Aanvullende instellingen voor wachtwoorden configureren voor Web Security Appliance voor de WebEx-toepassing

Inleiding

In dit document wordt beschreven hoe u het beleid voor het omzeilen van de Secure Web Appliance (SWA/WSA) configureert om ervoor te zorgen dat de Cisco Webex-toepassing in speciale implementatieomstandigheden naar behoren functioneert.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Async OS for Secure Web Appliance 14.x of hoger.
- Gebruikerstoegang tot de Secure Web Appliance Graphic User Interface (GUI) beheren.
- Gebruikerstoegang tot de Secure Web Appliance Command Line-interface (CLI) beheren.

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.

Probleem

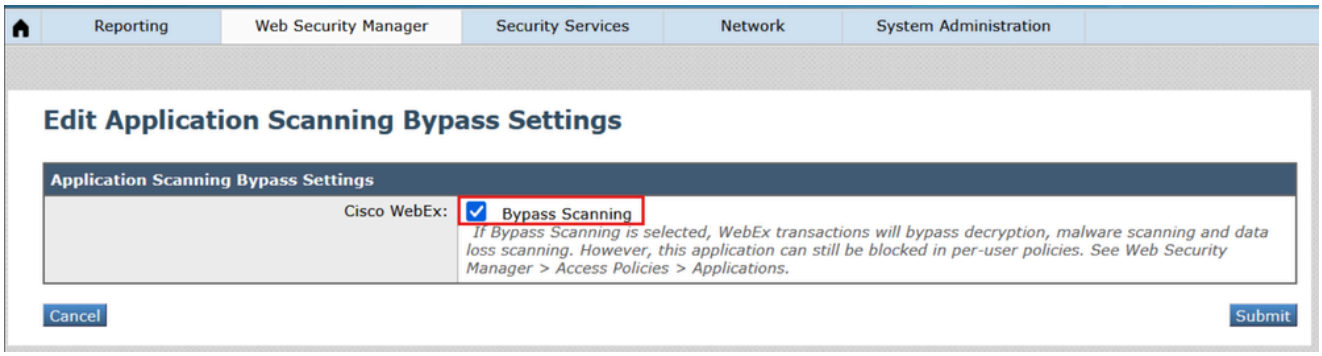
Op basis van de openbare Webex-documentatie voor netwerkvereisten voor Webex-services, moet de proxyserver worden geconfigureerd zodat Webex-signaleringsverkeer toegang heeft tot de domeinen/URL's die in het document worden vermeld. De Secure Web Appliance voldoet aan de vereisten voor de meeste omgevingen door het selectievakje Webex Application Bypass in te schakelen in de instellingen voor bypass, maar er kunnen enkele aanvullende configuraties vereist zijn op Secure Web Appliance om serviceonderbrekingen in de Webex-toepassing te voorkomen. De volgende stappen worden aanbevolen voor dergelijke casusscenario's:

Webex Application Scanning Bypass

De Cisco Webex: Bypass Scanning-functie is de eerste stap om het verkeer van de Webex-toepassing ongefilterd door de Secure Web Appliance te laten gaan. Het moet worden ingeschakeld in alle omgevingen en implementatiescenario's waar gebruikers van de Webex-desktop of mobiele toepassingen webverkeer hebben dat is geproxydeerd via de Secure Web Appliance.

Stappen voor het inschakelen van Webex Application Scanning Bypass:

1. Blader in de WSA GUI naar Web Security Manager > Instellingen omzeilen > Instellingen voor omzeilen van toepassingen bewerken.
2. Schakel het selectievakje in voor "Cisco WebEx".



1_WSA_BYPASS_SCANNING_INSTELLINGEN

3. Wijzigingen verzenden en vastleggen

Wanneer deze instelling is ingeschakeld, wordt het transparante verkeer niet omzeild, zoals zou worden verwacht zodra de FQDN's zijn toegevoegd aan de bypass-lijst op de Secure Web Appliance. In plaats daarvan wordt het Webex-applicatieverkeer nog steeds geproxydeerd via de Secure Web Appliance, maar het zal worden doorgegeven bij decodering met de beslissingstag "PASSTHRU_AVC". Hieronder ziet u een voorbeeld van hoe dit kan worden weergegeven in de toegangslogboeken:

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

Overwegingen voor unieke omgevingen

Er zijn een paar scenario's waarbij extra configuraties nodig zijn om de Webex-app te laten werken wanneer het verkeer wordt benaderd via de Secure Web Appliance.

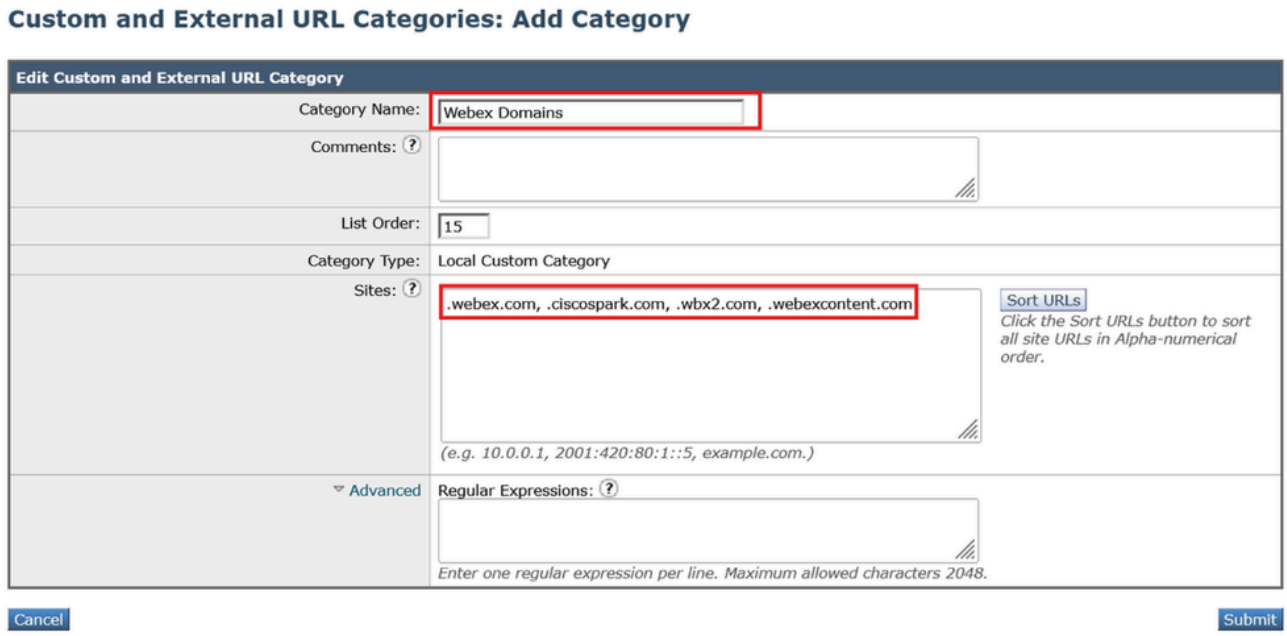
Scenario 1: Webex-domeinen moeten worden vrijgesteld van authenticatie

Dit is vooral duidelijk in omgevingen waar IP-surrogaten niet zijn ingeschakeld in het identificatieprofiel en transparante omleiding wordt gebruikt. Op basis van de bestaande documentatie kan de Webex-app NTLMSSP-verificatie uitvoeren op werkstations met een domeinverbinding waar de proxy expliciet is gedefinieerd. Anders is het een best practice om een aangepaste categorie voor de Webex-domeinen te configureren en deze vrij te stellen van authenticatie.

Stappen om Webex-domeinen vrij te stellen van authenticatie:

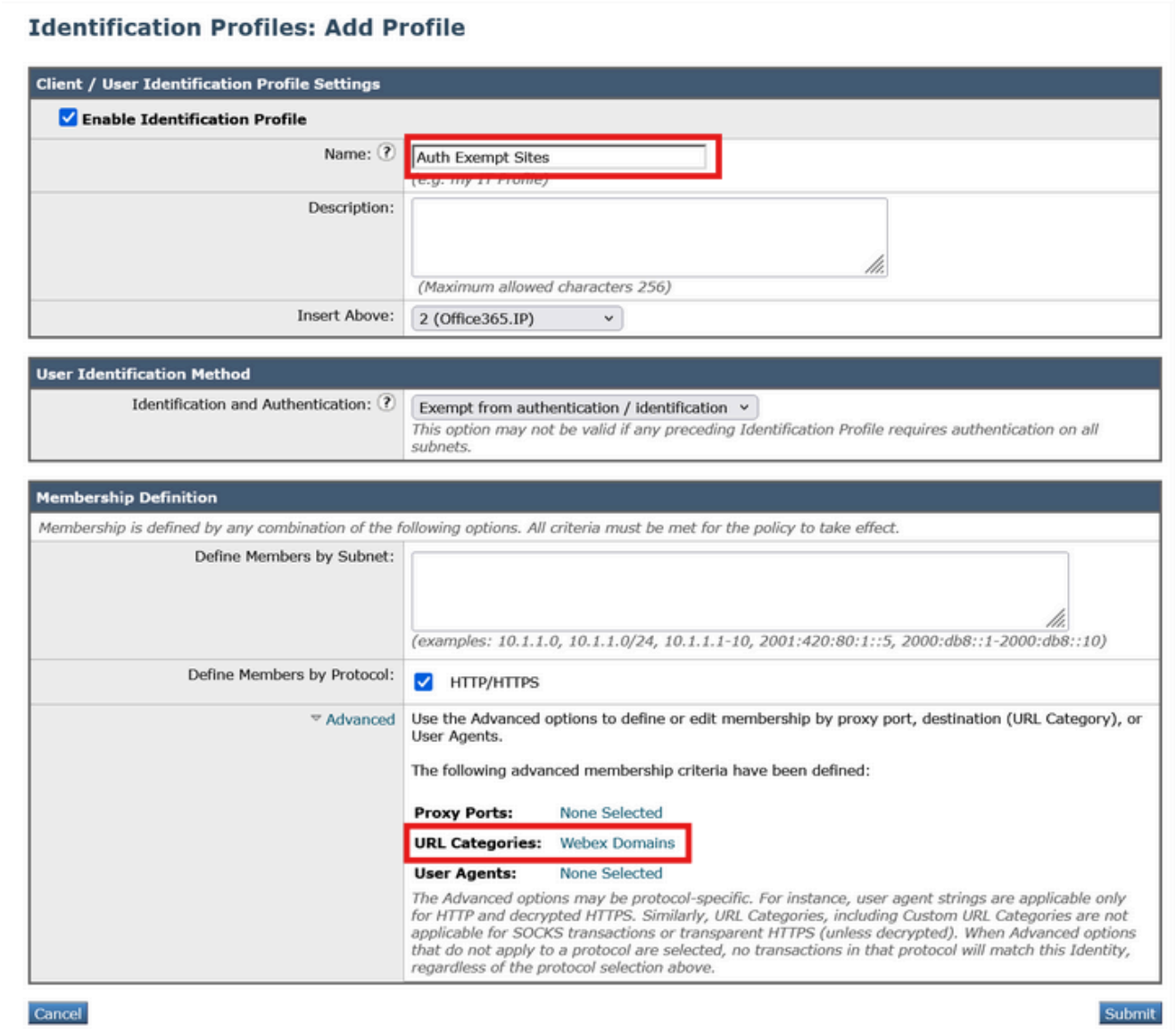
1. Navigeer in de WSA GUI naar Web Security Manager > Aangepaste en externe URL-categorieën > Categorie toevoegen.
2. Geef de nieuwe categorie een naam en plaats de volgende domeinen in de sectie Sites:

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



2_wsa_custom_url_category

3. Klik op Indienen. Navigeer vervolgens naar Web Security Manager > Identificatieprofielen > Identificatieprofiel toevoegen
4. Geef het nieuwe profiel een naam en selecteer in het gedeelte Geavanceerd voor URL-categorieën de nieuwe categorie die is gemaakt in stap # 2



3_WSA_ID_Profile

5. Ervoor zorgen dat de identificatie en verificatie in het nieuwe profiel is ingesteld op Vrijstellen van verificatie/identificatie
6. Verzenden en wijzigingen vastleggen.

Scenario 2: Webex Content-domeinen worden niet volledig gehonoreerd voor decodering bypass.

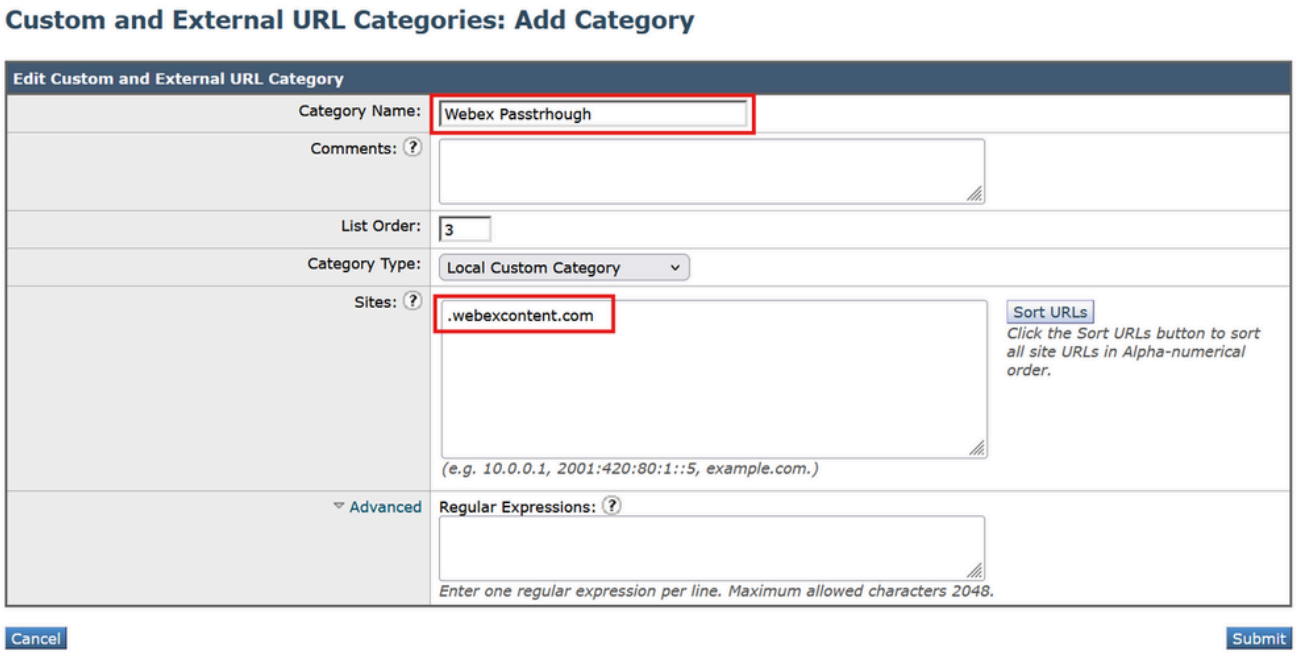
Er zijn een paar subdomeinen gerelateerd aan webexcontent.com die niet automatisch worden gedecodeerd wanneer Webex Application Scanning Bypass is ingeschakeld. De inhoud van deze domeinen wordt vertrouwd door de Webex-app wanneer deze wordt gedecodeerd, zolang het decoderingscertificaat van de Secure Web Appliance al is toegevoegd aan de vertrouwde rootcertificatenopslag van het apparaat of anderszins is ondertekend door een interne certificeringsinstantie die al wordt vertrouwd door het apparaat waarop de Webex-app wordt uitgevoerd. Als het apparaat echter niet wordt beheerd en het decoderingscertificaat van de Secure Web Appliance niet wordt vertrouwd, moeten deze domeinen worden geconfigureerd om door te gaan bij decodering.

Wanneer een transparante omleidingsimplementatie is geïmplementeerd en er meer dan één SWA langs client-IP-spoofing wordt gebruikt voor omleidingsgroepen, kan verkeer worden geconfigureerd om naar de Secure Web Appliance te leiden op basis van het IP-adres van de bestemming, en op dezelfde manier wordt het retourverkeer van de webservers geconfigureerd om terug te leiden via de Secure Web Appliance op basis van het bronadres. Wanneer de Secure Web Appliance is geconfigureerd om verbindingen met de webserver te maken met behulp van het IP-adres dat wordt opgelost met behulp van DNS-opzoeken, kan het retourverkeer per ongeluk worden omgeleid naar een andere Secure Web Appliance en vervolgens worden verwijderd. Dit probleem treft niet alleen Webex, maar ook andere videostreamingtoepassingen, vanwege het gebruik van roterende IP-adressen op de webservers.

Stappen voor het configureren van passthrough op decryptie voor alle Webex-domeinen:

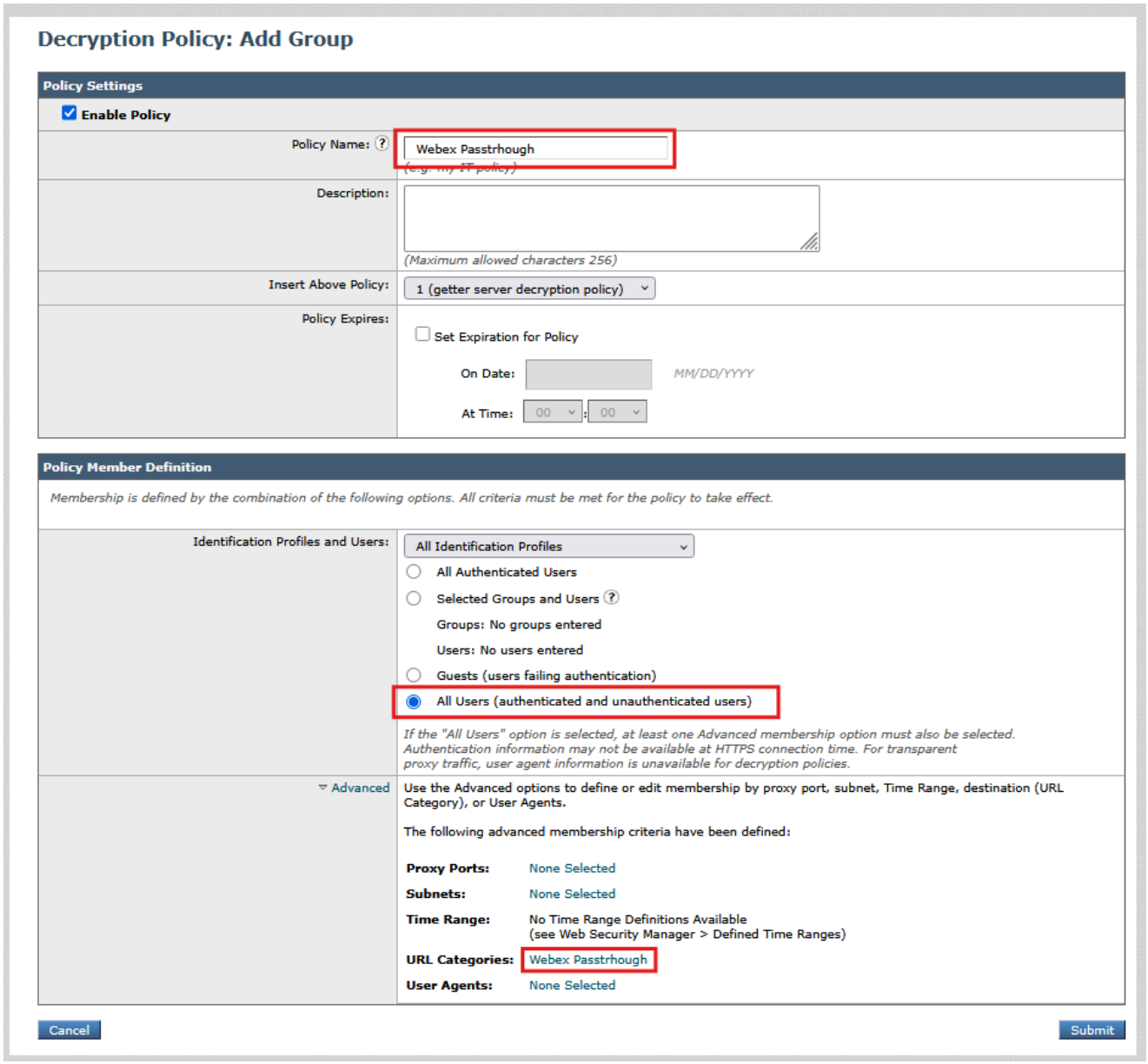
1. Zorg ervoor dat Webex Application Scanning Bypass is ingeschakeld volgens bovenstaande instructies.
2. Navigeer in de WSA GUI naar Web Security Manager > Aangepaste en externe URL-categorieën > Categorie toevoegen.
3. Geef de nieuwe categorie een naam en plaats het volgende domein in de sectie Sites:

```
.webexcontent.com
```



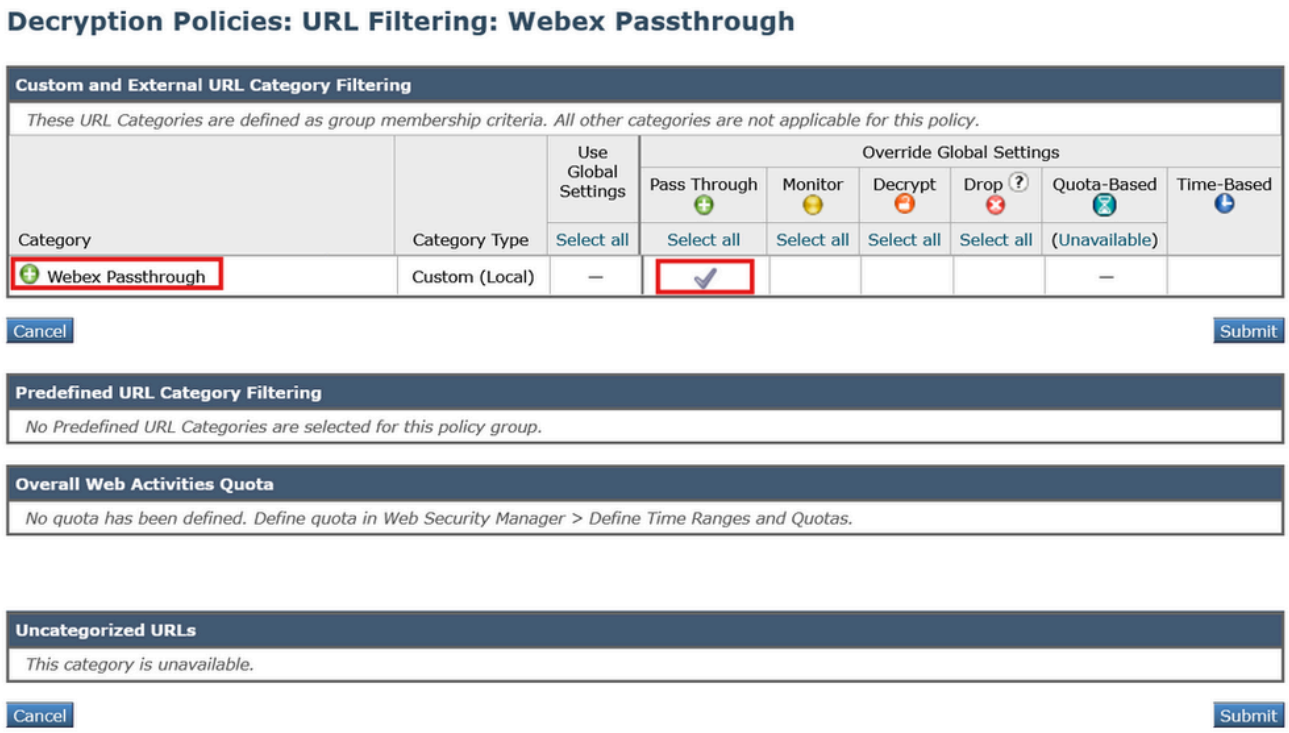
4_wsa_url_category

4. Klik op Indienen. Navigeer nu naar Web Security Manager > Decoderingsbeleid > Beleid toevoegen
5. Geef het nieuwe beleid een naam, stel Identificatieprofielen en gebruikers in op "Alle gebruikers", en selecteer in het gedeelte Geavanceerd voor URL-categorieën de nieuwe categorie die is gemaakt in stap #3



5_WSA_Decryption_Policy

6. Klik op Indienen. Klik vervolgens op de sectie URL-filtering en stel de aangepaste categorie die is gemaakt in stap # 3 in op "Doorgeven".



6_WSA_URL_FILTERING

7. Verzenden en vastleggen van de wijzigingen.

Als meerdere Secure Web Appliances worden geïmplementeerd voor transparante omleiding en client IP-spoofing is ingeschakeld, zijn er twee oplossingen voor dit:

1. Stel de uitgaande en geretourneerde WCCP-services in op de taakverdeling op basis van het clientadres in plaats van het serveradres.
2. Stel in de WSA CLI advanced proxyconfig > DNS > "Find web server by" in om altijd het door de client geleverde IP-adres te gebruiken bij verbindingen met de webserver (opties 2 en 3). Meer informatie over deze instelling is te vinden in de DNS-sectie van de handleiding Gebruik veilige webapparatuur voor best practices.

Verificatie

Wanneer de passthrough-instellingen zijn voltooid, wordt Webex-verkeer verwerkt in de toegangslogboeken als Pass Through volgens het beleid:

```
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
```

Controleer en bewaak de webEx-toepassing, als er vertraging of serviceonderbreking wordt gemeld, bekijk de toegangslogboeken nog een keer en valideer dat al het webEx-side-verkeer correct wordt verwerkt.

Gerelateerde informatie

- Netwerkvereisten voor Webex-services
- Best practices voor veilige webapparaten gebruiken

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.