Configuratie van Connection-time-out voor specifiek verkeer op ASA met ASDM

Inhoud

Inleiding

Dit document beschrijft de configuratie van een Connection-timeout op ASA en ASDM voor een specifiek toepassingsprotocol zoals HTTP, HTTPS, FTP of andere protocollen. De onderbreking van de verbinding is de periode van inactiviteit waarna een firewall of netwerkapparaat een nutteloze verbinding beëindigt om middelen vrij te maken en veiligheid te verbeteren. De eerste vraag vooraf is: wat is de vereiste voor deze configuratie? Als toepassingen de juiste TCP-keepalive-instellingen hebben, is het configureren van een verbindingstime-out op een firewall vaak onnodig. Als toepassingen echter niet over de juiste keepalive-instellingen of time-outconfiguraties beschikken, is het in dat geval van cruciaal belang dat de verbindingstime-out op een firewall wordt geconfigureerd voor het beheer van resources, het verbeteren van de beveiliging, het verbeteren van netwerkprestaties, het garanderen van naleving en het optimaliseren van de gebruikerservaring.

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Toegangscontrolelijst (ACL)

- Servicebeleid
- Time-out voor verbinding

Gebruikte componenten

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

- ASA 9.17(1)
- ASDM 7.17(1) switch

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 zorgen dat u de potentiële impact van elke opdracht begrijpt.

Standaard

 Opmerking: standaard timeout

De standaard embryonale timeout is 30 seconden.

De standaard half-closed idle timeout is 10 minuten.

De standaard dcd max_retries waarde is 5.

De standaard dcd retry_interval waarde is 15 seconden.

De standaard TCP idle timeout is 1 uur.

De standaard dup idle timeout is 2 minuten.

De standaard icmp idle timeout is 2 seconden.

De standaard sip idle timeout is 30 minuten.

De standaard sip_media idle timeout is 2 minuten.

De standaard esp en ha idle timeout is 30 seconden.

Voor alle andere protocollen is de standaard idle timeout 2 minuten.

Als u geen time-out wilt, voert u 0:0:0 in.

Verbindingstime-out configureren

ASDM

Als een bepaald verkeer een verbindingstabel heeft, heeft het een specifieke onbelaste onderbreking; in dit artikel, veranderen wij bijvoorbeeld de verbindingstijd voor DNS verkeer.

Hier zijn vele opties om de Time-out van de verbinding voor specifiek verkeer te configureren, rekening houdend met het netwerkdiagram van dit verkeer:

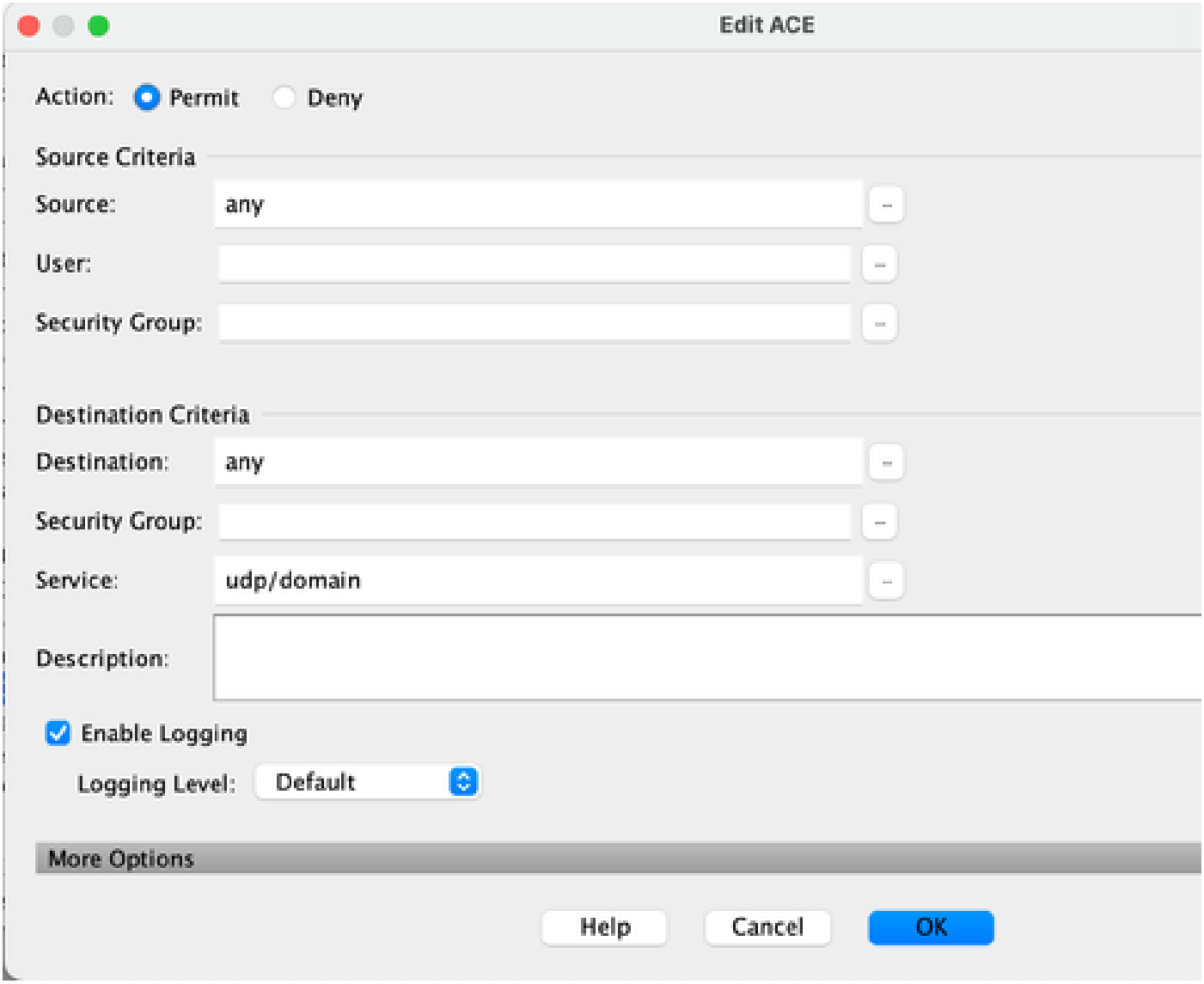
Client ----- [Interface: MNG] Firewall [Interface: OUT] ----- Server

Er is de mogelijkheid om een ACL aan de interface toe te wijzen.

Stap 1: Een ACL maken

We kunnen een bron, bestemming of service toewijzen

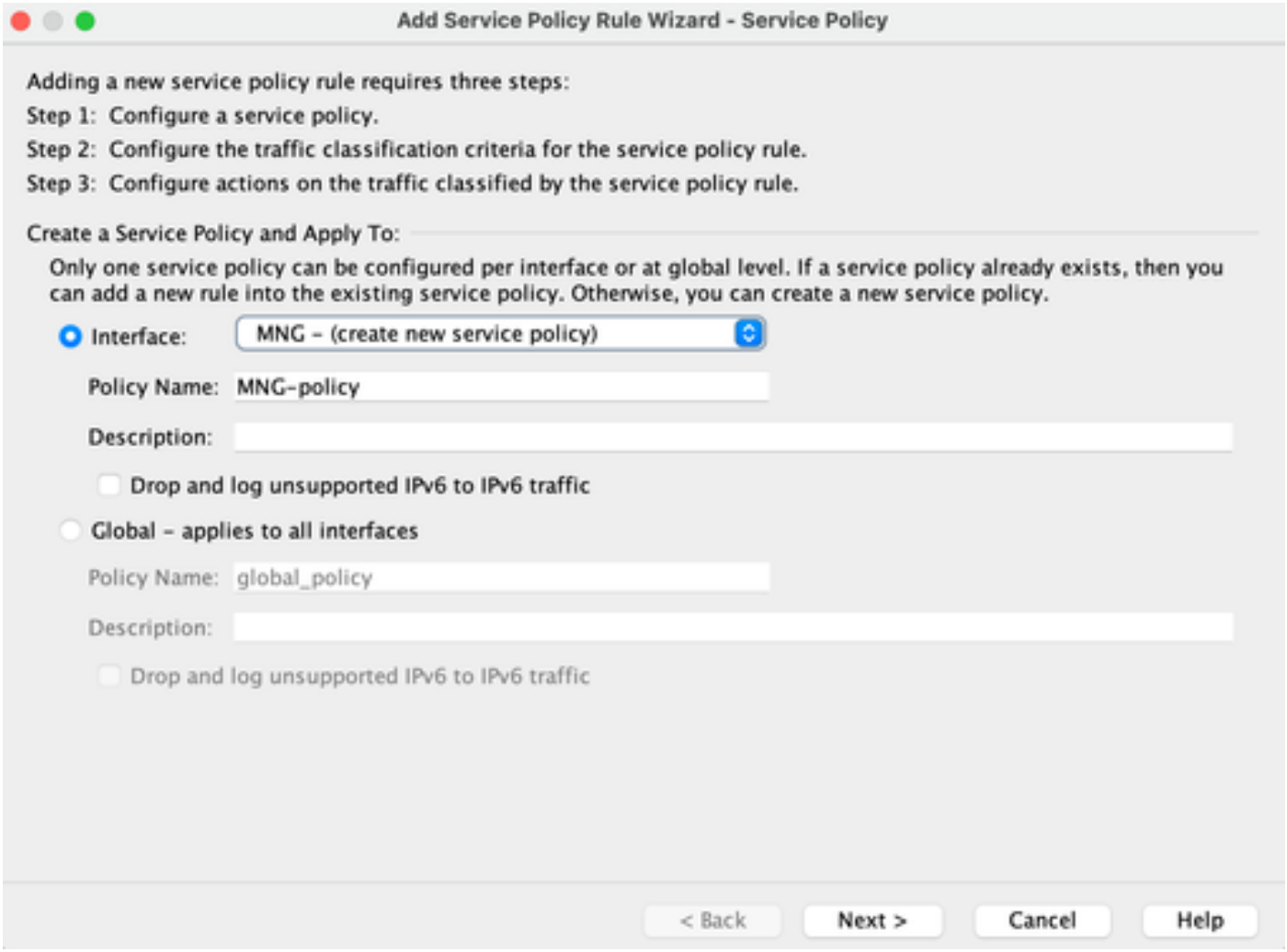
ASDM > Configuratie > Firewall > Geavanceerd > ACL-beheer



Stap 2: Servicebeleidsregel maken

U kunt de laatste stap overslaan als u al uw ACL hebt, of u kunt een van die parameters (bron, bestemming of service) aan het servicebeleid toewijzen aan de interface.

ASDM > Configuratie > Firewall > Regels voor servicebeleid

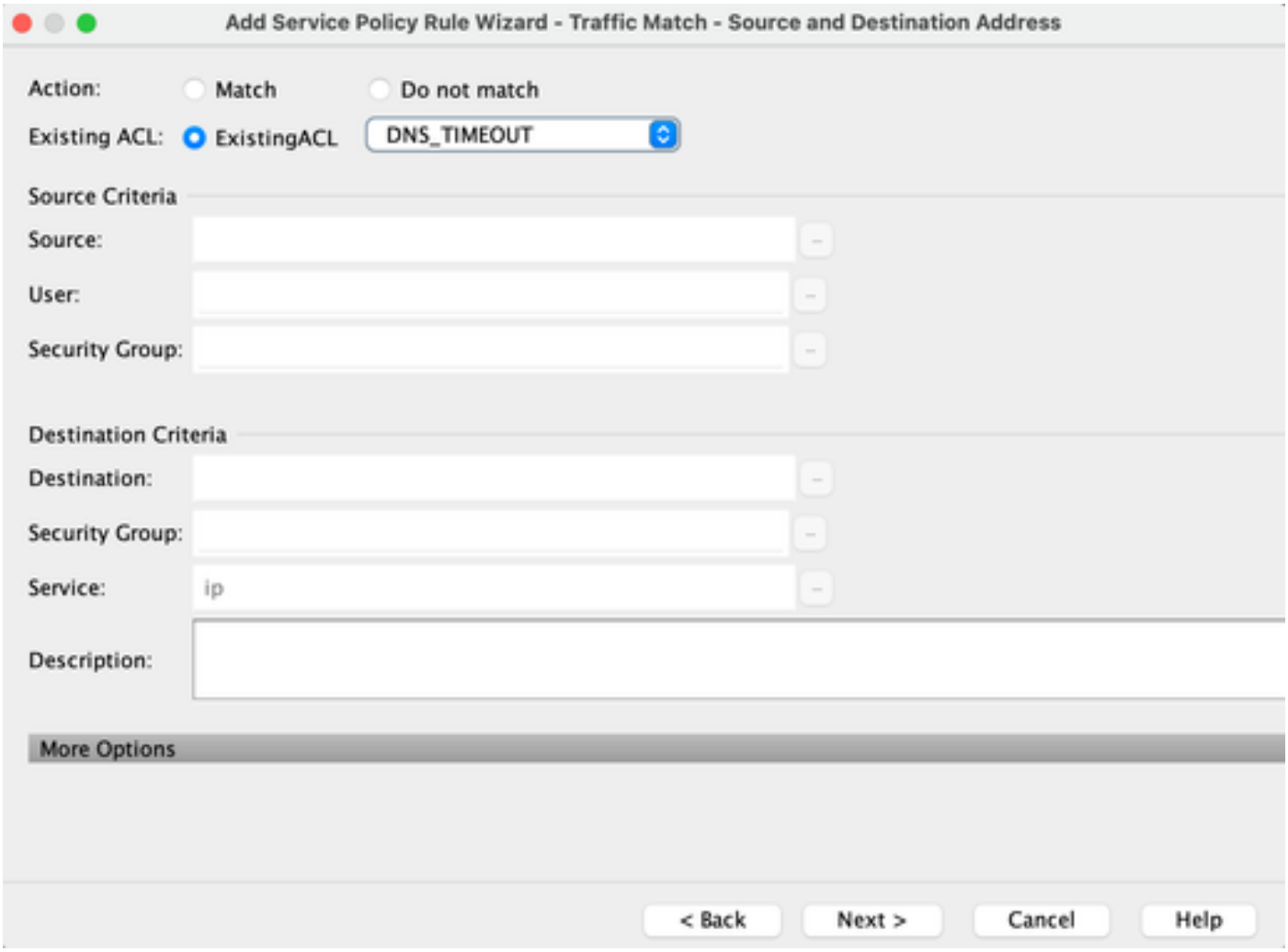


Stap 3: Verkeersklasse maken

Er is een mogelijkheid om IP-adres bron en bestemming te kiezen (gebruikt ACL)

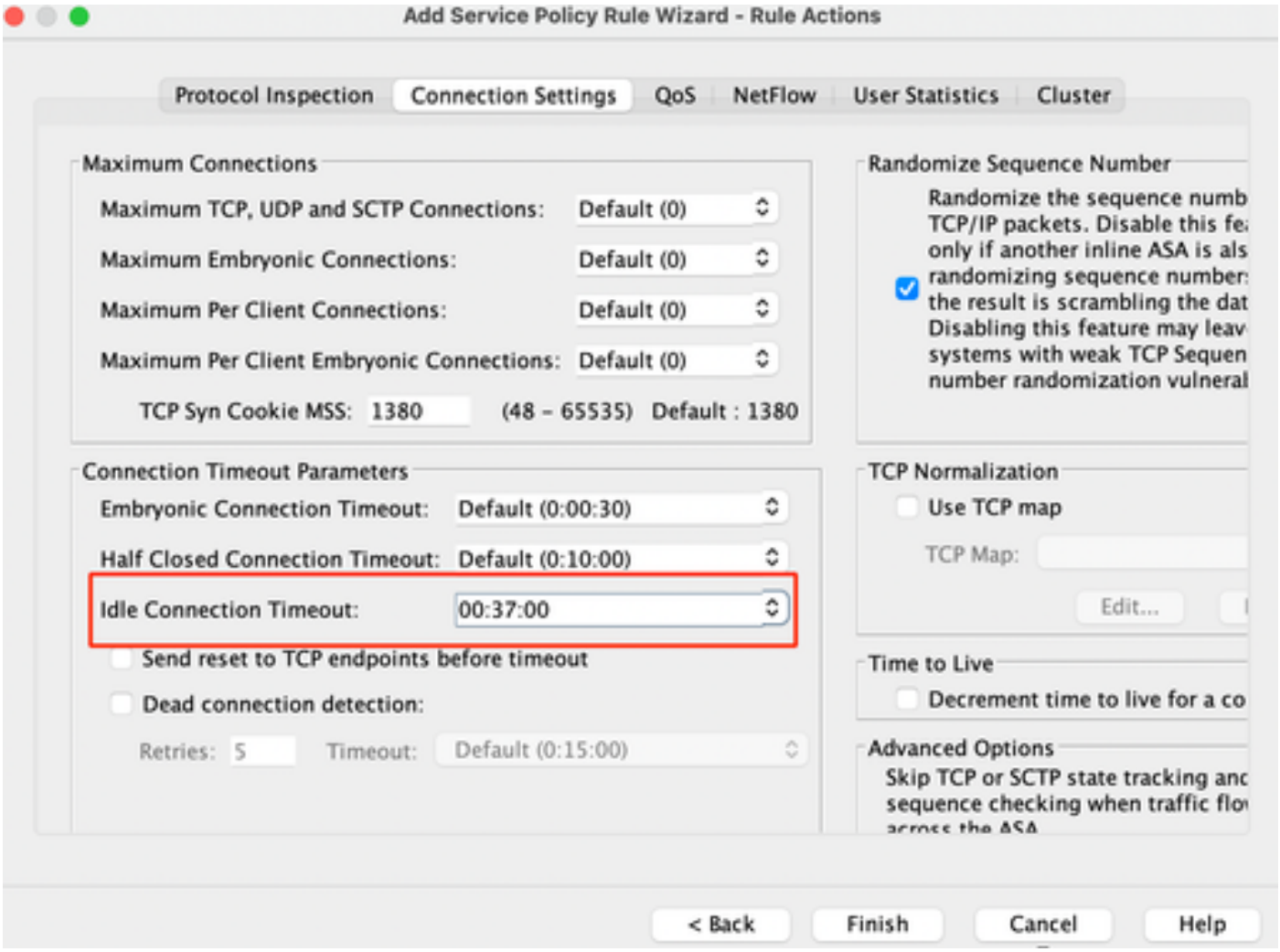
Stap 4: ACL toewijzen

In deze stap kunt u de bestaande ACL toewijzen of voorwaarden voor overeenkomsten selecteren (bron, bestemming of service)



Stap 5: Configureer de parameter voor Time-out bij inactivatie

Gebaseerd op geldig formaat HH:MM:SS configureer de Idle-time-out.



Duidelijke aansluitingen voor dat specifieke verkeer:

#clear-conn-adresVoer een IP-adres of een reeks IP-adressen in

Protocol voor #clear-verbindingen Voer dit trefwoord in om alleen SCP/TCP/UDP-verbindingen te wissen

ASA CLI

U kunt al deze instellingen configureren via de CLI:

ACL:

toegang-lijst DNS_TIJDOUT uitgebreide vergunning udp elk eq domein

Klasse-map:

class-map MNG-klasse
match access-list DNS_TIME-OUT

Beleidskaart:

beleid-kaart MNG-beleid
klasse MNG
ingesteld verbinding time-out inactief 0:37:00

Pas de Policy-map op de interface toe:

Service-policy MNG-beleidsinterface MNG

Verifiëren

Tip: Als we deze opdracht uitvoeren, kunnen we de verbindingstijd van het DNS-verkeer bevestigen:

ASA CLI > Enable mode > Toon conn long

Voorbeeld: toon conn lang adres 192.168.1.1

UDP MNG: 192.168.1.1/53 (192.168.1.1/53) OUT: 10.10.10.30/63327 (10.10.10.30/63327), flags - , idle 17s, uptime 17s, timeout 2m0s, bytes 36

UDP MNG: 192.168.1.1/53 (192.168.1.1/53) OUT: 10.10.10.30/62558 (10.10.10.30/62558), flags - , idle 40s, uptime 40s, timeout 2m0s, bytes 36

Vervolgens, na de configuratie, kunnen we de tijdelijke configuratie van het inactiviteitstimer bevestigen:

Voorbeeld: toon conn lang adres 192.168.1.1

UDP MNG: 192.168.1.1/53 (192.168.1.1/53) OUT: 10.10.10.30/63044 (10.10.10.30/63044), flags - , idle 8s, uptime 8s, timeout 37m0s, bytes 37

UDP MNG: 192.168.1.1/53 (192.168.1.1/53) OUT: 10.10.10.30/63589 (10.10.10.30/63589), flags - , idle 5s, uptime 5s, timeout 37m0s, bytes 41

Referenties

Wat zijn verbindingsinstellingen

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.