Cisco CP - ZFW configureren om peer te blokkeren tot peer verkeer

Inhoud

Inleiding Voorwaarden Vereisten Routerconfiguratie om Cisco CP te starten Gebruikte componenten Conventies Achtergrondinformatie Configureren Netwerkdiagram Configuratie door Cisco Configuration Professional Opdracht-lijnconfiguratie van ZFW router Verifiëren Gerelateerde informatie

Inleiding

Dit document biedt een stap-voor-stap benadering om een Cisco IOS-router te configureren als een op zone gebaseerde firewall om peer-to-peer (P2P) verkeer te blokkeren door de wizard Geavanceerde firewall in Cisco Configuration Professional (Cisco CP) te gebruiken.

Zone-Based Policy Firewall (ook bekend als Zone-Policy Firewall, of ZFW) verandert de firewallconfiguratie van het oudere op interface gebaseerde model in een flexibeler, beter begrepen zone-gebaseerd model. Interfaces worden toegewezen aan zones en het inspectiebeleid wordt toegepast op het verkeer tussen de zones. Het interzonebeleid biedt een aanzienlijke flexibiliteit en granulariteit. Daarom kan het verschillende inspectiebeleid worden toegepast op meerdere hostgroepen die zijn aangesloten op dezelfde routerinterface. Zones maken de beveiligingsgrenzen van uw netwerk vast. Een gebied definieert een grens waar verkeer aan beleidsbeperkingen wordt onderworpen wanneer het naar een andere regio van uw netwerk gaat. Het beleid van ZFW om in gebreke te blijven tussen zones ontkent iedereen. Als geen beleid expliciet wordt ingesteld, wordt al het verkeer dat tussen zones beweegt geblokkeerd.

P2P-toepassingen zijn een van de meest gebruikte toepassingen op het internet. P2P-netwerken kunnen fungeren als een geleider voor kwaadaardige dreigingen zoals wormen, die een gemakkelijk pad rond firewalls bieden en zorgen oproepen over privacy en veiligheid. Cisco IOS-softwarerelease 12.4(9)T geïntroduceerde ZFW-ondersteuning voor P2P-toepassingen. P2P-inspectie biedt Layer 4- en Layer 7-beleid voor toepassingsverkeer. Dit betekent dat ZFW een stateful inspection kan voorzien om het verkeer toe te staan of te ontkennen, evenals controle op granulaire Layer 7 op specifieke activiteiten in de verschillende protocollen, zodat bepaalde toepassingsactiviteiten toegestaan zijn terwijl anderen ontkend worden.

Cisco CP biedt een eenvoudig te volgen, stap-voor-stap benadering om de IOS router als een op zone gebaseerde firewall te configureren door de wizard Geavanceerde firewall te gebruiken.

Voorwaarden

Vereisten

Zorg ervoor dat u aan deze vereisten voldoet voordat u deze configuratie probeert:

- De IOS-router moet de softwareversie 12.4(9)T of hoger hebben.
- Voor IOS routermodellen die Cisco CP ondersteunen, raadpleeg de Cisco CP release Notes.

Routerconfiguratie om Cisco CP te starten

Opmerking: voer deze configuratiestappen uit om Cisco CP op een Cisco-router uit te voeren:

```
Router(config)# ip http server
Router(config)# ip http secure-server
Router(config)# ip http authentication local
Router(config)# username <username> privilege 15 password 0 <password>
Router(config)# line vty 0 4
Router(config-line)# privilege level 15
Router(config-line)# login local
Router(config-line)# transport input telnet
Router(config-line)# transport input telnet
Router(config-line)# transport input telnet ssh
Router(config-line)# exit
```

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco 1841 IOS-router die IOS-softwarerelease 12.4(15)T draait
- Cisco Configuration Professional (Cisco CP) release 2.1

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Achtergrondinformatie

Voor het voorbeeld van dit document, wordt de router gevormd als een op zone-gebaseerde firewall om het P2P verkeer te blokkeren. De ZFW router heeft twee interfaces, een binnen (vertrouwde) interface in-zone en een buiten (onvertrouwde) interface in Out-zone. De ZFW-router blokkeert P2P-toepassingen, zoals edonkey, fasttrack, gnutella en kazaa2, met houtkapactie voor het verkeer dat van In-zone naar de Out-zone gaat.

Configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

Opmerking: Gebruik het <u>Opname Gereedschap</u> (<u>alleen geregistreerde</u> klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



Configuratie door Cisco Configuration Professional

Deze sectie bevat de stap-voor-stap procedure op hoe u de wizard kunt gebruiken om de IOSrouter als een op zone gebaseerde firewall te configureren.

Voer de volgende stappen uit:

 Ga naar Configuratie > Veiligheid > Firewall en ACL. Kies vervolgens de knop Advanced Firewall. Klik op De geselecteerde taak starten.



 Dit volgende scherm toont een korte inleiding over de Wizard Firewall. Klik op Next om te beginnen met het configureren van de firewall.

Firewall Wizard	
Firewall Wizard	Advanced Firewall Configuration Wizard Advanced Firewall allows you to secure your private network in the following ways: It allows private network users to access the Internet; it protects your router and private network from the outside attacks; it allows you to configure managed services in DMZ that are accessible from the Internet.
	Advanced Firewall: * Applies default policies to inside(trusted), outside(untrusted) and DMZ zones.
	* Inspect TCP,UDP and other protocols from inside zone to outside zone, as well as router-generated ICMP traffic.
	* Block http port-misuse for im,p2p as well as block all msn, yahoo, aol servers and write the event to log.
	* Deny traffic from outside zones to inside zones.
~	To continue, click Next
	< Back Next > Finish Cancel Help

3. Selecteer de interfaces van de router die deel moet uitmaken van gebieden en klik op **Volgende**.

Firewall Wizard				8
Firewall Wizard	Advanced Firewall Interf Select inside(trusted) a more inside(trusted) an Note: Do not select the outside (untrusted) inte from that interface after Select a DMZ interface i the Internet. These are	ace Configuration nd outside(untrusted) int id outside(untrusted) inte interface through which y rface. If you do, you will n you complete the Firewal if you have servers that yo typically DNS, HTTP, FTP	erfaces. You can s iffaces. ou accessed Cisci ot be able to launcl II Wizard. uu want to make ac and SMTP servers	elect one or o CP as the h Cisco CP cessible from
	interface	outside(untrusted)	inside(trusted)	DMZ
	FastEthernet0/0		R I	Г
	☐ Allow secure Cisco o	CP access from outside)	nterfaces)	
		< Back	Next > Finish	Cancel Help

4. Het standaardbeleid met hoge veiligheid samen met de reeks opdrachten wordt in het volgende venster weergegeven. Klik op **Sluiten** om verder te



- gaan
- 5. Voer de gegevens van de DNS-server in en klik op **Volgende**.

Firewall Wizard	
Firewall Wizard	Advanced Firewall Domain Name Server Configuration Application Security requires that domain name lookup is enabled and at least one DNS server IP address is configured on your router for the policy to operate successfully. Enable domain lookup and enter at least one DNS server IP address.
	Enable DNS based hostname to address translation Primary DNS Server: 10.77.230.45 Secondary DNS Server: (Optional)
	* Back Next > Finish Cancel Help

 De Cisco CP geeft een configuratieoverzicht zoals hier weergegeven. Klik op Voltooien om de configuratie te voltooien.



gedetailleerde configuratie staat in deze tabel. Dit is de standaardconfiguratie volgens het Hoge Veiligheidsbeleid van de CP van Cisco.

7. Controleer het aanvinkvakje **Save the run configuratie to router**. Klik op **Delivery** om deze configuratie naar de router te

server name messenger hotmail.com server name webmessenger hotmail.com exit rearander men hine motional into and servere The differences between the running configuration and the startup configuration are lost whenever the router is turned off.	access-list 100 permit ip ho access-list 100 permit ip 12 access-list 100 permit ip 12 ip name-server 10.77.230 a	_ACL Category=128 if 255.255.255.255 eny 7.0.0.0.0.255.255.255 eny 9.165.201.0.0.0.0.31 eny 5 5			
The differences between the running configuration and the startup configuration are lost whenever the router is turned off.	server name messenger /v server name messenger /v server name gateway mes server name webmesseng exit meramater men time proton	Ainto mshi servers ămail.com senger hotmail.com er.msn.com d into ant cervare			X
	The differences betwee the router is turned off.	the running configuration	n and the startup co	nfiguration are lost w	henever

gehele configuratie wordt aan de router geleverd. Dit duurt enige tijd om te

Commands Delivery Status	
Command Delivery Status:	
Preparing commands for delivery Submitting 264 commands, please wait	~
3	2
ОК	

verwerken.

8. Klik op OK om verder te

Command Delivery Sta	atus:
Preparing commands	for delivery
Submitting 264 comma	ands, please wait
Copying the Running (config to Startup config of your router. Please wait
Running config copied	d successfully to Startup Config of your router.
5	

9. Klik nogmaals op



configuratie is nu in werking en wordt weergegeven als de regels onder het tabblad Firewallbeleid.

nfigure		👬 📄 🥘	Cisc	o Configurat	ion Profession	al dial CISC
Fir	ewall	~				
reate F	irewall	Edit Firewall Policy	0			
🔂 Add	• 🖬	di 🏦 Delete 🏠	Move Up 🐥 Move Down	🛛 🕺 Cut 🐚 Copy 🔞	Paste - Rule Flow Di	agram
	1		Traffic Classification		1 1 1 1 1 1 1	
	1D	Source	Destination	Service	Action	Rule Option
CCP-	permit 1 J 2	ompreply (self to any Unmatched Traffic	out-zone)	icmp tap udp	🛱 Inspect	
ccp-	inspect	t (in-zone to put-z	one)		and the second	
-	1	 100 255.255.255.2 127.0.0.0/0.2 209.165.201.0 	155 -> any 55.255.255 -> any)/0.0.0.31 -> any	🥥 any	🤤 Drop	C Log
	2 3	🧼 any 🎱 any	🏟 any ᡐ any	hitp smtp	HTTP Application I INSpect SMTP Application I	

10. De zones samen met de zone paren zij worden geassocieerd kunnen worden bekeken als u > Veiligheid > Geavanceerd Beveiliging > Gebieden gaat configureren. U kunt ook nieuwe zones toevoegen door op Toevoegen te klikken of de bestaande zones aan te passen door op Bewerken te klikken.

Manitor 🕺	e Cis	sco Configuration Professional	cisco
Configure > Security > A	dvanced Security > Zones		0
odditional Tasks	1		
Zone		Add Edit	Delete
Name	Associated Interfaces	Associated Zone Pairs	
out-zone	FastEthernet0/0	ccp-zp-self-out_ccp-zp-in-out, ccp-zp-out-self	
in-zone	FastEthernet0/1	ccp-zp-in-out	

11. Ga naar **Configureren > Beveiliging > Geavanceerde security > Zone paren** om de details van de zone paren te

- I 🔆 🛛		Cisco Configu	ration Professional	c
gure > Security > A	Advanced Security > Zo	ne Pairs		
Additional Task	s			
Additional Task Pers	\$		Add	D
Additional Task Pairs Zone Pair	Source	Destination	Add Edit	D
Additional Task Pairs Zone Pair cp-zp-self-out	Source self	Destination	Add. Edit. Policy ccp-permit-icmpreply	
Additional Task Pairs Zone Pair cp-zp-self-out cp-zp-in-out	Source self in-zone	Destination out-zone out-zone	Add	

De hulp van de installateur bij het wijzigen/toevoegen/verwijderen van zones/zoneparen en andere verwante informatie is gemakkelijk beschikbaar met de ingebouwde webpagina's in de Cisco

Edit a Zone		
Zone Name	: in-zone	
Choose the	interfaces to associate with the zone.	
	Interface	
🔽 FastEthe	met0/1	
1		
	and the second the second the	
	OK Cancel Help	
co Configuration Professional (nline Help - Windows Internet Lookorer	
💭 🕶 👔 tetju / kocalhost Seccifus	husphone-successfeet FS inclusion (1981-19	- 8
Edit Yose Figwaritas Joals Ha		
灯 Windows Line 🛛 🚺	💽 What's New Profile Mail Photos Calendar MSN Share 🖉 • 🕮 •	in the second se
warkes 🛛 🎪 🍘 Suggested Sites •	🖉 Free Hotmail 👸 SoftStub 🧃 Get Hore Add ens 🔹 🛞 I Price Foundation - Wilco	
sco Configuration Professional Ordine He		
tide da tack ab Forward (Print 🔞 Glassery 📆 Ver PCP	
paie AT Cipand AT	Zana Paler	
Easy VPN Remote	A zone-pair allows you to specify a undirectional firewall policy between two security	zones. The direction of the trai
6 Enly VM Server 6 Enhanced Epsy VM	security zone. The same zone cannot be defined as both the source and the destination of your work traffic to flow in both directions between two transfer on a much constant a	25. was only for such disartion. How
CHVPN GETVPN	indentace must be configured in a zone.	the pair for each department of
Cisco 305 SSL VPN SSL VPN Enhancements	Related Links >	
105 SSL VPN AnyConnect Client	Table 46-3 Zone Pairs	
VPN Options and VPN Keys Encryption		
VPN Troubleshooting	Element Description	<u>-</u>
Internet Key Exchange	Buttons To create a new zone pair, click Add.	
Certificate Authority Server	To edit an existing zone pair, choose the zone pair and click Edit.	
h Public Key Infrastructure Authentication,	To remove a zone pair, choose the zone pair, and click Delete.	
Authorization, and Accounting	Zone Pein The name of the zone pain.	
E Content Filtering Cisco 105 IPS		
Network Admission Control	Source For the selected zone pay, the name of the zone from which traffic ent	ers the router.
Classification Policy Language	Destination For the selected zone pair, the name of the zone to which traffic is seri	21
A 802.1x Authentication		
2010 Zone-Based Policy Firewall	rowsy the name of the policy applied to the 25he pair.	
BAdd or Edit a Zone	Zone Pair Examples h	
General Rules		
Contiguing Voice Features	Copyright © 2009, Cisco Systems, Inc. All rights reserved.	

12. Ga naar **Configuration > Security > Firewall en ACL** om de toepassingsspecifieke controlemogelijkheden voor bepaalde P2P-toepassingen te wijzigen. Klik vervolgens op **Firewallbeleid bewerken** en kies de desbetreffende regel in de beleidskaart. Klik op **Edit**

(Bewerken). Infigure > Security > Firewall and AUL

reate Fi	rewall	Edit Firewall P	olicy				
🔂 Add 🗸	(🖉 E	idit) 😭 Delete	🟫 Move Up 🐥 Move Down	🔏 Cut 🖻 Copy 🛍 Pa	aste 🔹	Rule Flow Dia	agram
	1		Traffic Classification	an ar a ar ar ar ar ar ar ar		A	
	ID	Source	Destination	Service		Action	RU
🗐 - ccp-i	nspect	t(in-zone to o	ut-zone)		1		
	1	 100 255.255.2 127.0.0.0 209.165.2 	255.255 -> any /0.255.255.255 -> any 201.0/0.0.0.31 -> any	🌍 any	9 (Drop	E Lo
	2	🏟 any	iny any	http		Inspect HTTP Application I	
	3	🇳 any	🏈 any	smtp		inspect 5MTP Application I	
-	4	🇳 any	any	imap		Inspect MAP Application I	
-	5	🏟 any	🍑 any	рор3		Inspect POP3 Application I	
2.02	6	🕫 any	🐔 any	ccp-cls-protocol-p2p		Drop	E Lo
1.31	7	all a	10 · · · · ·	VIDEOR	m r	Trop	£3 14

Dit toont de huidige P2P toepassingen die door standaardconfiguratie geblokkeerd zullen worden.

		Edta
		Delete
SDM Defined Service User Defined Service Protocol List BHTTP BIM BP2P Ceneral Network Services BTunneling	Add >> <pre></pre>	LOWD

13. U kunt de knoppen Toevoegen en verwijderen gebruiken om specifieke toepassingen toe te voegen of te verwijderen. Deze screenshot toont hoe je de winmenx-toepassing kunt toevoegen om dat te blokkeren.

and a second state of the	Destination Network	Add
		Edt
		- Dalaha
Service		
Service Name: ccp-cls-protocol-j	Up	Down
PL HTTP	odoplov	
E-IM	kaza a 2	
	bittorrent	
	Add >> fastirack	
	<< Remove	
l⊞General		
Hereineral Wetwork Services		
General Network Services	U U	
B General Network Services B Tunneling I Namion Services		
IB General Network Services IB Tunneling IB Namion Services	anced 7	
General Network Services H Tunneling N Namino Services on: Drop Adv	anced 🔽	

Courses blackmade		Destination No.	hunde	A A A
Source Network		Destination Ne	WUIK	MOULE
				Edit
c				Delete
EMail EMail Email Oreral Network Services Email Naming Services Emails Time Protocols		Add >>	fastfrack gnutella winmx	
tion: Dron	T DIME			

14. In plaats van de vervolgactie te kiezen, kunt u ook de actie Inspect kiezen om verschillende opties voor een diepe pakketinspectie toe te passen.

Traffic Name:	Move Up Move Down	
Source Network	Destination Network	Add
		Edit
		Delete
	Add >> Coperations of the second seco	Down
.og	sdvanced plication Inspection S	

P2P-inspectie biedt Layer 4- en Layer 7-beleid voor toepassingsverkeer. Dit betekent dat ZFW een stateful inspection kan voorzien om het verkeer toe te staan of te ontkennen, evenals controle op granulaire Layer 7 op specifieke activiteiten in de verschillende protocollen, zodat bepaalde toepassingsactiviteiten toegestaan zijn terwijl anderen ontkend worden. Bij deze toepassingsinspectie kunt u verschillende typen specifieke veldnamenniveau-inspecties toepassen voor P2P-toepassingen. Hierna zie je een voorbeeld voor de gnutella.

15. Controleer de P2P-optie en klik op Maken om hiervoor een nieuwe beleidskaart te

Г НТТР	5
Г ім	7 7
P2P	7 7
IT SMTP	Creat
	Edit
Г РОРЗ	۲
Sun RPC	

 Maak een nieuwe beleidslijn voor diepe pakketinspectie voor het protocol. Klik op Add en kies dan New Class Map.

Configure Deep Packet Inspection Policy Map Name: Ccp-pmap-gnutella	- Peer-to-Peer Description:		To
Match Class Name	Action	Log	Add
ок	Cancel Help		

17. Geef een nieuwe naam voor de class-map en klik op Add om een match criteria te

~
Add
Edit
Delete
Move Up

specificeren.

18. Gebruik bestands-overdracht als het matchcriterium en het gebruikte string is .exe. Dit geeft aan dat alle gnutella bestanden overdrachtverbindingen die de .exe string bevatten voor het

Add P2P Rule			
Match Criteria:	file-transfe	r	~
Enter Value:	.exe		
ок	Cancel	Help	É

verkeersbeleid. Klik op OK.

19. Klik nogmaals op OK om de class-map configuratie te

lass Map:	ccp-class-gnut	ella
lass Map Type:	gnutella	
escription: — Match Criteria		
file-transfer	exe	Auu
		Edit
		Delete
		Move Up
		Move Down

voltooien.

20. Kies de optie **Beginwaarden** of **toestaan**, die afhankelijk is van het beveiligingsbeleid van uw bedrijf. Klik op **OK** om de actie met de beleidskaart te bevestigen.

Configure Deep Packet Inspe	ection - Peer-to-Peer	X
Policy Map Name: ccp-pmap-gnutella	Description:	
Match Class Name ccp-class-gnutella	Action <none> <none> Reset Allow</none></none>	Add ∇ Edit Delete
OK	Cancel Help	

Op deze manier kunt u andere beleidskaarten toevoegen om diepe inspectiemogelijkheden voor andere P2P-protocollen te implementeren door verschillende reguliere expressies te specificeren als het matchcriterium. **Opmerking:** P2P-toepassingen zijn bijzonder moeilijk te detecteren als gevolg van het "port-hopping"-gedrag en andere trucs om detectie te voorkomen, evenals problemen die worden geïntroduceerd door frequente veranderingen en updates van P2P-toepassingen die het gedrag van de protocollen wijzigen. ZFW combineert de native firewall-stateful inspection met Network-Based Application Recognition (NBAR) aan de traffic-recognition-functies om P2P-toepassingscontrole te leveren. **Opmerking:** P2P-toepassingen ondersteund door Layer 4-

inspectie:eentonigvastklemmengnutellakazaa2**Opmerking:** Op dit moment heeft ZFW geen optie om het "bittorrent" toepassingsverkeer te inspecteren. BitTorrent-klanten communiceren doorgaans met trackers (peer directory servers) via HTTP dat op een niet-standaard poort loopt. Dit is typisch TCP 6969, maar je zou de torrent-specifieke tracker poort moeten controleren. Als u BitTorrent wilt toestaan, is de beste methode om de extra poort aan te passen HTTP als één van de overeenkomende protocollen te configureren en TCP 6969 aan HTTP toe te voegen met deze ip port-map opdracht: **ip port-map http port tcp 6969**. Je moet http en bitTorrent definiëren als de matchcriteria die in de class-map worden toegepast.

21. Klik op **OK** om de configuratie voor geavanceerde inspectie te voltooien.

Source Network	Destination Network	Add
obuice remote	Destination retroit	
		Edition
		Delete
Naming Services Note Protocols Network Management Authentication/Authorization Methods Authentications	Add >> fastira	ick ent
ion: Inspect 🖌 Adv	anced T	
on: Inspect 🖌 🖌 Adv:	anced 🔨	

De corresponderende reeks opdrachten wordt aan de router geleverd.

22. Klik op OK om het kopiëren van de reeks opdrachten naar de router te

Preparing com Submitting 52 c Configuration c Copying the Ru Running config	mands for delivery commands, please wait lelivered to router. unning config to Startup config of your router. Please wait copied successfully to Startup Config of your router.	~
		1

voltooien.

23. U kunt de nieuwe regels observeren die plaatsvinden vanuit het tabblad Firewallbeleid bewerken onder **Configureren > Security > Firewall en ACL**.

	Traffic Classification			Anting	Rula		
	ID	Source	Destination	Service	Action	KUle	
	2	🧼 any	🧼 any	http	HTTP Application I		
	3	🏟 any	🧼 any	smtp	SMTP Application I		
	4	🏟 any	any	imap	State Inspect		
	5	🇳 any	🎱 any	рор3	POP3 Application I		
	6	any	🥥 any (gnutella	Inspect		
aŭ.	7	🎱 any	🍑 any	ymsgr	Inspect M Application Insp		
- 10 - 11 - 11 - 11 - 11 - 11 - 11 - 11	8	any	i any	ccp-cls-protocol-p2p	Inspect	10 QoS	
	9	🧼 any	🧼 any	ymsgr msnmsgr aol	Drop	🗐 Log	
	10	any:	any any	CCD-cls-insp-traffic	M Inspect		

Opdracht-lijnconfiguratie van ZFW router

De configuratie in de vorige sectie van Cisco CP resulteert in deze configuratie op de ZFW router:

ZBF-router	
ZBF-Router# show run Building configuration	

```
Current configuration : 9782 bytes
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname ZBF-Router
1
boot-start-marker
boot-end-marker
logging buffered 51200 warnings
1
no aaa new-model
ip cef
!
!
1
ip name-server 10.77.230.45
multilink bundle-name authenticated
parameter-map type protocol-info msn-servers
server name messenger.hotmail.com
server name gateway.messenger.hotmail.com
server name webmessenger.msn.com
parameter-map type protocol-info aol-servers
server name login.oscar.aol.com
server name toc.oscar.aol.com
server name oam-d09a.blue.aol.com
parameter-map type protocol-info yahoo-servers
server name scs.msg.yahoo.com
server name scsa.msg.yahoo.com
server name scsb.msg.yahoo.com
server name scsc.msg.yahoo.com
server name scsd.msg.yahoo.com
server name cs16.msg.dcn.yahoo.com
server name cs19.msg.dcn.yahoo.com
server name cs42.msg.dcn.yahoo.com
server name cs53.msg.dcn.yahoo.com
 server name cs54.msg.dcn.yahoo.com
 server name ads1.vip.scd.yahoo.com
 server name radio1.launch.vip.dal.yahoo.com
 server name in1.msg.vip.re2.yahoo.com
server name data1.my.vip.sc5.yahoo.com
server name address1.pim.vip.mud.yahoo.com
server name edit.messenger.yahoo.com
server name messenger.yahoo.com
server name http.pager.yahoo.com
server name privacy.yahoo.com
server name csa.yahoo.com
server name csb.yahoo.com
server name csc.yahoo.com
parameter-map type regex ccp-regex-nonascii
pattern [^x00-x80]
1
!
1
```

crypto pki trustpoint TP-self-signed-1742995674 enrollment selfsigned subject-name cn=IOS-Self-Signed-Certificate-1742995674 revocation-check none rsakeypair TP-self-signed-1742995674 crypto pki certificate chain TP-self-signed-1742995674 certificate self-signed 02 30820242 308201AB A0030201 02020102 300D0609 2A864886 F70D0101 04050030 31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274 69666963 6174652D 31373432 39393536 3734301E 170D3130 31313236 31303332 32315A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649 4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D31 37343239 39353637 3430819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281 8100A84A 980D15F0 6A6B5F1B 5A3359DE 5D552EFE FAA8079B DA927DA2 4AF210F0 408131CE BB5B0189 FD82E22D 6A6284E3 5F4DB2A7 7517772B 1BC5624E A1A6382E 6A07EE71 E93A98C9 B8494A55 0CDD6B4C 442065AA DBC9D9CC 14D10B65 2FEFECC8 AA9B3064 59105FBF B9B30219 2FD53ECA 06720CA1 A6D30DA5 564FCED4 C53FC7FD 835B0203 010001A3 6A306830 0F060355 1D130101 FF040530 030101FF 30150603 551D1104 0E300C82 0A5A4246 2D526F75 74657230 1F060355 1D230418 30168014 OBDBE585 15377DCA 5F00A1A2 6644EC22 366DE590 301D0603 551D0E04 1604140B DBE58515 377DCA5F 00A1A266 44EC2236 6DE59030 0D06092A 864886F7 0D010104 05000381 810037F4 8EEC7AF5 85429563 F78F2F41 A060EEE8 F23D8F3B E0913811 A143FC44 8CCE71C3 A5E9D979 C2A8CD38 C272A375 4FCD459B E02A9427 56E2F1A0 DA190B50 FA091669 CD8C066E CD1A095B 4E015326 77B3E567 DFD55A71 53220F86 F006D31E 02CB739E 19D633D6 61E49866 C31AD865 DC7F4380 FFEDDBAB 89E3B3E9 6139E472 DC62 quit 1 1 username cisco privilege 15 password 0 cisco123 archive log config hidekeys class-map type inspect match-all sdm-cls-im match protocol ymsgr class-map type inspect imap match-any ccp-app-imap match invalid-command class-map type inspect match-any ccp-cls-protocol-p2p match protocol signature match protocol gnutella signature match protocol kazaa2 signature match protocol fasttrack signature

match protocol bitTorrent signature class-map type inspect smtp match-any ccp-app-smtp match data-length gt 5000000 class-map type inspect http match-any ccp-app-nonascii match req-resp header regex ccp-regex-nonascii class-map type inspect match-any CCP-Voice-permit match protocol h323 match protocol skinny match protocol sip class-map type inspect gnutella match-any ccp-classgnutella match file-transfer .exe class-map type inspect match-any ccp-cls-insp-traffic match protocol dns match protocol https match protocol icmp match protocol imap match protocol pop3 match protocol tcp match protocol udp class-map type inspect match-all ccp-insp-traffic match class-map ccp-cls-insp-traffic class-map type inspect match-any ccp-cls-icmp-access match protocol icmp match protocol tcp match protocol udp !!--- Output suppressed ! class-map type inspect matchall sdm-cls-p2p match protocol gnutella class-map type inspect match-all ccp-protocol-pop3 match protocol pop3 class-map type inspect kazaa2 match-any ccp-cls-p2p match file-transfer class-map type inspect pop3 matchany ccp-app-pop3 match invalid-command class-map type inspect match-all ccp-protocol-p2p match class-map ccpcls-protocol-p2p class-map type inspect match-all ccpprotocol-im match class-map ccp-cls-protocol-im classmap type inspect match-all ccp-invalid-src match accessgroup 100 class-map type inspect match-all ccp-icmpaccess match class-map ccp-cls-icmp-access class-map type inspect http match-any ccp-app-httpmethods match request method bcopy match request method bdelete match request method bmove match request method bpropfind match request method bproppatch match request method connect match request method copy match request method delete match request method edit match request method getattribute match request method getattributenames match request method getproperties match request method index match request method lock match request method mkcol match request method mkdir match request method move match request method notify match request method options match request method poll match request method post match request method propfind match request method proppatch match request method put match request method revadd match request method revlabel match request method revlog match request method revnum match request method save match request method search match request method setattribute match request method startrev match request method stoprev match request method subscribe match request method trace match request method unedit match request method unlock match request method unsubscribe class-map type inspect http match-any ccphttp-blockparam match request port-misuse im match request port-misuse p2p match request port-misuse tunneling match req-resp protocol-violation class-map type inspect match-all ccp-protocol-imap match protocol

imap class-map type inspect match-all ccp-protocol-smtp match protocol smtp class-map type inspect match-all ccp-protocol-http match protocol http ! ! policy-map type inspect ccp-permit-icmpreply class type inspect ccp-icmp-access inspect class class-default pass ! !---Output suppressed ! policy-map type inspect http ccpaction-app-http class type inspect http ccp-httpblockparam log reset class type inspect http ccp-apphttpmethods log reset class type inspect http ccp-appnonascii log reset class class-default policy-map type inspect smtp ccp-action-smtp class type inspect smtp ccp-app-smtp reset class class-default policy-map type inspect imap ccp-action-imap class type inspect imap ccp-app-imap log reset class class-default policy-map type inspect pop3 ccp-action-pop3 class type inspect pop3 ccp-app-pop3 log reset class class-default policymap type inspect ccp-inspect class type inspect ccpinvalid-src drop log class type inspect ccp-protocolhttp inspect service-policy http ccp-action-app-http class type inspect ccp-protocol-smtp inspect servicepolicy smtp ccp-action-smtp class type inspect ccpprotocol-imap inspect service-policy imap ccp-actionimap class type inspect ccp-protocol-pop3 inspect service-policy pop3 ccp-action-pop3 class type inspect sdm-cls-p2p inspect ! !--- Output suppressed ! class type inspect ccp-protocol-im drop log class type inspect ccp-insp-traffic inspect class type inspect CCP-Voicepermit inspect class class-default pass policy-map type inspect ccp-permit class class-default policy-map type inspect p2p ccp-pmap-gnutella class type inspect gnutella ccp-class-gnutella ! zone security out-zone zone security in-zone zone-pair security ccp-zp-self-out source self destination out-zone service-policy type inspect ccp-permit-icmpreply zone-pair security ccp-zpin-out source in-zone destination out-zone servicepolicy type inspect ccp-inspect zone-pair security ccpzp-out-self source out-zone destination self servicepolicy type inspect ccp-permit ! ! ! interface FastEthernet0/0 description \$FW_OUTSIDE\$ ip address 209.165.201.2 255.255.255.224 zone-member security outzone duplex auto speed auto ! interface FastEthernet0/1 description \$FW_INSIDE\$ ip address 10.77.241.114 255.255.255.192 zone-member security in-zone duplex auto speed auto ! ! !--- Output suppressed ! ! ip http server ip http authentication local ip http secure-server ! ! !--- Output suppressed ! ! ! control-plane ! ! line con 0 line aux 0 line vty 0 4 privilege level 15 login local transport input ssh ! scheduler allocate 20000 1000 ! webvpn cef end ZBF-Router#

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Het <u>Uitvoer Tolk</u> (<u>uitsluitend geregistreerde</u> klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

• ZBF-Router**#show beleid-map type inspecteert zone-paar sessies**-Hier wordt de run-kaart statistieken van het type inspect voor alle bestaande zone paren.

Gerelateerde informatie

- Zone-Based Policy Firewall Design and Application Guide
- Cisco IOS-configuratievoorbeeld voor cloudfirewall en Zone-gebaseerde virtuele firewall
- <u>Cisco Configuration Professional startpagina</u>