Snel IPS implementeren op Cisco geïntegreerde services routers 4000 Series

Inhoud

Inleiding

Dit document beschrijft hoe u de functie IPS en snort IDS op Cisco geïntegreerde services routers (ISR) 4000 Series kunt implementeren met behulp van de IOx-methode.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco geïntegreerde services routers 4000 Series met ten minste 8 GB DRAM.
- Basis IOS-XE opdrachtervaring.
- Basiskennis van snurken.
- Een handtekeningabonnement van 1 jaar of 3 jaar is vereist
- IOS-XE 16.10.1a en hoger.

Gebruikte componenten

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

- ISR4331/K9 met 17.9.3a release.
- UTD Engine TAR voor 17.9.3a release.
- SecurityMark9 licentie voor ISR4331/K9.

De VMAN-methode wordt nu afgekeurd.

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.

Achtergrondinformatie

De korte IPS-functie maakt inbraakpreventiesysteem (IPS) of inbraakdetectiesysteem (IDS) voor filialen op Cisco 4000 Series geïntegreerde services routers en Cisco Cloud Services router 1000v Series mogelijk. Deze functie gebruikt de opensourcesnelheid om IPS- en IDS-functies in te schakelen.

Sneltoets is een opensource-IPS die realtime verkeersanalyse uitvoert en waarschuwingen genereert wanneer bedreigingen op IP-netwerken worden gedetecteerd. Het kan ook protocolanalyse, contentonderzoek of marcheren uitvoeren en een verscheidenheid aan aanvallen en sondes detecteren, zoals bufferoverlopen, onzichtbare poortscans, enzovoort. De Snortengine wordt uitgevoerd als een virtuele containerservice op Cisco geïntegreerde services routers uit 4000 Series en Cloud Services Router 1000v Series.

De snelle IPS-functie werkt als modus voor netwerkinbraakdetectie of -preventie en biedt IPS- of IDS-mogelijkheden op Cisco geïntegreerde services routers uit 4000 Series en Cloud Services Router 1000v Series.

- Controleert netwerkverkeer en analyseert tegen een bepaalde regelreeks.
- Voert een classificatie toe.
- Voert acties tegen overeenkomende regels in.

Gebaseerd op netwerkvereisten. Snel IPS kan worden ingeschakeld als IPS of IDS. In de IDS-modus inspecteert Snort het verkeer en rapporteert waarschuwingen, maar onderneemt geen actie om aanvallen te voorkomen. In de IPS-modus wordt het verkeer geïnspecteerd en worden meldingen gemeld zoals IDS, maar er worden acties uitgevoerd om aanvallen te voorkomen.

Snel IPS wordt uitgevoerd als een service op ISR-routers. Servicecontainers maken gebruik van virtualisatietechnologie om een hostomgeving op Cisco-apparaten voor toepassingen te bieden. De inspectie van het snortverkeer wordt of op een per-interfacebasis of globaal op alle ondersteunde interfaces toegelaten. De sensor Snort vereist twee VirtualPortGroup interfaces. De eerste VirtualPortGroup wordt gebruikt voor beheerverkeer en de tweede voor dataverkeer tussen het verzendvliegtuig en de Snort virtuele containerservice. U moet IP-adressen configureren voor deze VirtualPortGroup-interfaces. Het IP-subnetbeheer dat is toegewezen aan de VirtualPortGroup-interface voor beheer, moet kunnen communiceren met de Signature-server en de waarschuwings-/rapportageserver.

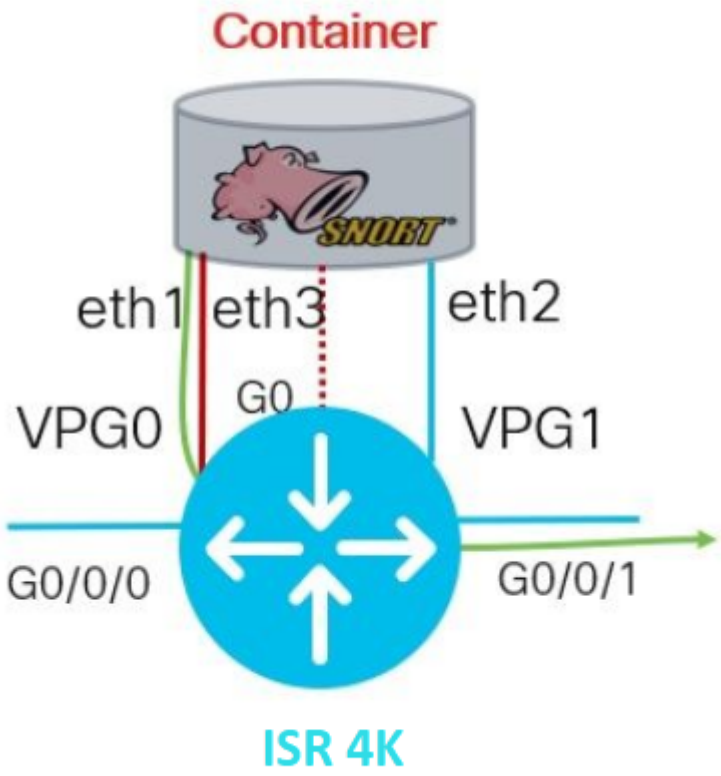
Snel IPS controleert het verkeer en rapporteert gebeurtenissen aan een externe logserver of IOS syslog. Het inschakelen van de logboekregistratie in de IOS-syslog kan gevolgen hebben voor de prestaties als gevolg van het potentiële volume aan logberichten. Externe bewakingstools van derden, die Snortlogboeken ondersteunen, kunnen worden gebruikt voor het verzamelen en analyseren van logbestanden.

Snelwerkende IPS op Cisco 4000 Series geïntegreerde services routers en Cisco Cloud Services Router 1000v Series is gebaseerd op downloaden van handtekeningspakket. Er zijn twee soorten abonnementen:

- Pakket voor communautaire handtekeningen.
- Op abonnee gebaseerd handtekeningenpakket.

De reeks van de communautaire handtekeningspakketregel biedt beperkte dekking tegen bedreigingen. De op de abonnee gebaseerde handtekeningspakketset biedt de beste bescherming tegen bedreigingen. Het omvat dekking vooraf van exploits en verleent ook de snelste toegang tot bijgewerkte handtekeningen in antwoord op een veiligheidsincident of de pro-actieve ontdekking van een nieuwe bedreiging. Dit abonnement wordt volledig ondersteund door Cisco en het pakket wordt bijgewerkt op Cisco.com. Het handtekeningenpakket kan worden gedownload van software.cisco.com. Snorthandtekeninginformatie vindt u op snort.org.

Netwerkdiagram



Configureren

Platform UTD-configuratie

Stap 1. Configureer virtuele poortgroepen interfaces.

```
Router#configure terminal
Router(config)#interface VirtualPortGroup0
Router(config-if)#description Management Interface
Router(config-if)#ip address 192.168.1.1 255.255.255.252
Router(config-if)#no shutdown
Router(config-if)#exit

Router(config)#interface VirtualPortGroup1
Router(config-if)#description Data Interface
Router(config-if)#ip address 192.168.2.1 255.255.255.252
Router(config-if)#no shutdown
Router(config-if)#exit
```

Stap 2. Schakel de IOx-omgeving in in Global Configuration-modus.

```
Router(config)#iox
```

Stap 3. App-hosting configureren met vnic configuratie.

```
Router(config)#app-hosting appid UTD
Router(config-app-hosting)#app-vnic gateway0 virtualportgroup 0 guest-interface 0
Router(config-app-hosting-gateway0)#guest-ipaddress 192.168.1.2 netmask 255.255.255.252
Router(config-app-hosting-gateway0)#exit

Router(config-app-hosting)#app-vnic gateway1 virtualportgroup 1 guest-interface 1
Router(config-app-hosting-gateway0)#guest-ipaddress 192.168.2.2 netmask 255.255.255.252
Router(config-app-hosting-gateway0)#exit
```

Stap 4 (optioneel). Resourceprofiel configureren.

```
Router(config-app-hosting)#app-resource package-profile low [low,medium,high]
Router(config-app-hosting)#end
```

> **Opmerking:** *Als dit niet is gedefinieerd, gebruikt het systeem de standaard app-resource configuratie (Laag). Zorg ervoor dat u voldoende beschikbare bronnen op ISR hebt als de standaardprofielconfiguratie wordt gewijzigd.*

Stap 5. Installeer de app-hosting met behulp van het UTD.tar-bestand.

```
Router#app-hosting install appid UTD package bootflash:iox-iosxe-utd.16.12.08.1.0.24_SV2.9.16.1_XE16.12.
```

> **Opmerking**: Houd het juiste UTD.tar bestand op bootflash: om verder te gaan met het installeren van het. Snelversie wordt op de naam van een UTD-bestand gespecificeerd.

De volgende syslogs moeten worden gezien erop wijzend UTD de dienst correct werd geïnstalleerd.

```
Installing package 'bootflash:iox-iosxe-utd.16.12.08.1.0.24_SV2.9.16.1_XE16.12
*Jun 26 19:25:35.975: %VMAN-5-PACKAGE_SIGNING_LEVEL_ON_INSTALL: R0/0: vman: Pa
*Jun 26 19:25:50.746: %VIRT_SERVICE-5-INSTALL_STATE: Successfully installed vi
*Jun 26 19:25:53.176: %IM-6-INSTALL_MSG: R0/0: ioxman: app-hosting: Install su
```

> **Opmerking**: *'Toon app-hosting lijst'* de status moet worden *'uitgezet'*

Stap 6. Start de app-hosting service.

```
Router#configure terminal
Router(config)#app-hosting appid UTD
Router(config-app-hosting)#start
Router(config-app-hosting)#end
```

> **Opmerking**: Na het starten van de app-hosting service, moet de app-hosting status *'Running'*. Gebruik *'Toon app-hosting lijst' of 'toon app-hosting detail'* om meer details te zien.

Volgende syslogberichten moeten worden gezien om aan te geven dat de UTD-service correct is geïnstalleerd.

```
*Jun 26 19:55:05.362: %VIRT_SERVICE-5-ACTIVATION_STATE: Successfully activated
*Jun 26 19:55:07.412: %IM-6-START_MSG: R0/0: ioxman: app-hosting: Start succee
```

Configuratie van serviceplane en dataplane.

Na een succesvolle installatie moet het servicevlak worden geconfigureerd. Snel IPS kan als inbraakpreventiesysteem (IPS) of inbraakdetectiesysteem (IDS) voor inspectie worden geconfigureerd.

> **Waarschuwing**: Bevestig dat de *'security*k9*'* licentiefunctie ingeschakeld is om met UTD-servicevliegtuigconfiguratie verder te gaan.

Stap 1. Configureer de Unified Threat Defense (UTD)-standaardengine (Serviceplatform)

```
Router#configure terminal
Router(config)#utd engine standard
```

Stap 2. Schakel de logboekregistratie van noodberichten voor een externe server in.

```
Router(config-utd-eng-std)#logging host 192.168.10.5
```

Stap 3. Schakel Threat Inspection for Snort Engine in.

```
Router(config-utd-eng-std)#threat-inspection
```

Stap 4. Configureer bedreigingsdetectie als inbraakpreventiesysteem (IPS) of inbraakdetectiesysteem (IDS)

```
Router(config-utd-engstd-insp)#threat [protection,detection]
```

Opmerking: *'Bescherming'* wordt gebruikt voor IPS en *'Detectie'* voor IDS. *'Detectie'* is de standaardinstelling.

Stap 5. Beveiligingsbeleid configureren.

```
Router(config-utd-engstd-insp)#policy [balanced, connectivity, security]
Router(config-utd-engstd-insp)#exit
Router(config-utd-eng-std)#exit
```

Opmerking: Standaardbeleid is *'gebalanceerd'*

Stap 6 (optioneel). De lijst met toegestane UTD-bestanden maken (Whitelist)

```
Router#configure terminal
Router(config)#utd threat-inspection whitelist
```

Stap 7 (optioneel). Configureer de snelhandtekeningen-ID's om in de whitelist te verschijnen.

```
Router(config-utd-whitelist)#generator id 40 signature id 54621 comment FILE-OFFICE traffic from networ
Router(config-utd-whitelist)#end
```

Opmerking: ID *'40'* wordt als voorbeeld gebruikt. Om de informatie over Snort-handtekeningen te controleren, raadpleegt u de officiële documentatie bij Snort.

Stap 8 (optioneel). Toegestane lijst inschakelen bij configuratie van Threat Inspection.

```
Router#config terminal
Router(config)#utd engine standard
Router(config-utd-eng-std)#threat-inspection
Router(config-utd-engstd-insp)#whitelist
```

Stap 9. Configureer de update-interval voor handtekeningen om automatisch handtekeningen te downloaden.

```
Router#config terminal
Router(config)#utd engine standard
```

```
Router(config-utd-eng-std)#threat-inspection
Router(config-utd-engstd-insp)#signature update occur-at [daily, monthly, weekly] 0 0
```

Opmerking: het eerste nummer definieert het uur in de indeling van 24 uur en het tweede nummer geeft minuten aan.

Waarschuwing: UTD-handtekeningupdates genereren een korte onderbreking van de service tijdens de update.

Stap 10. Configureer de serverparameters voor het bijwerken van handtekeningen.

```
Router(config-utd-engstd-insp)#signature update server [cisco, url] username cisco password cisco12
```

Opmerking: gebruik *'Cisco'* om de Cisco-server of *'url'* te gebruiken om een aangepast pad voor de updateserver te definiëren. Voor de Cisco-server moet u uw eigen gebruikersnaam en wachtwoord opgeven.

Stap 11. Logboekniveau inschakelen.

```
Router(config-utd-engstd-insp)#logging level [alert,crit,debug,emerg,info,notice,warning]
Router(config-utd-engstd-insp)#exit
Router(config-utd-eng-std)#exit
```

Stap 12. Schakel de volledige service in.

```
Router#configure terminal
Router(config)#utd
```

Stap 13 (optioneel). Richt gegevensverkeer van de VirtualPortGroup-interface naar de UTD-service.

```
Router#configure terminal
Router(config)#utd
Router(config-utd)#redirect interface virtualPortGroup
```

Opmerking: als de omleiding niet is geconfigureerd, wordt deze automatisch gedetecteerd.

Stap 14. UTD inschakelen op alle Layer 3-interfaces op ISR.

```
Router(config-utd)#all-interfaces
```

Stap 15. Schakel de motorstandaard in.

```
Router(config-utd)#engine standard
```

Volgende syslog berichten moeten worden gezien erop wijzend UTD werd behoorlijk toegelaten.

```
*Jun 27 23:41:03.062: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0,
*Jun 27 23:41:13.039: %IOSXE-2-PLATFORM: R0/0: cpp_cp: QFP:0.0 Thread:000 TS:0
*Jun 27 23:41:22.457: %IOSXE-5-PLATFORM: R0/0: cpp_cp: QFP:0.0 Thread:000 TS:0
```

Stap 16 (optioneel). Bepaal de actie voor UTD-motorstoring (UTD Data Plane)

```
Router(config-engine-std)#fail close
Router(config-engine-std)#end
Router#copy running-config startup-config
Destination filename [startup-config]?
```

> **Opmerking**: de optie *'Sluiten* mislukt' verlaagt al het IPS/IDS-verkeer wanneer de UTD-motor uitvalt. *'Fail open'* optie staat al het IPS/IDS verkeer op UTD-storingen toe. De standaardoptie is *'fail open'*.

Verifiëren

Controleer het IP-adres en de interfacestatus van de VirtualPort-groepen.

```
Router#show ip interface brief | i VirtualPortGroup
VirtualPortGroup0 192.168.1.1 YES NVRAM up up
VirtualPortGroup1 192.168.2.1 YES NVRAM up up
```

Controleer de configuratie van de VirtualPort-groep.

```
Router#show running-config | b interface
interface VirtualPortGroup0
description Management Interface
ip address 192.168.1.1 255.255.255.252
!
interface VirtualPortGroup1
```

```
description Data Interface
ip address 192.168.2.1 255.255.255.252
!
```

Controleer de configuratie van de app-hosting.

```
Router#show running-config | b app-hosting
app-hosting appid UTD
app-vnic gateway0 virtualportgroup 0 guest-interface 0
guest-ipaddress 192.168.1.2 netmask 255.255.255.252
app-vnic gateway1 virtualportgroup 1 guest-interface 1
guest-ipaddress 192.168.2.2 netmask 255.255.255.252
start
end
```

Controleer de iox-activering.

```
Router#show running-config | i iox
iox
```

Controleer de configuratie van het UTD-servicevlak.

```
Router#show running-config | b engine
utd engine standard
logging host 192.168.10.5
threat-inspection
threat protection
policy security
signature update server cisco username cisco password KcEDIO[gYafNZheBHBD`CC\g`_cSeFAAB
signature update occur-at daily 0 0
logging level info
whitelist
utd threat-inspection whitelist
generator id 40 signature id 54621 comment FILE-OFFICE traffic
utd
all-interfaces
redirect interface VirtualPortGroup1
engine standard
fail close
```

```
Router#show utd engine standard config
UTD Engine Standard Configuration:

IPS/IDS : Enabled

Operation Mode : Intrusion Prevention
Policy : Security
```

```
Signature Update:
Server : cisco
User Name : cisco
Password : KcEDIO[gYafNZheBHBD`CC\g`_cSeFAAB
Occurs-at : daily ; Hour: 0; Minute: 0

Logging:
Server : 192.168.10.5
Level : info
Statistics : Disabled
Hostname : router
System IP : Not set

Whitelist : Enabled
Whitelist Signature IDs:
54621, 40

 Port Scan : Disabled

Web-Filter : Disabled
```

Controleer de status van de app.

```
Router#show app-hosting list
App id                                   State
---------------------------------------------------------
UTD                                      RUNNING
```

Controleer de app-hostinggegevens.

```
Router#show app-hosting detail
App id : UTD
Owner : ioxm
State : RUNNING
Application
Type : LXC
Name : UTD-Snort-Feature
Version : 1.0.7_SV2.9.18.1_XE17.9
Description : Unified Threat Defense
Author :
Path : /bootflash/secapp-utd.17.09.03a.1.0.7_SV2.9.18.1_XE17.9.x86_64.tar
URL Path :
Multicast : yes
Activated profile name :

Resource reservation
Memory : 1024 MB
Disk : 752 MB
CPU :
CPU-percent : 25 %
VCPU : 0

Platform resource profiles
```

```
Profile Name CPU(unit) Memory(MB) Disk(MB)
------------------------------------------------------------

Attached devices
Type Name Alias
------------------------------------------
Disk /tmp/xml/UtdLogMappings-IOX
Disk /tmp/xml/UtdIpsAlert-IOX
Disk /tmp/xml/UtdDaqWcapi-IOX
Disk /tmp/xml/UtdUrlf-IOX
Disk /tmp/xml/UtdTls-IOX
Disk /tmp/xml/UtdDaq-IOX
Disk /tmp/xml/UtdAmp-IOX
Watchdog watchdog-503.0
Disk /tmp/binos-IOX
Disk /opt/var/core
Disk /tmp/HTX-IOX
Disk /opt/var
NIC ieobc_1 ieobc
Disk _rootfs
NIC mgmt_1 mgmt
NIC dp_1_1 net3
NIC dp_1_0 net2
Serial/Trace serial3

Network interfaces
---------------------------------------
eth0:
MAC address : 54:0e:00:0b:0c:02
IPv6 address : ::
Network name :
eth:
MAC address : 6c:41:0e:41:6b:08
IPv6 address : ::
Network name :
eth2:
MAC address : 6c:41:0e:41:6b:09
IPv6 address : ::
Network name :
eth1:
MAC address : 6c:41:0e:41:6b:0a
IPv4 address : 192.168.2.2
IPv6 address : ::
Network name :

------------------------------------------------------------------------
Process Status Uptime # of restarts
------------------------------------------------------------------------
climgr UP 0Y 0W 0D 21:45:29 2
logger UP 0Y 0W 0D 19:25:56 0
snort_1 UP 0Y 0W 0D 19:25:56 0

Network stats:
eth0: RX packets:162886, TX packets:163855
eth1: RX packets:46, TX packets:65

DNS server:
domain cisco.com
nameserver 192.168.90.92

Coredump file(s): core, lost+found
```

```
Interface: eth2
ip address: 192.168.2.2/30
Interface: eth1
ip address: 192.168.1.2/30

Address/Mask Next Hop Intf.
--------------------------------------------------------------------------------
0.0.0.0/0 192.168.2.1 eth2
0.0.0.0/0 192.168.1.1 eth1
```

Probleemoplossing

1. Zorg ervoor dat Cisco geïntegreerde services router (ISR) XE 16.10.1a en hoger uitvoert (voor IOSx-methode)

2. Controleer of Cisco geïntegreerde services router (ISR) is gelicentieerd en de Security9 optie ingeschakeld is.

3. Controleer of het ISR-hardwaremodel voldoet aan het minimumprofiel van de bron.

4. Functie niet compatibel met Zone-Based Firewall SYN-cookie en netwerkadresomzetting 64 (NAT64)

5. Controleer of de UTD-service na de installatie is gestart.

6. Zorg er tijdens het downloaden van handmatige handtekeningen voor dat het pakket dezelfde versie heeft als de Snort-motorversie. De update van het handtekeningspakket kan mislukken als er een versiemismatch is.

7. In het geval van prestatiekwesties, gebruik de ***'show app-hosting resource'*** en ***'show app-hosting gebruik toegepast ''UTD-NAME'*** voor het leren over CPU/geheugen/opslag verbruiken.

```
Router#show app-hosting resource
CPU:
Quota: 75(Percentage)
Available: 50(Percentage)
VCPU:
Count: 6
Memory:
Quota: 10240(MB)
Available: 9216(MB)
Storage device: bootflash
Quota: 4000(MB)
Available: 4000(MB)
Storage device: harddisk
Quota: 20000(MB)
Available: 19029(MB)
Storage device: volume-group
Quota: 190768(MB)
Available: 169536(MB)
Storage device: CAF persist-disk
Quota: 20159(MB)
Available: 18078(MB)
```

```
Router#show app-hosting utilization appid utd
Application: utd
CPU Utilization:
CPU Allocation: 33 %
CPU Used: 3 %
Memory Utilization:
Memory Allocation: 1024 MB
Memory Used: 117632 KB
Disk Utilization:
Disk Allocation: 711 MB
Disk Used: 451746 KB
```

> **Waarschuwing**: als u een hoge CPU, veel geheugen of veel schijfgebruik kunt zien, neemt u contact op met Cisco TAC.

Debuggen

Gebruik de onderstaande debug-opdrachten om IPS-informatie te verzamelen als er een fout is opgetreden.

<#root>

```
debug virtual-service all
```

```
debug virtual-service virtualPortGroup
```

```
debug virtual-service messaging
```

```
debug virtual-service timeout
```

```
debug utd config level error [error, info, warning]
debug utd engine standard all
```

Gerelateerde informatie

Aanvullende documenten met betrekking tot snelle IPS-implementatie zijn hier te vinden:

Configuratiehandleiding voor IPS-beveiliging

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_utd/configuration/xe-17/sec-data-utd-xe-17-book/snort-ips.html

Profiel van virtuele serviceresources

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_utd/configuration/xe-17/sec-data-utd-xe-17-

book/snort-ips.html#id_31952

Snel IPS op routers - stapsgewijze configuratie.

https://community.cisco.com/t5/security-knowledge-base/router-security-snort-ips-on-routers-step-by-step-configuration/ta-p/3369186

Sneltoets IPS voor probleemoplossing

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_utd/configuration/xe-17/sec-data-utd-xe-17-book/snort-ips.html#concept_C3C869E633A6475890475931DF83EBCC

ISR4K snort IPS wordt niet geïmplementeerd omdat HW niet genoeg platformbronnen heeft

https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwf57595

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.