ASA 7.x/PIX 6.x及更高版本:開啟/封鎖連線埠組 態範例

```
目錄
```

<u> 簡介</u>

本文提供一個範例組態,說明如何為安全裝置中各種型別的流量(例如http或ftp)開啟或封鎖連線 埠。

注意:「開啟埠」和「允許埠」這兩個術語具有相同的含義。同樣,「阻塞埠」和「限制埠」也具 有相同的含義。

必要條件

<u>需求</u>

本文檔假設PIX/ASA已配置且工作正常。

<u>採用元件</u>

本文中的資訊係根據以下軟體和硬體版本:

- 執行8.2(1)版的Cisco 5500系列調適型安全裝置(ASA)
- •思科調適型安全裝置管理員(ASDM)版本6.3(5)

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設

)的組態來啟動。如果您的網路正在作用,請確保您已瞭解任何指令可能造成的影響。

<u>相關產品</u>

此配置還可以與軟體版本6.x及更高版本的Cisco 500系列PIX防火牆裝置配合使用。

<u>慣例</u>

請參閱<u>思科技術提示慣例以瞭解更多有關文件慣例的資訊。</u>

<u>設定</u>

每個介面的安全級別必須介於0(最低)到100(最高)之間。 例如,您必須將最安全的網路(例如 內部主機網路)分配到第100級。雖然連線到Internet的外部網路可以是0級,但其他網路(例如 DMZ)可以位於兩者之間。您可以將多個介面分配給相同的安全級別。

預設情況下,在外部介面(安全級別0)上阻止所有埠,並且在安全裝置的內部介面(安全級別 100)上開啟所有埠。通過這種方式,所有出站流量都可以通過安全裝置,而無需進行任何配置 ,但可以通過安全裝置中的訪問清單和靜態命令配置來允許入站流量。

注意:一般情況下,從較低安全區域到較高安全區域的所有埠都會被阻止,並且從較高安全區域到 較低安全區域的所有埠都會開啟,前提是對入站和出站流量啟用狀態檢查。

本節包括以下小節:

- 網路圖表
- 阻塞埠配置
- 開啟埠配置

本節提供用於設定本文件中所述功能的資訊。

註:使用<u>Command Lookup Tool</u>(僅<u>供</u>已註冊客戶使用)可獲取本節中使用的命令的詳細資訊。

網路圖表

本檔案會使用以下網路設定:



<u>阻塞埠配置</u>

除非擴展訪問清單明確阻止任何出站流量,否則安全裝置允許任何出站流量。

訪問清單由一個或多個訪問控制條目組成。視存取清單型別而定,您可以指定來源和目的地位址、 通訊協定、連線埠(適用於TCP或UDP)、ICMP型別(適用於ICMP)或EtherType。

注意:對於無連線協定(如ICMP),安全裝置會建立單向會話,因此您需要訪問清單來允許兩個方向的ICMP(通過將訪問清單應用到源和目標介面),或者需要啟用ICMP檢測引擎。ICMP檢測引擎將ICMP會話視為雙向連線。

完成這些步驟即可封鎖連線埠,這些連線埠通常適用於從內部(較高安全區域)到DMZ(較低安全 區域)或DMZ到外部的流量。

1. 以阻止指定埠流量的方式建立訪問控制清單。

access-list

2. 然後使用access-group命令繫結訪問清單以便處於活動狀態。

示例:

 1. 阻止HTTP埠流量:若要阻止內部網路10.1.1.0存取IP為172.16.1.1且位於DMZ網路中的 http(Web伺服器),請建立一個ACL,如下所示: ciscoasa(config)#access-list 100 extended deny tcp 10.1.1.0 255.255.255.0 host 172.16.1.1 eq 80 ciscoasa(config)#access-list 100 extended permit ip any any ciscoasa(config)#access-group 100 in interface inside
 注意:使用no,然後使用access list命令以刪除埠阻塞。
 封鎖FTP連線埠流量:若要阻止內部網路10.1.1.0存取FTP(檔案伺服器)(IP為 172.16.1.2)且放在DMZ網路中,請建立一個ACL,如下所示: ciscoasa(config)#access-list 100 extended deny tcp 10.1.1.0 255.255.255.0 host 172.16.1.2 eq 21

ciscoasa(config)#access-list 100 extended permit ip any any ciscoasa(config)#access-group 100 in interface inside

注意:請參閱<u>IANA埠</u>以瞭解有關埠分配的更多資訊。

本節顯示了通過ASDM執行此操作的逐步配置。

1. 前往Configuration > Firewall > Access Rules。按一下Add Access Rule以建立訪問清單。 Configuration > Firewall > Access Rules



2. 定義訪問規則的源、目標和操作以及與此訪問規則關聯的介面。選擇詳細資訊以選擇要阻止的

🜃 Add Acc	ess Rule
Interface: (inside 🔽
Action: 🔘	Permit 💿 Deny
Source: (10.1.1.0
Destination	172,16.1.1
Service:	ip (
Description:	
💌 Enable L	ogging
Logging I	Level: Default
More Opt	ions
	OK Cancel Help

3. 從可用埠清單中選擇http,然後按一下OK以恢復到「新增訪問規則」視窗。

Filter.							FitteriO
Nerr		Protocol	Source Ports	Destination Ports	ICMP Type	Description	
	18 decard	top	defauk (1-65535)	9			
i i	- me- daman	top	default (1-65535)	53			
- ł	11 echo	top	default (1-65535)	7			
	130-000C	top	default (1-65535)	512			
- F	10 finger	trp	default (1-65535)	79			
- H	at ftp	top	default (1-65535)	21			
1	12- ftp-data	top	default (1-65535)	20			
	- 12 gopher	top	default (1-65535)	70			
	10 h323	top	default (1-65535)	1720			
	32 hostname	top	default (1-65535)	101			
	ap http	top.	default (1-65535)	10			
ł	m https	top	default (1-65535)	443	· · · · · ·		
1	10-ident	top	default (1-65535)	113			
-	10 intep4	top	default (1-65535)	143			
	me ire	top	default (1-65535)	194			
- 1	12 kerberos	top.	default (1-65535)	250			
	ne-klogn	top	defauk (1-65535)	543			
-	m Juhel	top	default (1-65535)	544			
	- 12 Idap	top	default (1-65835)	389			
-	- 102- Idaps	top	defauk (1-65535)	636			
Select	ed Service						······ .
0	feater a lite						

4. 按一下OK完成訪問規則的配置。

特定埠。

🖆 Add Acc	ess Rule	
Interface:	inside 🔽	
Action: 🔿 P	Permit 💿 Deny	
Source:	10,1.1,0	
Destination	172.16.1.1	
Service:	tcp/http	
Description:		
💌 Enable Lo	ogging	
Logging L	evel: Default	
More Opti	ons	
	C(OK Cancel Help
按一下 Insert A	fter將訪問規則新增到同	一訪問清單。
Configuratio	n > Firewall > Access R	tules
🔂 Add 🗕 [🕉 Edit 📋 Delete 🔶	↓ 🎖 🖻 💼 - 🔍 Fi
Add A	ccess Rule	Destination
🚱 Insert	1	-
🙀 Insert	After	
	es (2 inclinit is convine with a	any
i i mana	ge (2 implicit incoming rules	Any less secur
< 1 ·		

6. 允許從「any」到「any」的流量防止「Implicit deny」。 然後,按一下**OK**完成新增此訪問規

Action: Source: Destination Service: Description	Permit O Deny any any ip			
Source: Destination Service: Description	any any ip			
Destination Service: Description	ip			
Service: Description	ip			
Description	100			
	:			
💌 Enable	Logging			
Logging	Level: Default	~		
More Op	tions			
		ОК	Cancel	Help
Access Rule	s頁籤中看到已配置	ОК 【的訪問清單。按一】	Cancel	Help 傳送到安全裝置。
Access Rules	s頁籤中看到已配置 ·ewall > Access Rules	<u>ок</u> 1的訪問清單。按一1	Cancel 「Apply將此配置	Help 傳送到安全裝置。
Access Rules	s頁籤中看到已配置 `ewall > Access Rules 脅 Delete ↑ ↓	OK 0K 10 10 10 10 10 10 10 10 10 10 10 10 10	Cancel Apply將此配置	Help 傳送到安全裝置。 aport - 69 Clear Hits
Access Rules iguration > Fir Add + 2 Enabled Enabled	s頁籤中看到已配置 'ewall > Access Rules î Delete	OK 【的訪問清單。按一 】 【 配 配 - Q Find Destination	Cancel 「Apply將此配置 I Diagram 副Ex Service	Help 傳送到安全裝置。 aport - 69 Clear Hits Action H
Access Rules iguration > Fir Add + 2 Edit Enabled S inside (3 inco	s頁籤中看到已配置 * <mark>ewall > Access Rules</mark> 1 Delete	OK 直的訪問清單。按一 為 🗈 🛋 - Q Find Destination	Cancel 「Apply將此配置 I Diagram 訳Ex Service	Help 傳送到安全裝置。 sport - 69 Clear Hits Action H
Access Rule: iguration > Fir Add - 2 Edit Enabled inside (3 inco 1 2	s頁籤中看到已配置 <mark>rewall > Access Rules</mark>	OK 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0	Cancel 「Apply將此配置 I Diagram 訳 Ex Service	Help 傳送到安全裝置。 sport - 分 Clear Hits Action H
Access Rule: Iquration > Fir Add + 2 Edit Enabled M inside (3 inco 1 2	s頁籤中看到已配置 œwall > Access Rules ① Delete	OK 直的訪問清單。按一 為 配 配 - Q Find Destination 里 172.16.1.1	Cancel 「Apply將此配置 I Diagram 赢 Ex Service 1 ● http 1 ● ip	Help 傳送到安全裝置。 oport - 69 Clear Hits Action H So Deny
Access Rules Iguration > Fir Add + 2 Edit Enabled Image: Enabled Image: Edite (3 inco) Enabled I	s頁籤中看到已配置 ewall > Access Rules ① Delete	OK 2的訪問清單。按一 3	Cancel 「Apply將此配置 」 Diagram Service ション ト た ション レ の し ション レ し し し し し し し し し し し し し	Help 傳送到安全裝置。 aport - 69 Clear Hits Action H S Deny Permit S Deny
Access Rule: iguration > Fir Add - 2 Edit Enabled inside (3 inco 1 2 2 2 3 manage (2 in	s 頁 籤 中 看 到 已 配 置 rewall > Access Rules ① Delete	OK 直的訪問清單。按一 送 配 配 - Q Find Destination 图 172.16.1.1 《 any ② any	Cancel Apply將此配置 I Diagram 副Ex Service 1 题 http 1 题 p	Help 傳送到安全裝置。 aport + 分 Clear Hits Action H ② Deny 《 Permit ③ Deny
Access Rules Iguration > Fir Add + 2 Edit Enabled Inside (3 inco I I IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	s 頁籤中看到已配置 ewall > Access Rules Delete	OK LI的訪問清單。按一 LIDESTINATION LIDE	Cancel 「Apply將此配置 「 Diagram	Help 傳送到安全裝置。 oport - 69 Clear Hits Action H So Deny Permit So Deny
Access Rule: iguration > Fir Add + 2 Edit Enabled inside (3 inco 1 2 2 2 3 manage (2 in 1 2	s 頁 籤 中 看 到 已 配 置 ewall > Access Rules Delete	OK 在的訪問清單。按一 L Destination 型 172.16.1.1 《 any 《 any 《 any 《 any 《 any	Cancel 不Apply將此配置 Service Service 1 型 http 1 型 ip 1 型 ip 1 型 ip 1 型 ip 1 型 ip	Help 傳送到安全裝置。 sport ~ 分 Clear Hits Action H ② Deny ② Deny ② Deny
Access Rules Iguration > Fir Add + 2 Edit Enabled I 2 2 Manage (2 in 1 2 S outside (1 in)	s 頁籤中看到已配置 ewall > Access Rules Delete	OK Lib 訪問清單。按一 Lib 訪問清單。按一 Destination Lib Lib Lib Lib Lib Lib Lib Lib Lib Lib	Cancel Apply將此配置 Diagram 副Ex Service 1 受 IP 1 定 IP 1 定 IP 1 定 IP	Help 傳送到安全裝置。 port - 分 Clear Hits Action H ② Deny ② Deny ② Deny

從ASDM傳送的配置將在ASA的命令列介面(CLI)上生成這組命令。

7.

access-list inside_access_in extended deny tcp host 10.1.1.0 host 172.16.1.1 eq www access-list inside_access_in extended permit ip any any access-group inside_access_in in interface inside

通過這些步驟,已通過ASDM執行示例1以阻止10.1.1.0網路訪問Web伺服器172.16.1.1。示例 2還可以以相同的方式阻止整個10.1.1.0網路訪問FTP伺服器172.16.1.2。唯一的區別是在選擇 埠時。**注意:**例如2的此訪問規則配置假定為全新配置。

8. 定義用於阻止FTP流量的訪問規則,然後按一下**Details**頁籤選擇目標埠。

🜃 Add Acc	ess Rule
Interface:	inside 💌
Action: 🚫 I	Permit 💿 Deny
Source:	10.1.1.0
Destination	172.16.1.1
Service:	ip (
Description:	
💽 Enable L	ogging
Logging I	Level: Default 💙
More Opt	ions
	OK Cancel Help

9. 選擇ftp埠,然後按一下OK以恢復到Add Access Rule視窗。

er:					
ame	Protocol	Source Ports	Destination Ports	ICMP Type	Description
ter cibrix-ica	top	default (1-65535)	1494		
tiqbe	tcp	default (1-65535)	2748		
- 100 daytime	tcp	default (1-65535)	13		
ter discard	top	default (1-65535)	9		
ter domain	tcp	default (1-65535)	53		
- 💷 echo	top	default (1-65535)	7		
to exec	tcp	default (1-65535)	512		
10 finger	tcp	default (1-65535)	79		
- ttp	top	default (1-65535)	21		-
ter ftp-data	tcp	default (1-65535)	20		
gopher	tcp	default (1-65535)	70		
- 10 h323	tcp	default (1-65535)	1720		
- 😰 hostname	tcp	default (1-65535)	101		
tte http	top	default (1-65535)	80		
- 💷 https	top	default (1-65535)	443		
- 🚾 ident	top	default (1-65535)	113		
- 100> imap4	top	default (1-65535)	143		
TO inc	tcp	default (1-65535)	194		
- 🚾 kerberos	tcp	default (1-65535)	750		
and Mainta	hen	dofault (1.40000)	END		1
ected Service					

_____ 10. 按一下**OK**完成訪問規則的配置。

🖆 Add Acc	ess Rule
Interface:	inside 💌
Action: 🔿	Permit 💿 Deny
Source:	10.1.1.0
Destination	172.16.1.1
Service:	tcp/ftp
Description:	
🛃 Enable L	ogging
Logging	Level: Default 💙
More Opt	ions
	OK Cancel Help

11. 新增其他訪問規則以允許任何其他流量。否則,隱式拒絕規則將阻止此介面上的所有流量。

🖆 Insert A	fter Access Rule
Interface:	inside 🔽
Action: 💿 i	Permit 🔿 Deny
Source:	any
Destination	any
Service:	ip
Description:	
🛃 Enable Li	ogging
Logging l	.evel: Default
More Opt	ions
	OK Cancel

12. 在Access Rules頁籤下,完整的訪問清單配置如下所示。

#	Enabled	Source	Destination	Service	Action
- 54	inside (3 incom	ing rules)			
1	V	凰 10.1.1.0	172.16.1.1	🚾 ftp	3 Deny
2		🔄 any	📌 any	😰 ip	🖌 Permi
3		🥥 any	🧼 any	ᢧ ip	😮 Deny
.54	manage (2 imp	licit incoming rules)			
1		🧼 any	Any less secure ne	JP/ ip	🛷 Permit
2		🌍 any	🧼 any	🥑 ip	😮 Deny
	outside (1 impl	icit incoming rule)			
1		🧼 any	🥥 any	😕 ip	🕄 Deny
ccess P	tule Type 🔿	IPv4 and IPV6 💿 IPv4 O	nly () IPv6 Only		

13. 按一下Apply將配置傳送到ASA。等效的CLI配置如下所示: access-list inside_access_in extended deny tcp host 10.1.1.0 host 172.16.1.1 eq ftp access-list inside_access_in extended permit ip any any access-group inside_access_in in interface inside

<u>開啟埠配置</u>

除非擴展訪問清單明確允許,否則安全裝置不允許任何入站流量。

如果要允許外部主機訪問內部主機,可以在外部介面上應用入站訪問清單。您需要指定訪問清單中 內部主機的轉換地址,因為轉換後的地址是可用於外部網路的地址。完成以下步驟,即可開啟從較 低安全區域到較高安全區域的連線埠。例如,允許從外部(較低安全區域)到內部介面(較高安全 區域)或DMZ到內部介面的流量。

 靜態NAT將實際地址轉換為對映地址。此對映地址是託管在Internet上的地址,可用於訪問 DMZ上的應用伺服器,而無需知道伺服器的實際地址。

static (real_ifc,mapped_ifc) mapped_ip {real_ip [netmask mask] |
 access-list access_list_name | interface}

請參閱<u>PIX/ASA命令參考的靜態NAT</u>部分以瞭解詳細資訊。

2. 建立ACL以允許特定連線埠流量。

access-list

3. 使用access-group命令繫結訪問清單以便處於活動狀態。

access-group

示例:

 開啟SMTP埠流量:開啟埠tcp 25,以允許來自外部(Internet)的主機訪問位於DMZ網路中的郵件伺服器。Static命令將外部地址192.168.5.3對映到實際DMZ地址172.16.1.3。 ciscoasa(config)#static (DMZ,Outside) 192.168.5.3 172.16.1.3 netmask 255.255.255.255 ciscoasa(config)#access-list 100 extended permit tcp any host 192.168.5.3 eq 25 ciscoasa(config)#access-group 100 in interface outside

2. 開啟HTTPS連線埠流量:開啟埠tcp 443,以允許來自外部(Internet)的主機訪問放置在DMZ網路中的Web伺服器(安全)。 ciscoasa(config)#static (DMZ,Outside) 192.168.5.5 172.16.1.5 netmask 255.255.255.255 ciscoasa(config)#access-list 100 extended permit tcp any host 192.168.5.5 eq 443 ciscoasa(config)#access-group 100 in interface outside

3. 允許DNS流量:開啟埠udp 53,以允許來自外部(Internet)的主機訪問位於DMZ網路中的 DNS伺服器(安全)。 ciscoasa(config)#static (DMZ,Outside) 192.168.5.4 172.16.1.4 netmask 255.255.255.255 ciscoasa(config)#access-list 100 extended permit udp any host 192.168.5.4 eq 53 ciscoasa(config)#access-group 100 in interface outside

注意:請參閱<u>IANA埠</u>以瞭解有關埠分配的更多資訊。

通過ASDM配置

本節顯示了通過ASDM執行上述任務的逐步方法。

1. 建立允許到192.168.5.3伺服器的smtp流量的訪問規則。



2. 定義訪問規則的源和目標,以及與此規則繫結的介面。另外,將操作定義為**允許**。

🖆 Add Ac	cess Rule
Interface:	outside 💌
Action: 🧿	Permit) O Deny
Source: (any
Destination	192.168.5.3
Service;	ip 💽
Description:	
💽 Enable I	.ogging
Logging	Level: Default 🕑
More Op	tions
	OK Cancel Help

3. 選擇SMTP作為埠,然後按一下OK。

CY 201						
Name	1.0	Protocol	Source Ports	Destination Ports	ICMP Type	Descripti
Inter He	PIP Th	hen	default (1.65535)	514		
-		ben .	default (1-65535)	514		
200-11	sp	top .	default (1-60000)	5040		
123-5	P.	lten	default (1+65555)	9000		ń –
100.9	aloot	box	def 2 (1 (1 (55575)	1521		1
	dine:	here.	default (1-65535)	104		
190 5	SIT.	tup tur	default (1-65555)	111		
<u>19</u> , 8	unrpc	ccp	default (1-65535)	10		
- 1	acacs	cop	default (1-65535)	89		
100 La	alk.	ccp	derault (1-00000)	517		
Note to	sinet	ccp	deraulc (1-65535)	23		
100 U	ucp	ccp	default (1-65535)	540		
- 100 W	hois	ccp	deraut (1-65535)	93		
see b	11	udp	default (0-65535)	512		
- Ret - B	ootpc	udp	default (0-65535)	68		
Not P	ootps	udp	default (0-65535)	67		
102 C	ŕs	udp	default (0-65535)	3020		
w d	iscard	udp	default (0-65535)	9		
-102 d	nsix	udp	default (0-65535)	195		
b 🚥	omain	udp	default (0-65535)	53		
	£		L.C. A. IN JORNOPH			

4. 按一下**OK**完成訪問規則的配置。

🖆 Add Aco	ess Rule
Interface:	outside 🔽
Action: 💿	Permit 🔘 Deny
Source:	any 💮
Destination	192.168.5.3
Service: (tcp/smtp
Description:	
🗹 Enable L	ogging
Logging	Level: Default 💙
More Opt	ions
	OK Cancel

5. 配置靜態NAT以將172.16.1.3轉換為192.168.5.3轉到Configuration > Firewall > NAT Rules > Add Static NAT Rule以新增靜態NAT條目。



選擇Original Source和Translated IP

address及其關聯的介面,然後按一下OK完成靜態NAT規則的配置。

🚰 Add Static NAT	Rule	0
Original		
Interface:	DMZ	~
Source:	172.16.1.3	
Translated		
Interface: (outside	~
💿 Use IP Address:	192.168.5.3	-
🚫 Use Interface If	Address	
Port Address Translati	on (PAT)	
Enable Port A	ddress Translation (PAT)	
Protocol:		
Original Port:		
Translated Po	d)	
Constanting Control		
Lonnection Settin	gs	Ť
		-

:

:

Config	uration > Firewa	all > NAT Rules Delete ★ 🐇 🐰 🞚	🗈 🏛 - 🛛 Q. Find	Per Diagram	Packet Trace		
#	Туре	Original	Original			Translated	
		Source	Destination	Service	Interface	Address	
DM2	:						
1	• Static	3 172.16.1.3			outside	3 192.168.5.3	
2	• • Static	I 172.16.1.5			outside	192.168.5.5	
3	Static	172.16.1.4			outside	192.168.5.4	

此圖說明<u>範例</u>一節中列出的所有三個存取規則

#	Enabled	Source	Destination	Service	Action
ə 🦊 I	OMZ (2 implicit	incoming rules)	Paste		
1		🏟 any	Any less secure ne	IP ip	🖌 Permit
2		🏟 any	🏟 any	IP/ ip	🕴 Deny
i 🦊 i	nside (2 implic	it incoming rules)			
1		🧼 any	Any less secure ne	IP ip	🖌 Permit
2		🧼 any	🏟 any	IP/ ip	🕴 Deny
i 🥵 🗄	manage (2 imp	licit incoming rules)			
1		🏟 апу	Any less secure ne	IP ip	🖌 Permit
2		🍥 any	🏟 any	JE> ip	🕴 Deny
a 🥵	outside (4 inco	ming rules)			
1	V	🧼 any	192.168.5.3	smtp	🖌 Permit
2	\checkmark	🏟 any	192.168.5.5	100 https	🖌 Permit
3	V	🦛 any	A 192.168.5.4	🚥 domain	💉 Permit
4		 any 	 any 	IP/ ip	🔞 Deny

<u>驗證</u>

您可以使用某些show命令進行驗證,如下所示:

- show xlate 顯示當前轉換資訊
- show access-list 顯示訪問策略的命中計數器
- show logging 顯示緩衝區中的日誌。

<u>輸出直譯器工具</u>(僅供<u>已註冊</u>客戶使用)(OIT)支援某些**show**命令。使用OIT檢視**show**命令輸出的分析 。

<u>疑難排解</u>

目前尚無適用於此組態的具體疑難排解資訊。

相關資訊

- PIX/ASA 7.x:啟用/禁用介面之間的通訊
- 使用nat、global、static、conduit和access-list命令的PIX 7.0和自適應安全裝置埠重定向(轉發)
- 在PIX上使用nat、global、static、conduit和access-list命令和埠重定向(轉發)
- PIX/ASA 7.x: 啟用FTP/TFTP服務配置示例
- PIX/ASA 7.x: 啟用VoIP(SIP、MGCP、H323、SCCP)服務配置示例
- PIX/ASA 7.x:DMZ上的郵件伺服器訪問配置示例
- 技術支援與文件 Cisco Systems