使用NAT配置ASA版本9端口转发

目录

简介 先决条件 要求 使用的组件 配置 网络图 <u>允许内部主机使用 PAT 访问外部网络</u> 允许内部主机使用 NAT 访问外部网络 允许不受信任的主机访问受信任的网络中的主机 静态身份 NAT 使用静态方法的端口重定向(转发) 验证 连接 系统日志 packet tracer 捕获 故障排除

简介

相关信息

本文档介绍如何使用CLI或自适应安全设备管理器(ASDM)在自适应安全设备(ASA)软件版本9.x中配 置端口重定向(转发)和外部网络地址转换(NAT)功能。

有关更多信息,请参阅<u>《思科 ASA 系列防火墙 ASDM 管理指南》。</u>

先决条件

要求

参阅《配置管理访问权限》,了解如何允许 ASDM 对设备进行配置。

使用的组件

本文档中的信息基于以下软件和硬件版本:

- 思科 ASA 5525 系列安全设备软件版本 9.x 及更高版本
- ASDM 版本 7.x 及更高版本

"本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您的网络处于活动状态,请确保您了解任何命令的潜在影响。"



网络图



此配置中使用的 IP 编址方案在 Internet 上不能合法路由。这些地址是在实验室环境中使用的 RFC 1918 地址。

允许内部主机使用 PAT 访问外部网络

如果需要内部主机共享一个公共地址用于地址转换,可使用端口地址转换 (PAT) 功能。 一种最简单的 PAT 配置是转换所有内部主机,使其看起来像外部接口 IP 地址。当 ISP 提供的可路由 IP 地址 数量有限(或者只有 1 个)时,常会使用这种 PAT 配置。

要使用 PAT 允许内部主机访问外部网络,具体操作步骤如下:

1. 依次选择 Configuration > Firewall > NAT Rules。点击 Add,然后选择 Network Object,以配置动态 NAT 规则。

Monitoring 🔲 Save 🔇 Refresh 🔇 Back 📀	Forward 🦻 Help CISCO
Configuration > Firewall > NAT Rules	Addresses Services
💠 Add 🗸 🌈 Edit 🗊 Delete 🛧 🖌 👗 🖿	Addresses 고 무 ×
Match Criteria: Original Packet	🔁 Add 🗸 🗹 Edit 📋 Delete 🔍 Where Used 🔍 Not Used
# Source Intf Dest Intf Source	Network Object Filter Clear
"Network Object" NAT (Rule 1)	Network Object Group
1 Any outside 💁 Inside_h	Network Objects
	- 🧼 any
	- 🧼 any4
	📕 🛶 🥎 any6

2. 配置需要使用**动态 PAT 的网络/主机/范围。**下面的示例选择了一个内部子网。如果您还想以这 种方式转换其他子网,请执行同样的流程。

🕫 Add Networ	k Object 🛛 🔀	
Name:	obj_172.16.11.0	
Туре:	Network	
IP Version:	⊙ IPv4 ○ IPv6	
IP Address:	172.16.11.0	
Netmask:	255.255.2	
Description:		
NAT	۲	
	OK Cancel Help	

3. 展开 NAT。选中 Add Automatic Address Translation Rules 复选框。从"Type"下拉列表中选择 Dynamic PAT (Hide)。 在 Translated Addr 字段中,选择反映外部接口的选项。单击 Advanced。

NEWOR	s un er r
11010001	

auu networ	
Name:	abi 172.16.11.0
Tupo:	Network
туре:	
IP Version:	● IPv4 ○ IPv6
IP Address:	172.16.11.0
Netmask:	255.255.255.0
Description:	
NAT	۲
Add Automa	atic Address Translation Rules
Туре:	Dynamic PAT (Hide) 🔽
Translated Ac	ddr: outside
Use one-t	to-one address translation
PAT Pool	Translated Address:
Round	Robin
Extend	PAT uniqueness to per destination instead of per interface
🔄 Transla	te TCP and UDP ports into flat range 1024-65535 📄 Include range 1-1023
🔄 Fall throu	gh to interface PAT(dest intf): backup
Use IPv6	for interface PAT
	Advanced
	OK Cancel Help

4. 在"Source Interface"和"Destination Interface"下拉列表中,选择相应的接口。点击 OK,然后 点击 Apply 使更改生效。

🐻 Advanced NAT Set	ttings	×
Translate DNS repli	es for rule	
Interface		_
Source Interface:	inside	*
Destination Interface:	outside	~
ОК	Cancel Help	

与此 PAT 配置等效的 CLI 输出如下所示:

object network obj_172.16.11.0 subnet 172.16.11.0 255.255.255.0 nat (inside,outside) dynamic interface

允许内部主机使用 NAT 访问外部网络

您也可以通过配置动态 NAT 规则来允许一组内部主机/网络访问外部网络。与 PAT 不同的是,动态 NAT 会从地址池分配转换的地址。因此,主机会映射到自己的转换 IP 地址,而不会有两台主机共 用同一转换 IP 地址的情况。

要实现这一目的,您需要选择所要授予外部访问权限的主机/网络的真实地址,然后将其映射到转换 IP 地址池。

要使用 NAT 允许内部主机访问外部网络,具体操作步骤如下:

1. 依次选择 Configuration > Firewall > NAT Rules。点击 Add,然后选择 Network Object,以配置动态 NAT 规则。

Monitoring 🔚 Save 🔇 Refresh 🔇 Back 🜔	Forward 🦻 Help	CISCO
Configuration > Firewall > NAT Rules	Addresses Services	
💠 Add 🗸 📝 Edit 🏛 Delete 🛧 🗲 👗 🖿	Addresses	ъъ×
# Match Criteria: Original Packet # Source Intf Dest Intf Source	Add - C Edit Delete Q When	re Used 🔍 Not Used
"Network Object" NAT (Rule 1)		<u>▲ 1</u>
I Any outside <u>ap</u> Inside_h		

2. 配置需要使用动态 PAT 的网络/主机/范围。下面的示例选择了整个内部网络。

🛅 Add Networl	k Object	×
Name:	obj_172.16.11.0	
Туре:	Network	~
IP Version:	⊙ IPv4 ○ IPv6	
IP Address:	172.16.11.0	
Netmask:	255.255.255.0	*
Description:		
NAT	8	20
	OK Cancel Help	

3. 展开 NAT。选中 Add Automatic Address Translation Rules 复选框。从"Type"下拉列表中选择 **Dynamic**。在"Translated Addr"字段中,选择适当的选项。单击 **Advanced**。

📴 Edit Networ	k Object 🛛 🔀
ľ	
Name:	obj_172.16.11.0
Туре:	Network
IP Version:	⊙ IPv4 O IPv6
IP Address:	172.16.11.0
Netmask:	255.255.255.0
Description:	
NAT	
	atic Address Translation Bules
Туре:	Dynamic 👻
Translated A	ddr:
Use one-	to-one address translation
PAT Pool	Translated Address:
Round	Robin
Extend	PAT uniqueness to per destination instead of per interface
🗌 Transla	ate TCP and UDP ports into flat range 1024-65535 🔄 Include range 1-1023
🔄 Fall throu	ugh to interface PAT(dest intf): backup
Use IPv6	for interface PAT
	Advanced
	OK Cancel Help

4. 点击 Add,以添加网络对象。从"Type"下拉列表中选择 Range。在"Start Address"和"End Address"字段中,输入开始和结束 PAT IP 地址。Click **OK**.

🕫 Add Networ	k Object 🛛 🔀
Rame:	obj-my-range
Туре:	Range
IP Version:	⊙ IPv4 O IPv6
Start Address:	203.0.113.10
End Address:	203.0.113.20
Description:	
NAT	(S)
	OK Cancel Help

5. 在"Translated Addr"字段中,选择地址对象。点击 Advanced,以选择源接口和目的接口。

🕫 Edit Networ	k Object 🛛 🚺	K)
Name:	obi 172 16 11 0	1
Name: N	00]_172.16.11.0	
Туре:	Network	
IP Version:	⊙ IPv4 O IPv6	
IP Address:	172.16.11.0	
Netmask:	255.255.255.0	
Description:]
NAT	۵	
Add Autom	atic Address Translation Rules	
Туре:	Dynamic 🖌	
Translated A	ddr: obj-my-range 🛄	
Use one-	to-one address translation	
PAT Pool	Translated Address:	
Round	Robin	
Extend	PAT uniqueness to per destination instead of per interface	
Transla	ate TCP and UDP ports into flat range 1024-65535 👘 Include range 1-1023	
🔄 Fall throu	Igh to interface PAT(dest intf): backup	
Use IPv6	for interface PAT	
	Advanced	
	OK Cancel Help	

6. 在"Source Interface"和"Destination Interface"下拉列表中,选择相应的接口。点击 OK,然后 点击 Apply 使更改生效。

🐻 Advanced NAT Set	ttings	×
Translate DNS repli	es for rule	
Interface		
Source Interface:	inside 💉	
Destination Interface:	outside 💌	
ОК	Cancel Help	

与此 ASDM 配置等效的 CLI 输出如下所示:

object network obj-my-range range 203.0.113.10 203.0.113.20

object network obj_172.16.11.0
subnet 172.16.11.0 255.255.255.0
nat(inside,outside) dynamic obj-my-range

根据此配置,172.16.11.0网络中的主机将转换为NAT池203.0.113.10 - 203.0.113.20中的任意IP地 址。如果映射池的地址少于实际组,则地址可能会用尽。因此,您可以尝试通过动态PAT备份实施 动态NAT,也可以尝试扩展当前池。

1. 重复前一配置流程的第 1 步至第 3 步,然后再次点击 Add,以添加网络对象。从"Type"下拉列 表中选择 Host。在"IP Address"字段中,输入 PAT 备用 IP 地址。Click OK.

🔄 Add Networ	k Object 🗧	×
Name: (optional)	obj-pat-ip	
Туре:	Host	
IP Version:	⊙ IPv4 O IPv6	
IP Address:	203.0.113.21	1
Netmask:	255.255.255.0	
FQDN:		
Description:]
NAT	×	1
		1
	OK Cancel Help	

2. 点击 Add,以添加网络对象组。在"Group Name"字段中输入组名称,然后点击 Add 将两个地址对象(NAT 范围和 PAT IP 地址)均添加到该组。

scription:						
sciption						
Existing Network Ob	ijects/Groups:			Members in Group:		
Name	▲ 1 IP Address	Netmask	Description	Name	IP Address	NetmaskPre
Network Objects	5			😁 🖳 obj-pat-ip	203.0.113.21	
- 🥝 any				👘 🚅 obj-my-range	203.0.113.10-203.0	
🧼 any4						
- 🎱 any6						
- 📸 inside-ne	t 19.19.19.0	255.255.255.0				
- 🛃 obj_172	.1 172.16.11.0	255.255.255.0				
			Ad	d >>		

3. 选择配置好的 NAT 规则,并将"Translated Addr"更改为新配置的组"nat-pat-group"(之前为 "obj-my-range")。 Click **OK**.

4 Add - G	🖁 Edit 📋 Delete 🛛 🔍 Wh	ere Used 🔍 Not L	lsed	
Filter:	↓ 1 TD Address	Netwack	Description	Filter Clear
-Network O	hierts	Houndar	Description	Object INFL Address
- A ob	-my-ra 203.0.113.10-203	3		
- 🖳 obj	-pat-ip 203.0.113.21			
-Network O	bject Groups			
😐 🚅 na	-pat-g			
-Interfaces				
- 🔤 ba	:kup			
- 🔤 ins	ide			
i 🔤 out	side			
Selected Trans	slated Addr ed Addr -> nat-pat-grou	p		OK Cancel

4. 点击 OK,以添加 NAT 规则。点击 Advanced,以选择源接口和目的接口。

📧 Edit Networ	k Object 🛛 🔀
Name: Type: IP Version: IP Address:	obj_172.16.11.0 Network IPv4 IPv6
Netmask:	255.255.255.0
Description:	
NAT	atic Address Translation Pules
Type:	
Translated A	ddr: nat-pat-group
Use one-	to-one address translation
PAT Pool	Translated Address:
Round	Robin
Extenc	PAT uniqueness to per destination instead of per interface
Transla	ate TCP and UDP ports into flat range 1024-65535 📄 Include range 1-1023
🔄 Fall throu	igh to interface PAT(dest intf): backup
Use IPv6	for interface PAT
	Advanced
	OK Cancel Help

5. 在"Source Interface"和"Destination Interface"下拉列表中,选择相应的接口。Click **OK**.

🔄 Advanced NAT Set	tings 🛛 🔀						
Translate DNS replies for rule							
Interface							
Source Interface:	inside 🛛 👻						
Destination Interface:	outside 💌						
ОК	Cancel Help						

6. 点击 Apply 使更改生效。

	Home 🦓 Configuration 🔯 I	Monitorir		🛛 Save 🔇 R	afresh 🔇 E	Sack 🕐 Forward 🛛 🢡	Ныр	CISCO
	Firewall d	ι φ	Con	figuration > Fi	rewall > NAT	Rules 🗆	Addresses Services	
e Us	Access Rules	^		Add - 🏹 Edit	👔 Delete 👍	- 4 X % m m - 1	Addresses	a ta x
Devic	NAT Rules	~	Ē	Match Crit	eria: Original	Packet	🗣 Add - 📝 Edit 📋 De	slete 🔍 Where Used 🔍 Not Used
	Device Setup		*	Source Intf	Dest Intf	Source	Fiker:	Filter Clear
	Frewall			Network Object*	NAT (Rule 1)		Name	L.
				1 inside	outside	obj_172.16	Network Objects	<u>~</u>
	Remote Access VPN						- 🥥 any	
	C Site-to-Site VPN						- 🥥 any4	
	10-0 -		1			2	- 🥥 anyó	=
	Device Management					<u>.</u>	- M inside-network/2	4
		*		Ar Ar		leset	- 🏬 obj-my-range	
		-				10001	i- 📸 obj_172.16.11.0	×

与此 ASDM 配置等效的 CLI 输出如下所示:

object network obj-my-range range 203.0.113.10 203.0.113.20

object network obj-pat-ip
host 203.0.113.21

object-group network nat-pat-group network-object object obj-my-range network-object object obj-pat-ip

object network obj_172.16.11.0 subnet 172.16.11.0 255.255.255.0

允许不受信任的主机访问受信任的网络中的主机

通过应用静态 NAT 转换和访问规则,可以达到这个目的。当外部用户需要访问您的内部网络中的服务器时,您需要进行此配置。内部网络中的服务器可以拥有不可在Internet上路由的专用IP地址。因此,您需要使用静态 NAT 规则将该专用 IP 地址转换为公共 IP 地址。假设您有一个 IP 为 172.16.11.5 的内部服务器。要使外部用户能够访问该服务器,您需要将此专用服务器 IP 地址转换 为公共 IP 地址。下面的示例介绍如何使用双向静态 NAT 将 172.16.11.5 转换为 203.0.113.5。

1. 依次选择 Configuration > Firewall > NAT Rules。点击 Add, 然后选择 Network Object, 以配置静态 NAT 规则。展开 NAT。

📧 Add Networ	k Object	×
Name:	obj_172.16.11.5	
Туре:	Host	-
IP Version:	⊙ IPv4 ○ IPv6	
IP Address:	172.16.11.5	
Description:		
NAT	*	
	OK Cancel Help	

2. 选中 Add Automatic Address Translation Rules 复选框。从"Type"下拉列表中选择 **Static。**在 "Translated Addr"字段中,输入 IP 地址。点击 **Advanced,以选择源接口和目的接口。**

🔚 Add Networ	k Object 🛛 💦 📘	
Name:	obj_172.16.11.5]
Туре:	Host	
IP Version:	⊙ IPv4 ○ IPv6	
IP Address:	172.16.11.5]
Description:		
NAT	۲	
Add Automa	atic Address Translation Rules	
Type:	Static	
Translated Ac	idr: 203.0.113.5	
🔽 Use one-t	co-one address translation	
PAT Pool	Translated Address:	
Round	Robin	
Extend	PAT uniqueness to per destination instead of per interface	
Transla	te TCP and UDP ports into flat range 1024-65535 📃 Include range 1-1023	
Fall throu	gh to interface PAT(dest intf): backup	
Use IPv6	for interface PAT	
	Advanced	
	OK Cancel Help	

3. 在"Source Interface"和"Destination Interface"下拉列表中,选择相应的接口。Click **OK**.

🖀 Advanced NAT Set	tings 🛛 🔀					
Translate DNS replies for rule						
Interface						
Source Interface:	inside 🛛 🗠					
Destination Interface:	outside 💌					
ОК	Cancel Help					

4. 您可以在这里看到已配置的静态 NAT 条目。点击 Apply,以将配置发送到 ASA。

	Match Crite	eria: Original	Packet			Action: Transla	ed Packet	
F	Source Intf	Dest Intf	Source	Destination	Service	Source	Destination	Service
"h	ietwork Object"	NAT (Rule 1)						
1	inside	outside	🖳 obj_172.16	🌍 any	🥥 any	🖳 203.0.113.5 (S	Original	Original
	outside	inside	🏟 any	3 203.0.113.5	🏟 any	Original (S)	🖪 obj_172.16	Original

与此 NAT 配置等效的 CLI 输出如下所示:

object network obj_172.16.11.5
host 172.16.11.5
nat (inside,outside) static 203.0.113.5

静态身份 NAT

当内部用户尝试在不完成 NAT 的情况下访问远程 VPN 主机/服务器或与 ASA 的任何其他接口连接 的主机/服务器时,NAT 豁免是一项有用的功能。为此,内部服务器(具有私有IP地址)可以转换为 自己的身份,从而允许其访问执行NAT的目标。 在下面的示例中,内部主机 172.16.11.15 需要访问远程 VPN 服务器 172.20.21.15。 要在不完成 NAT 的情况下允许内部主机访问远程 VPN 网络,具体操作步骤如下:

1. 依次选择 Configuration > Firewall > NAT Rules。点击 Add,以配置 NAT 豁免规则。



2. 在"Source Interface"和"Destination Interface"下拉列表中,选择相应的接口。在"Source Address"字段中,选择相应的条目。

🔚 Add NAT Rule						×
Match Criteria: Original Packet						
Source Interface:	inside		🗸 Destin	ation Interface:	outside	~
Source Address:	any	(Destin	ation Address:	any	
			Service	е:	any	
Action: Translated Packet						
Source NAT Type:	Static	📴 Browse O	riginal So	urce Addres	s	
Source Address:	Origina					
Use one-to-one address transla	ation	🔂 Add 🗸	🗹 Edit 🥤	🖥 Delete 🛛 🔍	Where Used 🔍 N	ot Used
PAT Pool Translated Address:		Filter:				
Round Robin		Name	▲ 1	IP Address		Netmask
Extend PAT uniqueness to pe	er destinal		any			
Translate TCP and UDP ports	into flat r					
Fall through to interface PAT						
Use IPv6 for source interface P	AT					
Options						
Inable rule						
Translate DNS replies that mate	h this rule:					

3. 点击 Add,以添加网络对象。配置主机 IP 地址。

📧 Add Netwo	rk Object 🛛 🔀
Name:	obj_172.16.11.15
Туре:	Host
IP Version:	⊙ IPv4 ○ IPv6
IP Address:	172.16.11.15
Description:	
NAT	8
	OK Cancel Help

4. 同样,浏览 Destination Address。点击 Add,以添加网络对象。配置主机 IP 地址。

🔚 Add Netwo	rk Object	×
Name: Type: IP Version:	obj_172.20.21.15 Host IPv4 O IPv6	~
IP Address:	172.20.21.15	
Description:		
NAT		۲
	OK Cancel Help	

5. 选择配置好的源地址和目的地址对象。选中 Disable Proxy ARP on egress interface 和 Lookup route table to locate egress interface 复选框。Click OK.

🖀 Add NAT Rule				×			
Match Criteria: Original Packet							
Source Interface:	inside 💌	Destination Interface:	outside	~			
Source Address:	obj_172.16.11.15	Destination Address:	obj_172.20.21.15				
		Service:	any				
Action: Translated Packet							
Source NAT Type:	Static 💌						
Source Address:	Original	Destination Address:	Original	···			
Use one-to-one address transla	ation						
PAT Pool Translated Address:		Service:	Original				
Round Robin							
Extend PAT uniqueness to pe	er destination instead of per int	erface					
Translate TCP and UDP ports	into flat range 1024-65535	Include range 1-1023	3				
Fall through to interface PAT							
Use IPv6 for source interface P	AT	Use IPv6 for destin	ation interface PAT				
Options							
🔽 Enable rule	Enable rule						
Translate DNS replies that mate	Translate DNS replies that match this rule						
✓ Disable Proxy ARP on egress interface							
Cookup route table to locate egress interface							
Direction: Both 🔹							
Description:							
OK Cancel Help							

6. 点击 Apply 使更改生效。

🗞 Configuration 📴 Monitoring 🔚 Save 🔇 Refresh 🔇 Back 🚫 Forward 🢡 Help						
a e 🔀	Confi	guration > Fire	wall > NAT P	tules.		Addresses
ess Rules	• A	idd 🔻 📝 Edit 🕯	🖹 Delete 🛉	↓ よ陰臨・	Q, Find	🗣 Add 👻 🎬 Edit 🏢 Delete 🔍 Where Used 🔍
vice Policy Rules		Match Crite	ria: Original P	acket		Fiter:
(Rules	#	Source Intf	Dest Intf	Source	Destina	Name
r Rules	1	inside	outside	🖪 obj_172.16	🔳 obj_	 Network Objects
e Setup	"N	"Network Object" NAT (No rules)				- 🧇 any
						- 🏟 any4
-ali						🎱 any6
te Access VPN						- 🚎 inside-network/24
						- 📇 obj_172.16.11.15
to-Site VPN						i 🔳 obj_172.20.21.15
ze <u>M</u> anagement	<	Ш			>	
» *			Apply	Reset		

与 NAT 豁免或身份 NAT 配置等效的 CLI 输出如下所示:

object network obj_172.16.11.15 host 172.16.11.15 object network obj_172.20.21.15 host 172.20.21.15

nat (inside,outside) source static obj_172.16.11.15 obj_172.16.11.15
destination static obj_172.20.21.15 obj_172.20.21.15 no-proxy-arp route-lookup

使用静态方法的端口重定向(转发)

在外部用户需要访问特定端口上的内部服务器的情况下,端口转发(或端口重定向)功能十分有用 。为此,内部服务器(具有私有IP地址)可以转换为公有IP地址,从而允许访问特定端口。

在本示例中,外部用户想要访问端口25上的SMTP服务器203.0.113.15。这可通过两个步骤完成:

1. 将端口25上的内部邮件服务器172.16.11.15转换为端口25上的公共IP地址203.0.113.15。

2. 允许访问端口 25 上的公共电子邮件服务器 203.0.113.15。

当外部用户尝试访问端口25上的服务器203.0.113.15时,此流量被重定向到端口25上的内部邮件服 务器172.16.11 15。

1. 依次选择 Configuration > Firewall > NAT Rules。点击 Add,然后选择 Network Object,以配置静态 NAT 规则。

Monitoring 🔚 Save 🐼 Refresh 🔇 Back 🚫 Forward 🤗 Help							
	<u>Config</u>	uration > Fire	ewall > NAT I	Rules 🗆	Addresses Services		
🖨 Add 🗸 🌠 Edit 🏛 Delete 🛧 🚄 🐰 🖿				4 X 🖿	Addresses	급 후 ×	
		Match Crite	ria: Original I	Packet	🗣 Add 🔻 🕜 Edit 📋 Delete 🕻	🔪 Where Used 🔍 Not Used	
	# Source Intf Dest Intf Source		Source	Network Object	Filter Clear		
	"Network Object" NAT (Rule 1)				Network Object Group	▲ 1	
	1	Any	outside	📑 Inside_h	□-Network Objects		
					- 🌍 any		
					- 🌍 any4		
					- 🌍 any6		

2. 配置需要执行端口转发的主机。

🖼 Edit Network Object 🛛 🔀				
Name:	obj_172.16.11.15			
Туре:	Host			
IP Version:	IPv4 O IPv6			
IP Address:	172.16.11.15			
Description:				
NOT				
1001				
	OK Cancel Help			

3. 展开 NAT。选中 Add Automatic Address Translation Rules 复选框。从"Type"下拉列表中选择 Static。在"Translated Addr"字段中,输入 IP 地址。点击 Advanced,以选择服务、源接口和 目的接口。

🕫 Edit Network Object 🛛 🔀					
Name	obi 172 16 11 15				
Turne:	00_1/2.10.11.15				
Type:	Host	<u> </u>			
IP Grsion:	● IPv4 ○ IPv6				
IP Address:	172.16.11.15				
Description:					
NAT		*			
🖌 Add Automa	atic Address Translation Rules				
Туре:	Static 💌				
Translated Ad	idr: 203.0.115.15				
🗌 Use one-t	to-one address translation				
PAT Pool	PAT Pool Translated Address:				
Round Robin					
Extend PAT uniqueness to per destination instead of per interface					
Translate TCP and UDP ports into flat range 1024-65535 Include range 1-1023					
Fall through to interface PAT(dest intf): backup					
Use IPv6 for interface PAT					
Advanced					
OK Cancel Help					

4. 在"Source Interface"和"Destination Interface"下拉列表中,选择相应的接口。配置服务。Click OK.

📧 Advanced NAT Settings 🛛 🛛 🔀						
Translate DNS repli	es for rule					
Disable Proxy ARP	on egress interface					
Lookup route table	to locate egress interface					
Interface						
Source Interface:	inside 💌					
Destination Interface:	outside 🔽					
Service						
Protocol:	🚥> tcp 🛛 🔽					
Real Port:	smtp					
Mapped Port:	smtp					
OK Cancel Help						

5. 点击 Apply 使更改生效。

0 P	Configuration > Firewall > NAT Rules					Addresses
^	💠 A	dd 👻 🗹 Edit	👔 Delete 🛧	€ % m m .	💠 Add 🔻 🗹 Edit 📋 Delete 🔍 Where Used 🔾	
		Match Crite	ria: Original F	Packet	Filter:	
~	#	Source Intf	Dest Intf	Source	Destina	Name
	😑 "N	etwork Object" I	IAT (Rule 1)			-Network Objects
	1	inside	outside	📕 obj_172.16	🉁 any	🎱 any
		outside	inside	🧼 any	르, 203.	🧼 any4
						🧼 any6
						- 📫 inside-network/24
						🔜 obj_172.16.11.15
						· 🖳 203.0.115.15
	<				>	
÷			Apply	Reset		

与此 NAT 配置等效的 CLI 输出如下所示:

object network obj_172.16.11.15
host 172.16.11.15
nat (inside,outside) static 203.0.113.15 service tcp smtp smtp

验证

使用本部分可确认配置能否正常运行。

思科 CLI 分析器(仅适用于注册客户)支持某些 show 命令。要查看对 show 命令输出的分析,请

使用思科 CLI 分析器。

在 Web 浏览器上使用 HTTP 访问一个网站。此示例使用托管在198.51.100.100的站点。如果连接 成功,可在ASA CLI上看到此输出。

连接

ASA(config)# show connection address 172.16.11.5 6 in use, 98 most used TCP outside 198.51.100.100:80 inside 172.16.11.5:58799, idle 0:00:06, bytes 937, flags UIO

ASA 是状态化防火墙,来自 Web 服务器的返回流量会因为与防火墙连接表中的连接匹配,而被允 许通过防火墙。与既有连接匹配的流量不会被接口 ACL 阻止,即可通过防火墙。

在上面的输出中,内部接口上的客户端已经与外部接口上的主机 198.51.100.100 建立了连接。此连 接是通过 TCP 协议建立的,而且已空闲 6 秒。连接标记表明此连接的当前状态。有关连接标记的 更多信息,可参阅 ASA TCP 连接标记。

系统日志

ASA(config)# show log | in 172.16.11.5

Apr 27 2014 11:31:23: %ASA-6-305011: Built dynamic TCP translation from inside: 172.16.11.5/58799 to outside:203.0.113.2/58799

Apr 27 2014 11:31:23: %ASA-6-302013: Built outbound TCP connection 2921 for outside: 198.51.100.100/80 (198.51.100.100/80) to inside:172.16.11.5/58799 (203.0.113.2/58799)

在正常运行期间,ASA 防火墙会生成系统日志。根据日志记录配置,系统日志的内容十分丰富。上面的输入显示了两个第 6 级别(即"信息"级别)的系统日志。

在此示例中,防火墙生成了两个系统日志。第一个系统日志记录的消息表明,防火墙已建立了转换 ,并明确指出是动态 TCP 转换 (PAT)。 从中可以看出流量从内部接口流向外部接口时的源 IP 地址 和端口以及转换 IP 地址和端口。

第二个日志记录表明,防火墙已在其连接表中为该客户端与服务器之间的特定流量创建了一条连接 。如果防火墙已配置为阻止此连接尝试,或者有其他因素禁止创建此连接(资源限制或配置错误),防火墙不会生成日志来表明建立了此连接。在这种情况下,防火墙会生成一条日志来说明连接 被拒绝的原因,或者指明禁止创建连接的因素。

packet tracer

ASA(config)# packet-tracer input inside tcp 172.16.11.5 1234 198.51.100.100 80

--Omitted--

Result: input-interface: inside input-status: up input-line-status: up output-interface: outside output-status: up 利用 ASA 的 Packet Tracer 功能,您可以指定一个*模拟数据包,以便查看防火墙在处理流量时的各种步骤、检查和功能。*使用此工具,识别您认为可以允许通过防火墙的流量示例*并使用*该5元组来模拟流量很有帮助。在上面的示例中,我们使用 Packet Tracer 来模拟符合下列条件的连接尝试:

- 模拟数据包到达网络内部。
- 使用的协议是 TCP。
- •模拟客户端 IP 地址为 172.16.11.5。
- 客户端发送的流量源于端口 1234。
- 流量的目的位置是 IP 地址为 198.51.100.100 的服务器。
- 流量抵达于端口 80。

需要注意的是,命令中未提及外部接口。这是由于 Packet Tracer 设计上的原因。该工具会帮助您 了解防火墙如何处理这类连接尝试,包括如何执行路由、从哪个接口离开等等。有关 Packet Tracer 的更多信息,请参阅使用 Packet Tracer 跟踪数据包。

捕获

应用捕获

ASA# capture capin interface inside match tcp host 172.16.11.5 host 198.51.100.100 ASA# capture capout interface outside match tcp any host 198.51.100.100

ASA#show capture capin

3 packets captured

1: 11:31:23.432655 172.16.11.5.58799 > 198.51.100.100.80: S 780523448: 780523448(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK> 2: 11:31:23.712518 198.51.100.100.80 > 172.16.11.5.58799: S 2123396067: 2123396067(0) ack 780523449 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8> 3: 11:31:23.712884 172.16.11.5.58799 > 198.51.100.100.80: . ack 2123396068 win 32768

ASA#**show** capture capout

3 packets captured

1: 11:31:23.432869 203.0.113.2.58799 > 198.51.100.100.80: S 1633080465: 1633080465(0) win 8192 <mss 1380,nop,wscale 2,nop,nop,sackOK> 2: 11:31:23.712472 198.51.100.100.80 > 203.0.113.2.58799: S 95714629: 95714629(0) ack 1633080466 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8> 3: 11:31:23.712914 203.0.113.2.58799 > 198.51.100.100.80: . ack 95714630 win 32768/pre>

ASA 防火墙可以捕获进入或离开接口的流量。这个捕获功能非常有用,因为它可以明确证明流量是 否已经到达或离开防火墙。上面提供了两个捕获的配置示例(在内部接口上执行的名为 capin 的捕 获和在外部接口上执行的名为 capout 的捕获)。capture 命令中使用了 match 关键字,用于指定需 要捕获的流量。

对于捕获**,您表示想要匹配在与TCP主机172.16.11.5主机198.51.100.100匹配的内部接口(入口或 出口)上看到的流量。换句话说,您要捕获从主机172.16.11.5发送到主机198.51.100.100的任何 TCP流量,反之亦然。**使用 match 关键字可以使防火墙双向捕捉流量。为外部接口定义的 capture 命令未引用内部客户端 IP 地址,因为防火墙会在该客户端 IP 地址上执行 PAT,所以我们无法对该 客户端 IP 地址进行匹配操作。因此,示例中使用 any 关键字来指代所有可能与该条件匹配的 IP 地 址。

配置捕获后,我们应尝试再次建立连接,然后使用 show capture<capture_name> 命令查看捕获结果。在上面的示例中可以看到,捕获结果中显示了 TCP 三次握手,可以证明客户端能够连接到服务器。

故障排除

目前没有针对此配置的故障排除信息。

相关信息

- ASA 系统日志配置示例
- 通过 CLI 和 ASDM 配置实现 ASA 数据包捕获示例
- <u>技术支持和文档 Cisco Systems</u>

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言,希望全球的用户都能通过各 自的语言得到支持性的内容。

请注意:即使是最好的机器翻译,其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任,并建议您总是参考英文原始文档(已提供 链接)。