Verificatie via bypass in beveiligde web-applicatie

Inhoud

Inleiding

In dit document worden de stappen beschreven om verificatie in Secure Web Applicatie (SWA) uit te sluiten.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Toediening van SWA.

Cisco raadt aan deze tools te installeren:

- Fysieke of virtuele SWA
- Administratieve toegang tot de grafische gebruikersinterface (GUI) van de SWA

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

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.

Vrijgestelde verificatie

Het vrijstellen van verificatie voor bepaalde gebruikers of systemen in de Cisco-SWA kan van cruciaal belang zijn voor het behoud van de operationele efficiëntie en het voldoen aan specifieke vereisten. Ten eerste vereisen sommige gebruikers of systemen ononderbroken toegang tot kritieke bronnen of diensten die door authenticatieprocessen kunnen worden belemmerd. Geautomatiseerde systemen of servicerekeningen die regelmatig updates of back-ups uitvoeren, hebben bijvoorbeeld naadloze toegang nodig zonder de vertragingen of mogelijke fouten die door verificatiemechanismen worden geïntroduceerd.

Daarnaast zijn er scenario's waarin de webservice provider aanraadt geen proxy te gebruiken om toegang te krijgen tot hun service. In dergelijke gevallen garandeert een vrijstelling van authenticatie de naleving van de richtlijnen van de aanbieder en behoudt zij de betrouwbaarheid van de dienst. Bovendien is het, om verkeer voor bepaalde gebruikers effectief te blokkeren, vaak nodig om ze eerst vrij te stellen van authenticatie en vervolgens het juiste blokkeringsbeleid toe te passen. Deze benadering staat voor nauwkeurige controle over toegangstoestemmingen toe.

In sommige gevallen wordt de webservice die wordt benaderd, vertrouwd en universeel geaccepteerd, zoals Microsoft-updates. Het vrijstellen van authenticatie voor dergelijke diensten vereenvoudigt de toegang voor alle gebruikers. Bovendien zijn er situaties waarin het besturingssysteem of de toepassing van de gebruiker het ingestelde authenticatiemechanisme in de SWA niet ondersteunt, waardoor een omzeiling nodig is om connectiviteit te garanderen.

Tot slot vereisen servers met vaste IP-adressen zonder gebruikersaanmelding en beperkte, vertrouwde internettoegang niet dat ze worden geauthenticeerd, omdat hun toegangspatronen voorspelbaar en veilig zijn.

Door authenticatie strategisch vrij te stellen voor deze gevallen, kunnen organisaties beveiligingsbehoeften in balans brengen met operationele efficiency.

Methoden voor vrijstelling van verificatie in Cisco SWA

Vrijstelling van authenticatie in SWA kan worden bereikt door middel van verschillende methoden, elk aangepast aan specifieke scenario's en vereisten. Hier zijn een aantal veelvoorkomende manieren om verificatie-vrijstellingen te configureren:

- IP-adres of subnetmasker: een van de eenvoudigste methoden is het vrijstellen van specifieke IP-adressen of volledige subnetten van verificatie. Dit is met name handig voor servers met vaste IP-adressen of vertrouwde netwerksegmenten die ononderbroken toegang tot het internet of interne bronnen vereisen. Door deze IP-adressen of subnetmaskers in de SWA-configuratie op te geven, kunt u ervoor zorgen dat deze systemen het verificatieproces omzeilen.
- Proxy-poorten: u kunt de SWA configureren om verkeer vrij te stellen op basis van specifieke proxy-poorten. Dit is nuttig wanneer bepaalde toepassingen of diensten aangewezen poorten voor communicatie gebruiken. Door deze poorten te identificeren, kunt u de SWA instellen om de verificatie voor verkeer op deze poorten te omzeilen, waardoor naadloze toegang voor de relevante toepassingen of services wordt gewaarborgd.

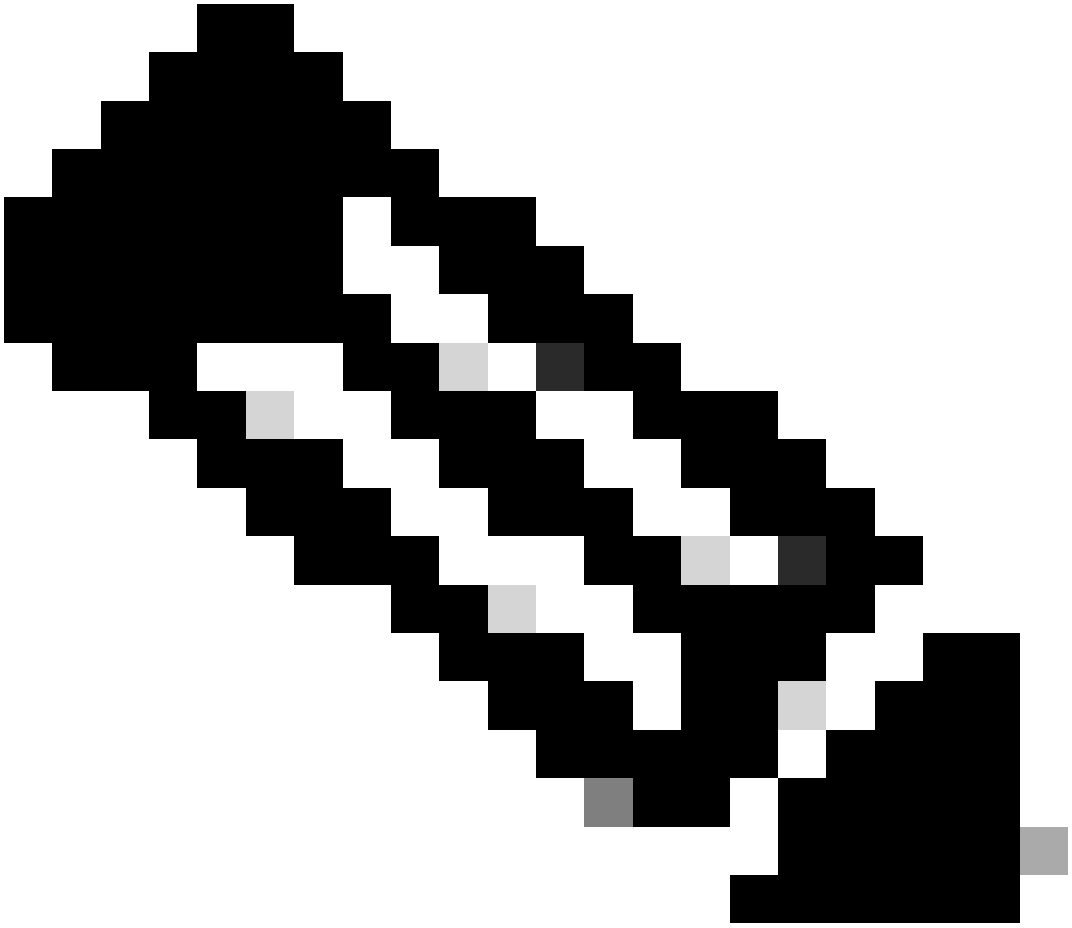
- URL-categorieën: Een andere methode is om verificatie op basis van URL-categorieën vrij te stellen. Dit kan zowel vooraf gedefinieerde Cisco-categorieën als aangepaste URL-categorieën omvatten die u definieert op basis van uw organisatiespecifieke behoeften. Bijvoorbeeld, als bepaalde webservices, zoals Microsoft updates, worden beschouwd als vertrouwd en universeel aanvaardbaar, kunt u de SWA configureren om verificatie voor deze specifieke URL-categorieën te omzeilen. Dit zorgt ervoor dat alle gebruikers toegang tot deze diensten kunnen krijgen zonder dat zij daarvoor moeten worden geauthentificeerd.
- Gebruikersagents: het vrijstellen van verificatie op basis van gebruikersagents is nuttig bij de omgang met specifieke toepassingen of apparaten die de ingestelde verificatiemechanismen niet ondersteunen. Door de gebruikersagent-strings van deze toepassingen of apparaten te identificeren, kunt u de SWA configureren om de verificatie voor verkeer dat uit deze toepassingen of apparaten voortkomt te omzeilen, waardoor een naadloze verbinding wordt gegarandeerd.

.

Stappen om verificatie te omzeilen

Hier volgen de stappen voor het maken van een Identificatieprofiel dat is vrijgesteld van verificatie:

Stap 1. Kies in GUI Web Security Manager en klik vervolgens op Identificatieprofielen.
Stap 2. Klik op Profiel toevoegen om een profiel toe te voegen.
Stap 3. Gebruik het aanvinkvakje Enable Identification Profile om dit profiel in te schakelen of om het snel uit te schakelen zonder het te verwijderen.
Stap 4. Wijs een uniek profiel Naam toe.
Stap 5. (optioneel) Beschrijving toevoegen.
Stap 6. Kies in de vervolgkeuzelijst Invoegen waar dit profiel in de tabel moet worden weergegeven.

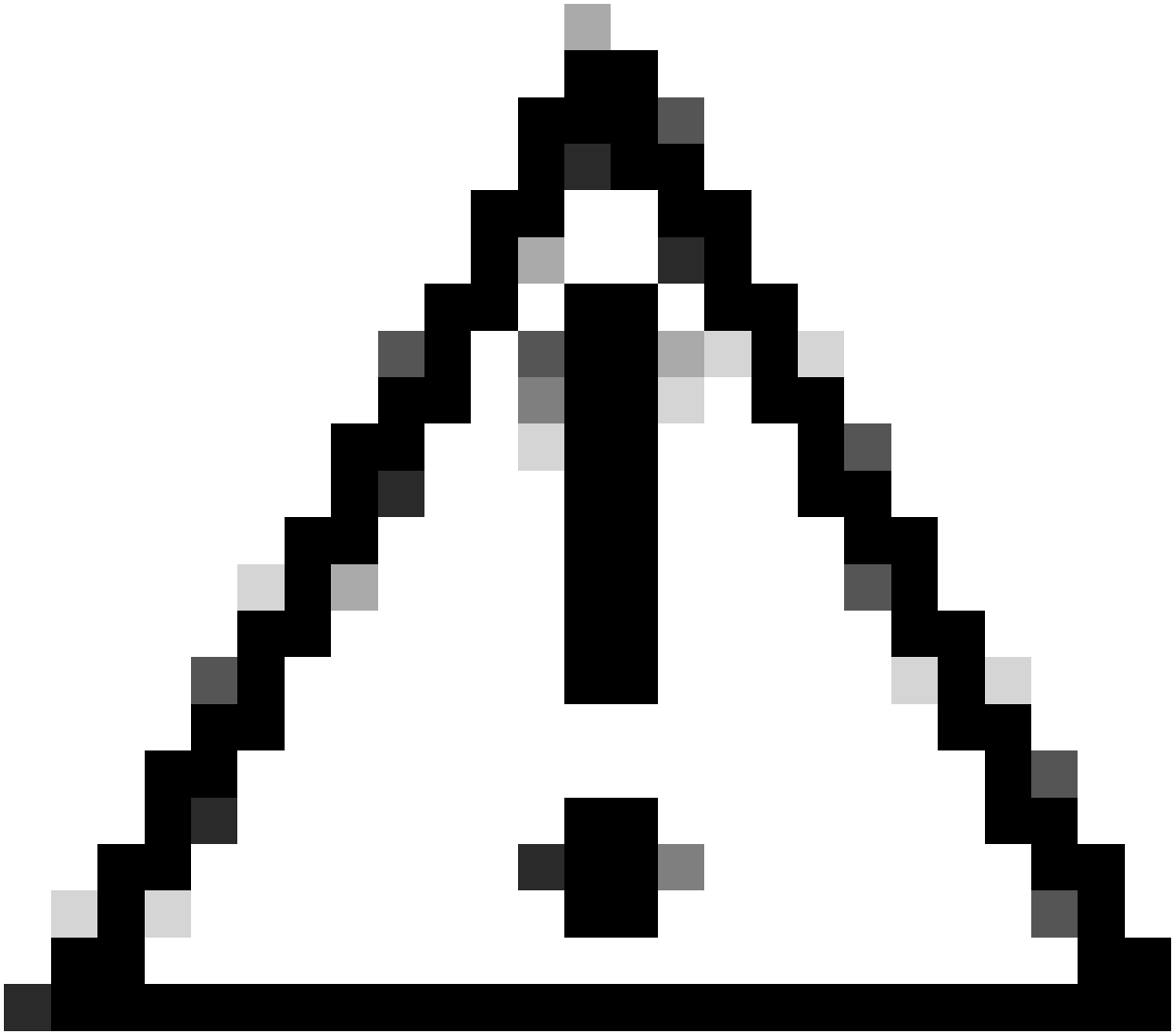


Opmerking: positidentificatieprofielen die geen verificatie bovenaan de lijst vereisen. Deze aanpak vermindert de belasting op de SWA, minimaliseert de verificatievrije en resulteert in snellere verificatie voor andere gebruikers.

Stap 7. Kies in het gedeelte Gebruikersidentificatiemethode Vrijstelling van verificatie/identificatie.

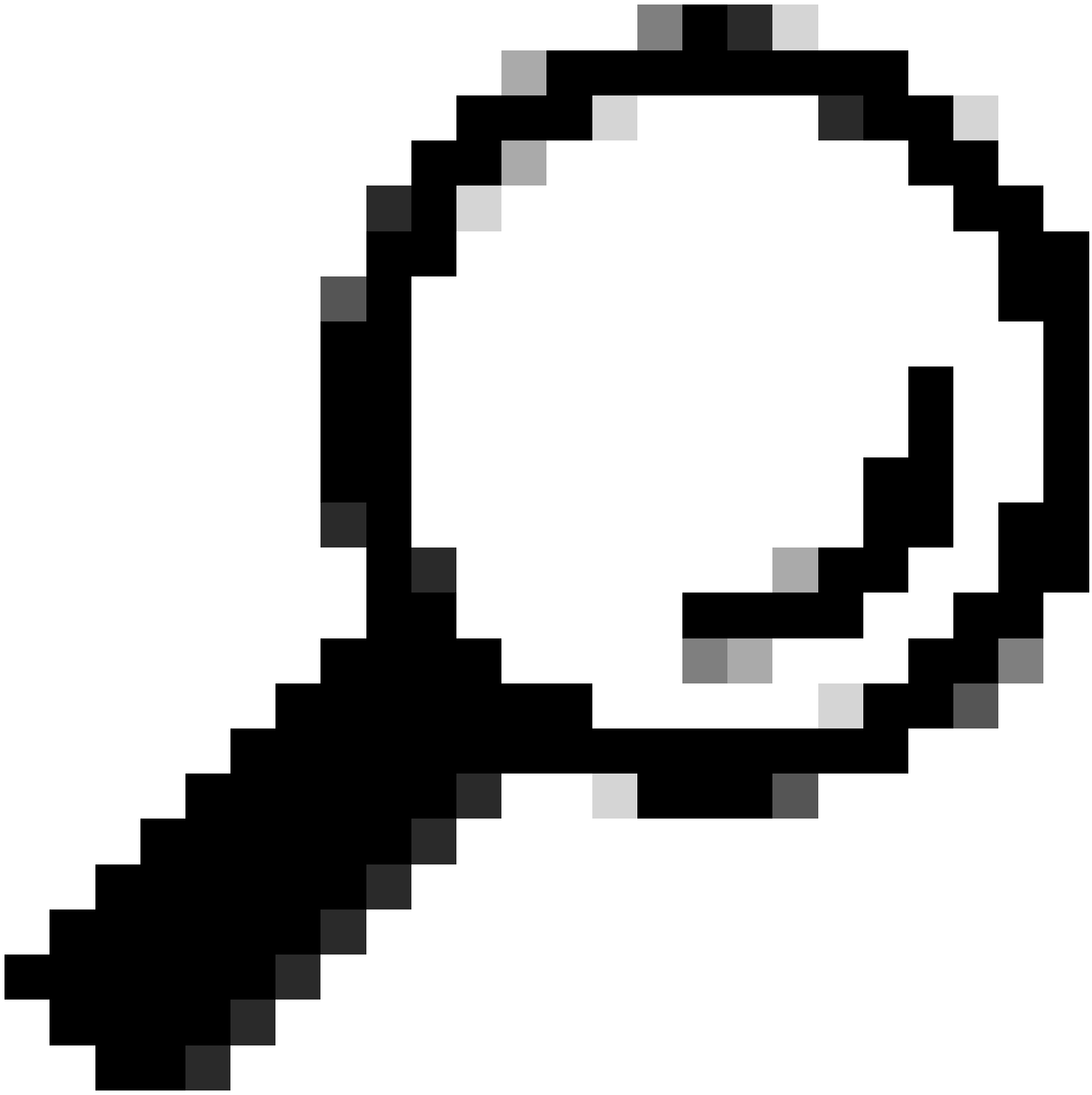
Stap 8. Voer in het veld Leden per subnet definiëren de IP-adressen of subnetten in die dit identificatieprofiel moet toepassen. U kunt IP-adressen, Classless Inter-Domain Routing (CIDR)-blokken en subnetten gebruiken.

Stap 9. (Optioneel) Klik op Advanced om extra lidmaatschapscriteria te definiëren, zoals Proxy Ports, URL Categorieën of User Agents.

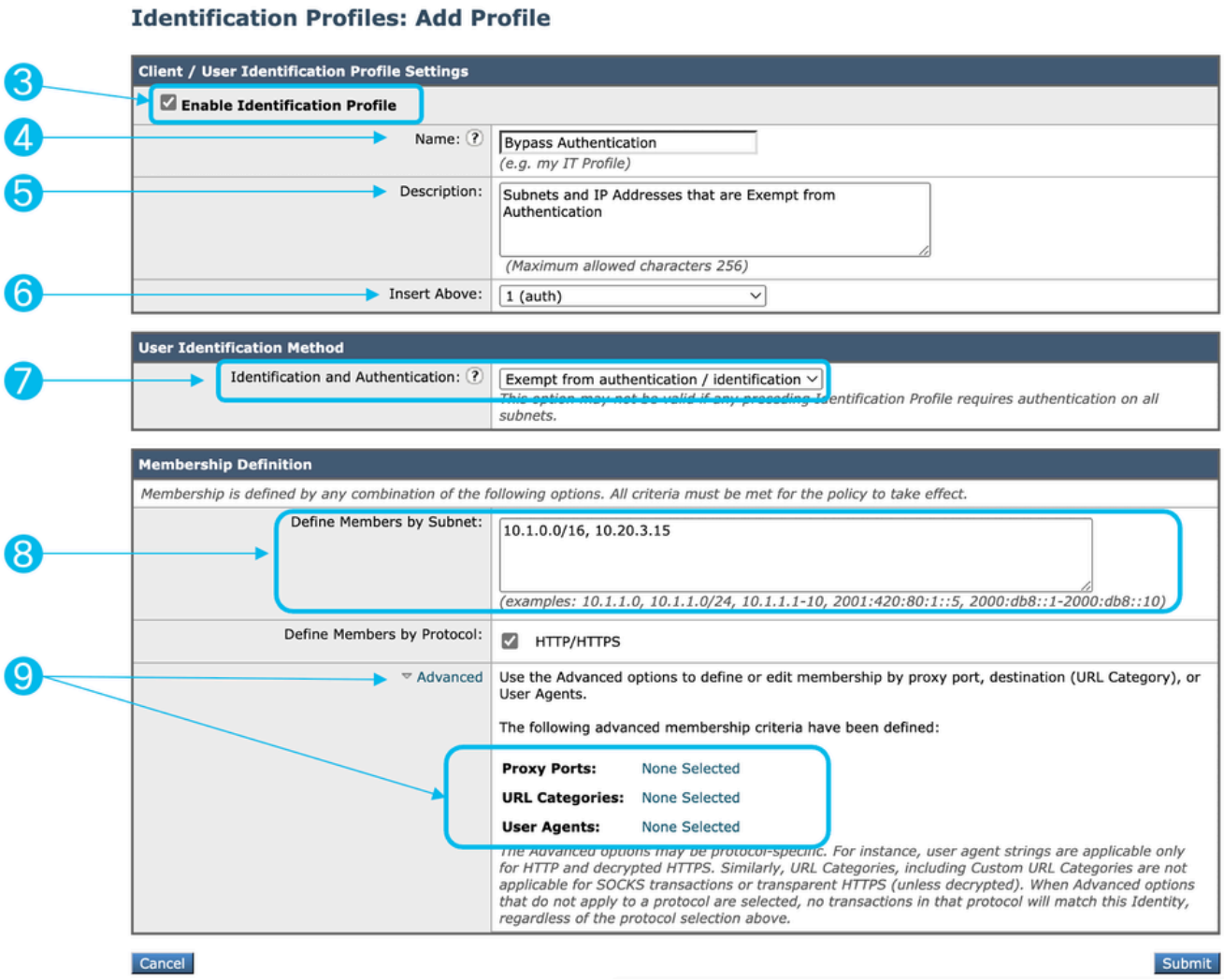


Waarschuwing: bij een transparante proxyimplementatie kan SWA geen gebruikersagents of de volledige URL voor HTTPS-verkeer lezen tenzij het verkeer wordt gedecodeerd. Als u het Identificatieprofiel configureert met gebruikersagents of een aangepaste URL-categorie met reguliere expressies, dan komt dit verkeer niet overeen met het Identificatieprofiel.

Voor meer informatie over het configureren van aangepaste URL-categorie gaat u naar: [Aangepaste URL-categorieën configureren in Secure Web Applicatie - Cisco]



Tip: Het beleid gebruikt een AND-logica, wat betekent dat aan alle voorwaarden moet zijn voldaan om het ID-profiel te kunnen matchen. Als er geavanceerde opties worden ingesteld, moet aan alle eisen worden voldaan om het beleid te kunnen toepassen.



Afbeelding - Stappen voor het maken van een ID-profiel om verificatie te omzeilen

Stap 10. Wijzigingen verzenden en vastleggen

Gerelateerde informatie

- Gebruikershandleiding voor AsyncOS 15.0 voor Cisco Secure Web Applicatie - GD (Algemene implementatie) - Classificatie van eindgebruikers voor beleidstoepassing [Cisco Secure Web Applicatie] - Cisco
- Aangepaste URL-categorieën configureren in applicatie voor beveiligd web - Cisco
- Office 365 Traffic vrijstellen van verificatie en decryptie op Cisco Web Security Applicatie (WSA) - Cisco

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.