Upstream-proxy configureren in Secure Web Appliance

Inhoud

Inleiding

Voorwaarden

- Vereisten
- Gebruikte componenten

Upstream-proxy configureren

- Stap 2. (Optioneel) Maak een identificatieprofiel om de upstream-proxy te gebruiken
- Stap 3. De upstream proxy maken
- Stap 4. (Optioneel) Upload het decoderingscertificaat
- Stap 5. Het routeringsbeleid configureren
- Stap 6. (Optioneel) De instellingen voor de niet-reagerende upstream-proxy configureren

Logboekregistratie

- Accessoires
- proxylogen

Gerelateerde informatie

Inleiding

In dit document worden de stappen beschreven voor het configureren van Upstream Proxy in Secure Web Appliance (SWA).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- SWA-beheer.
- Basisprotocollen voor netwerken en proxy's.

Cisco raadt u aan deze hulpprogramma's te installeren:

- Fysieke of virtuele SWA

- Administratieve toegang tot de grafische gebruikersinterface (GUI) van SWA
- Administratieve toegang tot de SWA Command Line Interface (CLI)

Gebruikte componenten

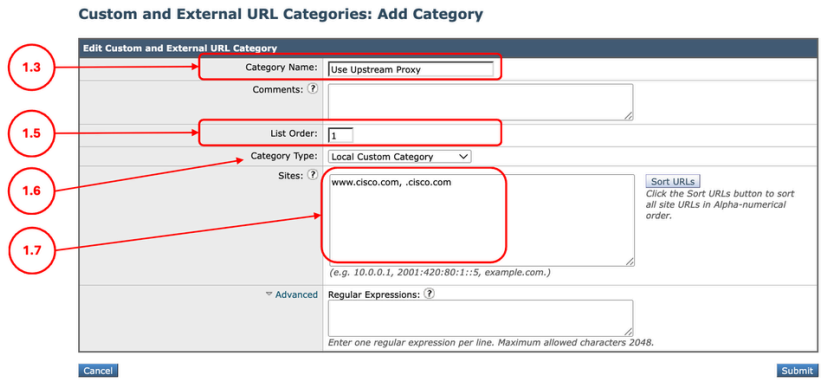
Dit document is niet beperkt tot specifieke software- en hardware-versies.

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.

Upstream-proxy configureren

Gebruik deze stappen om een upstream-proxy in SWA te configureren.

Stappen	Stappen
Stap 1. (Optioneel) Maak een aangepaste URL-categorie voor de URL's Opmerking: Als u de upstream-proxy voor al het verkeer wilt definiëren, kunt u deze stap overslaan.	Stap 1.1.Kies Web Security Manager van GUI en klik op Aangepaste en Externe URL-categorieën. Stap 1.2.Klik op Categorie toevoegen om een aangepaste URL-rubriek toe te voegen. Stap 1.3.Een unieke categorienaam toewijzen. Stap 1.4. (Optioneel) Beschrijving toevoegen. Stap 1.5. Kies in Lijstvolgorde de eerste categorie die u bovenaan wilt plaatsen. Stap 1.6. Kies in de vervolgkeuzelijst Categorie de optie Lokale aangepaste rubriek. Stap 1.7. Voeg de gewenste URL's toe in de sectie Sites. Stap 1.8. Verzenden.

<table>
<tr>
<td></td>
<td> 

Afbeelding - Een aangepaste URL-rubriek maken</td>
</tr>
<tr>
<td>Stap 2. (Optioneel) Maak een identificatieprofiel om de upstream-proxy te gebruiken

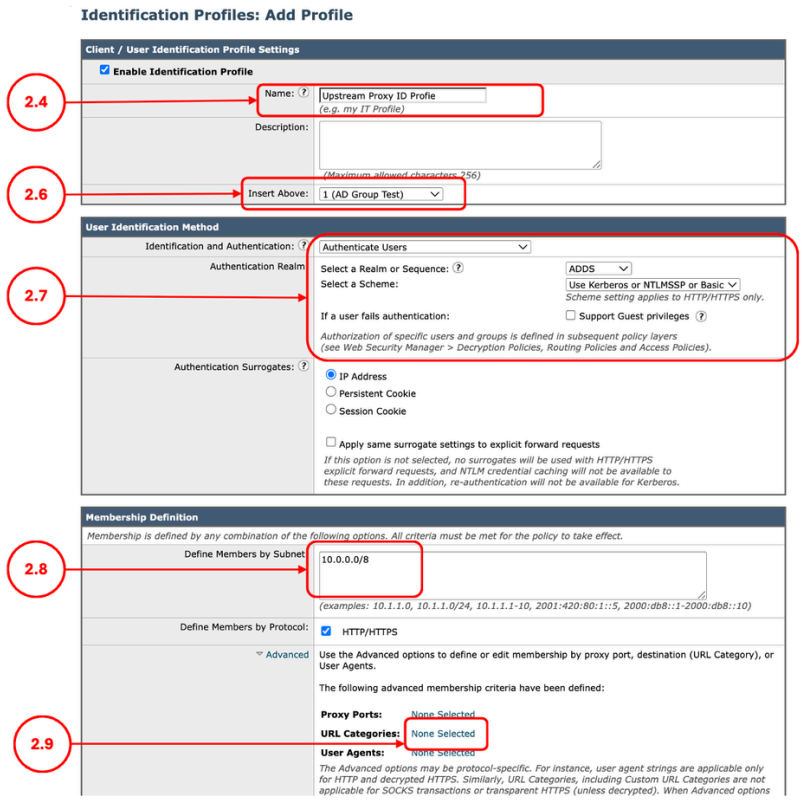
Opmerking: Als u de upstream-proxy voor al het verkeer wilt definiëren, kunt u deze stap overslaan.</td>
<td>Stap 2.1.Kies Web Security Manager van GUI en klik op Identificatieprofielen.
Stap 2.2.Klik op Profiel toevoegen om een profiel toe te voegen.
Stap 2.3.Gebruik het selectievakje Identificatieprofiel inschakelen om dit profiel in te schakelen of snel uit te schakelen zonder het te verwijderen.
Stap 2.4.Een unieke profielnaam toewijzen.
Stap 2.5. (Optioneel) Beschrijving toevoegen.
Stap 2.6.Kies in de vervolgkeuzelijst Invoegen hierboven waar dit profiel in de tabel moet worden weergegeven.

Stap 2.7. Als u niet wilt verifiëren welke gebruikers op dit beleid van toepassing zijn, kiest u in het gedeelte Gebruikersidentificatiemethoden de optie Vrijstellen van verificatie/identificatie, anders configureert u de verificatieparameters.

Stap 2.8.In de Leden definiëren op subnet, laat dit veld leeg om alle client IP-adres op te nemen, tenzij u wilt passeren door het verkeer voor een bepaald IP-adres.

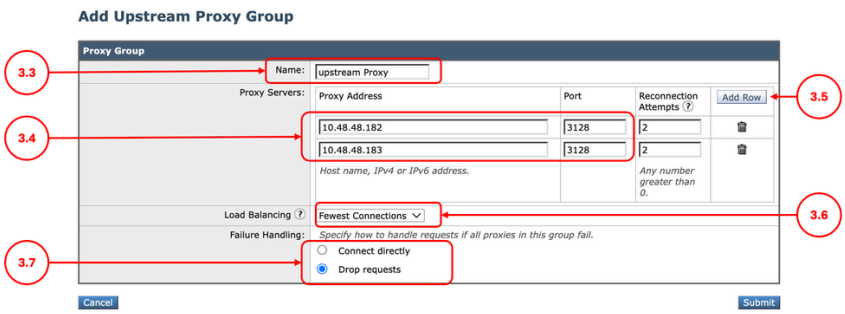
Stap 2.9. (Optioneel: Als u een upstream-proxy moet gebruiken voor specifieke gebruikers die toegang hebben tot bepaalde websites, voltooit u deze stap.) Kies in de sectie Geavanceerd de optie Aangepaste URL-categorieën en voeg de Aangepaste URL-categorie toe die is gemaakt in stap 1

Stap 2.10. Verzenden.</td>
</tr>
</table>



Afbeelding - Een identificatieprofiel maken

Stap 3. De upstream proxy maken	Stap 3.1.Van GUI, Kies Network en klik vervolgens op Upstream Proxy. Stap 3.2. Klik op Groep toevoegen. Stap 3.3.Een unieke naam toewijzen. Stap 3.4. Definieer het proxy-adres en poortnummer. Stap 3.5. (Optioneel) Als u meer dan één Upstream-proxy hebt, klikt u op Rij toevoegen om de volgende proxy te definiëren. Stap 3.6. (Optioneel) Als u meer dan één Upstream-proxy hebt ingevoerd in het gedeelte Load Balancing, definieert u de gewenste Load Balancing-methode, • Geen (failover): de webproxy leidt transacties naar één externe proxy in de groep. Het probeert verbinding te maken met de proxy's in de volgorde waarin ze worden vermeld. Als één proxy niet kan worden bereikt, probeert de webproxy verbinding te maken met de volgende in de lijst. • Minder verbindingen: De Web Proxy houdt bij hoeveel actieve verzoeken er zijn met de verschillende proxy's in de groep en stuurt een transactie naar de proxy die momenteel het minste aantal verbindingen onderhoudt.

	• Op hash gebaseerd: minst recent gebruikt. De webproxy stuurt een transactie naar de proxy die het minst recent een transactie heeft ontvangen als alle proxy's momenteel actief zijn. Deze instelling is vergelijkbaar met round robin, behalve dat de Web Proxy ook rekening houdt met transacties die een proxy heeft ontvangen door lid te zijn van een andere proxygroep. Dat wil zeggen, als een proxy in meerdere proxygroepen wordt vermeld, is de optie "minst recent gebruikt" minder waarschijnlijk om die proxy te overbelasten. • Round robin: De Web Proxy cycluseert transacties gelijkelijk tussen alle proxy's in de groep in de vermelde volgorde. Stap 3.7. Kies de optie Mislukking is afhankelijk van uw interne beleid. • Direct verbinding maken: de verzoeken rechtstreeks naar de bestemmingsservers sturen. • Drop requests: gooi de requests weg zonder ze door te sturen. Stap 3.8. Verzenden.  Afbeelding - Upstream-proxygroep toevoegen
Stap 4. (Optioneel) Upload het decoderingscertificaat Opmerking: als de Upstream-proxy het verkeer niet decodeert of als de CA-server al vertrouwd is in de SWA, kunt u deze stap overslaan	Stap 4.1.Van GUI, Kies Network en klik vervolgens op Certificate Management. Stap 4.2. Klik in het gedeelte Certificaatbeheer op Vertrouwde basiscertificaten beheren.

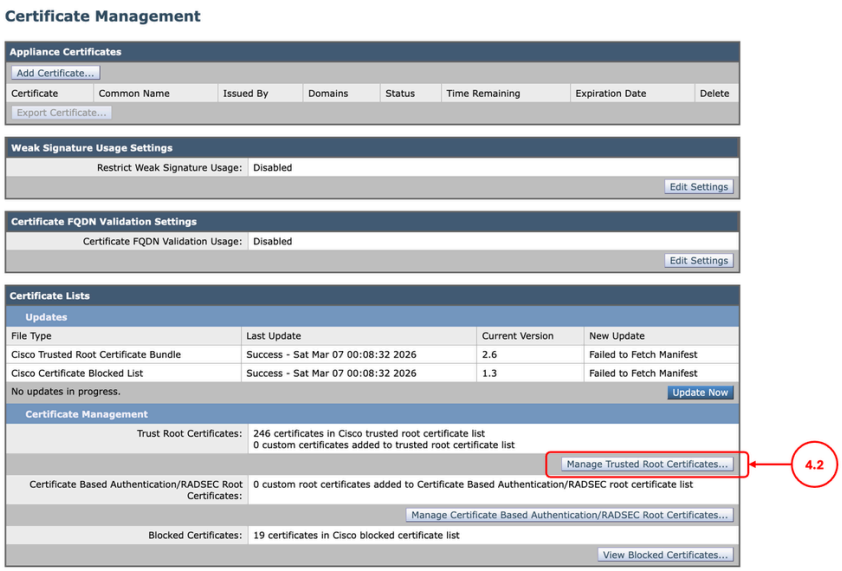


Image - Vertrouwd basiscertificaat beheren

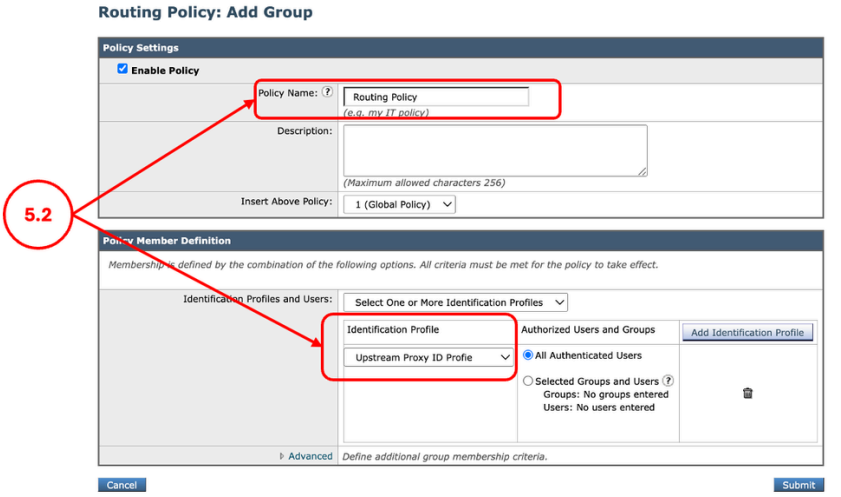
Stap 4.3. Verzenden en wijzigingen vastleggen.

⚠ Let op: Als zowel root- als intermediaire CA-certificaten vereist zijn, uploadt u eerst het root CA-certificaat en klikt u vervolgens op Indienen en vastleggen. Nadat de commit is voltooid, importeert u het tussenliggende CA-certificaat en dient u de wijzigingen opnieuw in en legt u ze vast.

Stap 5. Het routeringsbeleid configureren

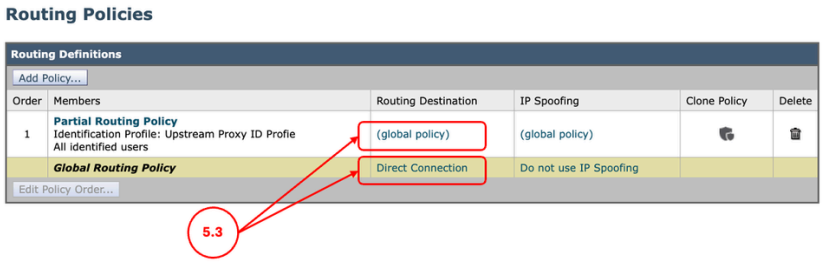
Stap 5.1. Kies Web Security Manager in GUI en klik op Routeringsbeleid.

Stap 5.2. (Optioneel) Als u de upstream-proxy voor specifieke gebruikers of websites wilt gebruiken, klikt u op Beleid toevoegen en selecteert u het identificatieprofiel dat u in stap 2 hebt gemaakt.



Afbeelding - ID-profiel toevoegen aan routeringsbeleid

Stap 5.3. Voor de gewenste voorwaarden, die u wilt gebruiken de upstream proxy, klikt u op Routing Destination link en selecteer de Upstream Proxy Group die u hebt gemaakt op stap 3.



Afbeelding - Routeringsbestemming configureren

Opmerking: Als u al het verkeer wilt gebruiken met behulp van upstream-proxy, in het algemene routeringsbeleid, selecteert u de gewenste upstream-proxy.

Stap 5.4. Verzenden en vastleggen van de wijzigingen.

Stap 6. (Optioneel) De instellingen voor de niet-reagerende upstream-proxy configureren

Tip: Het wordt aanbevolen om deze waarden niet aan te passen, tenzij u volledig begrijpt wat hun gedrag en potentiële impact is.

Stap 6.1. Meld u aan bij de CLI en voer geavanceerde proxyconfig uit

Stap 6.2. Selecteer DIVERSEN

Stap 6.3. Druk op Enter totdat u Enter minimum idle timeout ziet voor het controleren van niet-reagerende upstream proxy (in seconden). u kunt de minimale hoeveelheid tijd configureren, SWA wacht om de upstream proxy die eerder ziek was verklaard opnieuw te proberen. De standaardwaarde is 10 seconden.

Stap 6.4. Druk op Enter om door te gaan naar de volgende instelling. Wanneer u de maximale time-out voor inactieve tijd definieert voor het controleren van een niet-reagerende upstream-proxy, moet u er rekening mee houden dat als deze time-outwaarde wordt bereikt voordat het geconfigureerde aantal herverbindingspogingen is uitgeput (stap 3), de SWA de upstream-proxy offline beschouwt.

Stap 6.7. Blijf op Enter drukken totdat u de wizard afsluit, voer commit uit om de wijzigingen op te slaan.

Logboekregistratie

Accessoires

In de Accesslogs wordt het verkeer dat naar upstream proxy is geleid weergegeven als DEFAULT_PARENT gevolgd door de naam van de upstream proxy. Hier is een voorbeeld:

```
1775659642.780 462 10.20.3.15 TCP_MISS_SSL/200 129 CONNECT tunnel://www.cisco.com:443/ "AMOJARRA\amojar
```

proxylogen

Vanuit de proxylogs kunt u de gezondheidsstatus van de upstream-proxy's controleren.

Tip: U kunt filteren op peer om de logs met betrekking tot de upstream-proxy te bekijken.

Hier zijn enkele voorbeelden, omdat we de herverbindingspogingen in stap 3 tot twee keer hebben geconfigureerd, wordt de upstream-proxy na twee fouten verbinding maken met de upstream-proxy als dad verklaard en SWA verwijdert deze upstream-proxy uit de lijst totdat het proxyproces opnieuw wordt gestart.

```
Thu Apr  2 13:52:35 2026 Info: PROX_CONNTRACK : 940 : [15968:0] Peer-upstream 10.48.48.182:3128 was hea
Thu Apr  2 13:52:36 2026 Info: PROX_CONNTRACK : 940 : [15968:0] Peer 10.48.48.182:3128 was sick, now he
...
Thu Apr  2 13:59:37 2026 Info: PROX_CONNTRACK : 60 : [71197:0] Peer 10.48.48.183:3128 remains sick afte
Thu Apr  2 13:59:39 2026 Warning: PROX_CONNTRACK : 70 : [71197:0] Peer-upstream 10.48.48.183:3128 decla
```

Opmerking: Als de upstream-proxy niet reageert op TCP-SYN-verzoeken, een HTTP-antwoordcode niet retourneert of een HTTP 504-respons (Gateway Timeout) retourneert, beschouwt de SWA de upstream-proxy als niet beschikbaar en wijzigt de status van Gezond naar Ziek.

Tip: De SWA beschouwt een upstream-proxy als gezond als deze een VIA-header retourneert.

Gerelateerde informatie

- Gebruikershandleiding voor AsyncOS 15.0 voor Cisco Secure Web Appliance
- Aangepaste URL-categorieën configureren in Secure Web Appliance - Cisco
- Hoe Office 365-verkeer vrij te stellen van verificatie en decodering op Cisco Web Security Appliance (WSA) - Cisco
- Best practices voor veilige webapparaten gebruiken - Cisco
- Verkeer blokkeren in Secure Web Appliance
- Uploadverkeer blokkeren in Secure Web Appliance
- Executable File Download blokkeren in SWA
- Microsoft Updates-verkeer omzeilen in Secure Web Appliance
- Verificatie omzeilen in Secure Web Appliance - 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.