Upstreamproxy in sicherer Webappliance konfigurieren

Inhalt

Einleitung

In diesem Dokument werden die Schritte zum Konfigurieren des Upstreamproxys in der sicheren Webappliance (SWA) beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- SWA-Verwaltung.
- Grundlegende Netzwerk- und Proxy-Protokolle.

Cisco empfiehlt die Installation der folgenden Tools:

- Physisches oder virtuelles SWA

- Administratorzugriff auf die grafische Benutzeroberfläche (GUI) von SWA
- Administratorzugriff auf die SWA-Befehlszeilenschnittstelle (CLI)

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Upstream-Proxy konfigurieren

Gehen Sie folgendermaßen vor, um einen Upstream-Proxy in SWA zu konfigurieren.

<table>
<tr><th>Schritte</th><th>Schritte</th></tr>
<tr><td>Schritt 1. (Optional) Erstellen Sie eine benutzerdefinierte URL-Kategorie für die URLs

Anmerkung: Wenn Sie den Upstream-Proxy für den gesamten Datenverkehr definieren möchten, können Sie diesen Schritt überspringen.</td><td>Schritt 1.1.Wählen Sie aus der GUI den Websicherheits-Manager aus, und klicken Sie dann auf Benutzerdefinierte und externe URL-Kategorien.
Schritt 1.2.Klicken Sie aufKategorie hinzufügen,um eine benutzerdefinierte URL-Kategorie hinzuzufügen.
Schritt 1.3.Zuweisen eines eindeutigen Kategorienamens.
Schritt 1.4. (Optional) Beschreibung hinzufügen.

Schritt 1.5. Wählen Sie aus der Listenreihenfolge die erste Kategorie für die Positionierung an der Spitze aus.

Schritt 1.6. Wählen Sie aus der Dropdown-Liste Kategorie Typ die Option Lokale benutzerdefinierte Kategorie aus.

Schritt 1.7. Fügen Sie die gewünschten URLs im Abschnitt Sites hinzu.

Schritt 1.8: Senden.</td></tr>
</table>

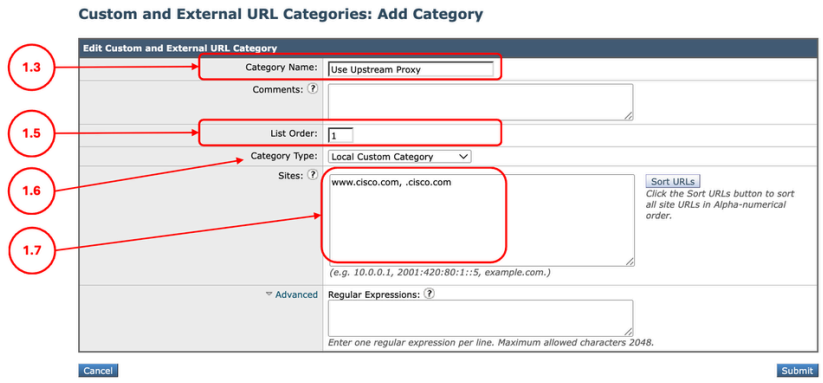


Bild - Erstellen einer benutzerdefinierten URL-Kategorie

Schritt 2: (Optional) Erstellen Sie ein Identifizierungsprofil für den Upstream-Proxy.

Anmerkung: Wenn Sie den Upstream-Proxy für den gesamten Datenverkehr definieren möchten, können Sie diesen Schritt überspringen.

Schritt 2.1.Wählen Sie aus der GUI den Websicherheits-Manager aus, und klicken Sie dann auf Identifikationsprofile.
Schritt 2.2.Klicken Sie auf Profil hinzufügen, um ein Profil hinzuzufügen.
Schritt 2.3.Verwenden Sie das Kontrollkästchen Identifikationsprofil aktivieren, um dieses Profil zu aktivieren oder es schnell zu deaktivieren, ohne es zu löschen.
Schritt 2.4.Zuweisen eines eindeutigen profileName.
Schritt 2.5. (Optional) Beschreibung hinzufügen.
Schritt 2.6.Wählen Sie aus der Dropdown-Liste Einfügen aus, wo dieses Profil in der Tabelle angezeigt werden soll.

Schritt 2.7. Wenn Sie keine Authentifizierung für die Benutzer wünschen, die diese Richtlinie erreichen, wählen Sie im Abschnitt User Identification Methods (Benutzeridentifizierungsmethode) die OptionExempt from authentication/identification (Von Authentifizierung/Identifizierung ausnehmen) aus, andernfalls konfigurieren Sie die Authentifizierungsparameter.

Schritt 2.8.Lassen Sie dieses Feld im Feld Mitglieder nach Subnetz definieren leer, um alle Client-IP-Adressen einzuschließen, es sei denn, Sie möchten den Datenverkehr für eine bestimmte IP-Adresse weiterleiten.

Schritt 2.9 (Optional: Wenn Sie einen Upstream-Proxy für bestimmte Benutzer verwenden müssen, die auf bestimmte Websites zugreifen, führen Sie diesen Schritt aus.) Wählen Sie im Abschnitt Erweitert die Option Benutzerdefinierte URL-Kategorien aus, und fügen Sie die benutzerdefinierte URL-Kategorie hinzu, die in Schritt 1 erstellt wurde.

Schritt 2.10: Senden.

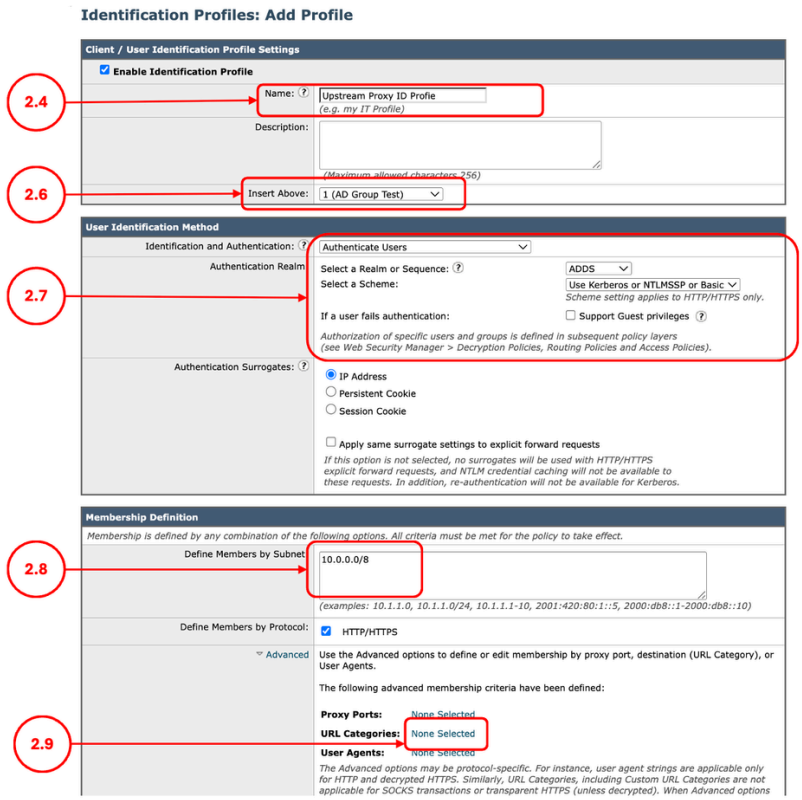
<table>
<tr>
<td></td>
<td> 

Bild - Identifikationsprofil erstellen</td>
</tr>
<tr>
<td>Schritt 3: Erstellen des Upstream-Proxys</td>
<td>Schritt 3.1.AusGUI: Wählen SieNetzwerk aus, und klicken Sie dann auf Upstream-Proxy.

Schritt 3.2. Klicken Sie auf Gruppe hinzufügen.

Schritt 3.3.Zuweisen eines eindeutigen Namens.
Schritt 3.4: Definieren der Proxyadresse und der Portnummer.
Schritt 3.5. (Optional) Wenn Sie mehr als einen Upstream-Proxy haben, klicken Sie auf Zeile hinzufügen, um den nächsten Proxy zu definieren.

Schritt 3.6. (Optional) Wenn Sie mehr als einen Upstream-Proxy aus dem Abschnitt Load Balancing eingegeben haben, definieren Sie die gewünschte Load Balancing-Methode.

• Keine (Failover): Der Webproxy leitet Transaktionen an einen externen Proxy in der Gruppe weiter. Er versucht, eine Verbindung zu den Proxys in der Reihenfolge herzustellen, in der sie aufgeführt sind. Wenn ein Proxy nicht erreichbar ist, versucht der Webproxy, eine Verbindung mit dem nächsten in der Liste herzustellen.
• Geringste Anzahl an Verbindungen: Der Webproxy</td>
</tr>
</table>

überwacht, wie viele aktive Anforderungen mit den verschiedenen Proxys in der Gruppe vorhanden sind, und leitet eine Transaktion an den Proxy weiter, der derzeit die geringste Anzahl an Verbindungen bedient.
- Hash-basiert: Zuletzt verwendet. Der Webproxy leitet eine Transaktion an den Proxy weiter, der zuletzt eine Transaktion empfangen hat, wenn alle Proxys derzeit aktiv sind. Diese Einstellung ähnelt dem Round-Robin-Verfahren, jedoch berücksichtigt der Webproxy auch Transaktionen, die ein Proxy empfangen hat, indem er Mitglied einer anderen Proxygruppe ist. Das heißt, wenn ein Proxy in mehreren Proxy-Gruppen aufgelistet ist, ist die Option "zuletzt verwendet" weniger wahrscheinlich, dass dieser Proxy überlastet wird.
- Round Robin: Der Webproxy durchläuft die Transaktionen gleichmäßig zwischen allen Proxys in der Gruppe in der aufgelisteten Reihenfolge.

Schritt 3.7. Wählen Sie die Option Fehlerbehandlung abhängig von Ihrer internen Richtlinie aus.

- Direkte Verbindung herstellen:Senden Sie die Anforderungen direkt an die Zielserver.
- Anforderungen verwerfen:Verwerfen Sie die Anforderungen, ohne sie weiterzuleiten.

Schritt 3.8: Senden.

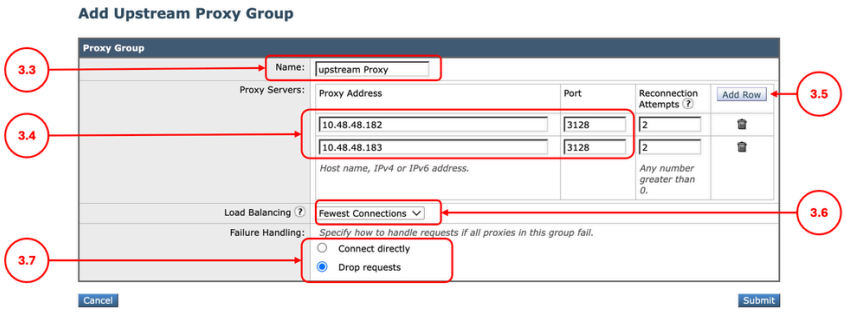


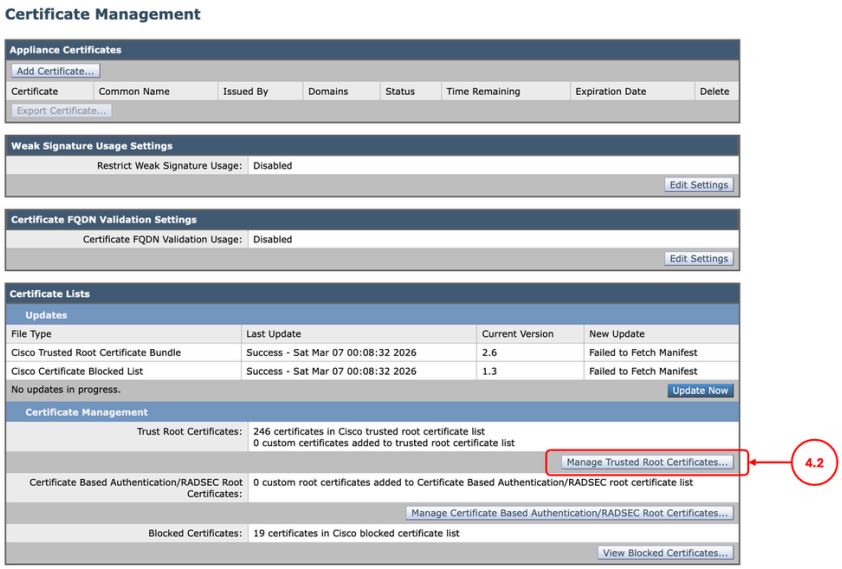
Image: Upstream-Proxygruppe hinzufügen

Schritt 4. (Optional) Laden Sie das Entschlüsselungszertifikat hoch.

Anmerkung: Wenn der Upstream-Proxy den

Schritt 4.1.AusGUI: Wählen SieNetzwerk aus, und klicken Sie dann auf Zertifikatsverwaltung.

Schritt 4.2. Klicken Sie im Abschnitt Zertifikatsverwaltung auf Vertrauenswürdige Stammzertifikate verwalten.

Datenverkehr nicht entschlüsselt oder sein CA-Server bereits im SWA vertrauenswürdig ist, können Sie diesen Schritt überspringen.	 Image - Vertrauenswürdiges Stammzertifikat verwalten Schritt 4.3 Änderungen einsenden und bestätigen. Achtung: Wenn sowohl Root- als auch Zwischenzertifikate erforderlich sind, laden Sie zuerst das Root-Zertifizierungsstellenzertifikat hoch, und klicken Sie dann auf Senden und bestätigen. Nach Abschluss der Bestätigung importieren Sie das Zwischenzertifikat der Zertifizierungsstelle, und senden Sie die Änderungen erneut, und bestätigen Sie sie.
Schritt 5: Konfigurieren der Routing-Richtlinie	Schritt 5.1. Wählen Sie in der GUI den Websicherheits-Manager aus, und klicken Sie dann auf Routingrichtlinie. Schritt 5.2. (Optional) Wenn Sie den Upstreamproxy für bestimmte Benutzer oder Websites verwenden möchten, klicken Sie auf Richtlinie hinzufügen, und wählen Sie das Identifikationsprofil aus, das Sie in Schritt 2 erstellt haben.

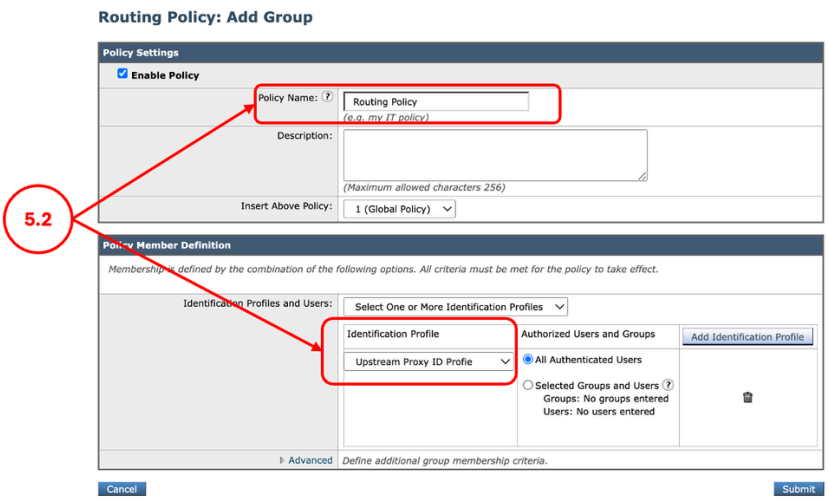


Image - Hinzufügen eines ID-Profils zur Routing-Richtlinie

Schritt 5.3. Um die gewünschten Bedingungen zu erhalten, die Sie für den Upstream-Proxy verwenden möchten, klicken Sie auf den Link Routing Destination (Routing-Ziel), und wählen Sie die Upstream-Proxygruppe aus, die Sie in Schritt 3 erstellt haben.

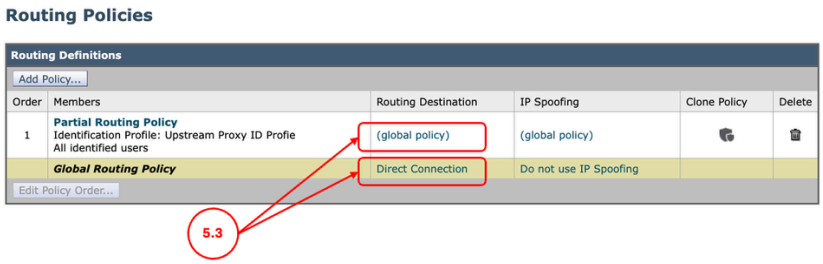


Image - Konfigurieren des Routing-Ziels

Anmerkung: Wenn der gesamte Datenverkehr, der den Upstream-Proxy verwendet, von der globalen Routingrichtlinie erwartet werden soll, wählen Sie den gewünschten Upstream-Proxy aus.

Schritt 5.4. Senden und bestätigen Sie die Änderungen.

Schritt 6: (Optional) Konfigurieren der Einstellungen für das nicht reagierende Upstream-Proxytimeout

Tipp: Es wird empfohlen,

Schritt 6.1. Melden Sie sich bei der CLI an, und führen Sie advancedproxyconfig aus.

Schritt 6.2. Wählen Sie VERSCHIEDENES

Schritt 6.3. Drücken Sie die Eingabetaste, bis Enter minimum idle timeout (Minimaler Leerlaufzeitüberschreitungswert für Prüfung des nicht antwortenden Upstreamproxys) (in Sekunden) angezeigt

diese Werte nur dann zu ändern, wenn Sie ihr Verhalten und ihre potenziellen Auswirkungen vollständig verstehen.	wird. Wenn Sie die minimale Zeitspanne konfigurieren können, wartet SWA darauf, den Upstreamproxy, der zuvor als krank deklariert wurde, erneut zu versuchen. Der Standardwert ist 10 Sekunden. Schritt 6.4. Drücken Sie die Eingabetaste, um zur nächsten Einstellung zu gelangen. Wenn Sie den maximalen Timeout für Leerlaufzeiten zum Überprüfen eines nicht antwortenden Upstreamproxys definieren, beachten Sie, dass der SWA den Upstreamproxy als offline betrachtet, wenn dieser Timeoutwert erreicht wird, bevor die konfigurierte Anzahl von erneuten Verbindungsversuchen erschöpft ist (Schritt 3). Schritt 6.7. Drücken Sie die Eingabetaste, bis Sie den Assistenten beenden, und führen Sie commit aus, um die Änderungen zu speichern.

Protokollieren

Zugriffsprotokolle

In den Access-Protokollen wird der Datenverkehr, der an den Upstreamproxy weitergeleitet wurde, als DEFAULT_PARENT angezeigt, gefolgt vom Namen des Upstreamproxys. Hier ein Beispiel:

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

Proxy-Protokolle

Aus den Proxyprotokollen können Sie den Diagnosestatus der Upstreamproxys überprüfen.

Tipp: Sie können nach Peer filtern, um die Protokolle des Upstreamproxys zu überprüfen.

Hier einige Beispiele: Da wir die Neuverbindungsversuche in Schritt 3 bis zweimal konfiguriert haben, wird nach zwei Fehlern beim Herstellen einer Verbindung mit dem Upstreamproxy der Upstreamproxy als 'dad' deklariert, und SWA entfernt diesen Upstreamproxy aus der Liste, bis der Proxyprozess neu gestartet wird.

```
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
```

Anmerkung: Wenn der Upstreamproxy nicht auf TCP-SYN-Anfragen antwortet, keinen HTTP-Antwortcode zurückgibt oder eine HTTP 504 (Gateway-Zeitüberschreitung)-Antwort zurückgibt, hält der SWA den Upstreamproxy für nicht verfügbar und ändert seinen Status von fehlerfrei in fehlerfrei.

Tipp: Der SWA betrachtet einen Upstream-Proxy als fehlerfrei, wenn er einen VIA-Header zurückgibt.

Zugehörige Informationen

- Bedienungsanleitung für AsyncOS 15.0 für Cisco Secure Web Appliance
- Benutzerdefinierte URL-Kategorien in einer sicheren Web-Appliance konfigurieren - Cisco
- Wie kann Office 365-Datenverkehr auf der Cisco Web Security Appliance (WSA) von der Authentifizierung und Entschlüsselung ausgenommen werden - Cisco
- Best Practices für sichere Web-Appliances - Cisco
- Blockieren von Datenverkehr in einer sicheren Web-Appliance
- Upload-Verkehr in sicherer Web-Appliance blockieren
- Download ausführbarer Dateien in SWA blockieren
- Umgehen des Datenverkehrs von Microsoft Updates in einer sicheren Web-Appliance
- Umgehung der Authentifizierung in einer sicheren Web-Appliance - Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.