So konfigurieren Sie zusätzliche Passthrough-Einstellungen für die WebEx Anwendung

Einleitung

In diesem Dokument wird beschrieben, wie die Richtlinien zur Umgehung der Secure Web Appliance (SWA/WSA) konfiguriert werden, um unter besonderen Bereitstellungsbedingungen die ordnungsgemäße Funktion der Cisco WebEx Anwendung sicherzustellen.

Voraussetzungen

Anforderungen

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

- Async OS für Secure Web Appliance 14.x oder höher.
- Administratorzugriff auf die grafische Benutzeroberfläche (GUI) der sicheren Web-Appliance.
- Administratorzugriff auf die Secure Web Appliance Command Line Interface (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.

Problem

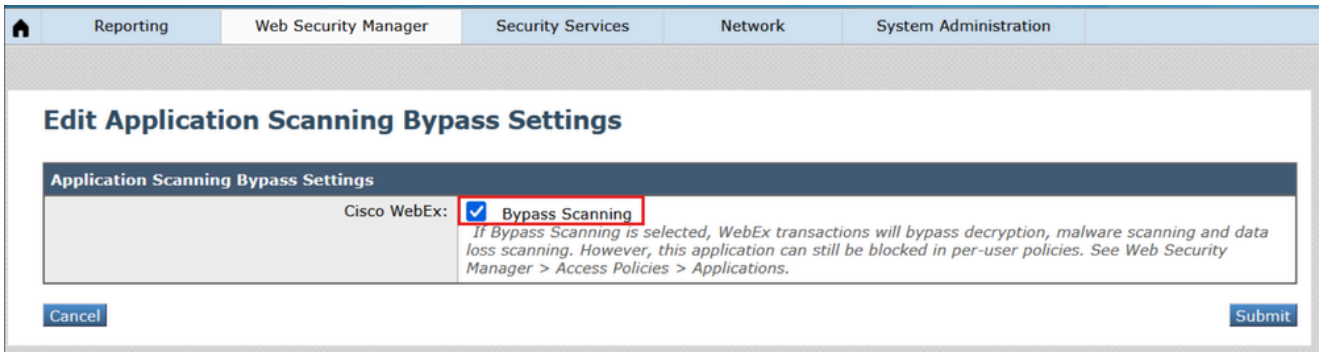
Basierend auf der öffentlichen WebEx-Dokumentation für die Netzwerkanforderungen für WebEx Services muss der Proxyserver so konfiguriert werden, dass der WebEx-Signalisierungsverkehr auf die im Dokument aufgeführten Domänen/URLs zugreifen kann. Die Secure Web Appliance erfüllt die Anforderungen für die meisten Umgebungen, indem sie das Kontrollkästchen WebEx Application Bypass in den Umgehungseinstellungen aktiviert. Unter Umständen sind jedoch zusätzliche Konfigurationen für die Secure Web Appliance erforderlich, um eine Unterbrechung des Dienstes in der WebEx Anwendung zu vermeiden. Die nächsten Schritte werden für solche Fallszenarien empfohlen:

Umgehung des WebEx-Anwendungs-Scanning

Die Funktion Cisco WebEx: Bypass Scanning ist der erste Schritt, damit Datenverkehr aus der WebEx Anwendung ungefiltert durch die sichere Web-Appliance geleitet wird. Die Funktion sollte in allen Umgebungen und Bereitstellungsszenarien aktiviert werden, in denen für Benutzer der WebEx Desktop- oder mobilen Anwendungen der Web-Datenverkehr über die sichere Web-Appliance geleitet wird.

Schritte zum Aktivieren der WebEx-Anwendungs-Scanumgehung:

1. Navigieren Sie in der WSA-GUI zu Web Security Manager > Bypass Settings > Edit Application Bypass Settings.
2. Aktivieren Sie das Kontrollkästchen für "Cisco WebEx".



1_wsa_bypass_scanning_settings

3. Änderungen übermitteln und bestätigen

Wenn diese Einstellung aktiviert ist, wird kein transparenter Datenverkehr umgangen, wie dies nach dem Hinzufügen der FQDNs zur Umgehungsliste der sicheren Webappliance zu erwarten wäre. Vielmehr wird der WebEx Anwendungsdatenverkehr weiterhin über die sichere Web-Appliance geleitet, er wird jedoch bei der Entschlüsselung mit dem Entscheidungskennzeichen "PASSTHRU_AVC" weitergeleitet. Im Folgenden finden Sie ein Beispiel, wie dies in den Zugriffsprotokollen angezeigt wird:

```
1761695285.658 55398 192.168.100.100 TCP_MISS/200 4046848 TCP_CONNECT 3.161.225.70:443 - DIRECT/binarie
```

Überlegungen für spezielle Umgebungen

In einigen Szenarien sind zusätzliche Konfigurationen erforderlich, damit die WebEx App funktioniert, wenn der Datenverkehr über die sichere Web-Appliance geleitet wird.

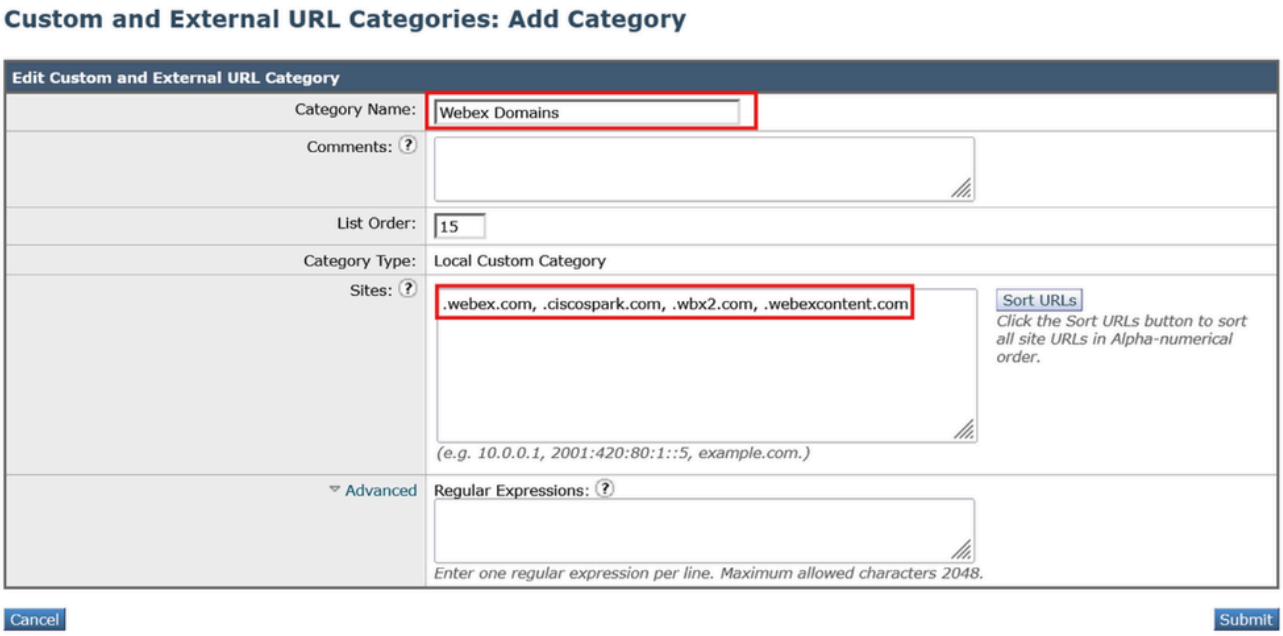
Szenario 1: WebEx-Domänen müssen von der Authentifizierung ausgenommen werden

Dies wird besonders in Umgebungen deutlich, in denen IP-Surrogate im Identifikationsprofil nicht aktiviert sind und eine transparente Umleitung verwendet wird. Basierend auf der vorhandenen Dokumentation ist die WebEx App in der Lage, NTLMSSP-Authentifizierung auf domänenverbundenen Workstations durchzuführen, auf denen der Proxy explizit definiert ist. Andernfalls empfiehlt es sich, eine benutzerdefinierte Kategorie für die WebEx Domänen zu

konfigurieren und sie von der Authentifizierung auszunehmen.
Schritte, um WebEx-Domänen von der Authentifizierung auszunehmen:

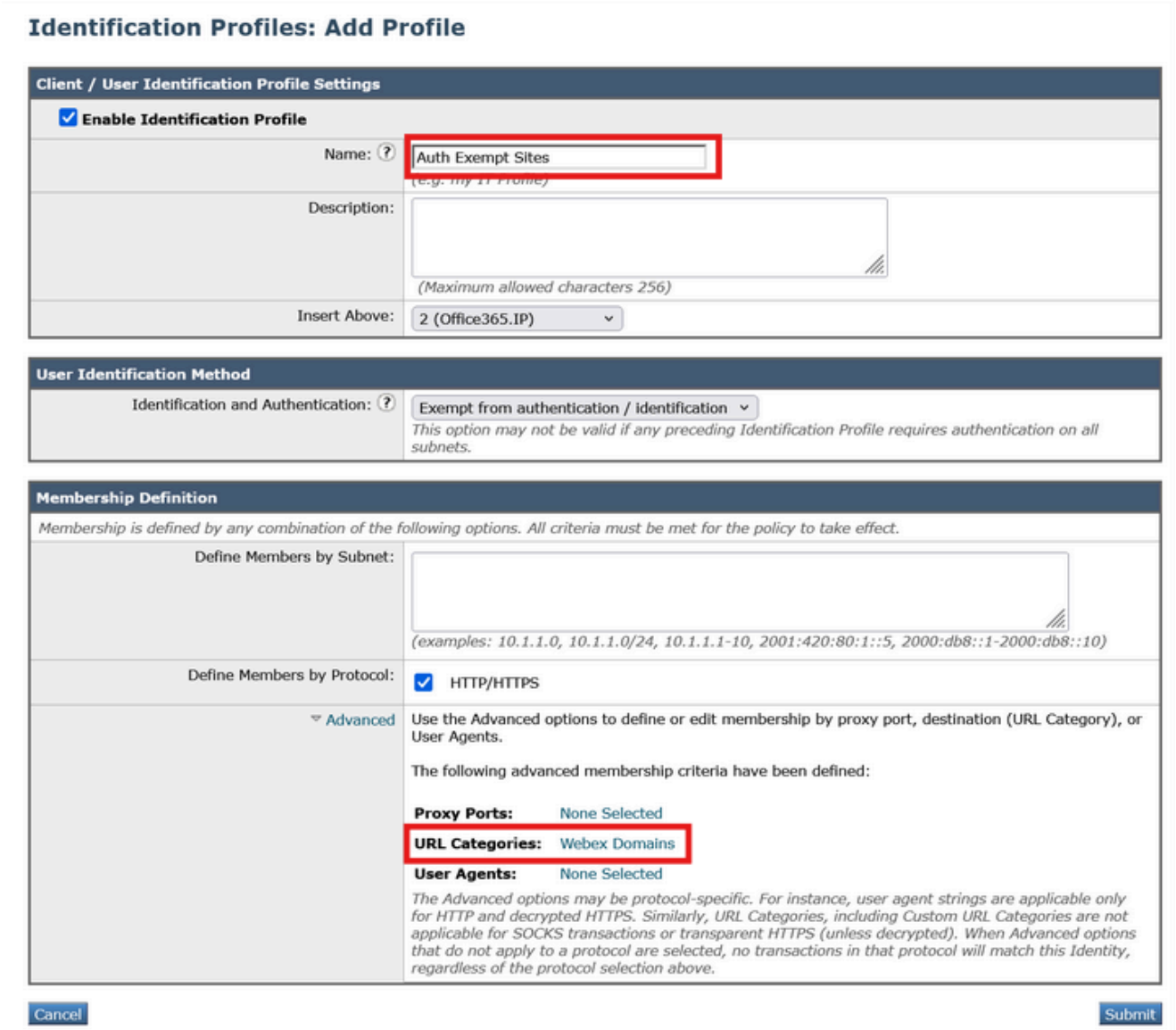
1. Navigieren Sie in der WSA-GUI zu Websicherheits-Manager > Benutzerdefinierte und externe URL-Kategorien > Kategorie hinzufügen.
2. Geben Sie der neuen Kategorie einen Namen, und platzieren Sie die folgenden Domänen im Abschnitt Sites:

```
.webex.com, .ciscospark.com, .wbx2.com, .webexcontent.com
```



2_wsa_custom_url_category

3. Klicken Sie auf Senden. Navigieren Sie anschließend zu Web Security Manager > Identification Profiles > Add Identification Profile.
4. Geben Sie dem neuen Profil einen Namen, und wählen Sie im Abschnitt Erweitert für URL-Kategorien die neue Kategorie aus, die in Schritt #2 erstellt wurde.



3_wsa_id_profil

5. Stellen Sie sicher, dass die Identifikation und Authentifizierung im neuen Profil auf Von Authentifizierung/Identifizierung ausnehmen eingestellt ist.
6. Änderungen einsenden und bestätigen.

Szenario 2: WebEx Content-Domänen werden nicht vollständig für die Umgehung der Entschlüsselung berücksichtigt.

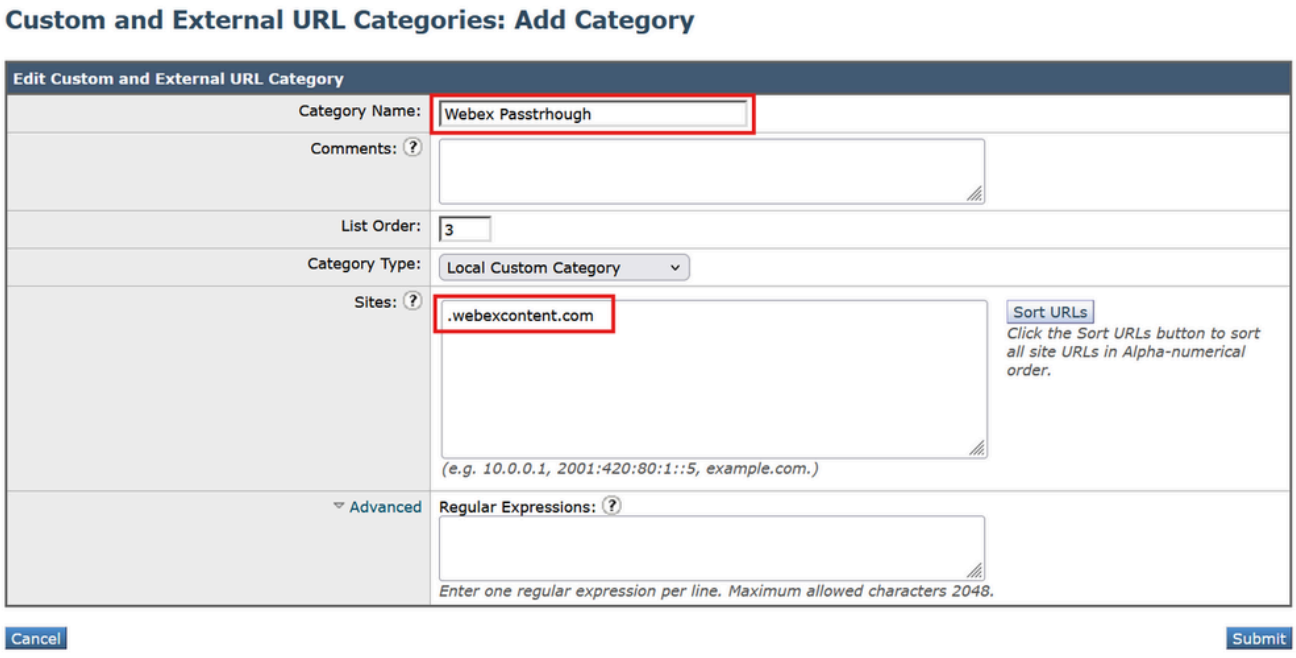
Es gibt einige Subdomänen für webexcontent.com, die bei aktivierter WebEx-Anwendungsscanumgehung die Entschlüsselung nicht automatisch weiterleiten. Der Inhalt dieser Domänen wird von der WebEx-App als vertrauenswürdig angesehen, wenn er entschlüsselt wird, solange das Entschlüsselungszertifikat der sicheren Web-Appliance bereits dem vertrauenswürdigen Stammzertifikatsspeicher des Geräts hinzugefügt oder anderweitig von einer internen Zertifizierungsstelle signiert wird, die bereits von das Gerät, auf dem die WebEx App ausgeführt wird. Wenn das Gerät jedoch nicht verwaltet wird und das Entschlüsselungszertifikat der Secure Web Appliance nicht vertrauenswürdig ist, sollten diese Domänen so konfiguriert werden, dass bei der Entschlüsselung ein Passthrough durchgeführt wird.

Wenn eine transparente Umleitungsbereitstellung vorhanden ist und für die Umleitungsgruppen mehr als ein SWA zusammen mit Client-IP-Spoofing verwendet wird, kann der Datenverkehr entsprechend der Ziel-IP-Adresse für die Umleitung an die sichere Web-Appliance konfiguriert werden. Entsprechend wird der Rückverkehr von den Webservern für die Umleitung über die sichere Web-Appliance basierend auf der Quelladresse konfiguriert. Wenn die Secure Web Appliance so konfiguriert ist, dass sie Verbindungen zum Webserver über die IP herstellt, die sie mithilfe der DNS-Suche auflöst, kann der zurückgegebene Datenverkehr versehentlich an eine andere Secure Web Appliance umgeleitet und anschließend gelöscht werden. Dieses Problem betrifft nicht nur WebEx, sondern auch andere Video-Streaming-Anwendungen, da auf den Webservern rotierende IP-Adressen verwendet werden.

Schritte zur Konfiguration des Passthrough bei der Entschlüsselung für alle WebEx Domänen:

1. Stellen Sie sicher, dass WebEx Application Scanning Bypass wie oben beschrieben aktiviert ist.
2. Navigieren Sie in der WSA-GUI zu Websicherheits-Manager > Benutzerdefinierte und externe URL-Kategorien > Kategorie hinzufügen.
3. Geben Sie der neuen Kategorie einen Namen, und platzieren Sie die nächste Domäne im Abschnitt Sites:

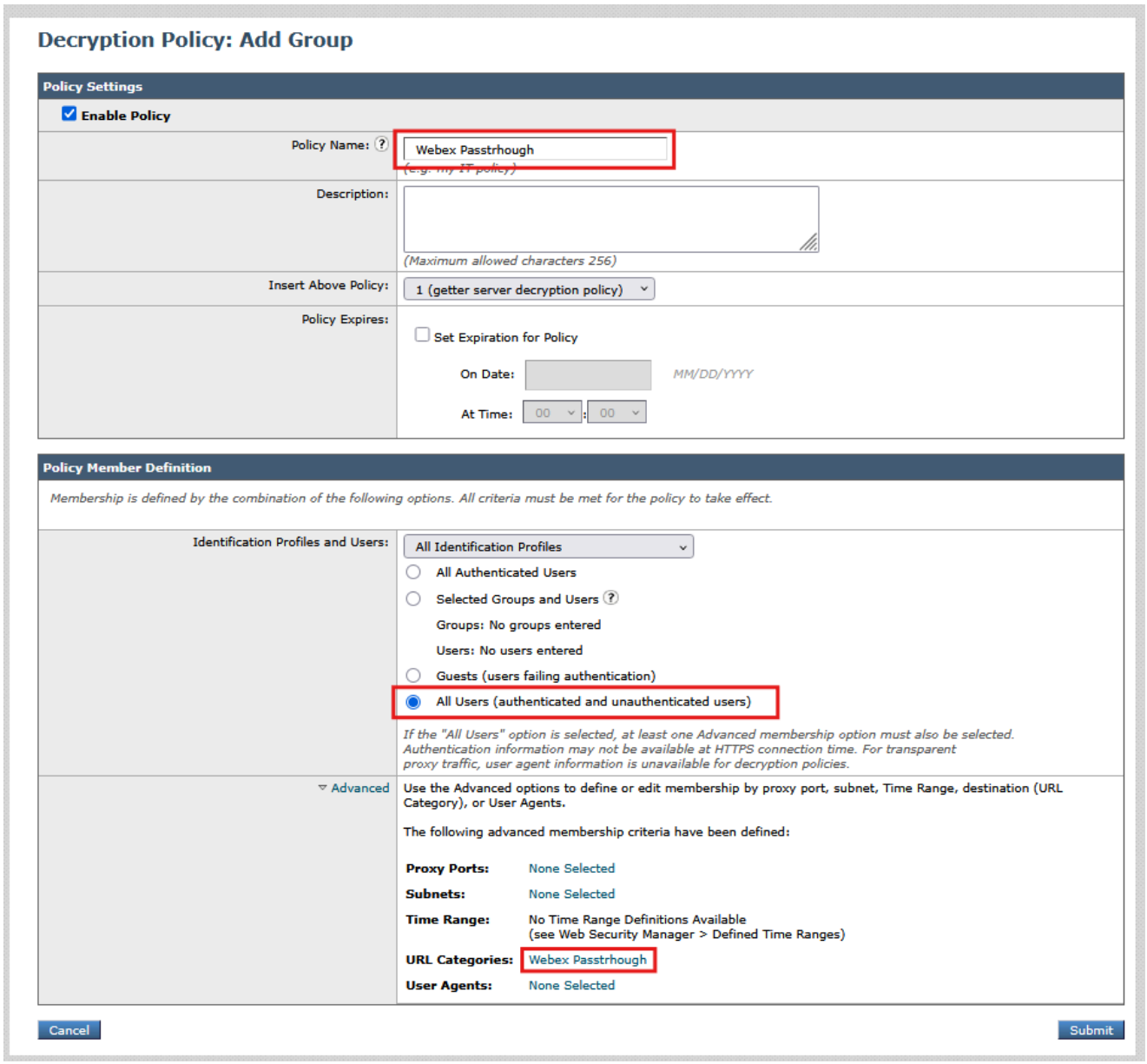
```
.webexcontent.com
```



4_wsa_url_Kategorie

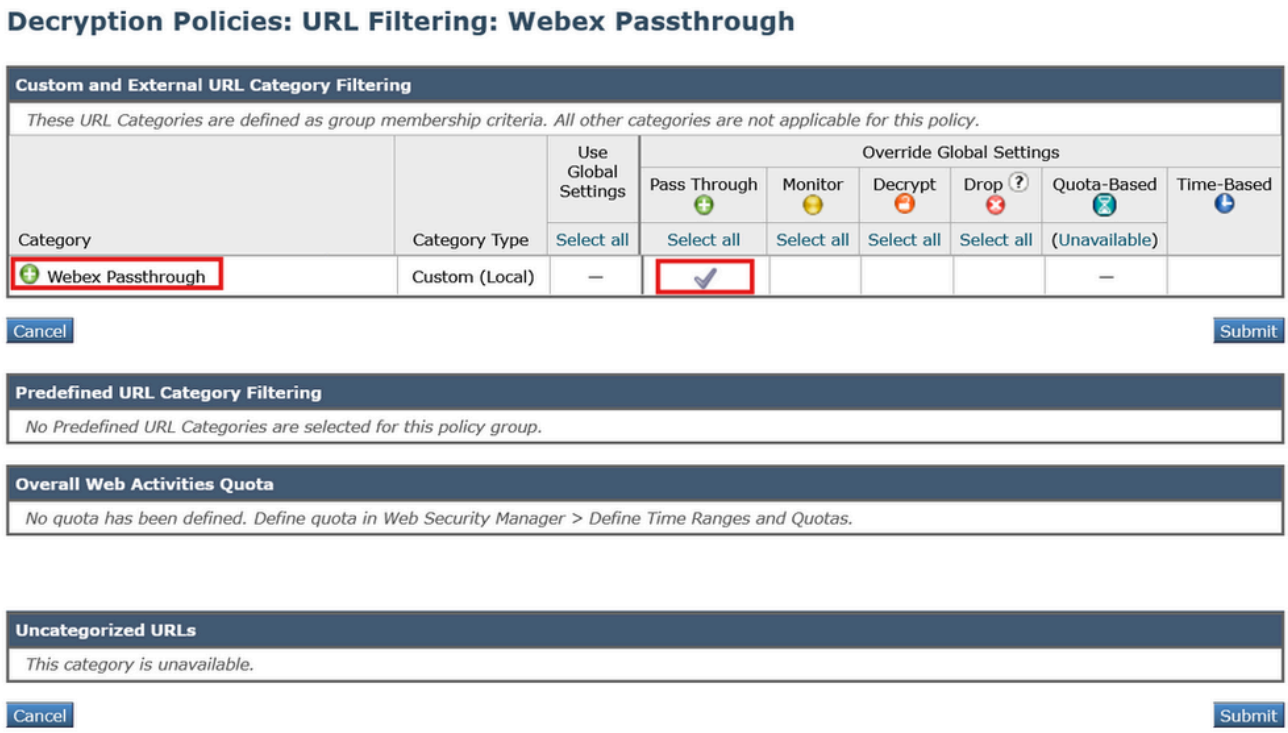
4. Klicken Sie auf Senden. Navigieren Sie jetzt zu Websicherheits-Manager > Entschlüsselungsrichtlinien > Richtlinie hinzufügen.
5. Geben Sie der neuen Richtlinie einen Namen, setzen Sie Identifikationsprofile und Benutzer auf "Alle Benutzer", und wählen Sie im Abschnitt "Erweitert" für URL-Kategorien die neue

Kategorie aus, die in Schritt #3 erstellt wurde.



5_wsa_decryption_policy

6. Klicken Sie auf Senden. Dann klicke auf den Abschnitt URL-Filterung und setze die benutzerdefinierte Kategorie, die in Schritt #3 erstellt wurde, auf "Pass Through".



6_wsa_url_filterung

7. Senden und bestätigen Sie die Änderungen.

Wenn mehrere sichere Web-Appliances für die transparente Umleitung bereitgestellt werden und Client-IP-Spoofing aktiviert ist, gibt es zwei Lösungen:

1. Legen Sie den Lastenausgleich für ausgehende und zurückgehende WCCP-Dienste basierend auf der Client- und nicht der Serveradresse fest.
2. Legen Sie in der WSA-CLI advanced proxyconfig > DNS > "Find web server by" fest, um die vom Client bereitgestellte IP-Adresse bei Verbindungen zum Webserver immer zu verwenden (Optionen 2 und 3). Weitere Informationen zu dieser Einstellung finden Sie im DNS-Abschnitt des Leitfadens für die Verwendung sicherer Web-Appliances.

Verifizierung

Wenn die Passthrough-Einstellungen abgeschlossen sind, wird der WebEx Datenverkehr gemäß den folgenden Richtlinien in den Zugriffsprotokollen als "Passthrough" verarbeitet:

```
1763752739.797 457 192.168.100.100 TCP_MISS/200 6939 TCP_CONNECT 135.84.171.165:443 - DIRECT/da3-wxt08-
1763752853.942 109739 192.168.100.100 TCP_MISS/200 7709 TCP_CONNECT 170.72.245.220:443 - DIRECT/avatar-
1763752862.299 109943 192.168.100.100 TCP_MISS/200 8757 TCP_CONNECT 18.225.2.59:443 - DIRECT/highlights
1763752870.293 109949 192.168.100.100 TCP_MISS/200 8392 TCP_CONNECT 170.72.245.190:443 - DIRECT/retenti
```

Überprüfen und überwachen Sie die WebEx-Anwendung. Wenn eine Verzögerung oder eine Serviceunterbrechung gemeldet wird, überprüfen Sie die Zugriffsprotokolle noch einmal, und stellen Sie sicher, dass der gesamte WebEx-seitige Datenverkehr korrekt verarbeitet wurde.

Zugehörige Informationen

- Netzwerkanforderungen für WebEx Services
- Best Practices für sichere Web-Appliances

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.