# ASA 8.2: Port Redirection (Forwarding) mit nat-, global, statischen und Zugriffslistenbefehlen mithilfe von ASDM

# Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Konventionen Netzwerkdiagramm Ausgehenden Zugriff zulassen Zugriff für interne Hosts auf externe Netzwerke mit NAT zulassen Zugriff für interne Hosts auf externe Netzwerke mit PAT zulassen Einschränken des Zugriffs von internen Hosts auf externe Netzwerke Datenverkehr zwischen Schnittstellen mit derselben Sicherheitsstufe zulassen Zugriff für nicht vertrauenswürdige Hosts auf Hosts in Ihrem vertrauenswürdigen Netzwerk zulassen Deaktivieren von NAT für bestimmte Hosts/Netzwerke Port Redirection (Forwarding) mit Statics Begrenzen Sie die TCP/UDP-Sitzung mithilfe von statisch. Zeitbasierte Zugriffsliste Zugehörige Informationen

# **Einführung**

Dieses Dokument beschreibt die Funktionsweise der Port-Umleitung auf der Cisco Adaptive Security Appliance (ASA) mit ASDM. Es befasst sich mit der Zugriffskontrolle für den Datenverkehr über die ASA und der Funktionsweise von Übersetzungsregeln.

# Voraussetzungen

### Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- <u>NAT-Übersicht</u>
- PIX/ASA 7.X: Port-Umleitung

#### Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco ASA der Serie 5500, Version 8.2
- Cisco ASDM Version 6.3

**Hinweis:** Diese Konfiguration funktioniert nur von der Cisco ASA-Software Version 8.0 bis 8.2 einwandfrei, da die NAT-Funktionalität nicht wesentlich verändert wird.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

#### **Konventionen**

Weitere Informationen zu Dokumentkonventionen finden Sie unter <u>Cisco Technical Tips</u> <u>Conventions</u> (Technische Tipps zu Konventionen von Cisco).

# **Netzwerkdiagramm**



Die in dieser Konfiguration verwendeten IP-Adressierungsschemata sind im Internet nicht rechtlich routbar. Es handelt sich um RFC 1918-Adressen, die in einer Laborumgebung verwendet wurden.

# Ausgehenden Zugriff zulassen

Der ausgehende Zugriff beschreibt Verbindungen von einer Schnittstelle mit höherer Sicherheitsstufe zu einer Schnittstelle mit niedrigerer Sicherheitsstufe. Dazu gehören Verbindungen von innen nach außen, von innen nach Demilitarized Zones (DMZs) und von DMZs nach außen. Dies kann auch Verbindungen von einer DMZ zu einer anderen umfassen, sofern die Schnittstelle der Verbindungsquelle eine höhere Sicherheitsstufe als das Ziel hat.

Ohne eine konfigurierte Übersetzungsregel kann keine Verbindung die Sicherheits-Appliance passieren. Diese Funktion wird als <u>NAT-Control</u> bezeichnet. Das hier abgebildete Bild zeigt, wie diese Funktion über ASDM deaktiviert wird, um Verbindungen über die ASA ohne

Adressübersetzung zu ermöglichen. Wenn Sie jedoch eine Übersetzungsregel konfiguriert haben, bleibt die Deaktivierung dieser Funktion für den gesamten Datenverkehr ungültig und Sie müssen die Netzwerke explizit von der Adressübersetzung ausnehmen.

#### Zugriff für interne Hosts auf externe Netzwerke mit NAT zulassen

Sie können einer Gruppe von internen Hosts/Netzwerken den Zugriff auf die Außenwelt ermöglichen, indem Sie die dynamischen NAT-Regeln konfigurieren. Um dies zu erreichen, müssen Sie die tatsächliche Adresse der Hosts/Netzwerke auswählen, die Zugriff erhalten sollen. Diese müssen dann einem Pool übersetzter IP-Adressen zugeordnet werden.

Gehen Sie wie folgt vor, um internen Hosts den Zugriff auf externe Netzwerke mit NAT zu ermöglichen:

 Gehen Sie zu Konfiguration > Firewall > NAT Rules, klicken Sie auf Hinzufügen, und wählen Sie dann die Option Dynamische NAT-Regel hinzufügen aus, um eine dynamische NAT-Regel zu konfigurieren.



 Wählen Sie den Namen der Schnittstelle aus, mit der die echten Hosts verbunden sind. Wählen Sie die tatsächliche IP-Adresse der Hosts/Netzwerke mithilfe der Schaltfläche Details im Feld Quelle

terface:	inside		
aurce:			
Jarce:			
slated -			
elect a glo	bal pool for dynamic translati	ion.	
Pool ID	Interface	Addresses Pool	
		Same as original address (identity)	
0	(outbound)	Same as original address (lacitacy)	
0	(outbound) (inbound)	Same as original address (identity)	
0	(outbound) (inbound)	Same as original address (identity)	
	for the or mode	Same as information ress inferiory.	

 In diesem Beispiel wurde das gesamte *interne Netzwerk* ausgewählt. Klicken Sie auf OK, um die Auswahl abzuschließen.

Mame	. 1	IP Address	Netmask	Description	Object NA
- IPv4 Nets	work Ohie	acts	Treatment	Construction of the second sec	Starfords file
- 🎱 ar	ny	0.0.0.0	0.0.0.0		
n De	side-n	172.16.11.0	255.255.255.0		antina interior interior
	anage	10.77.241.64	255.255.255.192		
	utside	209.165.200.0	255.255.255.224		
- 📇 20	0.1.1.10	20.1.1.10	255.255.255.255		
- 🗷 17	72.16	172.16.11.1	255.255.255.255		
- 🔳 17	72.16	172.16.11.10	255.255.255.255		
- 🔳 17	72.16	172.16.12.2	255.255.255.255		
. 20	09.16	209.165.200.10	255.255.255.255		

4. Klicken Sie auf **Verwalten**, um den Pool von IP-Adressen auszuwählen, dem das echte Netzwerk zugeordnet wird.

iterrace:			
ource:	nside-network/24		
slated —			
slect a glob	al pool for dynamic translat	ion.	
Pool ID	Interface	Addresses Pool	
0	(outbound)	Same as original address (identity)	
-0	(inbound)	Same as original address (identity)	
			Manage
			<u> </u>
nnection	Settings		

5. Klicken Sie auf Hinzufügen, um das Fenster Globalen Adresspool hinzufügen zu

P	ool ID	Interface	Addresses Pool

6. Wählen Sie die Option Range (Bereich) aus, und geben Sie die Start- und End-IP-Adressen zusammen mit der Ausgangsschnittstelle an. Geben Sie außerdem eine eindeutige Pool-ID an, und klicken Sie auf Hinzufügen, um diese dem Adresspool hinzuzufügen. Klicken Sie auf OK, um zum Fenster Globalen Pool verwalten zurückzukehren.

nterface:	outside		*	
Pool ID:	10			
IP Addre	esses to Add			Addresses Pool
Rang	ge	n		209.165.200.20 - 209.165.200.4
Starti	ng IP Address:	209.165.200.20		
Endin	g IP Address:	209.165.200.40		
Netm	ask (optional):	255.255.255.192		
O Port	Address Trans	lation (PAT)		
IP Ad	dress:			
Netm	ask (optional):			
O Port Addr	Address Trans ress of the inte	lation (PAT) using IF rface	,	

7. Klicken Sie auf OK, um zum Fenster Dynamische NAT-Regel hinzufügen

Pool ID	Interface	Addresses Pool
10	outside	209.165.200.20 - 209.165.200.40

zurückzukehren.

8. Klicken Sie auf **OK**, um die Konfiguration der dynamischen NAT-Regel abzuschließen.

	1300		
ource:	inside-network/24		
nslated —			
elect a glol	bal 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	Manag

 Klicken Sie auf Apply, damit die Änderungen wirksam werden. Hinweis: Die Option Verkehr durch die Firewall ohne Adressübersetzung aktivieren ist deaktiviert

		Original			Translated		
*	Type	Source	Destination	Service	Interface	Address	Service
insic	ie .						
	Dynamic	inside-network/24			outside	209.165.200.20 - 209.165.200.40	-

Dies ist die entsprechende CLI-Ausgabe für diese ASDM-Konfiguration:

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

Gemäß dieser Konfiguration werden die Hosts im Netzwerk 172.16.11.0 in eine beliebige IP-Adresse aus dem NAT-Pool, 209.165.200.20-209.165.200.40, umgewandelt. Hier ist die NAT-Pool-ID sehr wichtig. Sie können denselben NAT-Pool einem anderen internen/DMZ-Netzwerk zuweisen. Wenn der zugeordnete Pool weniger Adressen als die reale Gruppe hat, könnten Ihnen Adressen fehlen, wenn der Datenverkehr die erwartete Menge übersteigt. Als Ergebnis könnten Sie versuchen, PAT zu implementieren, oder Sie könnten versuchen, den vorhandenen Adresspool zu bearbeiten, um ihn zu erweitern.

Hinweis: Beachten Sie, dass Sie die vorhandene Übersetzungsregel ändern müssen, damit diese Änderungen wirksam werden, jedoch den Befehl <u>clear xlate</u> verwenden müssen. Andernfalls

verbleibt die vorherige bestehende Verbindung in der Verbindungstabelle, bis sie das Timeout erreicht hat. Seien Sie vorsichtig, wenn Sie den Befehl **clear xlate** verwenden, da er die vorhandenen Verbindungen sofort beendet.

#### Zugriff für interne Hosts auf externe Netzwerke mit PAT zulassen

Wenn interne Hosts eine einzige öffentliche Adresse für die Übersetzung freigeben möchten, verwenden Sie PAT. Wenn die **globale** Anweisung eine Adresse angibt, wird diese Adresse vom Port übersetzt. Die ASA ermöglicht eine Port-Übersetzung pro Schnittstelle, und die Übersetzung unterstützt bis zu 65.535 aktive **Xlate**-Objekte in eine globale Adresse.

Gehen Sie wie folgt vor, um internen Hosts den Zugriff auf externe Netzwerke mit PAT zu ermöglichen:

1. Gehen Sie zu Konfiguration > Firewall > NAT Rules, klicken Sie auf Hinzufügen, und wählen Sie dann die Option Dynamische NAT-Regel hinzufügen aus, um eine dynamische NAT-

1	Add Static NAT Rule
H	Add Dynamic NAT Rule
	Add NAT Exempt Rule
۵.	Add Static Policy NAT Rule
ø	Add Dynamic Policy NAT Rule
*	Insert
4	Insert After

#### Regel zu konfigurieren.

 Wählen Sie den Namen der Schnittstelle aus, mit der die echten Hosts verbunden sind. Wählen Sie die tatsächliche IP-Adresse der Hosts/Netzwerke mithilfe der Schaltfläche Details im Feld Source (Quelle) aus, und wählen Sie inside network (Netzwerkintern) aus. Klicken Sie auf Verwalten, um die Informationen zur übersetzten Adresse zu definieren.

nterface:	Inside	×	
ource:	inside-network/24		
nslated —			
elect a glol	oal pool for dynamic translat	ion.	
Pool ID	Interface	Addresses Pool	
- O	(outbound)	Same as original address (identity)	
0	(inbound)	Same as original address (identity)	
			Manage

3. Klicken Sie auf

Add	🕻 Edit 🏦 Delete	
Pool ID	Interface	Addresses Pool

4. Wählen Sie die Port Address Translation (PAT) mithilfe der IP-Adresse der Schnittstellenoption aus, und klicken Sie auf Add, um sie dem Adresspool hinzuzufügen. Vergessen Sie nicht, eine eindeutige ID für diesen NAT-Adresspool zuzuweisen.

erface:	outside	*			
ID:	20				
P Addre	esses to Add		-	Addresses Pool	_
Rang	ge			w outside	
Starti	ng IP Address:		6		2
Endin	g IP Address:				
Netm	ask (optional):		Add >>		
) Port	Address Translation (PAT	)	<< Delete	2	
IP Ad	dress:				
Netm	ask (optional);				
Port	Address Translation (PAT	) using IP			
Addr	ress of the interface				

5. Hier sehen Sie den konfigurierten Adresspool mit der externen Schnittstelle als einzige verfügbare Adresse in diesem Pool. Klicken Sie auf OK, um zum Fenster Dynamische NAT-Regel hinzufügen

Pool ID	Interface	Addresses Pool
20	outside	🔤 outside

OK.

iterface:	inside		
ource:	inside-network/24		
islated -			
elect a glo	bal pool for dynamic translat	ion.	
Pool ID	Interface	Addresses Pool	
0	(outbound)	Same as original address (identity)	
0	(inbound)	Same as original address (identity)	
20	outside	m outside	Manage
neertie	n Sattings		

 Die konfigurierte dynamische NAT-Regel wird hier im Bereich Konfiguration > Firewall > NAT Rules (Konfiguration > Firewall > NAT-Regeln)

	Time	Original	Translated			
-	Type	Source	Destination	Service	Interface	Address
inside	9					
1	Dynamic	inside-network/24			outside	autside

Dies ist die entsprechende CLI-Ausgabe für diese PAT-Konfiguration:

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

#### Einschränken des Zugriffs von internen Hosts auf externe Netzwerke

Wenn keine Zugriffsregeln definiert sind, können Benutzer über eine Schnittstelle mit höherer Sicherheit auf alle Ressourcen zugreifen, die einer Schnittstelle mit niedrigerer Sicherheit zugeordnet sind. Um den Zugriff bestimmter Benutzer auf bestimmte Ressourcen zu beschränken, verwenden Sie die Zugriffsregeln im ASDM. In diesem Beispiel wird beschrieben, wie ein einzelner Benutzer auf externe Ressourcen (über FTP, SMTP, POP3, HTTPS und WWW) zugreifen und alle anderen daran hindern kann, auf externe Ressourcen zuzugreifen.

Hinweis: Am Ende jeder Zugriffsliste gibt es eine "Implicit Deny"-Regel.

Gehen Sie wie folgt vor:

1. Gehen Sie zu Konfiguration > Firewall > Zugriffsregeln, klicken Sie auf Hinzufügen, und wählen Sie die Option Zugriffsregel hinzufügen aus, um einen neuen Zugriffslisteneintrag zu



#### erstellen.

 Wählen Sie die Quell-IP-Adresse aus, die im Feld Source (Quelle) zugelassen werden soll. Wählen Sie any als Destination (Ziel), inside als Interface (Schnittstelle) und Permit (Zulassen) als Action aus. Klicken Sie schließlich im Feld Service auf die Schaltfläche Details, um eine TCP-Servicegruppe für die erforderlichen Ports zu

Interface:	inside 💌		
Action: 💿	Permit 🔿 Deny		
Source:	172.16.10.100		
Destination	any		
Service:	ip		
Description:			
🕑 Enable L	ogging		
Logging	evel: Default	*	
More Opt	ons		
			Cascal

erstellen.

3. Klicken Sie auf Hinzufügen, und wählen Sie dann die Option TCP Service Group (TCP-



#### Servicegruppe) aus.

4. Geben Sie einen Namen für diese Gruppe ein. Wählen Sie alle erforderlichen Ports aus, und klicken Sie auf **Hinzufügen**, um sie in das Feld Mitglieder in Gruppe zu

Group Name	Permit-172.16.10.100		
Description:			
Existing	Service/Service Group:		Members in Group
Name			Name
B-TCP :	Service Groups	~	ttp
æ 🗄	RDP		
😑 - Pred	efined		
	🐲 aol		
	😰 bgp		
10	🔊 chargen		
19	⊛ cifs	- Carriel	
19	🐮 citrix-ica	E	
1	🗞 ctiqbe	Add	1>>
<u>n</u>	🔊 daytime	<< R	emove
13	🕑 discard		
11	😰 domain		
33	z echo		
200 33	exec		
	🤣 finger		
Ū	🕑 ftp-data		
	🐉 gopher	2	
Carl		in the second second	
O Create n	ew member:		
Port/Ran	ge:		

5. Alle ausgewählten Ports sollten im rechten Feld angezeigt werden. Klicken Sie auf **OK**, um die Auswahl der Service-Ports abzuschließen.

ription:			
xisting Service/Service Group;			Members in Grou
Name			Name
nfs	^		100 ftp
- too nnto	-		🕬 💷 ftp-data
100 pcanywhere-data			http
pim-auto-rp			nttps
100 pop2			pop3
pptp			to smtp
- 100> rsh			
- 100> rtsp		C add >>	
😥 sip			
😰 sqinet		<< Remove	
- 10) ssh	-		
- 100 sunrpc			
- 109 tacacs			
- 100- talk	30		
- 100> telnet			
- IS uucp			
- 🐲 whois	Y		
reate new member:			

6. Hier sehen Sie die konfigurierte TCP-Servicegruppe. Klicken Sie auf OK.

ICer:						
Name		Protocol	Source Ports	Destination Ports	ICMP Type	Description
😑 🥨 Perr	nit-1	tcp				
ISE f	τp	tcp	default (1-65535)	21		
<u>RE</u> > 1	tp-data	tcp	default (1-65535)	20		
100	nttp	tcp	default (1-65535)	80		
<u>10</u>	nttps	tcp	default (1-65535)	443		
<u>ISP</u> (	cop3	tcp	default (1-65535)	110		
	ambp	tcp	default (1-65535)	25		
E RDP	k i	tcp				
-Predefined						
- 102> aol		tcp	default (1-65535)	5190		
n 190 bgp		tcp	default (1-65535)	179		
102> char	rgen	tcp	default (1-65535)	19		
cifs		tcp	default (1-65535)	3020		
- 12 citrit	x-ica	tcp	default (1-65535)	1494		
- 19 ctiq	be	tcp	default (1-65535)	2748		
- 10 day	time	tcp	default (1-65535)	13		
- 10 disc	ard	tcp	default (1-65535)	9		
TCP> dom	ain	tcp	default (1-65535)	53		
- 10 ech	0	tcp	default (1-65535)	7		
- IO exe	c	tcp	default (1-65535)	512		
elected Servic						

7. Klicken Sie auf OK, um die Konfiguration

add Acc	ess Rule
Interface:	inside 💦
Action: 💿 I	Permit 🔿 Deny
Source:	172.16.10.100
Destination	any .
Service:	Permit-172.16.10.100
Description:	
🕑 Enable L	ogging
Logging	.evel: Default 🖌
More Opt	ions

- abzuschließen.
- 8. Die konfigurierte Zugriffsregel ist unter der internen Schnittstelle im Bereich Konfiguration > Firewall > Zugriffsregeln sichtbar

Cooffee	abien > Fire		Manager and Construction Construction						
Add	· G Edt (	Delete   ↑ ↓   .	🎉 🗈 🏨 - 🛛 Q, Find 🖭	Diagram	Export •	Clear	Hits 🔝 :	5how Log 🧯	Q P
#	Enabled	Source	Destination	Service	,	Action	Hits	Logging	
🛱 🔊 i	nside (2 incom	ing rules)							
1	<b>V</b>		🐔 any	III Perr	mit-172.1	🛹 Permit			
2	1	🏟 any	any	IP ip	TCP Grou	p: Permit-1	72.16.10.1	100	
😑 🔊 i	nside IPv6 (2 i	mplicit incoming rules)			TCP: ftp (	(21)			
1		🦚 any	Any less secure ne	IE ID	TCP: ftp-	data (20)		10000	
2		<ul> <li>any</li> </ul>	<li>any</li>	IP ip	TCP: http	(80) is (443)		1000	
😑 🛤 n	manage (2 imp	licit incoming rules)			TCP: pop	3 (110)			
1		any	Any less secure ne	IP ip	TCP: smt	25)			

9. Um die Verwendung zu vereinfachen, können Sie die TCP-Service-Gruppe auch direkt im rechten Bereich der Registerkarte **Services** bearbeiten. Klicken Sie auf **Bearbeiten**, um diese Servicegruppe direkt zu ändern.

	COMPACTO PORCA						Marked and and and and and and and and and an		
Edt	Delete + 4	🕺 🖻 💼 - 🔍 Find 🖽	Diagram _ Export	- 6 Clear	HRs 🔳	Show Log	Packet	Trace	Services d1 4
abled	Source	Destination	Service	Action	Hits	Logging	Time	Description	Add - CE Edt Delete Q Where U
(2 incor	ning rules)								Filter
2	172.16.10.100	d any	30 Permit-172.1	🖋 Pornit		Largerson	C. Constant	Section and the	Name
	any	any	JE∕ip	O Deny			1	Implicit rule	E TCP Service Groups
Pv6 (2	implicit incoming rules)								E 😨 Permit-172.16.10.100
	any	Any less secure ne	.m. ip	🖌 Pernit				Implicit rule: Per	- Mp Rp
	any	<ul> <li>any</li> </ul>	10 (p	(3 Deny				Implicit rule	- see Rp-data
e (2 im	plicit incoming rules)								- me http
	any any	Any less secure ne	12 ip	🖌 Pernit				Implicit rule: Per	- 🗰 https
	any	<ul> <li>any</li> </ul>	JE ip	O Deny				Implicit rule	
e IPv6	(2 implicit incoming rules)								- Mar smitp
	any	Any less secure ne	It ip	🖌 Pernit				Implicit rule: Per	B TR RDP
	any	any	JE ip	O Deny				Implicit rule	Predefined
t (2 inc	oming rules)								- tel ad
	20.1.1.10	A 209.165.200.10	THE ROP	🖌 Pernit	1.1.1.1	0		discussion and	- 189 bgp
	any any	any any	IE ID	O Deny				Implicit rule	- B2 chargen

10. Sie wird erneut zum Fenster "Edit TCP Service Group" (TCP-Servicegruppe bearbeiten) umgeleitet. Nehmen Sie Änderungen entsprechend Ihren Anforderungen vor, und klicken Sie auf **OK**, um die Änderungen zu speichern

ription:		
xisting Service/Service Group:		Members in Group:
Name		Name
S-TCP Service Groups	~	r-12> ftp
RDP		- 👥 ftp-data
Predefined		100- http
10> aol		100> https
- 😰 bgp		top pop3
- 10 chargen		smtp
🚥 cifs		
- 😰 citrix-ica		
- 102> ctiqbe	Add	>>
- 😥 daytime	<< Rei	move
- 😰 discard		
- 😎 domain		
echo		
10 exec		
finger		
- 12 gopher		
100/ h323		

11. Hier sehen Sie eine vollständige Übersicht über das ASDM:

É Cisco ASOM 6.3 for ASA 10.77.	241.115										
the Yeve Book Wigards Window	Pip							Look Fors			alada
🖏 Home 🔏 Carifgention 🕞 Mont	arra 🕞 Sava 🧿	teliesh 🔇 Bad	Orene ? Hel								CISCO
Device List 🚽 🕈 🗶	Configuration > Fin	reall > Access Rule	1					0	A	diverses Services	Time Ranges
🗣 Add 📋 Delete 🚿 Connect	🗣 Add - 📑 Edk	Deinto + 4	1 12 18 - Q md 18	Dagan 🗐	toport = 🏟 Clear HRs	🔝 Show Log 🔍	Packet Tr	ice	Serv	kes	d o ×
Firemall 20 2 ×	# Enabled	Source	Destination	Service	Action Hits	Logging	Time	Description		99 - 🖪 EAK 🔲 C	elete G Where Used
C. Israed	🖯 💭 inside (2 incar	sing rules)						-	Piter:		(AriChari
e.o.	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	172 16.10.100	ci ary	30 Period-11	72.1.5 Period 10	and Chanks	12000	1000000	Nam		
Remote Access NPN	12	@ ary	😂 MIY	B·Þ	O Deny			Implicit rule	(p. 10	P Service Groups	A
(1)	🗟 💭 manage (2 im	plicit incoming rules)							=	20 Permit-172.16.	10.100
Ske-to-Ske VPN	1	any any	Any less secure ne	20	📌 Pomit			Deplot rule : F		HID Rp	
PS S	<									as Rp-data	
30 -	Access Fade Type: C	Bet and Phil. (2) B	Put only C IPut only							- ago hetp	
Device Management			and Ormen							- me hitps	
			C Anti-	Devel	Chinese					Han page 1	
				PROST						the ship	*
	and the second sec					test	15				US011 8-10-17 AM URC

Dies ist die entsprechende CLI-Konfiguration:

```
object-group service Permit-172.16.10.100 TCP
port-object eq ftp
port-object eq ftp-data
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
!
Vollständige Informationen zur Implementierung der Zugriffskontrolle find
```

Vollständige Informationen zur Implementierung der Zugriffskontrolle finden Sie unter <u>Hinzufügen</u> oder Ändern einer Zugriffsliste über die ASDM-GUI.

# Datenverkehr zwischen Schnittstellen mit derselben Sicherheitsstufe zulassen

In diesem Abschnitt wird beschrieben, wie der Datenverkehr innerhalb von Schnittstellen mit den gleichen Sicherheitsstufen aktiviert wird.

In diesen Anweisungen wird beschrieben, wie die Kommunikation zwischen den Schnittstellen aktiviert wird.

Dies ist für VPN-Datenverkehr hilfreich, der in eine Schnittstelle eingeht, aber dann über dieselbe Schnittstelle weitergeleitet wird. Der VPN-Datenverkehr kann in diesem Fall unverschlüsselt oder für eine andere VPN-Verbindung neu verschlüsselt werden. Gehen Sie zu **Configuration > Device Setup > Interfaces**, und wählen Sie die **Option Enable traffic between two or more hosts connected to the same interface** aus.

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
<]						1
Enable traffic betw	een two or more inter	faces which a	re configured	with same security le	vels	
<ul> <li>Enable traffic betw</li> </ul>	een two or more host	s connected t	o the same ini	terface		
• Endblo crame both	contents of more nose	s com occou c	o cho odnio in			

In diesen Anweisungen wird beschrieben, wie die Kommunikation zwischen den Schnittstellen aktiviert wird.

Dies ist nützlich, um die Kommunikation zwischen Schnittstellen mit gleichen Sicherheitsstufen zu ermöglichen. Gehen Sie zu **Configuration > Device Setup > Interfaces**, und wählen Sie **Enable traffic between two or more interfaces**, which are configured with same security levels option.

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	een two or more inter een two or more host	faces which a s connected t	re configured o the same in	with same security le terface	Apply Res	

Dies ist die entsprechende CLI für beide Einstellungen:

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

# Zugriff für nicht vertrauenswürdige Hosts auf Hosts in Ihrem vertrauenswürdigen Netzwerk zulassen

Dies kann durch die Anwendung einer statischen NAT-Übersetzung und einer Zugriffsregel erreicht werden, die diese Hosts zulässt. Sie müssen dies immer konfigurieren, wenn ein externer Benutzer auf einen Server im internen Netzwerk zugreifen möchte. Der Server im internen Netzwerk verfügt über eine private IP-Adresse, die im Internet nicht routbar ist. Daher müssen Sie diese private IP-Adresse mithilfe einer statischen NAT-Regel in eine öffentliche IP-Adresse übersetzen. Angenommen, Sie haben einen internen Server (172.16.11.5). Damit dies funktioniert, müssen Sie diese private Server-IP in eine öffentliche IP-Adresse übersetzen. In diesem Beispiel wird beschrieben, wie die bidirektionale statische NAT für die Übersetzung von 172.16.11.5 in 209.165.200.5 implementiert wird.

Der Abschnitt, der es externen Benutzern ermöglicht, durch Implementierung einer Zugriffsregel auf diesen Webserver zuzugreifen, wird hier nicht angezeigt. Hier wird ein kurzer CLI-Ausschnitt angezeigt, um Ihnen das Verständnis zu erleichtern:

access-list 101 permit TCP any host 209.165.200.5

Weitere Informationen finden Sie unter <u>Hinzufügen oder Ändern einer Zugriffsliste über die ASDM-</u><u>GUI</u>.

**Hinweis:** Durch die Angabe des Schlüsselworts "any" können beliebige Benutzer von außerhalb auf diesen Server zugreifen. Wenn sie für keine Service-Ports angegeben ist, kann der Zugriff auf den Server auf jedem Service-Port erfolgen, wenn diese offen bleiben. Seien Sie vorsichtig, wenn Sie die Implementierung durchführen. Wir empfehlen Ihnen, die Berechtigung auf den einzelnen externen Benutzer und auch auf den erforderlichen Port des Servers zu beschränken.

Gehen Sie wie folgt vor, um die statische NAT zu konfigurieren:

1. Gehen Sie zu **Konfiguration > Firewall > NAT Rules**, klicken Sie auf **Hinzufügen**, und wählen Sie **Statische NAT-Regel hinzufügen** 



aus.

2. Geben Sie die ursprüngliche IP-Adresse und die übersetzte IP-Adresse zusammen mit den zugehörigen Schnittstellen an, und klicken Sie auf

Interface:	ipside	~
Incondect.		
Source:	172.16.11.5	
Translated		
Interface:	outside	~
() Use IP Address:	209.165.200.5	-
O Use Interface IP	Address	
Port Address Translatio	n (PAT)	
Enable Port Ad	dress Translation (PAT)	
Protocol:	TCP UDP	
Original Port:		
Translated Dor		
in ansiaceu ron		

3. Hier sehen Sie den konfigurierten statischen NAT-Eintrag. Klicken Sie auf **Apply**, um dies an die ASA zu

-		Original			Translated	
#	Type	Source	Destination	Service	Interface	Address
insid	e (1 Static rules, 1 l	Dynamic rules)				
1	Static	S 172.16.11.5			outside	209.165.200.5
2	Dynamic	inside-network/24	the state of the s		outside	outside

Dies ist ein kurzes CLI-Beispiel für diese ASDM-Konfiguration:

!

static (inside,outside) 209.165.200.5 172.16.11.5 netmask 255.255.255.255

# Deaktivieren von NAT für bestimmte Hosts/Netzwerke

Wenn Sie bestimmte Hosts oder Netzwerke von der NAT ausnehmen müssen, fügen Sie eine NAT-Freistellungsregel hinzu, um die Adressumwandlung zu deaktivieren. Dadurch können sowohl übersetzte als auch Remote-Hosts Verbindungen initijeren.

Gehen Sie wie folgt vor:

1. Gehen Sie zu Konfiguration > Firewall > NAT Rules, klicken Sie auf Hinzufügen, und wählen



#### Sie NAT-Befreiungsregel hinzufügen aus.

2. Hier wurde das interne Netzwerk 172.18.10.0 von der Adressumwandlung ausgenommen. Vergewissern Sie sich, dass die Option **Exempt** aktiviert wurde. NAT Exempt Direction hat zwei Optionen:Ausgehender Datenverkehr an niedrigere SicherheitsschnittstellenEingehender Datenverkehr an Schnittstellen mit höherer SicherheitDie Standardoption ist für den ausgehenden Datenverkehr. Klicken Sie auf **OK**, um den Schritt

📬 Add NAT I	xempt Rule	
Action:	Exempt     O Do not exempt	
Original		
Interface:	inside 😽	
Source:	172.18.10.0	
Destination:	any -	
NAT Exempt Di NAT Exer NAT Exer	rection mpt outbound traffic from interface 'inside' to lower security mpt inbound traffic from interface 'inside' to higher security	
Description		
	OK Cancel Help	<b>-linweis</b> : Wenn

abzuschließen.

Sie die Option **Nicht ausnehmen** auswählen, wird dieser Host nicht von NAT ausgenommen, und es wird eine separate Zugriffsregel mit dem Schlüsselwort "Verweigern" hinzugefügt. Dies ist hilfreich, um zu verhindern, dass bestimmte Hosts von NAT ausgenommen werden, da das gesamte Subnetz mit Ausnahme dieser Hosts von der NAT ausgenommen wird.

 Hier sehen Sie die NAT-Ausschlussregel f
ür die ausgehende Richtung. Klicken Sie auf Apply, um die Konfiguration an die ASA zu senden.

	Tune	Original			Translated
	type	Source	Destination	Service	Interface
inside	(1 Exempt rules, 1	1 Static rules, 1 Dynamic rule	es)		· · · · · · · · · · · · · · · · · · ·
1	🚟 Exempt	172.18.10.0	📽 any		(outbound)
2	1 Static	3 172.16.11.5		-	outside
3	Dynamic	📸 inside-network/24			outside
		00		<u> </u>	

#### ist die entsprechende CLI-Ausgabe für Ihre Referenz:

access-list inside\_nat0\_outbound extended permit ip host 172.18.10.0 any
!

4. Hier sehen Sie, wie Sie die NAT-Ausschlussregel für die entsprechende Richtung bearbeiten. Klicken Sie auf **OK**, damit die Option wirksam

Driginal	
Interface:	inside
Source:	172.18.10.0
Destination:	any -
O NAT Exe	mpt outbound traffic from interface 'inside' to lower security interfaces (
NAT Exe     NAT Exe	mpt outbound traffic from interface 'inside' to lower security interfaces ( mpt inbound traffic from interface 'inside' to higher security interfaces
NAT Exe	mpt outbound traffic from interface "inside" to lower security interfaces mpt inbound traffic from interface "inside" to higher security interfaces

5. Sie können jetzt sehen, dass die Richtung in *eingehend* geändert wurde.

	Turne	Original			Translated	
•	туре	Source	Destination	Service	Interface	
insid	le (1 Exempt rules, 1	1 Static rules, 1 Dynamic rule	es)			
1	🚍 Exempt	A 172.18.10.0	🧆 any		(inbound)	
2	1 Static	📇 172.16.11.5			outside	1
3	Dynamic	🛃 inside-network/24			outside	5
<		.00				

KIICKEN SIE AUF Apply, UM diese CLI-Ausgabe an die ASA zu senden: access-list inside\_nat0\_outbound extended permit ip host 172.18.10.0 any ! nat (inside) 0 access-list inside\_nat0\_outbound **outside** 

**Hinweis:** Aus diesem Grund sehen Sie, dass am Ende des Befehls **nat 0** ein neues Schlüsselwort (außerhalb) hinzugefügt wurde. Diese Funktion wird als **Outside NAT** bezeichnet.

6. NAT kann auch durch die Implementierung von Identity NAT deaktiviert werden. Identity NAT übersetzt einen Host in dieselbe IP-Adresse. Im folgenden Beispiel wird die NAT für die reguläre statische Identität veranschaulicht, bei der der Host (172.16.11.20) bei einem externen Zugriff in dieselbe IP-Adresse übersetzt

Incentace:	inside	*
Source:	172.16.11.20	
anslated		
Interface:	outside	~
• Use IP Address:	172.16.11.20	
rt Address Translation Translation Frotocol: Original Port: Translated Port	TCP O UDP	
onnection Setting	s K Cancel Help	(*)

# Port Redirection (Forwarding) mit Statics

!

Port Forwarding oder Port Redirection ist eine nützliche Funktion, bei der externe Benutzer versuchen, auf einen internen Server an einem bestimmten Port zuzugreifen. Um dies zu erreichen, wird der interne Server, der über eine private IP-Adresse verfügt, in eine öffentliche IP-Adresse übersetzt, die wiederum Zugriff für den jeweiligen Port erlaubt.

In diesem Beispiel möchte der externe Benutzer auf den SMTP-Server 209.165.200.15 an Port 25 zugreifen. Dies erfolgt in zwei Schritten:

- 1. Übersetzen Sie den internen Mailserver 172.16.11.15 an Port 25 in die öffentliche IP-Adresse 209.165.200.15 an Port 25.
- 2. Zugriff auf den öffentlichen Mail-Server 209.165.200.15 an Port 25 zulassen.

Wenn der externe Benutzer versucht, an Port 25 auf den Server 209.165.200.15 zuzugreifen, wird

dieser Datenverkehr an den internen Mailserver 172.16.11 15 an Port 25 umgeleitet.

1. Gehen Sie zu Konfiguration > Firewall > NAT Rules, klicken Sie auf Hinzufügen, und wählen

<u>c</u>	onfic	guration > Firewall > NAT Rules	
	💠 A	idd 🚽 📝 Edit 📋 Delete 🖙 🗲	X
	111	Add Static NAT Rule	
	몖	Add Dynamic NAT Rule	
		Add NAT Exempt Rule	-
	Ω.	Add Static Policy NAT Rule	P
	<b>@</b> .	Add Dynamic Policy NAT Rule	
	+	Insert	2
	争	Insert After	þ
1			

#### Sie Statische NAT-Regel hinzufügen aus.

2. Geben Sie die ursprüngliche Quelle und die übersetzte IP-Adresse zusammen mit den zugehörigen Schnittstellen an. Wählen Sie **Enable Port Address Translation (PAT aktivieren)**, geben Sie die Ports an, die umgeleitet werden sollen, und klicken Sie auf

Interface:	inside	
Source:	172.16.11.15	(
Translated		
Interface:	outside	i
💿 Use IP Address:	209.165.200.15	[
Port Address Translation	n (PAT)	
Port Address Translation	n (PAT) dress Translation (PAT) TCP O UDP	
Port Address Translation	n (PAT) dress Translation (PAT) TCP O UDP 25	
Port Address Translation Protocol: Original Port: Translated Port	n (PAT) dress Translation (PAT) TCP O UDP 25 25 25	

3. Die konfigurierte statische PAT-Regel wird hier angezeigt:

и Ту	Time	Original			Translated		
	type	Source	Destination	Service	Interface	Address	Servi
1	🗂 Exempt	A 172.18.10.0	any		(outbound)		
2	🗐 No Exempt	3 172.20.10.10	any		(outbound)		
3	Static	S 172.16.11.15		RD smtp	outside	209.165.200.15	🐲 sna
4	· Static	3 172.16.11.5			outside	A 209.165.200.5	
3							>

Dies ist die entsprechende CLI-Ausgabe:

4. Dies ist die Zugriffsregel, die es externen Benutzern ermöglicht, unter 209.165.200.15 auf den öffentlichen SMTP-Server

				TCF	P Group: smtp-access P: smtp (25)
3		🏈 any	any	IP/ ip	C Denv
2	<b></b>	🐔 any	🖳 209.165.200.15	w smtp-access	🖌 🧹 Permit
1	~	🖳 20.1.1.10	🚇 209.165.200.10	RDP	🖌 Permit
🗄 🥦 out	side (3 inc	oming rules)			
2		🇳 any	🏟 any	IP/ ip	🔇 Deny
	nen.	🧼 any	🧼 Any less secure ne	IP/ IP	V Permit

**Hinweis:** Stellen Sie sicher, dass Sie bestimmte Hosts verwenden, anstatt das **any**-Schlüsselwort in der Quelle der Zugriffsregel zu verwenden.

# Begrenzen Sie die TCP/UDP-Sitzung mithilfe von statisch.

Sie können die maximale Anzahl an TCP-/UDP-Verbindungen mithilfe der statischen Regel angeben. Sie können auch die maximale Anzahl an embryonalen Verbindungen angeben. Eine embryonale Verbindung ist eine Verbindung, die halb offen ist. Eine größere Anzahl dieser Aspekte wirkt sich auf die Leistung der ASA aus. Die Einschränkung dieser Verbindungen verhindert bestimmte Angriffe wie DoS und SYN. Um eine vollständige Eindämmung zu erreichen, müssen Sie die Richtlinie im MPF-Framework definieren, das über den Rahmen dieses Dokuments hinausgeht. Weitere Informationen zu diesem Thema finden Sie unter <u>Eindämmen</u> von Netzwerkangriffen.

Gehen Sie wie folgt vor:

-----

1. Klicken Sie auf die Registerkarte Verbindungseinstellungen, und geben Sie die Werte für die maximalen Verbindungen für diese statische Übersetzung

Onginal	10-12-1	
Interface:	inside	
Source:	172.16.11.15	
Translated		
Interface:	outside	~
💽 Use IP Address:	209.165.200.15	C:
O Use Interface IP	Address	
Port Address Translatio	n (PAT)	
Enable Port Ad	dress Translation (PAT)	
Protocol:		
Original Port:	smtp	
Translated Port	: smtp	
<b>Connection Setting</b>	s	(
Translate the D	NS replies that match the translation rule	
Randomize sequ	uence number	
Maximum TCP Conn	ections: 100	
Maximum UDP Conn	ections: 0	
Mavinum Embrunni	Connections: 50	
Maxim in Finnson	Connections: 50	

2. Diese Bilder zeigen die Verbindungsgrenzen für diese spezifische statische Übersetzung:

	Delece J 🐳	0 ····································		Turneland					
Original			Translated	Translated					
Source	Destination	Service	Interface	Address	Service				
atic rules, 1 Dynamic r	ules)								
A 172.18.10.0	any		(outbound)						
172.20.10.10	<ul> <li>any</li> </ul>		(outbound)						
<b>B</b> 172.16.11.15		ter smtp	outside	209.165.200.15	tto smtp				

Options				
DNS Rewrite	Max TCP Connections	Embryonic Limit	Max UDP Connections	Randomize Sequer
	100	50	Unlimited	Image: A start and a start
_			· · · · ·	

Dies ist die entsprechende CLI-Ausgabe:

# Zeitbasierte Zugriffsliste

1

Dieser Abschnitt behandelt die Implementierung zeitbasierter Zugriffslisten mithilfe des ASDM. Zugriffsregeln können je nach Zeit angewendet werden. Um dies zu implementieren, müssen Sie einen Zeitraum definieren, der die Zeitangaben nach Tag, Woche, Monat oder Jahr angibt. Anschließend müssen Sie diesen Zeitraum an die erforderliche Zugriffsregel binden. Der Zeitbereich kann auf zwei Arten definiert werden:

- 1. Absolut Definiert einen Zeitraum mit Startzeit und Endzeit.
- 2. Periodic (Periodisch) Wird auch als periodisch bezeichnet. Definiert einen Zeitraum, der in angegebenen Intervallen auftritt.

**Hinweis:** Stellen Sie vor dem Konfigurieren des Zeitbereichs sicher, dass die ASA mit den richtigen Datums-/Uhrzeiteinstellungen konfiguriert wurde, da diese Funktion die Systemuhr-Einstellungen für die Implementierung verwendet. Die Synchronisierung der ASA mit dem NTP-Server führt zu deutlich besseren Ergebnissen.

Gehen Sie wie folgt vor, um diese Funktion über ASDM zu konfigurieren:

1. Klicken Sie beim Definieren der Zugriffsregel auf die Schaltfläche Details im Feld

	🕯 Add Acc	ess Rule
	Interface:	inside 💌
	Action: O	Permit 💿 Deny
	Source:	172.16.10.50
	Destination	any -
	Service:	ip 🔄
	Description:	
	Enable L Logging I	ogging .evel: Default 💌
	More Opt	ions
	Enable	Rule
	Traffic Dire	ection: 🔘 In 💿 Out
	Source Ser	vice: (TCP or L
	Logging In	terval: 300 seconds
	Time Rang	•:
Zeitbereich.		OK Cancel Help

2. Klicken Sie auf Hinzufügen, um einen neuen Zeitraum zu



erstellen.

 Definieren Sie den Namen des Zeitbereichs, und geben Sie die Startzeit und Endzeit an. Klicken Sie auf OK.

ine roange n	une: Kosti		uge										
art Time —							End Time						
O Start n	wv						O Never e	end					
<li>Start at</li>							💿 End at	(inclusive)					
Month:	February	~	Day:	05 💌	Year: 2	2011 🛩	Month:	February	*	Day:	06 🛩	Year:	2011
Hours	6.4			C				100			-		
curring Tim You can fur start and st	e Ranges — ther constra op time spei	in the	Minute: active ti	me of this	s range by	/ specifying (	Hour: ecurring ranges,	16 The recurrin	ng tim	Minute: e ranges	30 💌	tive wit	hin the
ecurring Tim You can fur start and st	e Ranges — ther constra op time spe	in the	Minute: active ti	me of this	s range by	/ specifying (	Hour: ecurring ranges.	16 The recurrin	ng tim	Minute: e ranges	30 💌	tive wit	hin the Add
ecurring Tim You can fur start and st	e Ranges — ther constra op time spec	in the	Minute:	me of this	s range by	/ specifying (	Hour: ecurring ranges.	16 The recurri	ng tim	Minute: e ranges	30 💌		hin the Add Edit
You can fur	e Ranges — ther constra op time spe	in the	Minute: active ti	me of this	s range by	r specifying i	Hour: ecurring ranges.	The recurrin	ng tim	Minute: e ranges	30 💌		hin the Add Edit Delete
You can fur You can fur	e Ranges — ther constra op time spe	in the	Minute:	me of this	s range by	/ specifying (	Hour: ecurring ranges,	The recurrin	ng tim	Minute: e ranges	30 💌		hin the Add Edit Delete
You can fur start and st	e Ranges — ther constra op time spe	in the	Minute:	me of this	s range by	/ specifying (	Hour: ecurring ranges.	The recurri	ng tim	Minute: e ranges	30 💌		hin the Add Edit Delete

4. Hier sehen Sie den Zeitbereich. Klicken Sie auf OK, um zum Fenster Zugriffsregel

Add 💣 Edit 💼 Delete Name Start Time End Time Recurring Entries Res 14:00 05 Fe 16:30 06 F	Brows	e Time Rang	e	
Name Start Time End Time Recurring Entries Res 14:00 05 Fe 16:30 06 F	Add	🖬 Edk 💼 De	elete	
Res 14:00 05 Fe 16:30 06 F	Name	Start Time	End Time	Recurring Entries
	Res	14:00 05 Fe	. 16:30 D6 F	
	1			
	đ	ОК	Cancel	Help

hinzufügen zurückzukehren.

5. Sie können jetzt sehen, dass der Zeitbereich Beschränkung der Nutzung an diese Zugriffsregel gebunden

tenate:	
	ermit 🕑 Deny
ource:	172.16.10.50
estination	any -
ervice:	ip 🕢
accription :	
Enable L	ogging
Enable L	ogging .evel: Default
Enable L Logging I	ogging Level: Default
Enable L Logging I More Opt	ogging .evel: Default 💌 Ions Rule
Enable L Logging I More Opt	ogging Level: Default Ions Rule ection: O In O Out
Enable L Logging I More Opt Enable Traffic Dire Source Ser	ogging Level: Default ions Rule ection: O In O Out vice: (TCP or UDP service)
Enable L Logging I More Opt Enable Traffic Dire Source Ser	ogging Level: Default ions Rule ection: O In O Out vice: (TCP or UDP service terval: 300 seconds

#### wurde.

dieser Zugriffsregelkonfiguration ist der Benutzer von 172.16.10.50 auf die Verwendung von Ressourcen vom 05.02.2011, 14.06.2011, 16.30 Uhr, beschränkt. Dies ist die entsprechende CLI-Ausgabe:

```
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
```

 Im Folgenden finden Sie ein Beispiel zum Angeben eines sich wiederholenden Zeitbereichs. Klicken Sie auf Hinzufügen, um einen sich wiederholenden Zeitraum zu definieren.

Edit Time Range	
Time Range Name: Restrict-Usage	
Start Time	End Time
◯ Start now	O Never end
⊙ Start at	End at (inclusive)
Month: February 🖌 Day: 05 🖌 Year: 2011 🖌	Month: March 💌 Day: 06 🛩 Year: 2011
Hour: 00 Minute: 00 M	Hour: 00 Minute: 30 🛩
Peruring 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.	
	Add
	Edit

7. Geben Sie die Einstellungen entsprechend Ihren Anforderungen an, und klicken Sie auf **OK**, um den Vorgang

<ul> <li>Specify days of the week and times</li> </ul>	on which this recurring range will be active
For example, use this option when y Monday through Thursday, from 8:0	ou want the time range to be active every 0 through 16:59, only.
Days of the Week	
O Every day	
🔿 Weekdays	
O Weekends	
On these days of the week:	
Mon V Tue V Wed	V Thu V Fri Sat Sun
Daily Start Time	Daily End Time (Inclusive)
Daily Start Time Hour 15 🖌 Minute 00 🛩	Daily End Time (Inclusive) Hour 🔯 💉 Minute 00 💉
Daly Start Time Hour 15 Minute 00 V	Daily End Time (Inclusive) Hour 🔯 💉 Minute 00 💉
Daily Start Time Hour 15 Minute 00 Minute     Specify a weekly interval when this in For example, use this option when y continuously from Monday at 8:00 th	Daily End Time (Inclusive) Hour I Minute 00 Minute Co Mi
Daly Start Time Hour 15 Minute 00 Minute Specify a weekly interval when this in For example, use this option when y continuously from Monday at 8:00 the Weekly Interval	Daily End Time (Inclusive)         Hour       Minute         Minute       00         ecurring range will be active         ou want the time range to be active         rough Friday at 16:59.
Daly Start Time Hour 15 Minute 00 Minute Specify a weekly interval when this in For example, use this option when y continuously from Monday at 8:00 th Weekly Interval From: Monday Monday Hour:	Daily End Time (Inclusive)         Hour       Minute         ecurring range will be active         ou want the time range to be active         rough Friday at 16:59.         OO         Minute:         OO

8. Klicken Sie auf **OK**, um zum Fenster Zeitbereich zurückzukehren.

🚳 Edit Time	e Range											
Time Range N	lame: Restric	t-Usage										
Start Time —						End Time						
🔿 Start no	DW					O Never e	end					
<ul> <li>Start at</li> </ul>	:					💿 End at	(inclusive)					
Month:	February	Y Day:	05 🛩	Year:	2011 💌	Month:	March	~	Day:	06	Year	: 201
Hour:	00	Minute:	00 🗸			Hour:	00	~	Minute:	30	~	
You can fur start and st weekdays	ther constrai top time spec 15:00 throug	in the active ti ified. h 20:00	me of thi	s range t	iy specifying	recurring ranges.	The recur	ring tim	e ranges	will be	active w	thin the
												Edk
											L	Delete
-												
			đ	ОК		ancel H	lelp 📄					

Laut dieser Konfiguration wurde dem Benutzer am 17.16.10.50 von 15:00 bis 20:00 Uhr an allen Wochentagen außer Samstag und Sonntag der Zugriff auf Ressourcen verweigert.

```
!
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
```

**Hinweis:** Wenn ein **Zeitbereichsbefehl** sowohl absolute als auch periodische Werte angegeben hat, werden die **periodischen** Befehle erst nach Erreichen der absoluten Startzeit ausgewertet und nach Erreichen der absoluten Endzeit nicht weiter ausgewertet.

# Zugehörige Informationen

- <u>Cisco ASA-Dokumentationsseite</u>
- <u>Technischer Support und Dokumentation Cisco Systems</u>