Executable File Download blokkeren in SWA

Inhoud

Inleiding

Dit document beschrijft het proces van het configureren van Secure Web Appliance (SWA) om het downloaden van uitvoerbare bestanden te blokkeren.

Voorwaarden

Vereisten

Cisco raadt kennis van deze onderwerpen aan:

- Toegang tot grafische gebruikersinterface (GUI) van SWA
- Administratieve toegang tot 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.

Voordat u begint

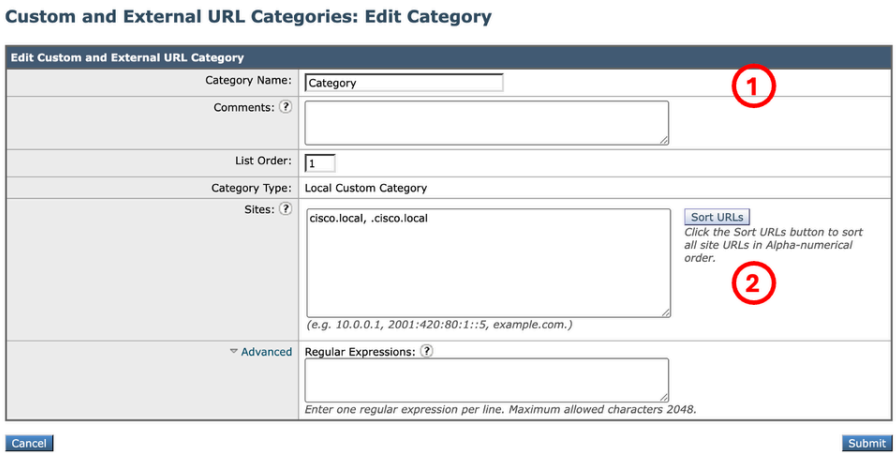
Cisco SWA kan het downloaden van uitvoerbare bestanden effectief blokkeren door het MIME-type (Multipurpose Internet Mail Extensions) van webinhoud te inspecteren. Door bestandstypen te identificeren zoals application/x-msdownload, application/x-msi en andere gerelateerde MIME-typen, handhaaft SWA beleid dat voorkomt dat uitvoerbare bestanden aan gebruikers worden geleverd. Naast MIME-typedetectie kan SWA gebruikmaken van bestandsextensiefiltering, op

reputatie gebaseerde analyse en aangepaste beleidsregels om de bescherming tegen ongewenste of risicovolle downloads verder te versterken. Deze mogelijkheden helpen organisaties een veilige browse-omgeving te behouden en het risico op malware-infecties te verminderen.

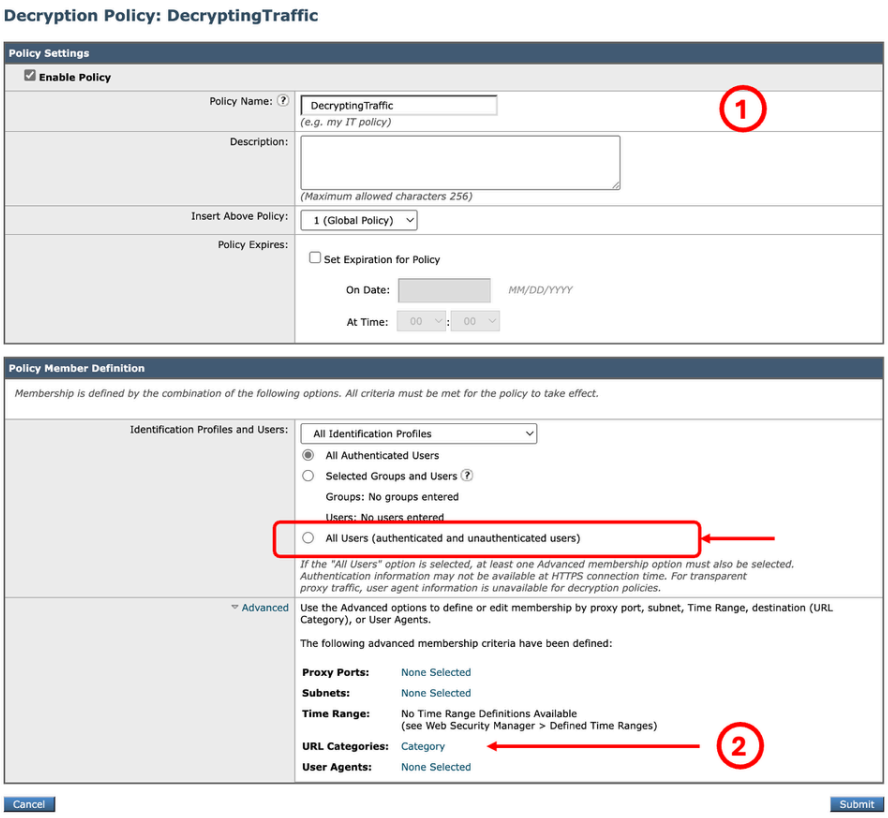
Tip: SWA kan het MIME-type van het bestand niet identificeren, tenzij het verkeer is gedecodeerd.

application/octet-stream is een generiek MIME-type dat wordt gebruikt om aan te geven dat een bestand binaire gegevens bevat. Het specificeert niet de aard van het bestand, dus het kan worden gebruikt voor elk bestand dat niet past bij een meer specifiek MIME-type. Dit type wordt gewoonlijk toegewezen aan uitvoerbare bestanden, installatieprogramma's en andere niet-tekstbestanden wanneer de webserver geen preciezer type kan bepalen.

Configuratiestappen

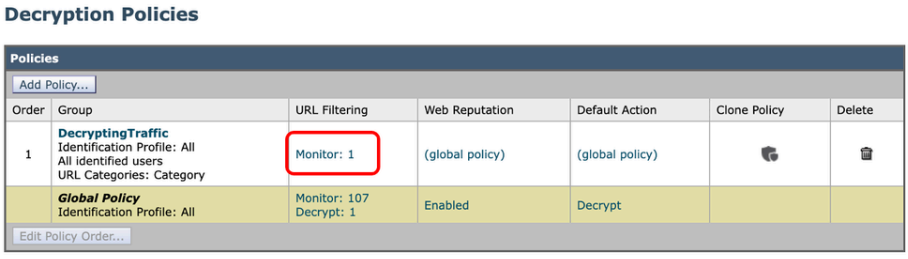
Stap 1. Maak een aangepaste URL-categorie voor de website.	Stap 1.1.Navigeer van de GUI naar Web Security Manager en kies Aangepaste en Externe URL-categorieën. Stap 1.2.Klik op Rubriek toevoegen om een nieuwe aangepaste URL-rubriek te maken. Stap 1.3.Voer de naam in voor de nieuwe categorie. Stap 1.4.Definieer het domein en/of de subdomeinen van de website die u probeert te blokkeren (in dit voorbeeld is cisco.local en al zijn subdomeinen). Stap 1.5.Wijzigingen indienen.  Afbeelding - Aangepaste URL-rubriek maken Tip: Ga voor meer informatie over het configureren van

	aangepaste URL-categorieën naar: https://www.cisco.com/c/en/us/support/docs/security/secure-web-appliance-virtual/220557-configure-cu...
Stap 2.Het verkeer voor de URL decoderen	Let op: het decoderen van een groot aantal URL's kan leiden tot verslechtering van de prestaties. Stap 2.1. Navigeer vanuit de GUI naar Web Security Manager en kies Decryptiebeleid Stap 2.2.Klik op Beleid toevoegen. Stap 2.3.Voer een naam in voor het nieuwe beleid. Stap 2.4. (Optioneel) Selecteer het identificatieprofiel waarop dit beleid van toepassing is. Tip: (Optioneel) Als u het beleid voor alle gebruikers wilt toepassen, zelfs als ze niet zijn geverifieerd, kiest u Alle gebruikers (geverifieerde en niet-geverifieerde gebruikers). Stap 2.5.Klik in het gedeelte Definitie van beleidslid op URL-categoriekoppelingen om de aangepaste URL-categorie toe te voegen. Stap 2.6.Selecteer de URL-categorie die is gemaakt in Stap 1. Stap 2.7.Klik op Indienen.



Afbeelding - Een decoderingsbeleid maken

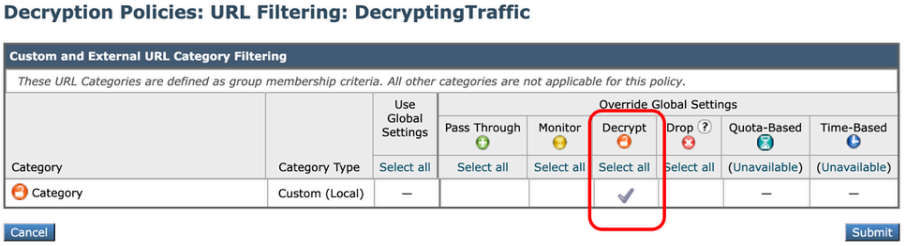
Stap 2.8.InDecryptie Beleid pagina, klik op de link van URL Filtering voor het nieuwe beleid.

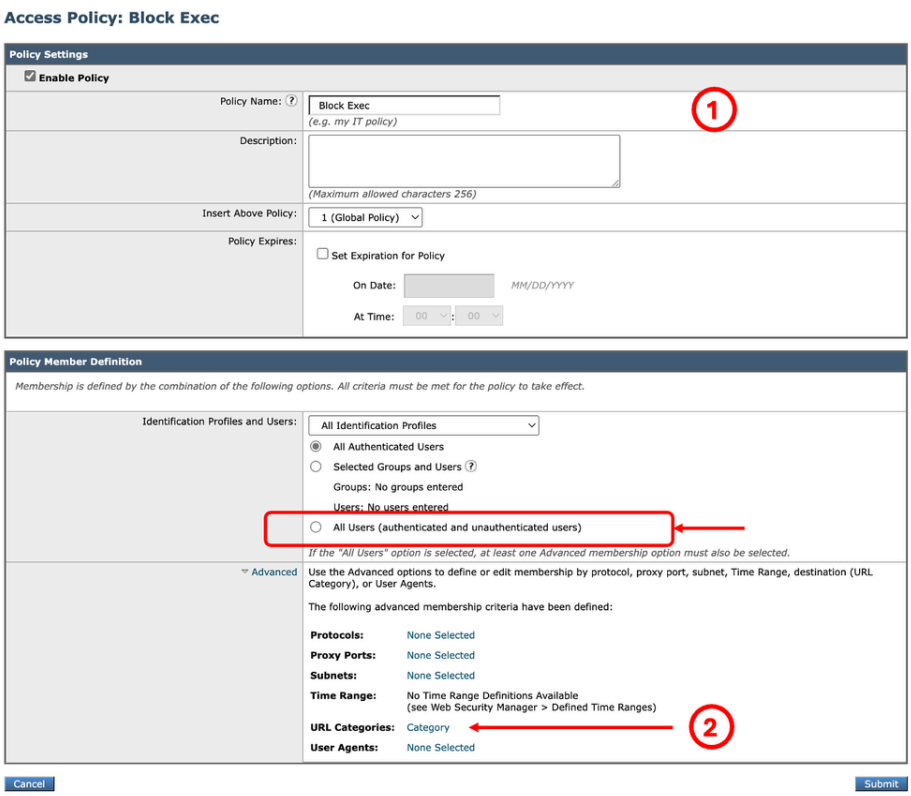


Afbeelding - Selecteer de URL-filtering

Stap 2.9.Kies Decrypt als de actie voor de aangepaste URL-categorie.

Stap 2.10.Klik op Indienen.



	Afbeelding - Decoderen als actie instellen
Stap 3.De uitvoerbare bestanden blokkeren	Stap 3.1.Navigeer vanuit de GUI naar Web Security Manager en kies Access Policies. Stap 3.2.Klik op Beleid toevoegen. Stap 3.3.Voer een naam in voor het nieuwe beleid. Stap 3.4. (Optioneel) Selecteer het identificatieprofiel waarop dit beleid van toepassing is. Tip: (Optioneel) Als u het beleid voor alle gebruikers wilt toepassen, zelfs als ze niet zijn geverifieerd, kiest u Alle gebruikers (geverifieerde en niet-geverifieerde gebruikers). Stap 3.5.Klik in het gedeelte Definitie van beleidslid op URL-categorieën links om de aangepaste URL-categorie toe te voegen. Stap 3.6.Selecteer de URL-categorie die is gemaakt in Stap 1. Stap 3.7.Klik op Indienen.  Afbeelding - Toegangsbeleid

Tip: Voor de rapportage is het het beste om een naam te kiezen die niet hetzelfde is als elk ander toegangs- / decoderingsbeleid.

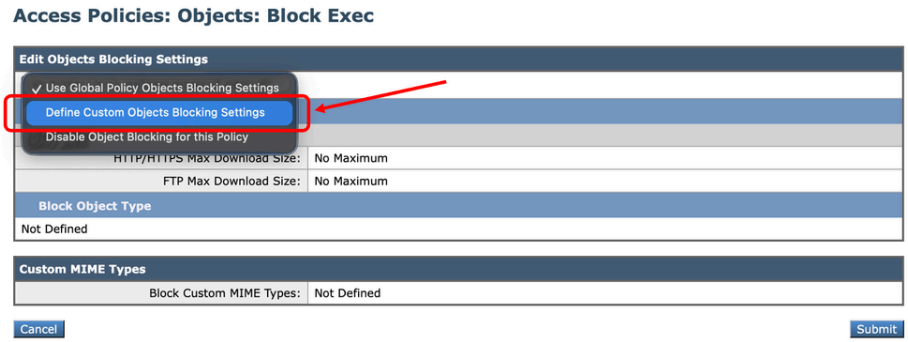
Stap 3.8.InAccess Policies pagina, zorg ervoor dat de URL Filtering actie is ingesteld op Monitor.

Stap 3.9. Klik op de pagina Access Policies op de koppeling van Objecten voor het nieuwe beleid.

Afbeelding - De objecten selecteren

Afbeelding - Selecteer de URL-filtering

Stap 3.10. Kies in de vervolgkeuzelijst Aangepaste objecten definiëren en blokinstellingen instellen.

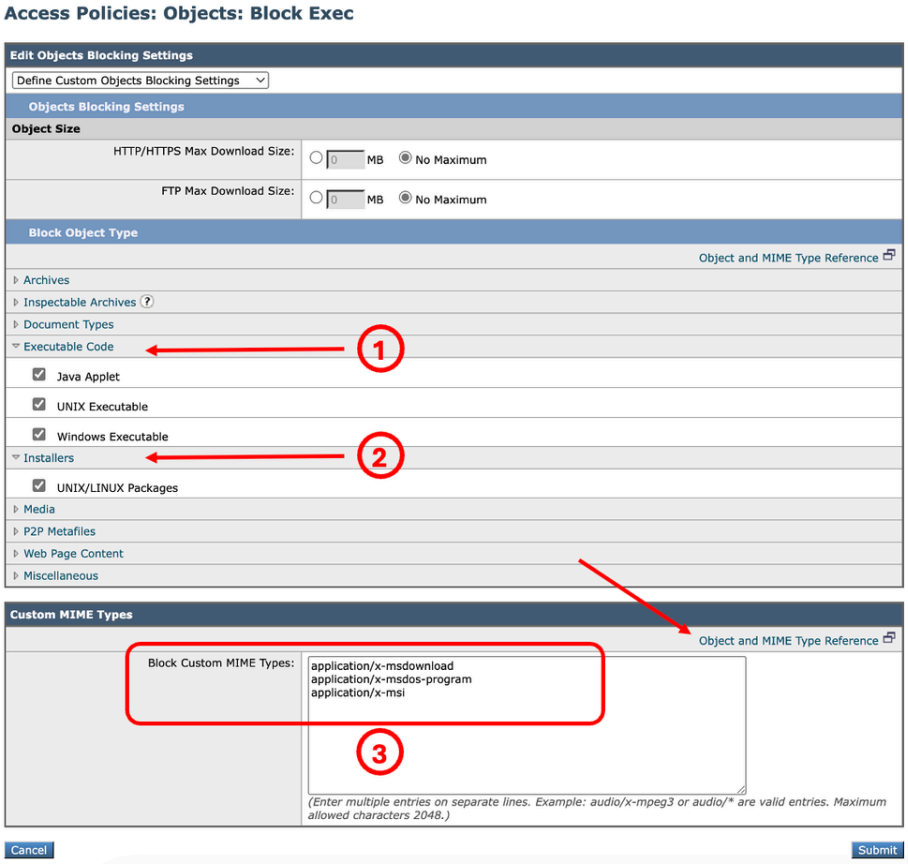


Afbeelding – Aangepaste objecten definiëren

Stap 3.11.ClickExecutable Code om de typen objecten te selecteren die u wilt blokkeren.

Stap 3.12.Klik op Installateurs om de typen objecten te selecteren die u wilt blokkeren.

Stap 3.13. Bovendien kunt u de MIME-typen invoeren van de bestanden die u wilt blokkeren in de sectie Aangepaste MIME-typen.



Afbeelding - Objecten configureren om te blokkeren

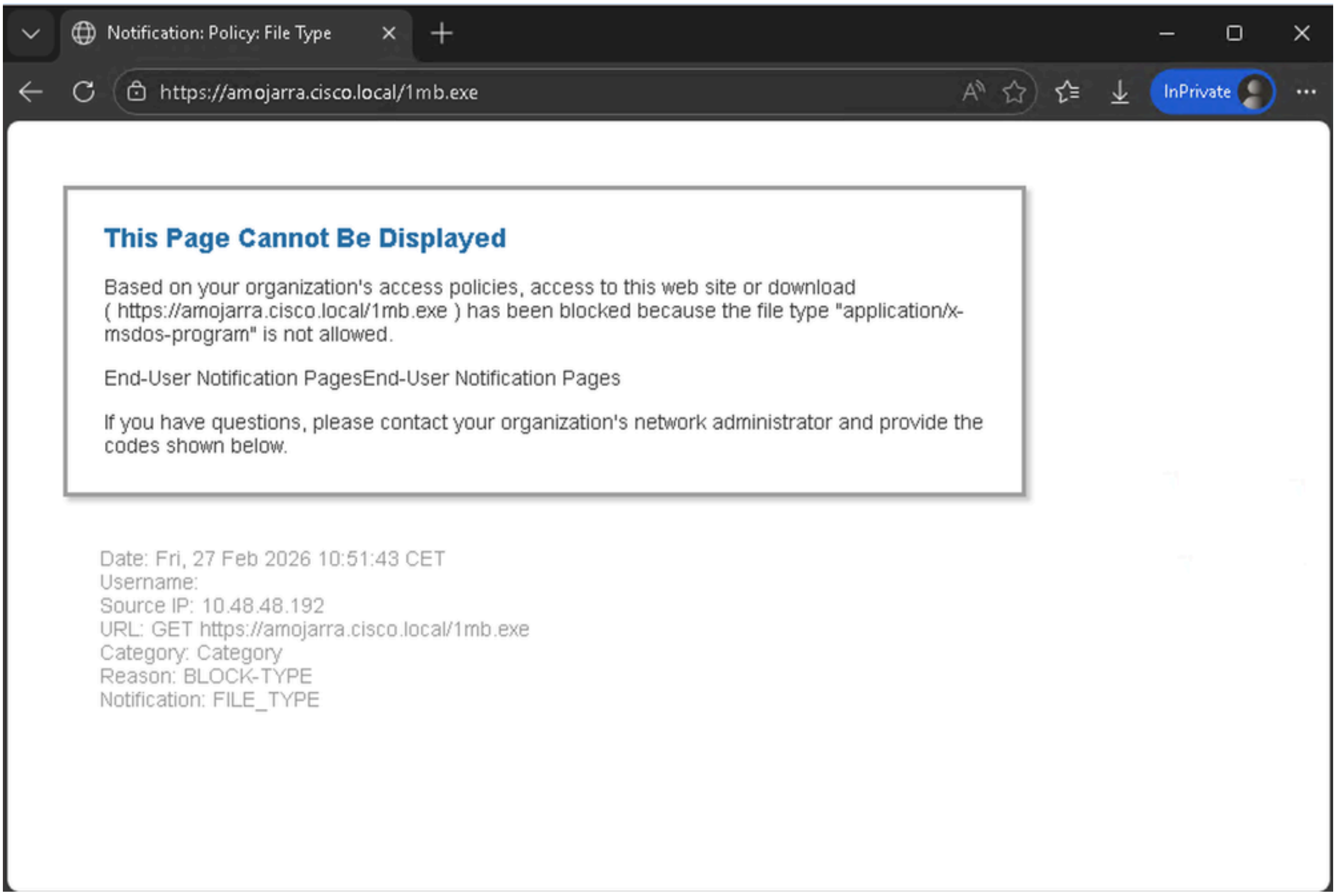
Tip: Als u de lijst met MIME-typen wilt weergeven, klikt u op Object en MIME-typeverwijzing.

Stap 3.14. Indienen.

Stap 3.15.Wijzigen vastleggen.

Validatie van blokkering van bestandsextensies

In dit voorbeeld wordt deze waarschuwingspagina weergegeven wanneer een gebruiker probeert een uitvoerbaar bestand te downloaden:



Afbeelding - Berichtpagina blokkeren

Tip: Als u de pagina Eindgebruikermeldingen (EUN) wilt configureren, gaat u vanuit de GUI naar Beveiligingsservices en klikt u op Eindgebruikermeldingen en wijzigt u de sectie Eindgebruikermeldingen.

In de toegangslogboeken ziet u twee logboekregels met betrekking tot het verkeer.

De eerste logregel is gerelateerd aan het Decryptiebeleid (Naam: DecryptingTraffic) dat het verkeer decodeert. De actie is DECRYPT_CUSTOMCAT

De tweede regel voor het toegangslogboek is gerelateerd aan het toegangsbeleid (naam: Block_Exec) dat we in stap 3 hebben gemaakt. De actie is BLOCK_ADMIN_FILE_TYPE

Beleid	toegangslogboek
decoderingsbeleid	1772186569.823 182 10.48.48.192 TCP_MISS_SSL/200 39 CONNECT tunnel://amojarra.cisco.local:443/ - DIRECT/amojarra.cisco.local - DECRYPT_CUSTOMCAT_7-DecryptingTraffic-DefaultGroup-NONE-NONE-NONE-LAB_Access-NONE <"C_Cate",-,-",-",--,--,"-",-,--",--",--",-",-",-",-",-",-","-","-","-","-","-","-","-","-","-", 1.71,0,-","-","-","-",-",-"-,"-"-",-"-",-"-,-"-,---"-,--> -

toegangsbeleid	1772186576.735 2242 10.48.48.192 TCP_DENIED_SSL/403 0 GET https://amojarra.cisco.local:443/1mb.exe - DIRECT/amojarra.cisco.local application/x-msdos-program BLOCK_ADMIN_FILE_TYPE_12-Block_Exec-DefaultGroup-NONE-NONE-NONE-LAB_Access-NONE <"C_Cate", ns,0"-", 0,0,0,-",-",-,--",-",--",-",-",-",--",-",-","-","Unknown","-","Unknown","-","-","-","-", 0.00,-,"Unknown","-","-","-,"-,"-,"-","-",-,-"-",-"-,--"-,-,---->

Gerelateerde informatie

- Gebruikershandleiding voor AsyncOS 15.2 voor Cisco Secure Web Appliance
- Installatiehandleiding voor Cisco Secure Email and Web Virtual Appliance
- Aangepaste URL-categorieën configureren in Secure Web Appliance - Cisco
- Best practices voor veilige webapparaten gebruiken
- Firewall configureren voor Secure Web Appliance
- Decryptiecertificaat configureren in Secure Web Appliance
- SNMP configureren en oplossen in SWA
- SCP Push Logs configureren in Secure Web Appliance met Microsoft Server
- Specifieke YouTube-kanaal / video inschakelen en de rest van YouTube blokkeren in SWA
- Inzicht in HTTPS-toegangslogindeling in Secure Web Appliance
- Toegang tot beveiligde logbestanden van webapparaten
- Verificatie omzeilen in Secure Web Appliance
- Verkeer blokkeren in Secure Web Appliance
- Microsoft Updates-verkeer omzeilen in Secure Web Appliance

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.