# ASA 7.x/PIX 6.x und höher: Beispiel für die Port-Konfiguration öffnen/blockieren

## Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Zugehörige Produkte Konventionen Konfigurieren Netzwerkdiagramm Blockieren der Port-Konfiguration Öffnen der Port-Konfiguration Öffnen der Port-Konfiguration Konfiguration über ASDM Überprüfen Fehlerbehebung Zugehörige Informationen

# **Einführung**

Dieses Dokument enthält eine Beispielkonfiguration zum Öffnen oder Blockieren der Ports für die verschiedenen Datenverkehrstypen, z. B. http oder ftp, in der Sicherheits-Appliance.

**Hinweis:** Die Begriffe "Öffnen des Ports" und "Zulassen des Ports" haben dieselbe Bedeutung. Ebenso bieten "Blockieren des Ports" und "Einschränken des Ports" dieselbe Bedeutung.

# **Voraussetzungen**

### **Anforderungen**

In diesem Dokument wird davon ausgegangen, dass PIX/ASA konfiguriert ist und ordnungsgemäß funktioniert.

### Verwendete Komponenten

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

- Cisco Adaptive Security Appliance (ASA) der Serie 5500 mit Version 8.2(1)
- Cisco Adaptive Security Device Manager (ASDM) Version 6.3(5)

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.

### Zugehörige Produkte

Diese Konfiguration kann auch mit der Cisco PIX Firewall Appliance der Serie 500 mit der Software 6.x und höher verwendet werden.

### **Konventionen**

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

## **Konfigurieren**

Jede Schnittstelle muss eine Sicherheitsstufe zwischen 0 (niedrigste Stufe) und 100 (höchste Stufe) aufweisen. Beispielsweise müssen Sie Ihr sicherstes Netzwerk, z. B. das interne Hostnetzwerk, Ebene 100 zuweisen. Das mit dem Internet verbundene externe Netzwerk kann die Ebene 0 sein, während andere Netzwerke, z. B. DMZs, dazwischen positioniert werden können. Sie können derselben Sicherheitsstufe mehrere Schnittstellen zuweisen.

Standardmäßig sind alle Ports an der externen Schnittstelle (Sicherheitsstufe 0) blockiert, und alle Ports sind an der internen Schnittstelle (Sicherheitsstufe 100) der Sicherheits-Appliance offen. Auf diese Weise kann der gesamte ausgehende Datenverkehr ohne Konfiguration durch die Security Appliance geleitet werden. Eingehender Datenverkehr kann jedoch durch die Konfiguration der Zugriffsliste und der statischen Befehle in der Security Appliance zugelassen werden.

**Hinweis:** Im Allgemeinen werden alle Ports von der unteren Sicherheitszone zur oberen Sicherheitszone blockiert, und alle Ports sind von der oberen Sicherheitszone zur unteren Sicherheitszone geöffnet, sofern die Stateful Inspection sowohl für eingehenden als auch für ausgehenden Datenverkehr aktiviert ist.

Dieser Abschnitt besteht aus den folgenden Unterabschnitten:

- <u>Netzwerkdiagramm</u>
- Blockieren der Port-Konfiguration
- <u>Öffnen der Port-Konfiguration</u>

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

**Hinweis:** Verwenden Sie das <u>Command Lookup Tool</u> (nur <u>registrierte</u> Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

#### **Netzwerkdiagramm**

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



### Blockieren der Port-Konfiguration

Die Sicherheits-Appliance erlaubt jeglichen ausgehenden Datenverkehr, es sei denn, er wird explizit von einer erweiterten Zugriffsliste blockiert.

Eine Zugriffsliste besteht aus einem oder mehreren Zugriffskontrolleinträgen. Abhängig vom Zugriffslistentyp können Sie Quell- und Zieladressen, Protokolle, Ports (für TCP oder UDP), ICMP-Typ (für ICMP) oder EtherType angeben.

**Hinweis:** Für verbindungslose Protokolle wie ICMP erstellt die Sicherheitsappliance unidirektionale Sitzungen. Sie benötigen daher entweder Zugriffslisten, um ICMP in beide Richtungen zuzulassen (durch die Anwendung von Zugriffslisten auf die Quell- und Zielschnittstellen), oder Sie müssen die ICMP-Prüfungs-Engine aktivieren. Die ICMP Inspection Engine behandelt ICMP-Sitzungen als bidirektionale Verbindungen.

Führen Sie diese Schritte aus, um die Ports zu blockieren, die normalerweise für Datenverkehr gelten, der von der Innenseite (der höheren Sicherheitszone) zur DMZ (der unteren Sicherheitszone) oder zur DMZ zur Außenseite stammt.

1. Erstellen Sie eine Zugriffssteuerungsliste, sodass der angegebene Port-Datenverkehr blockiert wird.

access-list

2. Binden Sie dann die Zugriffsliste mit dem Befehl access-group, um aktiv zu sein.

access-group

#### **Beispiele:**

1. HTTP-Port-Datenverkehr blockieren: Um den Zugriff des internen Netzwerks 10.1.1.0 auf das http (Webserver) zu blockieren, wobei IP 172.16.1.1 im DMZ-Netzwerk platziert wird, erstellen Sie eine ACL wie folgt:

```
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
```

Hinweis: Verwenden Sie no gefolgt von den Befehlen der Zugriffsliste, um die Port-Blockierung zu entfernen.

2. Blockieren des FTP-Port-Datenverkehrs: Um den Zugriff des internen Netzwerks 10.1.1.0 auf den FTP (Dateiserver) zu blockieren, in dem IP 172.16.1.2 im DMZ-Netzwerk platziert wird, erstellen Sie eine ACL wie folat:

```
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
```

Hinweis: <u>IANA-Ports</u> bieten weitere Informationen zu Portzuweisungen.

In diesem Abschnitt wird die schrittweise Konfiguration zur Durchführung dieser Aufgabe über das ASDM dargestellt.

1. Gehen Sie zu Konfiguration > Firewall > Zugriffsregeln. Klicken Sie auf Zugriffsregel hinzufügen, um die Zugriffsliste zu



2. Definieren Sie Quelle und Ziel sowie die Aktion der Zugriffsregel zusammen mit der Schnittstelle, der diese Zugriffsregel zugeordnet wird. Wählen Sie die Details aus, um den zu blockierenden Port

	🖆 Add Access Rule
	Interface: 🚺
	Action: O Permit O Deny
	Source: (10.1.1.0)
	Destination 172.16.1.1
	Service: ip
	Description:
	Enable Logging
	Logging Level: Default 💉
	More Options
	OK Cancel Help
auszuwanien.	

3. Wählen Sie **http** aus der Liste der verfügbaren Ports aus, und klicken Sie dann auf **OK**, um zum Fenster Zugriffsregel hinzufügen

discard	Protocol	Source Ports	Paultin Mine Paula	the second second second second	the second se	
discard			Descriation Ports	ICMP Type	Description	
	top	default (1-65535)	9			
damain	top	default (1-65535)	\$3			
echo	top	default (1-65535)	7			
OVEC	top	default (1-65535)	512			
finger	trp	default (1-65535)	79			
ftp.	top	default (1-65535)	21			
ftp-data	top	default (1-65535)	20			
gopher	top	default (1-65535)	70			
h323	top	default (1-65535)	1720			
hostname	top	default (1-65535)	101			
hitp	top	default (1-65535)	160		E	3
Ntps	top	default (1-65535)	443			
ident	top	default (1-65535)	113			
iniap4	top	default (1-69535)	143			
irc.	top	default (1-65535)	194			
kerberos.	top.	default (1-65535)	750			
klogin	top	defauk (1-65535)	543			
Subel	top	default (1-69535)	544			
Idap	top	default (1-65535)	389			
idaps	top	defauk (1-69535)	636			
	echo exec finger Ap Ap Ap Ap Ada Ada Ada Ada Ada Ada Ada Ada Ada Ada	echo top exec top finger top Ap too Ap too Ap too Adda top Adda top Adda top intent top	echo         top         default (1-65535)           exerc         top         default (1-65535)           finger         top         default (1-65535)           ftp         top         default (1-65535)           ftp-data         top         default (1-65535)           gapher         top         default (1-65535)           h323         top         default (1-65535)           h450         top         default (1-65535)           h450         top         default (1-65535)           h450         top         default (1-65535)           ident         top         default (1-65535)           ince         top         default (1-65535)           icc         top         default (1-65535)           isogn         top         default (1-65535)           isogn         top         default (1-65535)           iden         top         default (1-65535)           idap         top         default (1-65535) <td>echo         top         default (1-65535)         7           exerc         top         default (1-65535)         512           finger         top         default (1-65535)         512           fup         top         default (1-65535)         79           fup         top         default (1-65535)         20           gapher         top         default (1-65535)         20           gapher         top         default (1-65535)         70           h323         top         default (1-65535)         1720           hastname         top         default (1-65535)         101           https         top         default (1-65535)         101           https         top         default (1-65535)         113           ident         top         default (1-65535)         113           inc         top         default (1-65535)         143           inc         top         default (1-65535)         194           kerberos         top         default (1-65535)         543           jaheil         top         default (1-65535)         544           idap         top         default (1-65535)         544           idap<!--</td--><td>echo         tup         default (1-65535)         7           exerc         tup         default (1-65535)         512           finper         tup         default (1-65535)         512           fup         tup         default (1-65535)         79           fup         tup         default (1-65535)         21           fup-data         tup         default (1-65535)         20           gapher         tup         default (1-65535)         20           hstrame         tup         default (1-65535)         1720           hstrame         tup         default (1-65535)         101           https         tup         default (1-65535)         101           https         tup         default (1-65535)         113           incert         tup         default (1-65535)         143           inc         tup         default (1-65535)         194           kerberos         tup         default (1-65535)         543           kogn         tup         default (1-65535)         543           kabal         tup         default (1-65535)         544           idap         tup         default (1-65535)         544           i</td><td>exho         top         default (1-65535)         7           exec         top         default (1-65535)         512           finper         trp         default (1-65535)         21           ftp-data         top         default (1-65535)         20           gapher         top         default (1-65535)         20           gapher         top         default (1-65535)         20           hstname         top         default (1-65535)         10           h323         top         default (1-65535)         101           h323         top         default (1-65535)         101           h423         top         default (1-65535)         101           h455         top         default (1-65535)         143           ident         top         default (1-65535)         143           inc         top         default (1-65535)         143           irc         top         default (1-65535)         194           kerberos         top         default (1-65535)         194           kerberos         top         default (1-65535)         543           label         top         default (1-65535)         544           ida</td></td>	echo         top         default (1-65535)         7           exerc         top         default (1-65535)         512           finger         top         default (1-65535)         512           fup         top         default (1-65535)         79           fup         top         default (1-65535)         20           gapher         top         default (1-65535)         20           gapher         top         default (1-65535)         70           h323         top         default (1-65535)         1720           hastname         top         default (1-65535)         101           https         top         default (1-65535)         101           https         top         default (1-65535)         113           ident         top         default (1-65535)         113           inc         top         default (1-65535)         143           inc         top         default (1-65535)         194           kerberos         top         default (1-65535)         543           jaheil         top         default (1-65535)         544           idap         top         default (1-65535)         544           idap </td <td>echo         tup         default (1-65535)         7           exerc         tup         default (1-65535)         512           finper         tup         default (1-65535)         512           fup         tup         default (1-65535)         79           fup         tup         default (1-65535)         21           fup-data         tup         default (1-65535)         20           gapher         tup         default (1-65535)         20           hstrame         tup         default (1-65535)         1720           hstrame         tup         default (1-65535)         101           https         tup         default (1-65535)         101           https         tup         default (1-65535)         113           incert         tup         default (1-65535)         143           inc         tup         default (1-65535)         194           kerberos         tup         default (1-65535)         543           kogn         tup         default (1-65535)         543           kabal         tup         default (1-65535)         544           idap         tup         default (1-65535)         544           i</td> <td>exho         top         default (1-65535)         7           exec         top         default (1-65535)         512           finper         trp         default (1-65535)         21           ftp-data         top         default (1-65535)         20           gapher         top         default (1-65535)         20           gapher         top         default (1-65535)         20           hstname         top         default (1-65535)         10           h323         top         default (1-65535)         101           h323         top         default (1-65535)         101           h423         top         default (1-65535)         101           h455         top         default (1-65535)         143           ident         top         default (1-65535)         143           inc         top         default (1-65535)         143           irc         top         default (1-65535)         194           kerberos         top         default (1-65535)         194           kerberos         top         default (1-65535)         543           label         top         default (1-65535)         544           ida</td>	echo         tup         default (1-65535)         7           exerc         tup         default (1-65535)         512           finper         tup         default (1-65535)         512           fup         tup         default (1-65535)         79           fup         tup         default (1-65535)         21           fup-data         tup         default (1-65535)         20           gapher         tup         default (1-65535)         20           hstrame         tup         default (1-65535)         1720           hstrame         tup         default (1-65535)         101           https         tup         default (1-65535)         101           https         tup         default (1-65535)         113           incert         tup         default (1-65535)         143           inc         tup         default (1-65535)         194           kerberos         tup         default (1-65535)         543           kogn         tup         default (1-65535)         543           kabal         tup         default (1-65535)         544           idap         tup         default (1-65535)         544           i	exho         top         default (1-65535)         7           exec         top         default (1-65535)         512           finper         trp         default (1-65535)         21           ftp-data         top         default (1-65535)         20           gapher         top         default (1-65535)         20           gapher         top         default (1-65535)         20           hstname         top         default (1-65535)         10           h323         top         default (1-65535)         101           h323         top         default (1-65535)         101           h423         top         default (1-65535)         101           h455         top         default (1-65535)         143           ident         top         default (1-65535)         143           inc         top         default (1-65535)         143           irc         top         default (1-65535)         194           kerberos         top         default (1-65535)         194           kerberos         top         default (1-65535)         543           label         top         default (1-65535)         544           ida

zurückzukehren.

4. Klicken Sie auf **OK**, um die Konfiguration der Zugriffsregel abzuschließen.

🖆 Add Aco	cess Rule
Interface:	inside 😽
Action: 🔘	Permit 💿 Deny
Source:	10.1.1.0
Destination	172.16.1.1
Service:	(tcp/http
Description:	
💌 Enable L	ogging
Logging	Level: Default 🖌
More Opt	ions
	OK Cancel Help

5. Klicken Sie auf **Nach einfügen**, um derselben Zugriffsliste eine Zugriffsregel

🖶 Add 👻 🖸	r Edit 前 Delete	+ +	👗 🖻 💼 - 🔍 Fi
🚱 Add Ac	tess Rule		Destination
🚱 Insert	9 		
💠 Insert A	After	1.0	📕 172.16.1.1
-	See any	9	🏟 any
🗄 🧢 manag	e (2 implicit incomin	g rules)	
1	🌍 any		Any less secur
2	anv		i anv

hinzuzufügen.

6. Zulassen des Datenverkehrs von "any" zu "any", um die "implizite Verweigerung" zu verhindern. Klicken Sie anschließend auf **OK**, um diese Zugriffsregel hinzuzufügen.

🖆 Insert A	fter Access Rule
Interface:	inside 🖌 🗠
Action: 💿	Permit 🔿 Deny
Source:	any
Destination	any
Service:	ip
Description:	
💌 Enable L	ogging
Logging	Level: Default 🛛 🔛
More Opt	ions
	OK Cancel Help

7. Die konfigurierte Zugriffsliste wird auf der Registerkarte "Zugriffsregeln" angezeigt. Klicken Sie auf **Apply**, um diese Konfiguration an die Sicherheits-Appliance zu senden.

1	Enabled	Source	Destination	Service	Action	Hits
St ins	ide (3 incom	ing rules)				
1	~	團 10,1.1.0	A 172.16.1.1	10 http	3 Deny	
2	<b>V</b>	any	🔹 any	😰 ip	🥩 Permit	
3		🧼 any	🏟 any	<u>⊥r&gt;</u> ip	😻 Deny	
🥵 ma	nage (2 imp	olicit incoming rules)				
1		🌍 апу	Any less secure ne	💷 ip	🖌 Permit	
2		🍥 any	🏟 any	<mark>⊥e</mark> > ip	🕴 Deny	
🝠 ou	tside (1 imp	licit incoming rule)		-		
1		any	any	IP ip	3 Deny	
ess Rul	е Туре 🔿	IPv4 and IPV6 💿 IPv	/4 Only 🔿 IPv6 Only			

Die vom ASDM gesendete Konfiguration führt zu dieser Gruppe von Befehlen in der Befehlszeilenschnittstelle (CLI) der ASA.

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

In diesen Schritten wurde Beispiel 1 über ASDM durchgeführt, um den Zugriff des Netzwerks 10.1.1.0 auf den Webserver zu blockieren (172.16.1.1). Beispiel 2 kann auch auf die gleiche Weise erreicht werden, um den Zugriff des gesamten 10.1.1.0-Netzwerks auf den FTP-Server 172.16.1.2 zu blockieren. Der einzige Unterschied besteht darin, dass der Port ausgewählt wird.**Hinweis:** Bei dieser Zugriffsregelkonfiguration für Beispiel 2 wird von einer neuen Konfiguration ausgegangen.

8. Definieren Sie die Zugriffsregel für die Blockierung von FTP-Datenverkehr, und klicken Sie dann auf die Registerkarte **Details**, um den Zielport

	📬 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
auszuwählen.		

9. Wählen Sie den **FTP-**Port aus, und klicken Sie auf **OK**, um zum Fenster Zugriffsregel hinzufügen zurückzukehren.

er:					
lame	Protocol	Source Ports	Destination Ports	ICMP Type	Description
ter citrix-ica	top	default (1-65535)	1494		
tiqbe	top	default (1-65535)	2748		
- 100 daytime	tcp	default (1-65535)	13		
tte discard	top	default (1-65535)	9		
tte domain	top	default (1-65535)	53		
echo	top	default (1-65535)	7		
ter exec	top	default (1-65535)	512		
100 finger	tcp	default (1-65535)	79		
- 😥 ftp	tcp	default (1-65535)	21		-
no ftp-data	top	default (1-65535)	20		
gopher	tcp	default (1-65535)	70		
- 100 h323	tcp	default (1-65535)	1720		
👷 hostname	tcp	default (1-65535)	101		
- ter 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		
- III irc	tcp	default (1-65535)	194		
- 🚾 kerberos	tcp	default (1-65535)	750		
Ann Mania	hen	default (1 (EEDE)	E49		
ected Service					

10. Klicken Sie auf **OK**, um die Konfiguration der Zugriffsregel abzuschließen.

📧 Add Acc	ess Rule
Interface:	inside 💌
Action: 🚫 I	Permit 💿 Deny
Source:	10.1.1.0
Destination	172,16.1.1
Service:	tcp/ftp
Description:	
💽 Enable L	ogging
Logging I	Level: Default
More Opt	ions
	OK Cancel Help

11. Fügen Sie eine andere Zugriffsregel hinzu, um anderen Datenverkehr zuzulassen. Andernfalls wird der gesamte Datenverkehr auf dieser Schnittstelle durch die Regel "Implicit

🌃 Insert A	fter Access Rule
Interface:	inside 😽
Action: 💿 I	Permit 🔿 Deny
Source:	any
Destination	any 💮
Service:	ip
Description:	
💽 Enable L	ogging
Logging I	Level: Default 💙
More Opt	ions
	OK Cancel

Deny" blockiert. 12. Die vollständige Konfiguration der Zugriffslisten sieht auf der Registerkarte "Zugriffsregeln" wie folgt

aus.

#	Enabled	Source	Destination	Service	Action
🗟 🔧 i	nside (3 incom	ning rules)			
1	<b>v</b>	🔳 10.1.1.0	🖳 172.16.1.1	🚾 ftp	🕴 Den
2		🐔 any	🐑 any	😰 ip	🛹 Pern
3		🧼 any	🧼 any	🗶 ip	🕴 Den
i 🍕 🍦	nanage (2 imp	licit incoming rules)			
1		🏈 any	Any less secure ne	JP> ip	🛹 Perr
2		🌍 any	🧼 any	10 ip	🕄 Den
🛓 🦊 e	outside (1 impl	licit incoming rule)			
1		🥥 any	iny any	😕 ip	😮 Den

 Klicken Sie auf Apply, um die Konfiguration an die ASA zu senden. Die entsprechende CLI-Konfiguration sieht wie folgt aus:

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

### Öffnen der Port-Konfiguration

Die Sicherheits-Appliance erlaubt keinen eingehenden Datenverkehr, es sei denn, dieser wird ausdrücklich von einer erweiterten Zugriffsliste zugelassen.

Wenn Sie einem externen Host den Zugriff auf einen internen Host gestatten möchten, können Sie eine Liste eingehender Zugriffe auf die externe Schnittstelle anwenden. Sie müssen die übersetzte Adresse des internen Hosts in der Zugriffsliste angeben, da die übersetzte Adresse die Adresse ist, die im externen Netzwerk verwendet werden kann. Führen Sie diese Schritte aus, um die Ports von der unteren Sicherheitszone zur höheren Sicherheitszone zu öffnen. Zulassen des Datenverkehrs von außen (untere Sicherheitszone) zur internen Schnittstelle (obere Sicherheitszone) oder der DMZ zur internen Schnittstelle.

 Static NAT erstellt eine feste Übersetzung einer echten Adresse in eine zugeordnete Adresse. Diese zugeordnete Adresse ist eine Adresse, die im Internet gehostet wird und für den Zugriff auf den Anwendungsserver der DMZ verwendet werden kann, ohne dass die tatsächliche Adresse des Servers bekannt sein muss.

static (real\_ifc,mapped\_ifc) mapped\_ip {real\_ip [netmask mask] |
 access-list access\_list\_name | interface}

Weitere Informationen finden Sie im Abschnitt Static NAT der Befehlsreferenz für PIX/ASA.

2. Erstellen Sie eine ACL, um den spezifischen Port-Datenverkehr zuzulassen.

```
access-list
```

3. Binden Sie die Zugriffsliste mit dem Befehl access-group, um aktiv zu sein.

```
access-group
```

#### **Beispiele:**

 Öffnen Sie den SMTP-Port-Datenverkehr: Öffnen Sie den Port tcp 25, damit die Hosts von außen (Internet) auf den im DMZ-Netzwerk angeordneten Mailserver zugreifen können.Der statische Befehl ordnet die externe Adresse 192.168.5.3 der echten DMZ-Adresse

```
172.16.1.3 ZU.

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
```

 Öffnen Sie den HTTPS-Port-Datenverkehr: Öffnen Sie den Port tcp 443, damit die Hosts von außen (Internet) auf den im DMZ-Netzwerk (sicher) eingerichteten Webserver zugreifen können.

```
ciscoasa(config)#static (DMZ,Outside) 192.168.5.5 172.16.1.5
netmask 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. DNS-Datenverkehr zulassen: Öffnen Sie den Port udp 53, um den Hosts von außen (Internet) den Zugriff auf den DNS-Server (sicher) im DMZ-Netzwerk zu ermöglichen. 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

Hinweis: <u>IANA-Ports</u> bieten weitere Informationen zu Portzuweisungen.

#### Konfiguration über ASDM

In diesem Abschnitt wird ein schrittweiser Ansatz zur Durchführung der oben genannten Aufgaben über ASDM dargestellt.

1. Erstellen Sie die Zugriffsregel, um den SMTP-Datenverkehr zum Server 192.168.5.3



zuzulassen.

2. Definieren Sie die Quelle und das Ziel der Zugriffsregel und die Schnittstelle, mit der diese Regel verknüpft ist. Definieren Sie die Aktion auch als

	🖆 Add Access Rule
	Interface: Outside 💌
	Action: O Permit O Deny
	Source: any
	Destination 192.168.5.3
	Service: ip
	Description:
	Enable Logging
	Logging Level: Default 💽
	More Options
	OK Cancel Help
assen.	

3. Wählen Sie SMTP als Port aus, und klicken Sie dann auf

Filter:					
Name	Protocol	Source Ports	Destination Ports	ICMP Type	Descripti
Mar hhith	han .	defects (1 constant)	E76-0	1	
BOD rsn	COD	default (1-60000)	514		
- ne risp	top	default (1-65535)	504		
sp	lice	default (1+65555)	3060		
Look salesh	- boo	dof a(# (1.65535)	1521		
squer	hop	default (1-65030)	22		
531	top	default (1-65535)	111		
Surrec	hop	default (1-65535)	40		
tall tall	boo	dolarit (1-65535)	517		
helpet	han	default (1-60000)	22		
Est comec	ten.	default (1-65535)	540		
and a second	box	default (1.65535)	49		
L SE	uda	default (0.65535)	512		
100 beeter	uda	default (0-65555)	20		
- Mer bootpc	udo	default (0-65555)	67		
Mer bootps	ueto	dofault (0-65535)	3020		
- Mr. City	ude	default (0.65535)	0		
discard	ude	default (0-65555)	100		
Mar distri	udo	default (0-65535)	E2		
un coman	See.	L / A lo second			
Selected Service					
Service ->	io .				

4. Klicken Sie auf OK, um die Konfiguration der Zugriffsregel

🖆 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

abzuschließen.

5. Konfigurieren Sie die statische NAT f
ür die Übersetzung von 172.16.1.3 in 192.168.5.3.Gehen Sie zu Konfiguration > Firewall > NAT Rules > Add Static NAT Rule, um einen statischen NAT-Eintrag



hinzuzufügen.

Wählen Sie die ursprüngliche

und die umgewandelte IP-Adresse zusammen mit den zugehörigen Schnittstellen aus, und klicken Sie dann auf **OK**, um die Konfiguration der statischen NAT-Regel

	📧 Add Static NAT Rule	
	Original Interface: DMZ Source: 172.16.1.3	•
	Translated	
	Interface: (outside)	~
	OUse IP Address: 192.168.5.3	
	O Use Interface IP Address	
	Port Address Translation (PAT)	
	Enable Port Address Translation (PAT)	
	Protocol; 💿 TCP 🔿 UDP	
	Original Port:	
	Translated Port:	
	Connection Settings	*
abzuschließen.	OK Cancel Help	C

ieses Bild zeigt alle drei statischen Regeln, die im Abschnitt <u>Beispiele</u> aufgeführt sind:

onfiq	uration > Firewa	b <mark>il &gt; NAT Rules</mark> Delete ★ ◆ X □	🗈 🎆 - 🛛 Q, Find	🖽 Diagram 🕯	🕐 Packet Trace			
4	Туре	Original	Original			Translated		
#		Source	Destination	Service	Interface	Address		
DMZ		Proving land						
1	• Static	3 172.16.1.3			outside	₫ 192.168.5.3		
2	• • Static	<b>172.16.1.5</b>			outside	A 192.168.5.5		
3	Static	172.16.1.4			outside	192.168.5.4		

Dieses Bild zeigt alle drei Zugriffsregeln, die im Abschnitt <u>Beispiele</u> aufgeführt sind:

#	Enabled	Source	Destination	Service	Action
ي 🕰 (	OMZ (2 implicit	incoming rules)	Paste		
1		🏟 any	Any less secure ne	IP/ ip	🖌 Permit
2		🍥 any	🏟 any	IP> ip	🕴 Deny
<b>.</b> 科 i	nside (2 implic	t incoming rules)			
1		🌍 any	Any less secure ne	IP ip	🖌 Permit
2		🧼 any	🏟 any	IP/ ip	🔕 Deny
- <b>5</b>	manage (2 imp	licit incoming rules)			
1		🏟 any	Any less secure ne	IP ip	🖌 Permit
2		🏟 any	🏟 any	JE> ip	😢 Deny
<b>- P</b> o	outside (4 inco	ming rules)			
1	¥	🧼 any	📇 192.168.5.3	smtp	🖌 Permit
2		🏟 any	192.168.5.5	100 https	🖌 Permit
3	V	🥌 any	192.168.5.4	🚥 domain	🧹 Permit
4		<ul> <li>any</li> </ul>	any	IP/ ip	🕄 Deny

# <u>Überprüfen</u>

Sie können die Überprüfung mit bestimmten show-Befehlen wie folgt durchführen:

- Exlate anzeigen aktuelle Übersetzungsinformationen anzeigen
- show access-list Anzeige von Trefferzählern für Zugriffsrichtlinien
- show logging: Zeigt die Protokolle im Puffer an.

Das <u>Output Interpreter Tool</u> (nur <u>registrierte</u> Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

# **Fehlerbehebung**

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

# Zugehörige Informationen

- PIX/ASA 7.x: Aktivieren/Deaktivieren der Kommunikation zwischen Schnittstellen
- <u>PIX 7.0 und Adaptive Security Appliance Port Redirection (Forwarding) mit nat-, global,</u> statisch, rohr- und Zugriffslisten-Befehlen
- Verwendung von NAT-, globalen, statischen, Kanal- und Zugriffslisten-Befehlen und Port <u>Redirection (Forwarding) auf PIX</u>
- PIX/ASA 7.x: Beispiel für die Konfiguration von FTP- und TFTP-Services aktivieren
- PIX/ASA 7.x: Konfigurationsbeispiel für VoIP-Services (SIP, MGCP, H323, SCCP) aktivieren
- PIX/ASA 7.x: Mailserver-Zugriff auf das DMZ-Konfigurationsbeispiel
- <u>Technischer Support und Dokumentation Cisco Systems</u>