ASA 8.2: [هيجوتلا ةداع]) ذفنملا ميجوت ةداع]) ASA 8.2: [و Global و Static و Access و Access مادختساب ASDM مادختساب ASDM

المحتويات

<u>المقدمة</u> المتطلبات الأساسية المتطلبات المكونات المستخدمة الاصطلاحات الرسم التخطيطي للشبكة السماح بالوصول الصادر <u>السماح للمضيفين الداخليين بالوصول إلى الشبكات الخارجية باستخدام NAT</u> السماح للمضيفين الداخليين بالوصول إلى الشبكات الخارجية باستخدام PAT تقييد الوصول إلى الشبكات الخارجية للمضيفين الداخليين السماح بحركة المرور بين الواجهات ذات مستوى الأمان نفسه السماح للمضيفين غير الموثوق بهم بالوصول إلى الأجهزة المضيفة على شبكتك الموثوق بها تعطيل NAT للمضيفين/الشبكات المحددة اعادة توجبه المنفذ (اعادة توجبه) باستخدام الحالات الحد من جلسة TCP/UDP باستخدام ثابت قائمة الوصول المستندة الى الوقت معلومات ذات صلة

<u>المقدمة</u>

يوضح هذا المستند كيفية عمل إعادة توجيه المنفذ على جهاز الأمان القابل للتكيف (ASA) من Cisco باستخدام ASDM. وهو يتناول التحكم في الوصول لحركة المرور من خلال ASA وكيفية عمل قواعد الترجمة.

المتطلبات الأساسية

<u>المتطلبات</u>

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- <u>نظرة عامة على NAT</u>
- <u>PIX/ASA 7.x: إعادة توجيه المنفذ</u>

<u>المكونات المستخدمة</u>

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- 8.2 الإصدار، Cisco 5500 Series ASA
 - Cisco ASDM، الإصدار 6.3

ملاحظة: يعمل هذا التكوين بشكل جيد من برنامج Cisco ASA الإصدار 8.0 إلى 8.2 فقط، نظرا لعدم وجود تغييرات رئيسية في وظيفة NAT.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

<u>الاصطلاحات</u>

راجع <u>اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.</u>

<u>الرسم التخطيطي للشبكة</u>



172.18.10.0/24

مخططات عنونة IP المستخدمة في هذا التكوين غير قابلة للتوجيه من الناحية القانونية على الإنترنت. وهي عناوين1918 RFC التي تم استخدامها في بيئة مختبرية.

<u>السماح بالوصول الصادر</u>

يصف الوصول الصادر الاتصالات من واجهة مستوى أمان أعلى إلى واجهة مستوى أمان أقل. وهذا يشمل الاتصالات من الداخل إلى الخارج، ومن الداخل إلى المناطق المجردة من السلاح (المنطقة المجردة من السلاح)، والمنطقة المجردة من السلاح إلى الخارج. كما يمكن أن يتضمن ذلك إتصالات من DMZ إلى آخر، طالما كانت واجهة مصدر الاتصال تحتوي على مستوى أمان أعلى من الوجهة.

لا يمكن لأي اتصال المرور عبر جهاز الأمان دون تكوين قاعدة ترجمة. ويطلق على هذه الميزة <mark>عنصر تحكم nat</mark> . توضح الصورة الموضحة هنا كيفية تعطيل هذا الإجراء من خلال ASDM للسماح بالاتصالات عبر ASA دون أي ترجمة للعنوان. ومع ذلك، إذا كان لديك أي قاعدة ترجمة تم تكوينها، فإن تعطيل هذه الميزة لا يظل صالحا لجميع حركات المرور وستحتاج إلى إستثناء الشبكات بشكل صريح من ترجمة العنوان.

* Type Source Destination Service In	-	Turne	Original			Tra
	#	туре	Source	Destination	Service	Inte
	<		Tell ¹			

<u>السماح للمضيفين الداخليين بالوصول إلى الشبكات الخارجية باستخدام NAT</u>

أنت يستطيع سمحت مجموعة من الداخل مضيف/شبكة أن ينفذ العالم خارجي ب يشكل الحركي nat قاعدة. ومن أجل تحقيق ذلك، يلزمك تحديد العنوان الحقيقي للمضيفين/الشبكات التي سيتم منحها حق الوصول ومن ثم يتعين تعيينها إلى تجمع من عناوين IP المترجمة.

أتمت هذا steps in order to سمحت داخلي مضيف منفذ إلى شبكة خارجية مع NAT:

1. انتقل إلى التكوين > **جدار الحماية>قواعد NAT**، انقر **إضافة**، ثم أختر **خيار إضافة قاعدة NAT الديناميكية** لتكوين قاع<u>د</u>ة NAT



الديناميكية.

2. أخترت الإسم من القارن إلى أي المضيف حقيقي يكون ربطت. أخترت العنوان حقيقي من المضيف/شبكة

يستعمل ال **تفاصيل** زر في **المصدر**

Interface:	nside	M	
Source:			
anslated —			
Select a glob	al pool for dynamic translat	ion.	
Pool ID	Interface	Addresses Pool	
		Same as original address (identity)	
0	(outbound)	Same as original address (identicy)	
0	(outbound) (inbound)	Same as original address (identity)	
[0	(outbound) (inbound)	Same as original address (identity)	
0	(outbound) (inbound)	Same as original address (identity)	

3. في هذا المثال، تم تحديد *الشبكة الداخلية* بالكامل. انقر فوق **موافق** لإكمال التحديد.

Vame 1 IPv4 Network Object any 0 Conside Manage Dutside Conside Conside	IP Address cts 0.0.0.0 172.16.11.0 10.77.241.64	Netmask 0.0.0.0	Description	Object NAT Ac
Pv4 Network Object	tts 0.0.0.0 172.16.11.0 10.77.241.64	0.0.0.0		
	0.0.0.0 172.16.11.0 10.77.241.64	0.0.0.0		
	172.16.11.0 10.77.241.64	255 255 255 0		
- 📸 manage	10.77.241.64	1200-200-200-0		
- 🛃 outside 2		255.255.255.192		
. 8 20.1.1.10	209.165.200.0	255.255.255.224		
	20.1.1.10	255.255.255.255		
- 🔳 172.16	172.16.11.1	255.255.255.255		
- 🖪 172.16	172.16.11.10	255.255.255.255		
	172.16.12.2	255.255.255.255		
	209.165.200.10	255.255.255.255		

4. انقر فوق **إدارة** لتحديد تجمع عناوين IP التي سيتم تعيين الشبكة الحقيقية لها.

rce:	nside-network/24		
abed			
oct a glob	al pool for dynamic translati	on.	
ool ID	Interface	Addresses Pool	
0	(outbound)	Same as original address (identity)	
0	(inbound)	Same as original address (identity)	(
			Manage

5. طقطقة يضيف in order to فتحت الإضافة شامل عنوان بركة

Manage G	lobal Pool	epannye olangeolangeoletik (https://instanceoletika	
Add 🛒	Edit 🎬 Delete		
Pool ID	Interface	Addresses Pool	
	ОК	Cancel Help	

6. أخترت **النطاق** خيار وعينت البداية والنهاية عنوان مع المخرج قارن. عينت أيضا، فريد بركة id وطقطقة **يضيف** in order to أضفت هذا إلى العنوان بركة. طقطقة **ok** in order to رجعت إلى الإدارة بركة شامل نافذة.

Interface:	outside		*		
Pool ID:	10				
IP Addr	esses to Add ge				Addresses Pool
Start	ing IP Address:	209.165.200.20			
Endin	ng IP Address:	209.165.200.40			
Netm	ask (optional):	255.255.255.192		Id >>]]	
O Port	: Address Trans idress:	lation (PAT)		Delete	
Netm	ask (optional):				
O Add	Address Trans ress of the inte	lation (PAT) using IP rface			

7. طقطقة **ok** in order to رجعت إلى الإضافة حركي nat قاعدة

ool ID	Interface	Addresses Pool
10	outside	g <mark>8</mark> 209.165.200.20 - 209.165.200.40

8. طقطقة **ok** in order to أتمت الحركي nat قاعدة تشكيل.

nterface:	inside	~	
iource:	inside-network/24		
nslated - ielect a gl	obal pool for dynamic translat	ion.	
Pool ID	Interface	Addresses Pool	
0	(outbound)	Same as original address (identity)	
0	(inbound)	Same as original address (identity)	
10	outside	209.165.200.20 - 209.165.200.40	Manage

9. انقر فوق **تطبيق** لتفعيل التغييرات.**ملاحظة:** لا يتم تحديد خيار **تمكين حركة مرور البيانات عبر جدار الحماية بدون ترجمة**

		Original			Translated		
*	Туре	Source	Destination	Service	Interface	Address	Service
insi	de						
	Dynamic	inside-network/24			outside	209.165.200.20 - 209.165.200.40	
						-	

هذا هو إخراج واجهة سطر الأوامر (CLI) المكافئ لتكوين ASDM هذا:

nat-control global (outside) 10 209.165.200.20-209.165.200.40 netmask 255.255.255.192 nat (inside) 10 172.16.11.0 255.255.255.0

وفقا لهذا التكوين، ستتم ترجمة الأجهزة المضيفة في شبكة 172.16.11.0 إلى أي عنوان IP من تجمع NAT، 209.165.200.20-209.165.200.40. هنا، معرف تجمع NAT مهم جدا. أنت يستطيع عينت ال نفسه nat بركة إلى آخر داخلي/dmz شبكة. إذا كان التجمع الذي تم تعيينه يحتوي على عناوين أقل من المجموعة الحقيقية، يمكن أن تنفذ العناوين إذا كان مقدار حركة المرور أكثر من المتوقع. بالنتيجة، أنت يستطيع حاولت طبقت ضرب أو أنت يستطيع حاولت أن يحرر العنوان موجود بركة أن يمدده.

ملاحظة: أثناء إجراء أي تعديل على قاعدة الترجمة الموجودة، لاحظ أنك تحتاج إلى إستخدام الأمر <u>clear xlate</u> لتفعيل هذه التعديلات. وإلا، فسيظل الاتصال الموجود السابق موجودا في جدول الاتصال حتى ينتهي. توخى الحذر عند إستخدام الأمر clear xlate، لأنه ينهي الاتصالات الموجودة على الفور.

<u>السماح للمضيفين الداخليين بالوصول إلى الشبكات الخارجية باستخدام PAT</u>

إن يريد أنت داخل مضيف أن يشارك عنوان عام وحيد للترجمة، استعملت ضرب. إن **العالمي** يعين بيان واحد عنوان، أن عنوان يكون ميناء يترجم. يسمح ال ASA واحد ميناء ترجمة لكل قارن وأن ترجمة يساند ما يصل إلى 65،535 **نشط** كائن إلى العنوان شامل وحيد.

أتمت هذا steps in order to سمحت داخلي مضيف منفذ إلى شبكة خارجي مع ضرب:

1. انتقل إلى التكوين > **جدار الحماية>قواعد NAT**، انقر **إضافة**، ثم أختر **خيار إضافة قاعدة NAT الديناميكية**

⊕ A	dd 🗕 🛒 Edit 📋 Delete 🛧 🗲 .	<u>, n</u>
1	Add Static NAT Rule	
눼	Add Dynamic NAT Rule	
	Add NAT Exempt Rule	
Ω,	Add Static Policy NAT Rule	
ø	Add Dynamic Policy NAT Rule	
*	Insert	
4	Insert After	ddroc

لتكوين قاعدة NAT الديناميكية.

2. أخترت الإسم من القارن إلى أي المضيف حقيقي يكون ربطت. أخترت العنوان حقيقي من المضيف/شبكة يستعمل ال **تفاصيل** زر في **المصدر** مجال، واخترت **داخل شبكة**. طقطقة **يدير** in order to عينت ال يترجم عنوان

terface:	nside		
ource:	nside-network/24		
dated			
elect a clot	al pool for dupamic translat	inn	
Pool ID	Interface	Addresses Pool	
0	(outbound)	Same as original address (identity)	
0	(inbound)	Same as original address (identity)	Mapage
			manaye.

	Interface	Addresses Real	
0010	Incertage	Addresses Publ	

4. أخترت **الأيسر عنوان ترجمة (ضرب) يستعمل عنوان من القارن** خيار، وطقطقة **يضيف** in order to أضفت هو إلى العنوان بركة. لا تنس تعيين معرف فريد لتجمع عناوين NAT

arrace:	oucside	M				
ID:	20					
P Addre	esses to Add		Ť	Addresse	s Pool	
Ran	ge		1	w outsid	e	(11.11.11.11.11.11.1
Starti	ng IP Address:					
Endin	g IP Address:		2			
Netm	ask (optional):		Add >>			
Port	Address Translation (PAT)	<< Delete	\neg		
IP Ad	dress:					
Netm	ask (optional):					
Port	Address Translation (PAT) using IP				
Add	ress of the interface					

5. كما هو موضح هنا هو تجمع العناوين الذي تم تكوينه مع الواجهة الخارجية كعنوان متاح فقط في هذا التجمع. طقطقة **ok** in order to رجعت إلى الإضافة حركي nat قاعدة

	Pool ID	Interface	Addresses Pool
	20	outside	🔤 outside
		ОК	Cancel Help
		ОК	Cancel Help
		ОК	Cancel Help فوق
Dunamic NAT	Pulo	OK	Cancel Help فوق
Dynamic NAT	Rule	OK	Cancel Help فوق

Translated
Select a global pool for dynamic translation.

Pool ID	Interface	Addresses Pool	
0	(outbound)	Same as original address (identity)	
0	(inbound)	Same as original address (identity)	
20	outside	outside	Manage
onnection	Settings		*

7. تظهر قاعدة NAT الديناميكية التي تم تكوينها هنا في جزء التكوين > جدار الحماية > قواعد .nat

	Type	Original			Translated	
- Type	Source	Destination	Service	Interface	Address	
insid	le					
1	Dynamic	inside-network/24			outside	outside

global (outside) 20 interface nat (inside) 20 172.16.11.0 255.255.255.0

<u>تقييد الوصول إلى الشبكات الخارجية للمضيفين الداخليين</u>

عندما لا يتم تحديد قواعد وصول، يمكن للمستخدمين من واجهة أمان أعلى الوصول إلى أي موارد مقترنة بواجهة أمان أقل. لتقييد وصول مستخدمين معينين إلى موارد معينة، أستخدم قواعد الوصول في ASDM. يوضح هذا المثال كيفية السماح لمستخدم واحد بالوصول إلى الموارد الخارجية (باستخدام FTP و SMTP و POP3 و HTTPS و WWW) وتقييد جميع المستخدمين الآخرين من الوصول إلى الموارد الخارجية.

ملاحظة: ستكون هناك قاعدة "رفض ضمني" في نهاية كل قائمة وصول.

أكمل الخطوات التالية:

1. انتقل إلى التكوين > **جدار <u>الحماية</u> > قواعد الوصول**، انقر فوق **إضافة**، واختر خيار **إضافة قاعدة الوصول** لإنشاء

+	Add Access Rule	
•	Add IPv6 Access Rule	
+	Insert	
÷	Insert After	(20)

إدخال قائمة وصول جديد 💶 💶

2. أخترت المصدر عنوان أن يكون سمحت في **المصدر** مجال. أخترت **any** كغاية، **داخلي** كالقارن، **يسمح** كالإجراء. أخيرا، طقطقت **ال details** زر في الخدمة مجال in order to خلقت TCP خدمة مجموعة ل ال يتطلب

هذا هو مخرج CLI المكافئ لتكوين PAT هذا:

🕵 Add Acc	ess Rule		
Interface: Action: 💿 I	inside 💌 Permit 🔿 Deny	,	
Source:	172.16.10.100		-
Destination	any		
Service:	ip		
Description:			
🗹 Enable L	ogging		
Logging I	evel: Default	X	
More Opt	ions		
		OK Cance	
	مة محموعة	، وبعد ذلك بختار ال TCP خد	ميناء. 3. طقطقة يضيف
	Brow	se Service	
		dd 🗸 🛒 Edit 💼 Delete 🔍 🔍	Where U:
	<u></u>	Service Group	
	TOP	TCP Service Group	rce Po
	<u>101</u>	UDP Service Group	
		TCP-UDP Service Group	
	1089- 11-	ICMP Group Protocol Group	
		🕹 eigrp eigrp	

خيار. 4. أدخل اسما لهذه المجموعة. أخترت كل من ال يتطلب ميناء، وطقطقة **يضيف** in order to نقلتهم إلى الأعضاء

sisting Service/Service Group:		Members in Group:
Name		Name
- TCP Service Groups	~	no ftp
RDP		
-Predefined		
- ISP ad	HI .	
- ISP bgp		
199> chargen		
- KB> cifs	-See 1	
- 100 obrix-ica	En	
- 190 ctiqbe	Add	
- 100 daytime	<< R6	emove
··· 19> discard		
182> domain		
rse echo		
- ISP exec		
199> finger		
🚥 ftp-data		
- 192 gopher	3	
reate new member:		

5. يجب أن ترى جميع المنافذ المحددة في الحقل الأيمن. طقطقة **ok** in order to أتمت الخدمة ميناء يحدد

isong service/service Group;			Members in Group:
Vame			Name
- 🚥 nfs	~		Top ftp
102> nntp			- Itp-data
- 100- pcanywhere-data			nttp
🚾 pim-auto-rp			ig notps
100 pop2			ma cmto
- 10 pptp			- tes since
100> rsh			
100> rtsp		Add >>	
top sip	_		
III sqinet		<< Kellifiae	
10 ssh			
- top sunrpc			
tacacs			
- In taleat			
IN CONC.			
top whois			

.OK

	-		-		
10.00	BICO	LUC P	NP.	Րտ	C P
1000	010				
10000	-		-		-

ame	Protocol	Source Ports	Destination Ports	ICMP Type	Description
🔳 🚾 Permit-1	tcp				
ISE ftp	tcp	default (1-65535)	21		
ttp-dal	a top	default (1-65535)	20		
- ter http	tcp	default (1-65535)	80		
- 😥 https	tcp	default (1-65535)	443		
- KP pop3	tcp	default (1-65535)	110		
- TCP smtp	tcp	default (1-65535)	25		
E RDP	tcp				
Predefined					
- 100- aol	tcp	default (1-65535)	5190		
19> bgp	tcp	default (1-65535)	179		
- 102> chargen	tcp	default (1-65535)	19		
- 100 cifs	tcp	default (1-65535)	3020		
- 😰 citrix-ica	tcp	default (1-65535)	1494		
- 19 ctiqbe	tcp	default (1-65535)	2748		
🚽 😰 daytime	tcp	default (1-65535)	13		
- 10 discard	tcp	default (1-65535)	9		
- 100 domain	tcp	default (1-65535)	53		
100> echo	tcp	default (1-65535)	7		
102> exec	tcp	default (1-65535)	512	Real Property in the second	
ected Service					
Sendre ->	0				

7. طقطقة **ok** in order to أتمت

nterface:	inside 💌
Action: ()	172 16 10 100
Destination	any
Service:	Permit-172.16.10.100
Description:	
Enable L	ogging Level: Default
More Opt	ions
. Nic op.	

8. يمكن مُلاحظة قاعدة الوصول التي تم تكوينها أسفل الواجهة **الداخلية** في جزء التكوين > جدار الحماية > قواعد الوصول.

Configur	ration > Fire	wall > Access Rules	X 暗 聞 - O. Find 回す	Diagram	Export •	- 🔥 Clear	Hits 🗐	Show Log 🥥	🗇 Pa
#	Enabled	Source	Destination	Service		Action	Hits	Logging	1
🛱 🥵 i	inside (2 incom	ing rules)							
1	V	凰 172.16.10.100	🔹 any	TO Perr	nit-172.1	🕜 Permit			
2	1	any	any	IP ip	TCP Grou	o: Permit-1	72.16.10.	100	
a 🕬	inside IPv6 (2 i	mplicit incoming rules)			TCP: ftp ((21)			
1		any	Any less secure ne	IP ID	TCP: ftp-	data (20)			
2		any	any	It ip	TCP: http	(80)			
a 🛤	manage (2 imp	licit incoming rules)			TCP: pop	3 (110)			
1		🧼 any	Any less secure ne	IP ip	TCP: smtp	(25)			

9. لسهولة الاستخدام، يمكنك أيضا تحرير مجموعة خدمة TCP مباشرة على الجزء الأيمن في علامة التبويب **خدمات**. انقر فوق **تحرير** لتعديل مجموعة الخدمات هذه ميلشية

> Fin	ewall > Access Rules							0	Addresses Services Time Ranges
Edit	î Delete 🛧 🗲	🖁 🛍 - 🛛 Q, Find 🖽	Diagram 🔐 Export	- Ø Clear	Hits 🔳	Show Log	Packet	frace	Services d 4 X
abled	Source	Destination	Service	Action	Hits	Logging	Time	Description	What + H Ear Delete Q where used
(2 inco	ning rules)								Filter: Filter/Clear
	172.16.10.100	4 any	30 Permit-172.1	🖌 Pernit		Lanna	Lanses	1 Summer and	Name
	any	any	.Æ∕ip	O Deny				Implicit rule	TCP Service Groups
IPv6 (2	implicit incoming rules)								🗖 📅 Permt-172.16.10.100
	any	Any less secure ne	.m. ip	🖌 Pernit				Implicit rule: Per	- Mar Rep
	any	any	30 lp	(3 Deny				Implicit rule	- see Rp-data
je (2 im	plicit incoming rules)								- se http
	any	Any less secure ne	12 ip	🖌 Pernit				Implicit rule: Per	🗰 https
	🏟 απγ	any	32 ip	O Deny				Implicit rule	
10 IPv6	(2 implicit incoming rules)								the smtp
	any	Any less secure ne	Je ip	🖌 Pernit				Implicit rule: Per	B TRI RDP
	 any 	any	JE ip	(3 Deny				Implicit rule	Predefined
s (2 inc	oming rules)								100 ad
2	20.1.1.10	A 209.165.200.10	RDP	🖌 Permit		0			18 bgp
	any	any any	IE-ip	O Deny				Implicit rule	- 100- chargen

10. يعيد التوجيه مرة أخرى إلى نافذة تحرير مجموعة خدمة TCP. قم بإجراء التعديلات استنادا إلى متطلباتك،

وانقر فوق **موافق** لحفظ التغييرات.

• Exis	ting Service/Service Group:			Members in Group:
Na	ame			Name
P-	TCP Service Groups	~		The second second
	RDP			ttp-data
8.	Predefined			ise http
	- 102> aol			- 190 https
	- IO> bgp			ter pops
-	- 10 chargen			smtp
	to cits			
-	- IOF citrix-ica	- 1	Add >>	1
	- 102> ctiqbe			
	-10 daytime		< Remove	
	discard			
_	domain	_		
	echo			
-	exec			
-	100 ninger			
-	- 100 gopner			
	Nor haza	~		
O Cre Part	ate new member: /Range:			
	ОК		Cancel	Help
				ىما بلى عرض كامل ل
				ASDN:
DM 6.3 for ASA Tools Words	- 10.77.241.515			
Bentarmon	Mondauro - Save Q tolesh (tak () Help			cisco
Deleta 🖉 Cornes	Configuration > Forward > Access Subs. Anno. (Configuration > Forward > Access Subs.	ann Stort - 6	Char Mrs. (1) Security of	CI Addresses Services Time Ranges
ð	Enabled Source Destination	Service Act	tion Hits Logging	Time Description
a la	 A mode (* notang rate) 	West 1711		

هذا هو تكوين CLI المكافئ:

port-object eq ftp port-object eq ftp-data port-object eq www port-object eq www port-object eq pop3 port-object eq smtp ! access-list inside_access_in extended permit TCP host 172.16.10.100 any object-group Permit-172.16.10.100 ! access-group inside_access_in in interface inside ! ! MSDM J (GUI) ل ASDM

<u>السماح بحركة المرور بين الواجهات ذات مستوى الأمان نفسه</u>

يوضح هذا القسم كيفية تمكين حركة المرور داخل الواجهات التي تحتوي على نفس مستويات الأمان.

تصف هذه التعليمات كيفية تمكين الاتصال بين الواجهات.

هذا سيكون مفيد ل VPN حركة مرور أن يدخل قارن، غير أن بعد ذلك وجهت خارج ال نفسه قارن. قد تكون حركة مرور VPN غير مشفرة في هذه الحالة، أو قد يتم إعادة تشفيرها لاتصال VPN آخر. انتقل إلى **التكوين>إعداد الجهاز** > **الواجهات**، واختر **تمكين حركة مرور البيانات بين جهازين مضيفين أو أكثر متصلين بنفس خيار الواجهة**.

Interface	Name	Enabled	Security Level	IP Address	Subnet Mask Prefix Length	Redur
Ethernet0/0	outside	Yes	0	209.165.200.2	255.255.255.192	No
Ethernet0/1	inside	Yes	100	172.16.11.10	255.255.255.0	No
Ethernet0/2	manage	Yes	90	10.77.241.115	255.255.255.192	No
Ethernet0/3		No				No
<						
Enable traffic betw	een two or more inter een two or more host	faces which a s connected t	re configured o the same int	with same security le	vels	

تصف هذه التعليمات كيفية تمكين الاتصال بين الواجهة.

وهذا مفيد للسماح بالتواصل بين الواجهات ذات مستويات الأمان المتساوية. انتقل إلى **التكوين>إعداد الجهاز > الواجهات**، واختر **تمكين حركة مرور البيانات بين واجهات أو أكثر تم تكوينها باستخدام خيار مستويات الأمان نفسها**.

Interface	Name	Enabled	Security Level	IP Address	Subnet Mask Prefix Length	Redu
Ethernet0/0	outside	Yes		0 209.165.200.2	255.255.255.192	No
Ethernet0/1	inside	Yes	10	0 172.16.11.10	255.255.255.0	No
Ethernet0/2	manage	Yes	9	0 10.77.241.115	255.255.255.192	No
Ethernet0/3		No				No
<						
Enable traffic betw Enable traffic betw	veen two or more inter veen two or more host	faces which a s connected t	re configured o the same in	with same security le terface	Apply Res	æt]

هذا ال يماثل CLI ل كلا من هذا عملية إعداد:

same-security-traffic permit intra-interface
same-security-traffic permit inter-interface

<u>السماح للمضيفين غير الموثوق بهم بالوصول إلى الأجهزة المضيفة على</u> شبكتك الموثوق بها

يمكن تحقيق ذلك من خلال تطبيق ترجمة ثابتة ل NAT وقاعدة وصول للسماح لهذه الأجهزة المضيفة. أنت تحتاج إلى تكوين هذا كلما رغب مستخدم خارجي في الوصول إلى أي خادم موجود في شبكتك الداخلية. سيكون للخادم الموجود في الشبكة الداخلية عنوان IP خاص غير قابل للتوجيه على الإنترنت. ونتيجة لذلك، يلزمك ترجمة عنوان IP الخاص هذا إلى عنوان IP عام من خلال قاعدة NAT ثابتة. افترض أن لديك خادما داخليا (172.16.11.5). in order to جعلت هذا عمل، أنت تحتاج أن يترجم هذا نادل خاص نادل ون الى عام مار الريظ من مالي منالي المثال من المالي من الثابت ثنائي الإتجاه لترجمة المالي المالي الى 209.165.2005.

لا يتم عرض القسم الخاص بالسماح للمستخدم الخارجي بالوصول إلى خادم ويب هذا من خلال تنفيذ قاعدة وصول هنا. يتم عرض مقتطف CLI موجز هنا للفهم الخاص بك:

access-list 101 permit TCP any host 209.165.200.5 لمزيد من المعلومات، ارجع إلى إضافة قائمة وصول أو تعديلها من خلال واجهة المستخدم الرسومية (GUI) ل ASDM.

ملاحظة: يسمح تحديد الكلمة الأساسية "any" لأي مستخدم من العالم الخارجي بالوصول إلى هذا الخادم. أيضا، إذا لم يتم تحديده لأي منافذ خدمة، يمكن الوصول إلى الخادم على أي منفذ خدمة حيث يظل هذا المنفذ مفتوحا. توخ الحذر عند التنفيذ، وينصح بتقييد الإذن إلى المستخدم الخارجي الفردي وأيضا إلى المنفذ المطلوب على الخادم.

أتمت هذا steps in order to شكلت الساكن إستاتيكي nat:

1. انتقل إلى التكوين > جدار الحماية>قواعد NAT، وانقر إضافة، واختر إضافة قاعدة NAT

4 A	idd 🗸 🛒 Edit 📋 Delete 🛉 🗲	2
1 1	Add Static NAT Rule	
	Add Dynamic NAT Rule	D
Ð	Add NAT Exempt Rule	
Ω.	Add Static Policy NAT Rule	prk/24
(D	Add Dynamic Policy NAT Rule	
+	Insert	
4	Insert After	

الثابتة.

				.0	ատո
قارن، وطقطقة	ن مع هم	رجم عنوار	طبيعي وال يت	، العنوان أهلي	2. عينت

Interface:	inside	~
Source:	172.16.11.5	
anslated	2	
Interface:	outside	~
(Use IP Address:	209.165.200.5	
Use Interface IP	Address	
Use Interface IP ort Address Translation	Address n (PAT) dress Translation (PAT)	
Use Interface IP ort Address Translation Enable Port Ad Protocol:	Address n (PAT) dress Translation (PAT) TCP OUDP	
O Use Interface IP ort Address Translation Enable Port Ad Protocol: Original Port:	Address n (PAT) dress Translation (PAT) TCP OUDP	
Use Interface IP ort Address Translation Enable Port Ad Protocol: Original Port: Translated Port	Address n (PAT) dress Translation (PAT) TCP UDP	

3. أنت يستطيع رأيت ال يشكل ساكن إستاتيكي nat مدخل هنا. طقطقة **يطبق** in order to أرسلت هذا إلى ال ASA.

incide (1 Sta	pe	Source	-			
inside (1 Sta			Destination	Service	Interface	Address
monare (a pro	atic rules, 1 D	ynamic rules)				
1	Static	5 172.16.11.5			outside	209.165.200.5
2 111	Dynamic	inside-network/24			outside	utside 🔤
		in				

هذا مثال موجز على واجهة سطر الأوامر (CLI) لتكوين ASDM هذا:

static (inside,outside) 209.165.200.5 172.16.11.5 netmask 255.255.255.255 !

<u>تعطيل NAT للمضيفين/الشبكات المحددة</u>

عندما تحتاج إلى إستثناء مضيفين أو شبكات معينة من NAT، أضف قاعدة إستثناء NAT لتعطيل ترجمة العنوان. وهذا يسمح للمضيفين المترجمين والبعيدين على حد سواء ببدء الاتصالات.

أكمل الخطوات التالية:

1. انتقل إلى التكوين > **جدار الحماية > قواعد nat**، وانقر **إضافة**، واختر إضافة قاعدة إستثناء



2. هنا، تم إستثناء الشبكة الداخلية 172.18.10.0 من ترجمة العنوان. تأكد من تحديد خيار **الاستثناء**. إتجاه إستثناء NAT له خياران:حركة المرور الصادرة إلى واجهات الأمان الأقلحركة المرور الواردة إلى واجهات الأمان العلياالخيار الافتراضي هو لحركة المرور الصادرة. طقطقة **ok** in order to أتمت

Interface:	inside	
Fourrou	172.19.10.0	
source:	172.10.10.0	
Destination:	any	
NAT Exer	mpt outbound traffic from interface '	INSIDE LO IONYEL SECURICY

ملاحظة: عند إختيار خيار

عدم الاستثناء، لن يتم إعفاء ذلك المضيف المعين من NAT وستتم إضافة قاعدة وصول منفصلة باستخدام الكلمة الأساسية "deny". يفيد ذلك في تجنب الأجهزة المضيفة المحددة من إستثناء NAT حيث أن الشبكة الفرعية الكاملة، باستثناء هذه الأجهزة المضيفة، ستكون معفاة من NAT.

3. يمكنك رؤية قاعدة إستثناء NAT للاتجاه الصادر هنا. طقطقة **يطبق** in order to أرسلت التشكيل إلى ال ASA.

#	Туре	Original			Translate
		Source	Destination	Service	Interface
🗉 insid	de (1 Exempt rules,	1 Static rules, 1 Dynamic rule	es)		
1	🚟 Exempt	172.18.10.0	🐔 any	1	(outbound)
2	1 Static	3 172.16.11.5		-	outside
3	Dynamic	📸 inside-network/24			outside
<					
] Ena	ble traffic through t	he firewall without address	translation		

access-list inside_nat0_outbound extended permit ip host 172.18.10.0 any

nat (inside) 0 access-list inside_nat0_outbound

4. هنا يمكنك رؤية كيفية تحرير قاعدة إستثناء NAT لاتجاهها. انقر فوق **موافق**" لكي يسري هذا

1.00	ga i cai						
Ir	iterface:	inside					
5	ource:	172.18.10	.0		-		
D	estination:	any					
NAT	Exempt Di	rection					
(NAT Exer	mpt outbour	nd traffic from inte	rface 'inside' to lov	er security inte	erfaces (default)	
	~						
(NAT Exer	mpt inbound	traffic from interf	ace 'inside' to high	er security inte	rfaces	
Des	cription						
Des	enpoon						
L							-
		-					
			the second se				
		f	OK	Cancel	Help		
			ОК	Cancel	Help		
			ОК	Cancel	Help		نیار.
			ок) Cancel م إلى	Help لإتجاہ تم تغيير	الآن أن ترى أن ال	نیار. کنك ا
			ок) Cancel	Help لإتجاه تم تغيير	الآن أن ترى أن ال	تیار. کنك ا <i>ارد</i> .
uratio	on > Firew	all > NAT I	ок Rules	Cancel (Help لإتجاه تم تغيير	الآن أن ترى أن ال	تیار. کنك ا <i>ار</i> د.
uratio	on > Firew G Edt 🗍	all > NAT I	ок Rules ⊁ ∓ & №	د إلى م إلى Q Find (Help لإتجاه تم تغيير Diagram 🥰	الآن أن ترى أن ال Packet Trace	تیار. کنك ا <i>ارد</i> .
uratio id •	on > Firew G Edt î	<mark>all > NAT I</mark> Delete	ок Rules 7 🗲 👗 🗎	د إلى ه إلى ه إلى جind (Help لإتجاه تم تغيير Diagram 🔍	الآن أن ترى أن ال Packet Trace Translated	تیار. کنك ا <i>ارد</i> .
<mark>uratio</mark> Id •	o <mark>n > Firew</mark> Ø Edit M Type	all > NAT I Delete	ок Rules F + 🔏 🖻 ginal	Cancel (ه إلى ه إلى الم	Help لاتجاہ تم تغییر Diagram	الآن أن ترى أن ال Packet Trace Translated	ییار. کنك ا <i>ار</i> د.
uratio id •	on > Firew C Edit () Type Evernot a de	all > NAT I Delete ori Sou	ок Rules Э 🗲 👗 🗎 ginal urce	Cancel (م إلى ه إلى Destination (Help لإتجاه تم تغيير Diagram Service	الآن أن ترى أن ال Packet Trace Translated Interface	نیار. کنك ا <i>اِر</i> د.
uratio id - ide (1	on > Firew C Edit () Type Exempt rule	all > NAT I Delete Ori Sou	OK Rules F ← & B ginal urce ules, 1 Dynamic rul 172-18-10-0	Cancel (م إلى ه إلى Destination (es)	Help لاتجاہ تم تغییر Diagram ع Service	الآن أن ترى أن ال Packet Trace Translated Interface	تیار. کنك ا <i>ا</i> رد.
uratio id - ide (1	on > Firew C Edit Type Exempt rule Exempt Static	all > NAT I Delete Sou Sou Souther I Souther	ОК Rules → ↓ & В ginal urce ules, 1 Dynamic rul 172,16,11,5	Cancel (م إلى Q Find (Destination les) الأ any	Help لإتجاه تم تغيير Diagram Service	الآن أن ترى أن ال Packet Trace Translated Interface (inbound) outside	تیار. کنك ا <i>ار</i> د.
ide (1	on > Firew C Edit () Type Exempt rule Exempt Static Conservation	all > NAT I Delete Ori Sou s, 1 Static r	OK Rules → ↓ & jinal urce ules, 1 Dynamic rul 172.18.10.0 172.16.11.5 adda aatwaak/24	Cancel (الی Q Find (Destination les)	Help لاتجاہ تم تغییر Diagram کی	الآن أن ترى أن ال Packet Trace Translated Interface (inbound) outside	ییار. کنك ا <i>ار</i> د.
uratio id - ide (1	on > Firew C Edit Type Exempt rule Static Dynamic	all > NAT I Delete Sou is, 1 Static r	ОК Rules → ↓ & ginal urce ules, 1 Dynamic rul 172.16.11.5 nside-network/24	Cancel (م إلى Q Find (Destination les) الأ any	Help لاتجاہ تم تغییر Diagram کی	الآن أن ترى أن ال Packet Trace Translated Interface (inbound) outside outside	تیار. کنك ا <i>ار</i> د.

طقطقة **يطبق** in order to ارسلت هذا CLI إنتاج إلى ال ASA:

access-list inside_nat0_outbound extended permit ip host 172.18.10.0 any !

nat (inside) 0 access-list inside_nat0_outbound outside

ملاحظة: من هذا، يمكنك أن ترى أنه تمت إضافة كلمة أساسية جديدة (خارج) إلى نهاية الأمر **nat 0**. دعات هذا سمة **خارجي nat**.

6. آخر طريق أُن يعجز nat من خلال تنفيذ هوية nat. هوية nat يترجم مضيف إلى ال نفسه عنوان. هنا مثال ساكن إستاتيكي عادي NAT، حيث المضيف (172.16.11.20) ترجمت إلى ال نفسه عنوان عندما هو يكون

Interface:	inside	~
Source:	172.16.11.20	
ranslated		
Interface:	outside	~
() Use IP Address:	172.16.11.20	
Enable Port Add Protocol: Original Port: Translated Port	TCP O UDP	
onnection Setting	s and a state of the	*

إعادة توجيه المنفذ (إعادة توجيه) باستخدام الحالات

إعادة توجيه المنفذ أو إعادة توجيه المنفذ هي ميزة مفيدة حيث يحاول المستخدمون الخارجيون الوصول إلى خادم داخلي على منفذ معين. in order to أتمت هذا، ال داخلي، يتلقى عنوان خاص، يكون ترجمت إلى عنوان عام أي بدوره يسمح منفذ للميناء خاص.

في هذا المثال، يريد المستخدم الخارجي الوصول إلى خادم SMTP، 209.165.200.15 على المنفذ 25. ويتحقق ذلك في خطوتين:

1. ترجمة خادم البريد الداخلي، 172.16.11.15 على المنفذ 25، إلى عنوان IP العام، 209.165.200.15 في المنفذ 25.

2. السماح بالوصول إلى خادم البريد العام، 209.165.200.15 على المنفذ 25.

عندما يحاول المستخدم الخارجي الوصول إلى الخادم، 209.165.200.15 في المنفذ 25، ستتم إعادة توجيه حركة مرور البيانات هذه إلى خادم البريد الداخلي، 172.16.11 15 في المنفذ 25.

1. انتقل إلى التكوين > **جدار الحماية>قواعد NAT**، وانقر **إضافة**، واختر إضافة قاعدة NAT



2. حدد المصدر الأصلي وعنوان IP المترجم مع الواجهات المرتبطة بها. أخترت **يمكن أيسر عنوان ترجمة (ضرب)**، عينت الميناء أن يكون أعدت، وطقطقة

rigenal	
Interface:	inside 💌
Source:	172.16.11.15
Franslated	
Interface:	outside 💉
💿 Use IP Address:	209.165.200.15
Port Address Translation	(PAT) ress Translation (PAT) TCP O UDP 25
Original Port:	
Translated Port:	25
Translated Port:	25

	Tune	Original			Translated		
	type	Source	Destination	Service	Interface	Address	Servic
1	🗂 Exempt	172.18.10.0	iany any		(outbound)		
2	🗐 No Exempt	3 172.20.10.10	any		(outbound)		
3	Static	172.16.11.15		RD smtp	outside	209.165.200.15	STR -
4	• Static	3 172.16.11.5		nin Trender	outside	209.165.200.5	
3							>

هذا هو مخرج واجهة سطر الأوامر (CLI) المكافئ:

```
!
static (inside,outside) TCP 209.165.200.15 smtp 172.16.11.15 smtp netmask
255.255.255.255
!
```

4. هذه هي قاعدة الوصول التي تسمح للمستخدم الخارجي بالوصول إلى خادم SMTP العام على

					TCP Group: smtp-access TCP: smtp (25)
3		any	any	IP ip	C Denv
2	V	🧐 any	🖳 209.165.200.15	smtp-ac	:cess 🛛 🧹 Permit
1	~	🖳 20.1.1.10	🖳 209.165.200.10	RDP	🖌 Permit
🥦 out	side (3 inc	oming rules)			
2		🇳 any	🧼 any	<u>⊥P</u> ∕ ip	🔕 Deny
1		🧼 any	🧼 Any less secure ne	IP IP	:209.165.200.1

ملاحظة: تأكد من إستخدام مضيفين محددين بدلا من إستخدام **أي** كلمة أساسية في مصدر قاعدة الوصول.

<u>الحد من جلسة TCP/UDP باستخدام ثابت</u>

يمكنك تحديد الحد الأقصى لعدد إتصالات TCP/UDP باستخدام القاعدة الثابتة. يمكنك أيضا تحديد الحد الأقصى لعدد الاتصالات الجنينية. الاتصال الجنيني هو اتصال في حالة نصف مفتوحة. وسيؤثر عدد أكبر من هذه العوامل على أداء نظام المحاسبة المستقل. وسيؤدي الحد من هذه الاتصالات إلى منع هجمات معينة مثل DoS و SYN إلى حد ما. للحصول على تخفيف كامل، يلزمك تحديد السياسة في إطار عمل ميزة "حماية مستوى الإدارة (MPF)"، والتي تتجاوز نطاق هذا المستند. للحصول على معلومات إضافية حول هذا الموضوع، ارجع إلى <u>التخفيف من هجمات الشيكة</u>.

أكمل الخطوات التالية:

1. انقر فوق علامة التبويب **إعدادات الاتصال،** وحدد القيم الخاصة بالحد الأقصى للاتصالات لهذه الترجمة

iginal	1992 -	-
Interface:	inside	
Source:	172.16.11.15	
Iranslated		-
Interface:	outside 💌	
💽 Use IP Address:	209.165.200.15	
O Use Interface IP	Address	
Port Address Translatio	n (PAT)	
Enable Port Ad	dress Translation (PAT)	
Protocol:		
Original Port:	smbp	
Translated Port	t: smtp	
Connection Setting	15	
Translate the D	NS replies that match the translation rule	
Randomize seg	uence number	
Maximum TCP Copt	pertions: 100	
Maximum LIDD Com		
Maximum ODP Conr	ecoons: 0	
	c Connections: 50	

2. تظهر هذه الصور حدود الاتصال لهذه الترجمة الثابتة المحددة:

🗣 Add 🗕 🖪 Edit 🥤	Delete 🛧 🗲	* 🖻 🛍 -	🔍 Find 🖭 Di	agram ऌ Packet Trace	
Original			Translated		
Source	Destination	Service	Interface	Address	Service
Static rules, 1 Dynamic	rules)				
A 172.18.10.0	any		(outbound)		
172.20.10.10	any		(outbound)		
₿ 172.16.11.15		tte smtp	outside	209.165.200.15	to smtp

DNS Rewrite	Max TCP Connections	Embryonic Limit	Max UDP Connections	Randomize Sequer
				5.1
	100	50	Unlimited	

هذا هو مخرج واجهة سطر الأوامر (CLI) المكافئ:

```
static (inside,outside) TCP 209.165.200.15 smtp 172.16.11.15 smtp netmask
TCP 100 50 255.255.255
```

<u>قائمة الوصول المستندة إلى الوقت</u>

!

يتعامل هذا القسم مع تنفيذ قوائم الوصول المستندة إلى الوقت باستخدام ASDM. يمكن تطبيق قواعد الوصول استنادا إلى الوقت. لتنفيذ هذا الإجراء، يلزمك تحديد نطاق زمني يحدد التوقيتات حسب اليوم/الأسبوع/الشهر/السنة. بعد ذلك، تحتاج إلى ربط هذا النطاق الزمني بقاعدة الوصول المطلوبة. يمكن تعريف النطاق الزمني بطريقتين:

1. مطلق - يحدد الفترة الزمنية مع وقت البدء ووقت الانتهاء.

2. دوري - يعرف أيضا باسم متكرر. تعريف الفترة الزمنية التي تحدث على فترات زمنية محددة. **ملاحظة:** قبل تكوين النطاق الزمني، تأكد من تكوين ASA بإعدادات التاريخ/الوقت الصحيحة لأن هذه الميزة تستخدم إعدادات ساعة النظام للتنفيذ. سيؤدي مزامنة ASA مع خادم NTP إلى نتائج أفضل بكثير.

أتمت هذا steps in order to شكلت هذا سمة من خلال ASDM:

1. أثناء تحديد قاعدة الوصول، انقر فوق زر **التفاصيل** في حقل النطاق

Source:	172.16.10.50
Deallochia	
Destination	any -
Service:	ip 🔄
Description:	
🕑 Enable L	ogging
Logging I	Level: Default 💽
More Opt	ions
Enable	Rule
Traffic Dire	ection: 🔘 In 💿 Out
Source Ser	vice: (TCP o
Logging In	terval: [300] seconds
Time Rang	e:
	OK Cancel Help
owse Time	Range
	1 Delete
Add Mr. Edt	and a started

2. انقر فوق **إضافة** لإنشاء نطاق زمني جديد. 3. قم بتحديد اسم النطاق الزمني، وحدد وقت البدء ووقت الانتهاء. وانقر فوق OK.

t Time —						End Time						
) Start no	w					O Never	end					
Start at						💿 End at	(inclusive)					
Month:	February	~	Day:	05 💌	Year: 2011 🛩	Month:	February	*	Day:	06 🛩	Year:	2011
										the second secon		
Hour: uning Time ou can fur art and st	14 e Ranges — ther constra op time spe	in the	Minute: active ti	00 💌	s range by specifying	Hour: recurring ranges.	16 The recurri	ng tim	Minute: e ranges	30 💌	tive with	in the
Hour: urring Tim ou can fur art and st	14 e Ranges — ther constra op time spe	in the	Minute: active ti	ne of this	s range by specifying	Hour: recurring ranges.	16 The recurri	ng tim	Minute: e ranges	30 💌	tive with	in the Add
Hour: urring Time ou can fur art and st	14 e Ranges — ther constra op time spe	in the	Minute: active ti	ne of this	s range by specifying	Hour: recurring ranges.	16 The recurri	ng tim	Minute: e ranges	30 💌	tive with	in the Add Edit
Hour: urring Tim ou can fur art and st	14 e Ranges — ther constra op time spe	in the	Minute: active ti	00 💌	s range by specifying	Hour: recurring ranges.	The recurri	ng tim	Minute: e ranges	30 💌		nin the Add Edit Delete
Hour: urring Tim ou can fur art and st	14 e Ranges — ther constra op time spe	in the	Minute:	00 💌	s range by specifying	Hour: recurring ranges.	The recurri	ng tim	Minute: e ranges	30 vil be ac		in the Add Edit Delete

4. يمكنكم رؤية النطاق الزمني هنا. انقر فوق **موافق** للعودة إلى الإطار "قاعدة إضافة

Name Res	Start Time 14:00 05 Fe	End Time	Recurring Entries	

5. يمكنك الآن أن ترى أن نطاق وقت تقييد الاستخدام قد تم ربطه بقاعدة الوصول

	📬 Add Access Rule
	Interface: inside v
	Action: O Permit () Deny
	Source: 172.16.10.50
	Destination any
	Service: lp -
	Description:
	Enable Logging Logging Level: Default
	More Options
	Inable Rule
	Traffic Direction: 🔘 In 💿 Out
	Source Service:
	Logging Interval: 300 seconds
	Time Range: Restrict-Usage 💟
وفقا لتكوين	هذه.
ر 2011/5/05 a :	قاعدة الوصول هذه، تم منع المستخدم في 172.16.10.50 من إستخدام أي موارد من الساعذ إلى الساعة 2011/16/06 الساعة 17/4.30. هذا هو مخرج واجهة سطر الأوامر (CLI) المكافى
	time-range Restrict-Usage absolute start 14:00 05 February 2011 end 16:30 06 February 2011 ! access-list inside access out extended deny ip host 172.16.10.50 any
	time-range Restrict-Usage ! access-group inside_access_out in interface inside
	فيما با مثلا عار كيفية تحديد نطاق نيم: المتكان النقا فمقا م: افة اتحديد نطاق نيم:

6. فيما يلي مثال على كيفية تحديد نطاق زمني متكرر. انقر فوق **إضافة** لتحديد نطاق زمني متكرر.

t Tree End Time End Time Start now Start at Month: Pebruary ♥ Day: 05 ♥ Year: 2011 ♥ Month: March ♥ Day: 06 ♥ Year: 2011 ♥ Hour: 00 ♥ Minube: 00 ♥ For example, use this option when you want the time range to be active every Monday through Thursday, from 8:00 through 16:59, only. Days of the Week © On these days of the week: ♥ Mon ♥ Tue ♥ Wed ♥ Thu ♥ Fri Sat Sun Daly End Time (Inclusive) Hour: 15 ♥ Minube 00 ♥ Hour: 15 ♥	Dance Marrier Dani	with I kage	
et Time End Time Start now Start at Month: rebruary Day: 05 Year: 2011 Month: March Day: 06 Year: 2011 Hour: 00 Minute: 00 Min	ie Kange Name: Kest	uict-osage	
Start now Image: Start at Image: Start at Month: February Day: 05 Year: 2011 Month: Month: Month: Image: Start at	art Time		End Time
 Start at Month: Pebruary → Day: 05 √ Year: 2011 → Hour: 00 → Minute: 00 → Min	◯ Start now		O Never end
Wonth: Petruary Day: 05 Year: 2011 Month: March Day: 06 Year: 2011 Hour: 00 Minute: 2011 Hour: 2011 Hour	 Start at 		End at (inclusive)
Hour: 00 Minute: 00 Minute: 30 ecurring Time Ranges You can further constrain the active time of this range by specifying recurring ranges. The recurring time ranges will be active within the start and stop time specified. Image: Start Time Image:	Month: February	🖌 🗹 Day: 05 🖌 Year: 2011 🖌	Month: March 💌 Day: 06 🛩 Year: 2011
ecuring Time Ranges You can further constrain the active time of this range by specifying recurring ranges. The recurring time ranges will be active within the start and stop time specified.	Hour: 00	Minute: 00 🖌	Hour: 00 Minute: 30 🛩
You can further constrain the active time of this range by specifying recurring ranges. The recurring time ranges will be active within the start and stop time specified.	ecurring Time Ranges		
Add Ede Ede Ede Ede Ede Ede Ede E	You can further const	rain the active time of this range by specifying n	ecurring ranges. The recurring time ranges will be active within the
Image: Specify days of the week and times on which this recurring range will be active Image: Specify days of the week and times on which this recurring range will be active Image: Specify days of the week and times on which this recurring range will be active Image: Specify days of the week and times on which this recurring range will be active Image: Specify days of the week and times on which this recurring range will be active every Monday through Thursday, from 8:00 through 16:59, only. Days of the Week Image: Every day Image: Weekdays Image: Weekdays Image: Image	scarc and scop cline sp	ecreu.	Add
Content Content			C. C
Add Recurring Time Range Specify days of the week and times on which this recurring range will be active For example, use this option when you want the time range to be active every Monday through Thursday, from 8:00 through 16:59, only. Days of the Week Every day Weekdays Weekdays On these days of the week: Mon V Tue V Wed V Thu V Fri Sat Sun Daly Start Time Hour 15 Minute 00 Minut			EUR
Add Recurring Time Range Specify days of the week and times on which this recurring range will be active For example, use this option when you want the time range to be active every Monday through Thursday, from 8:00 through 16:59, only. Days of the Week Every day Weekdays Weekdays Weekends On these days of the week: Mon I tue Wed I thu I fri Sat Sun Daily Start Time Hour IS Minute 00			الاعدادات بناء على متطلباتك، وانقر موافة .
Specify days of the week and times on which this recurring range will be active Every Monday through Thursday, from 8:00 through 16:59, only. Days of the Week Every day Weekdays Weekends On these days of the week: Mon Tue Week Daily Start Time Hour TS	1	Add Bassing Time Bassin	
 Specify days of the week and times on which this recurring range will be active every Monday through Thursday, from 8:00 through 16:59, only. Days of the Week Every day Weekdays Weekends On these days of the week: Mon Tue Week Thu Fri Sat Sun 		as Add Recurring Time Range	March 1997
For example, use this option when you want the time range to be active every Monday through Thursday, from 8:00 through 16:59, only. Days of the Week		Specify days of the week and tim	es on which this recurring range will be active
For example, use this option when you want the time range to be active every Monday through Thursday, from 8:00 through 16:59, only. Days of the Week © Every day © Weekdays © Weekends © On these days of the week: © Mon © Tue © Wed © Thu © Fri © Sat © Sun Daily Start Time Hour 15 ♥ Minute 00 ♥ Hour 15 ♥ Minute 00 ♥			es ar miler ans recenting relige this be deare
Days of the Week ○ Every day ○ Weekdays ○ Weekends ③ On these days of the week: ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri □ Sat □ Sun Daly Start Time Hour 15 ☑ Minute 00 ☑		For example, use this option whe Monday through Thursday, from	n you want the time range to be active every 8:00 through 16:59, only,
 ○ Every day ○ Weekdays ○ Weekends ○ On these days of the week: ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri □ Sat □ Sun Daily Start Time Daily End Time (Inclusive) Hour 15 ☑ Minute 00 ☑ 		Days of the Week	
 ○ Every day ○ Weekdays ○ Weekends ○ On these days of the week: ○ Mon ○ Tue ○ Wed ○ Thu ○ Fri ○ Sat ○ Sun Daily Start Time Daily Start Time Hour 15 ○ Minute 00 ○ Hour 15 ○ Minute 00 ○ 		OSunda	
 ○ Weekdays ○ Weekends ○ On these days of the week: ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri □ Sat □ Sun Daily Start Time Daily Start Time Hour 15 ☑ Minute 00 ☑ 		O Every day	
 ○ Weekends ③ On these days of the week: ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri □ Sat □ Sun Daily Start Time Daily End Time (Inclusive) Hour 15 ☑ Minute 00 ☑ 		🔘 Weekdays	
 On these days of the week: ✓ Mon ✓ Tue ✓ Wed ✓ Thu ✓ Fri Sat Sun Daily Start Time Hour 15 ✓ Minute 00 ✓ Hour 20 ✓ Minute 00 ✓ 		O Weekends	
On these days of the week: I Mon I Tue V Wed I Thu I Fri Sat Sun Daily Start Time Hour 15 Minute 00 M		0	
Image: Mon image: The image: Mon image: The im		 On these days of the week 	aka.
Daily Start Time Daily End Time (Inclusive) Hour 15 Y Minute 00 Y Hour 20 Y		V Mon V Tue V W	/ed 🗸 Thu 🖉 Fri 🛄 Sat 🛄 Sun
Daily Start Time Daily End Time (Inclusive) Hour 15 Y Minute 00 Y Hour 20 Y			
Hour 15 🔽 Minute 00 🔽 🛛 Hour 🔯 🔽 Minute 00 😪		Daily Start Time	Daily End Time (Inclusive)
		Hour 15 🗙 Minute 00 🕚	🖌 Hour 🔯 😽 Minute 00 😪
		Specify a weekly interval when the	nis recurring range will be active
Specify a weekly interval when this recurring range will be active		For example, use this option whe	n we uwant the time range to be active
Specify a weekly interval when this recurring range will be active For example, use this option when you want the time range to be active.		continuously from Monday at 8:0	0 through Friday at 16:59.
Specify a weekly interval when this recurring range will be active For example, use this option when you want the time range to be active continuously from Monday at 8:00 through Friday at 16:59.		- Weekly Interval	
 Specify a weekly interval when this recurring range will be active For example, use this option when you want the time range to be active continuously from Monday at 8:00 through Friday at 16:59. 		From Monday	m m Mercer 00 w
 Specify a weekly interval when this recurring range will be active For example, use this option when you want the time range to be active continuously from Monday at 8:00 through Friday at 16:59. Weekly Interval From Monday and Provide Monday at 200 and Monday at 200 and Monday. 		From Monday (* 10	
Specify a weekly interval when this recurring range will be active For example, use this option when you want the time range to be active continuously from Monday at 8:00 through Friday at 16:59. Weekly Interval From: Monday Y Hour: 00 Y Minute: 00 Y		From: Friday 🖌 Ho	ur: 23 🛩 Minute: 59 🛩
 Specify a weekly interval when this recurring range will be active For example, use this option when you want the time range to be active continuously from Monday at 8:00 through Friday at 16:59. Weekly Interval From: Monday Hour: 00 Minute: 00 From: Friday Hour: 23 Minute: 59 	_		
 Specify a weekly interval when this recurring range will be active For example, use this option when you want the time range to be active continuously from Monday at 8:00 through Friday at 16:59. Weekly Interval From: Monday Hour: 00 Minute: 00 From: Friday Hour: 23 Minute: 59 			

للاكتمال.

8. طقطقة **ok** in order to رجعت إلى المدى الزمني نافذة.

Time Range N	lame: Restri	ict-Us	age											
Start Time — O Start n O Start a	ow t							End Time	ind					
Month:	February	~	Day:	05 🛩	Year:	2011	~	Month:	March	~	Day:	06 🗸	Year:	201
Hour:	00	~	Minute:	00 🗸				Hour:	00	~	Minute:	30 🗸		
You can fu start and s weekdays	ther constra top time spe 15:00 throu	ain the cified. gh 20	e active ti :00	me of th	nis range	by spe	cifying r	ecurring ranges.	The recurr	ing tim	e ranges (will be ad		Add Edit

وفقا لهذا التكوين، تم منع المستخدم في 172.16.10.50 من الوصول إلى أي موارد من الساعة 3 مساء إلى 8 مساء في جميع أيام الأسبوع باستثناء يومي السبت والأحد.

```
!
                                            time-range Restrict-Usage
      absolute start 00:00 05 February 2011 end 00:30 06 March 2011
                                   periodic weekdays 15:00 to 20:00
                                                                    !
access-list inside_access_out extended deny ip host 172.16.10.50 any
                                       time-range Restrict-Usage
                                                                    !
                  access-group inside_access_out in interface inside
```

ملاحظة: إذا كان للأمر **بالنطاق الزمني** قيم مطلقة ودورية محددة، فسيتم تقييم الأوامر **الدورية** فقط بعد الوصول إلى وقت البدء المطلق، ولا يتم تقييمها أكثر بعد الوصول إلى وقت النهاية المطلقة.

معلومات ذات صلة

- <u>صفحة وثائق Cisco ASA</u>
- الدعم التقني والمستندات Cisco Systems

ةمجرتاا مذه لوح

تمجرت Cisco تايان تايانق تال نم قعومجم مادختساب دنتسمل اذه Cisco تمجرت ملاعل العامي عيمج يف نيم دختسمل لمعد يوتحم ميدقت لقيرشبل و امك ققيقد نوكت نل قيل قمجرت لضفاً نأ قظعالم يجرُي .قصاخل امهتغلب Cisco ياخت .فرتحم مجرتم اممدقي يتل القيفارت عال قمجرت اعم ل احل اوه يل إ أم اد عوجرل اب يصوُتو تامجرت الاذة ققد نع اهتي لوئسم Systems الما يا إ أم الا عنه يل الان الانتيام الال الانتيال الانت الما