0.0		
Service Objects/Groups	inside-network 192.168.	0.0	255.255.255.0		
Gass Maps	- 35 outside-net 10.1.5.0		255.255.255.0		
Regular Expressions	···· 💐 192.168.0.233 192.168.	0.233	255.255.255.255		
TCP Maps	IPv6 Network Objects				
Time Ranges 💌	🍛 any 🛛		0		
Revice Setup					
Firewal					
Remote Access VPN					
Ste-to-Site VPN					
🖏 195					
Device Management					
:			Apply	Reset	

Het dialoogvenster Netwerkobject toevoegen

ľ	付 Add Netwo	rk Object	×
	Name:	OBJ_GENERIC_ALL	
	Туре:	Network	-
	IP Address:	0.0.0.0	
	Netmask:	0.0.0.0	-
	Description:		
	NAT		۲
		OK Cancel Help	

verschijnt.

- 3. Typ deze informatie in het dialoogvenster Netwerkobject toevoegen:Naam van het netwerkobject. (Dit voorbeeld gebruikt *OBJ_GENERIC_ALL*.)Type netwerkobject. (Dit voorbeeld gebruikt *Network*.)IP-adres voor het netwerkobject. (In dit voorbeeld wordt *0.0.0.0* gebruikt.)Netmask voor het netwerkobject. (In dit voorbeeld wordt *0.0.0.0* gebruikt.)
- Klik op OK.Het netwerkobject wordt aangemaakt en verschijnt in de lijst Netwerkobjecten/groepen, zoals in deze afbeelding:

Cisco ASDM 6.3 for ASA - 192.168.0	.1			
File View Tools Wizards Window	Help	un an arrene herrenen	Look	For:
Home of Configuration Monit	toring 📊 Save 🔇 Refr	esh 🔇 Back 🕥	Forward ? Help	
Firewall 라무×	Configuration > Firewall	> Objects > Netwo	rk Objects/Groups	
AAA Rules	◆ Add ・ 🕑 Edit 📋 Filter:	Delete Q Where	e Used	
	Name / 1	IP Address	Netmask	Desi
Objects	⊡-IPv4 Network Objects			
Network Objects/Groups	- 🏈 any	0.0.00	0.0.0.0	
Service Objects/Groups	- A inside-network	192.168.0.0	255.255.255.0	
€ Class Maps	outside-net	10.1.5.0	255.255.255.0	
Inspect Maps	OBJ_GENER	0.0.0	0.0.0.0	
TCP Maos	- 💐 192.168.0.233	192.168.0.233	255.255.255.255	
Time Ranges +	- IPv6 Network Objects			
	- 🧼 any	::	0	
Device Setup				
Second 1				
S Likewai				
Device Management				
÷			Apply	Reset
			cisco 15	

5. Herhaal de vorige stappen om een tweede netwerkobject toe te voegen en klik op **OK**.Dit voorbeeld gebruikt deze waarden:Name: *OBJ_SPECIFIC_192-168-1-0*Type: *Netwerknetwerk*IP-adres: *192.168.1.0*Netmasker:

	薩 Add Netwo	rk Object 🛛 🗙
	Name:	OBJ_SPECIFIC_192-168-1-0
	Туре:	Network
	IP Address:	192.168.1.0
	Netmask:	255.255.255.0
	Description:	
	NAT	۲
		OK Cancel Help
255.255.0		

tweede object wordt aangemaakt en verschijnt in de lijst Netwerkobjecten/groepen, zoals in deze afbeelding wordt weergegeven:

🚰 Cisco ASDM 6.3 for ASA - 192.168.0.	1				-0
File View Tools Wizards Window	Help		Look For	1	Go
Home 🔏 Configuration 📴 Monito	oring 🔛 Save 🔇 Ref	esh 🔇 Back 🔘	Forward 🦻 Help		CISCO
Firewall & X	Configuration > Firewal	> Objects > Netwo	rk Objects/Groups		
AAA Rules	◆ Add • 17 EdR 1	Delete Q Where	Used		
Filter Rules					
URL Filtering Servers	Fiker:				<u>Elter[Clear</u>
Threat Detection	Name / 1	IP Address	Netmask	Description	Object NAT Address
E-C Objects	IPv4 Network Objects				
- Metwork Objects/Groups	- 🧼 any	0.0.0.0	0.0.0.0		
Service Objects/Groups	- M inside-network	192.168.0.0	255.255.255.0		
Grad Class Maps	- 💑 outside-net	10.1.5.0	255.255.255.0		
P Republic Plaps	- 603_GENER	0.0.0.0	0.0.0.0		
TCP Maps	- 📇 192.168.0.233	192.168.0.233	255.255.255.255		
Time Ranges *	CB3_SPECIF	192.168.1.0	255.255.255.0		
	IPv6 Network Objects	_			
Device Setup	- 🧼 any	11	0		
🕄 Firewal					
Remote Access VPN					
Ste-to-Site VPN					
🔯 1 <u>9</u> 5					
Device Management	1				
:			Apply Res	et	

6. Herhaal de vorige stappen om een derde netwerkobject toe te voegen en klik op **OK**.Dit voorbeeld gebruikt deze waarden:Name: *10.1.5.5*Type: *Host*IP-adres:

付 Add Netwo	ork Object			×
Name:	10.1.5.5			
Туре:	Host			-
IP Address:	10.1.5.5			
Description:				
NAT				۲
	ок	Cancel	Help	

netwerkobjecten worden gecreëerd en weergegeven in de lijst van Netwerkobjecten/groepen.

🔂 Cisco ASDM 6.3 for ASA - 192.168.0.	l de la constante de	
File View Tools Wizards Window	Help	Look For:
Home 🍪 Configuration 🔯 Monit	oring 🔚 Save 🔇 Refresh 🔇 Back 🔘 For	ward 🦹 🦹 Help
Firewall 급 무 ×	Configuration > Firewall > Objects > Network (bjects/Groups
AAA Rules	💠 Add 🔹 📝 Edit 📋 Delete 🔍 Where Use	:d
Public Servers	Filter:	
Threat Detection	Name A1 IP Address	Netmask
Dijects	⊡ · IPv4 Network Objects	
Network Objects/Groups	🎲 any 0.0.0.0	0.0.0.0
Service Objects/Groups	- 🖳 10.1.5.5 10.1.5.5	255.255.255.255
Class Maps	🛃 inside-network 192.168.0.0	255.255.255.0
Inspect Maps	- 🚔 outside-net 10.1.5.0	255.255.255.0
TCP Maps	: : : : : : : : : : : : : : : : : :	0.0.0.0
Time Ranges	- 🖳 192.168.0.233 192.168.0.233	255.255.255.255
	OBJ_SPECIF 192.168.1.0	255.255.255.0
Device Setup	IPv6 Network Objects	
	any ::	0
S rrewall		

De lijst van netwerkobjecten/groepen moet nu de drie vereiste objecten bevatten die nodig zijn om de NAT-regels te kunnen verwijzen.

NAT/PAT-regels maken

Voltooi deze stappen om NAT/PAT-regels te maken:

1. Maak de eerste NAT/PAT-regel:Kies in ASDM **Configuration > Firewall > NAT-regels** en klik op

Add.



Het dialoogvenster NAT-regel toevoegen verschijnt.

🚰 Add NAT Rule		×
Match Criteria: Original Packet		
Source Interface: Any	Destination Interface:	Any
Source Address: Any	Destination Address:	any
outside	Service:	any
Action: Translated Packet If	lame: inside P Address: 192.168.0.1 / 25 ecurity Level:100 ort: GioshitEtherpet0	5.255.255.0
Source Address: Original	Destination Address:	Original
Fall through to interface PAT	Service:	Original
Options		
🔽 Enable rule		
🥅 Translate DNS replies that match this ru	ule	
Direction: Both		
Description:		
ОК	Cancel Help	

In de aanpassingscriteria: Het oorspronkelijke Packet-gebied van het dialoogvenster NATregel toevoegen kiest **binnen** uit de vervolgkeuzelijst Broninterface.

🞼 Add NAT Rule		×
Match Criteria: Original Packet		
Source Interface: inside	Destination Interface:	Any
Source Address: any	Destination Address:	any 🖳
	Service:	any
Action: Translated Packet		
Source NAT Type: Static		
Source Address: Original	Destination Address:	Original 👘
Fall through to interface PAT	Service:	Original
Options		
🔽 Enable rule		
Translate DNS replies that match this rule		
Direction: Both		
Description:		
		1
ОК	Cancel Help	

Klik op de knop Blader (...) rechts van het veld Tekst Bron-adres.Het dialoogvenster Bladeren origineel adres

verschijnt.

Name 🛆	IP Address	Netmask	Description	Object NAT Addr
IPv4 Network Obje	ects			
- 🖳 10.1.5.5	10.1.5.5	255.255.255.255		
<u>g</u> ª 083_GE	0.0.0.0	0.0.0.0		
🛃 OBJ_SP	192.168.1.0	255.255.255.0		
- 🥝 any	0.0.0.0	0.0.0.0		

In het dialoogvenster Bladeren origineel adres kiest u het eerste netwerkobject dat u hebt

gemaakt. (Kies bijvoorbeeld **OBJ_GENERIC_ALL**.)Klik op **Origineel Bron Adres** en klik op **OK**.Het *OBJ_GENERIC_ALL* netwerkobject verschijnt nu in het veld Bron Adres in de Match Criteria: Origineel pakketgebied van het dialoogvenster NAT-regel toevoegen.

🚰 Add NAT Rule			×
Match Criteria: Original	Packet		
Source Interface: insi	de 🔽	Destination Interface:	Any
Source Address: OB	J_GENERIC_ALL	Destination Address:	any 💮
		Service:	any
Action: Translated Pack	et		
Source NAT Type: Sta	tic 💌		
Source Address: C	Driginal 👘	Destination Address:	Original 📰
📃 Fall through to inter	rface PAT	Service:	Original 💮
Fall through to inter Options	face PAT	Service:	Original
Fall through to inter Options Enable rule	face PAT	Service:	Original
 ☐ Fall through to inter Options ☑ Enable rule ☐ Translate DNS replie 	face PAT	Service:	Original
 Fall through to inter Options Enable rule Translate DNS replie Direction: Both 	face PAT es that match this rule	Service:	Original
 Fall through to inter Options ✓ Enable rule ☐ Translate DNS replie Direction: Both Description: 	face PAT es that match this rule	Service:	Original
 Fall through to inter Options Enable rule Translate DNS replie Direction: Both Description: 	face PAT es that match this rule	Service:	Original

In de Actie: Het vertaalde pakketgebied van het dialoogvenster NAT-regel toevoegen kiest u **Dynamisch PAT (Verbergen)** uit het dialoogvenster Bron-NATtype.

🚰 Add NAT Rule		×
Match Criteria: Original Packet		
Source Interface: inside	Destination Interface:	Any
Source Address: OBJ_GENERIC_ALL	Destination Address:	any 🖳
	Service:	any
Action: Translated Packet		
Source NAT Type: Static		
Source Address: Static	Destination Address:	Original 📰
Fall through to Dynamic	Service:	Original 📰
Options		
🔽 Enable rule		
Translate DNS replies that match this rule		
Direction: Both		
Description:		
ОК	iancel Help	
(lik op do knop Bladorop () rochts van hot	vold Bron	

Klik op de knop Bladeren (...) rechts van het veld Bron Adres.

付 Add NAT Rule			×
Match Criteria: Ori	ginal Packet		
Source Interface:	inside 💌	Destination Interface:	Any
Source Address:	OBJ_GENERIC_ALL	Destination Address:	any
		Service:	any
Action: Translated	Packet		
Source NAT Type:	Dynamic PAT (Hide)	[
Source Address:	Original	Destination Address:	Original 🛛 🖳
Fall through to	interface PAT	Service:	Original 🛛 🖳
Options			
🔽 Enable rule			
🔲 Translate DNS	replies that match this rule		
Direction; Both	v		
Description:			
	ОК	Cancel Help	

Het dialoogvenster Bladeren vertaald adres verschijnt.

Name 🖂	IP Address	Netmask	Description	Object NAT Addr
Original				
IPv4 Network Obje	ects			
- 🖪 10.1.5.5	10.1.5.5	255.255.255.255		
Interfaces				
- 🔤 inside				
- se outside				

Kies het **externe** interfaceobject in het dialoogvenster Bladeren vertaald adres. (Deze interface is al gemaakt omdat het deel uitmaakt van de oorspronkelijke configuratie.)Klik op **Vertaald bronadres** en klik op **OK**.De externe interface verschijnt nu in het veld Bron Adres in

de Actie: Vertaald pakketgebied in het dialoogvenster NAT-regel toevoegen.

薩 Add NAT Rule			×
Match Criteria: Ori	ginal Packet		
Source Interface:	inside 🔹	Destination Interface:	outside 💌
Source Address:	OBJ_GENERIC_ALL	Destination Address:	any
		Service:	any
Action Translated	Daelaah		
Action: Translated			
Source NAT Type:	Dynamic PAT (Hide)		
Source Address:	outside	Destination Address:	Original 👘
Fall through to	interface PAT	Service:	Original 🔤
Options			
🔽 Enable rule			
🔲 Translate DNS	replies that match this rule		
Direction; Both	V		
Description:			
	ОК	Cancel Help	

Opmerking: het veld *Bestandsinterface* verandert ook in de externe interface.Controleer dat de eerste voltooide PAT-regel als volgt verschijnt:In de aanpassingscriteria: Controleer het oorspronkelijke Packet-gebied en deze waarden:Bron-interface = binnenkantBron Adres = OBJ_GENERIC_ALLDoeladres = eventueelService = elkeln de Actie: Vertaald pakketgebied, controleer deze waarden:Source NAT Type = Dynamic PAT (Verbergen)Bron Adres = buitenDoeladres = OorspronkelijkService = origineelKlik op **OK**.De eerste NAT-regel verschijnt in ASDM, zoals in deze afbeelding:

c	Configuration > Firewall > NAT Rules								
	💠 Add 🔹 🗹 Edit 👔 Delete 🗇 🗲 👗 🖻 🛍 - 🔍 Ç. Find 🖭 Diagram 📿 Packet Trace								
				Match Criteria: O	riginal Packet		Acti	on: Translated Pa	icket
		Source Intf	Dest Intf	Source	Destination	Service	Source	Destination	Servic
		inside	outside	ga OBJ_GENER	🤹 any	🤹 any	outside (P)	Original	Original
	"Network Object" NAT (No rules)								
	4								F
ľ	_								
					Apply	Reset			

2. De tweede NAT/PAT-regel maken:Kies in ASDM Configuration > Firewall > NAT-regels en klik op Add.In de aanpassingscriteria: Het oorspronkelijke Packet-gebied van het dialoogvenster NAT-regel toevoegen kiest binnen uit de vervolgkeuzelijst Bron-interface.Klik op de knop Bladeren (...) rechts van het veld Bron Adres.Het dialoogvenster Bladeren origineel adres

verschijnt.

		Nocinasia	Description	Object NAT Addr
-IPv4 Network Obje	ects			·
- 🖳 10.1.5.5	10.1.5.5	255.255.255.255		
🛃 OBJ_GE	0.0.0.0	0.0.0.0		
- 🗗 OBJ_SP	192.168.1.0	255.255.255.0		
any 🌍	0.0.0.0	0.0.0.0		
		• • • • •		· · · ·

In het dialoogvenster Bladeren origineel adres kiest u het tweede object dat u hebt gemaakt. (Kies bijvoorbeeld **OBJ_SPECIFIC_192-168-1-0**.)Klik op **Origineel Bron Adres** en klik op **OK**.Het *OBJ_SPECIFIC_192-168-1-0* netwerkobject verschijnt in het veld Bron Adres in de Match Criteria: Origineel pakketgebied van het dialoogvenster NAT-regel toevoegen.In de Actie: Het vertaalde pakketgebied van het dialoogvenster NAT-regel toevoegen kiest u **Dynamisch PAT (Verbergen)** uit het dialoogvenster Bron-NAT-type.Klik op de knop.. rechts van het veld Bron Adres.Het dialoogvenster Bladeren vertaald adres

verse	hii	nt.
10130		III.

ilter:				Filter Clear
Name 🛆 1	IP Address	Netmask	Description	Object NAT Addr
Original				
📮 IPv4 Network Obje	cts			
🔤 🖳 10.1.5.5	10.1.5.5	255.255.255.255		
- Interfaces				
- 🔤 inside				
🔤 outside				
elected Translated Sou	urce Address	.5.5		

Kies het object **10.1.5.5** in het dialoogvenster Bladeren van vertaald bronadres. (Deze interface is al gemaakt omdat deze deel uitmaakt van de oorspronkelijke configuratie).Klik op **Vertaald bronadres** en vervolgens op **OK**.Het netwerkobject **10.1.5.5** verschijnt in het veld Bron Adres in de Actie: Vertaald pakketgebied van het dialoogvenster NAT-regel toevoegen..In de aanpassingscriteria: Selecteer het oorspronkelijke pakketgebied **buiten** de vervolgkeuzelijst Bestandsinterface.**N.B.:** Als u voor deze optie niet *buiten* kiest, wordt de doelinterface verwezen naar *Any*.

🚰 Edit NAT Rule		×				
Match Criteria: Original Packet						
Source Interface: inside	Destination Interface:	outside				
Source Address:SPECIFIC_192-168-1-0	Destination Address:	any 🖳				
	Service:	any 🛄				
Action: Translated Packet						
Source NAT Type: Dynamic PAT (Hide)						
Source Address: 10.1.5.5	Destination Address:	Original 🔤				
Fall through to interface PAT	Service:	Original 👘				
Options						
🔽 Enable rule						
Translate DNS replies that match this rule						
Direction: Both						
Description:						
ОК	Cancel Help					
Controleer of de tweede voltooide NAT/PAT-	regel als volgt lijkt:Ir	de aanpassingscriteria:				

Controleer of de tweede voltoolde NAT/PAT-regel als volgt lijkt: In de aanpassingscriteria: Controleer het oorspronkelijke Packet-gebied en deze waarden:Bron-interface = binnenkantBron Adres = OBJ_SPECIFIC_192-168-1-0Doeladres = buitenService = elkeln de Actie: Vertaald pakketgebied, controleer deze waarden:Source NAT Type = Dynamic PAT (Verbergen)Bron Adres = 10.1.5.5Doeladres = OorspronkelijkService = origineelKlik op **OK**.De voltooide NAT-configuratie wordt weergegeven in ASDM, zoals in deze afbeelding wordt

getoond:

Cor	nfiguration > Firewall	> NAT Rules					
4	🕨 Add 👻 🗹 Edit 📋	Delete 🕈 🗲	🗴 🗈 🛍 -	🔍 Find End	agram 🛛 💐 Packet	Trace	
		Match Criteria: O	riginal Packet		Act	ion: Translated P	acket
	Source Intf Dest Int	f Source	Destination	Service	Source	Destination	Servic
	inside outside	GENER	🧐 any	🧼 any	outside (P)	Original	Original
	inside outside	CBJ_SPECIF	🧌 any	🧇 any	📕 10.1.5.5 (P)	Original	Original
	"Network Object" NAT (No rules)					
	1				_		
1							<u> </u>
			Apply	Reset			

3. Klik op de knop **Toepassen** om de wijzigingen in de draaiende configuratie toe te passen. Dit voltooit de configuratie van dynamisch PAT op een Cisco adaptieve security applicatie (ASA).

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Het <u>Uitvoer Tolk</u> (<u>uitsluitend geregistreerde</u> klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

Verificatie van generieke PAT-regel

• <u>tonen lokaal-host</u>-toont de netwerkstatus van lokale hosts.

```
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

    Toon online - Toont de verbindingsstaat voor het toegewezen connectietype.

 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
• laat zien ---geeft de informatie over de vertaalslots weer.
 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
```

Specifieke PAT-regel controleren

```
    tonen lokaal-host-toont de netwerkstatus van lokale hosts.

 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
```

• <u>Toon</u> online - Toont de verbindingsstaat voor het toegewezen connectietype.

• laat zien ---geeft de informatie over de vertaalslots weer.

```
ASA#show xlate
```

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Gerelateerde informatie

- <u>Cisco adaptieve security apparaatbeheer</u>
- <u>Cisco ASA 5500 Series adaptieve security applicaties</u>
- Verzoeken om opmerkingen (RFC's)
- <u>Technische ondersteuning en documentatie Cisco Systems</u>