URL-Filterung konfigurieren und überprüfen

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie die URL-Filterung auf Cisco IOS-XE®-Routern mithilfe der Cisco Catalyst Manager-GUI konfigurieren und überprüfen.

Voraussetzungen

Laden Sie ein kompatibles virtuelles UTD-Software-Image mit dem aktuellen Cisco IOS-XE-Code in vManage hoch. Anweisungen zur Installation des virtuellen UTD-Sicherheits-Images auf cEdge-Routern finden Sie im Abschnitt "Freigegebene Informationen".

Der Cisco Edge-Router muss sich im vManaged-Modus befinden, wobei die Vorlage bereits angefügt ist.

Anforderungen

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

- Cisco SD-WAN Overlay startet mit der Erstkonfiguration.
- Konfiguration der URL-Filterung in der Cisco Catalyst Manager-GUI.

Verwendete Komponenten

Dieses Dokument basiert auf den folgenden Software- und Hardwareversionen:

- Cisco Catalyst SD-WAN Manager Version 20.14.1
- Cisco Catalyst SD-WAN Controller Version 20.14.1
- Cisco Edge Router Version 17.14.1

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.

Konfigurieren

Netzwerkdiagramm

Konfigurieren von Komponenten für eine URL-Filterrichtlinie

In diesem Artikel wird erläutert, wie die URL-Filterung so konfiguriert wird, dass bestimmter Client-HTTPS-Datenverkehr basierend auf Kategorie, Reputation oder nach Domänenblock-/Zulassungslisten blockiert bzw. zugelassen wird. Dabei gelten folgende Beispielanforderungen:

- Diese HTTPS-Anfragen von Clients in den VPN-Webkategorien für Gäste blockieren:
  - Spiele
  - Glücksspiel
  - Hacking
  - Illegale Drogen

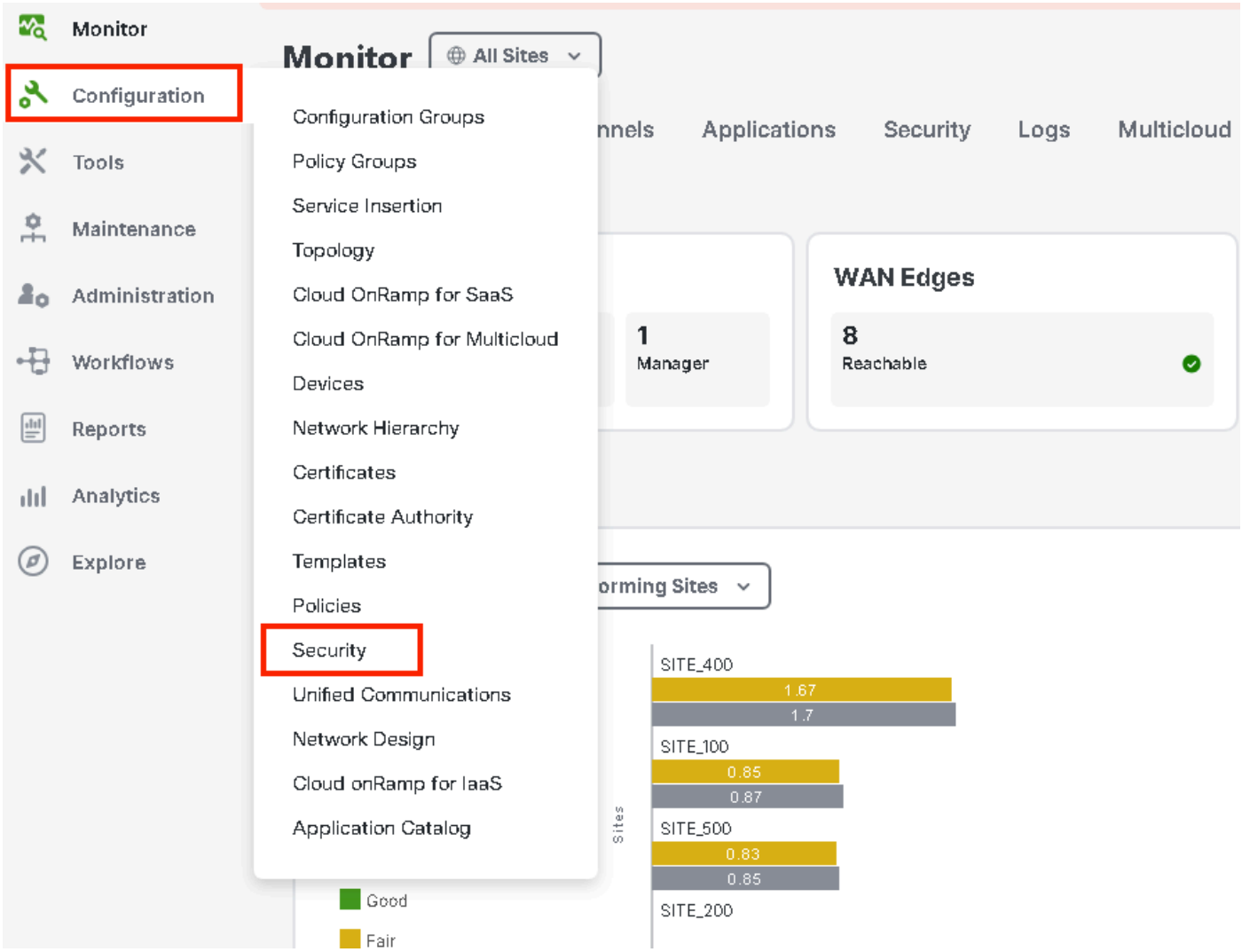
- Jede HTTPS-URL-Anfrage an Websites von Client auf Gast-VPN mit einer Web-Reputation kleiner/gleich 60 muss blockiert werden.

- HTTP(s)-Anfragen an Websites von Clients im Gast-VPN blockieren Facebook, Instagram und YouTube und ermöglichen gleichzeitig den Zugriff auf google.com und yahoo.com.

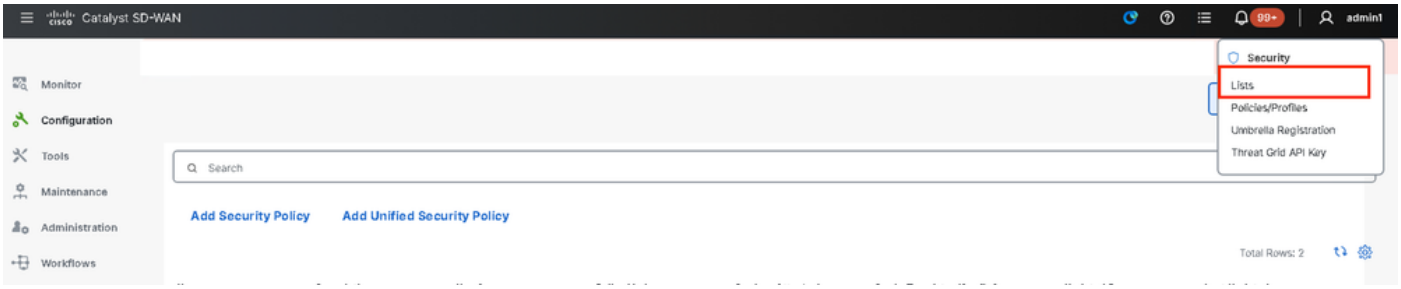
URL-Filterung konfigurieren:

Erstellen von URL-Interessenslisten

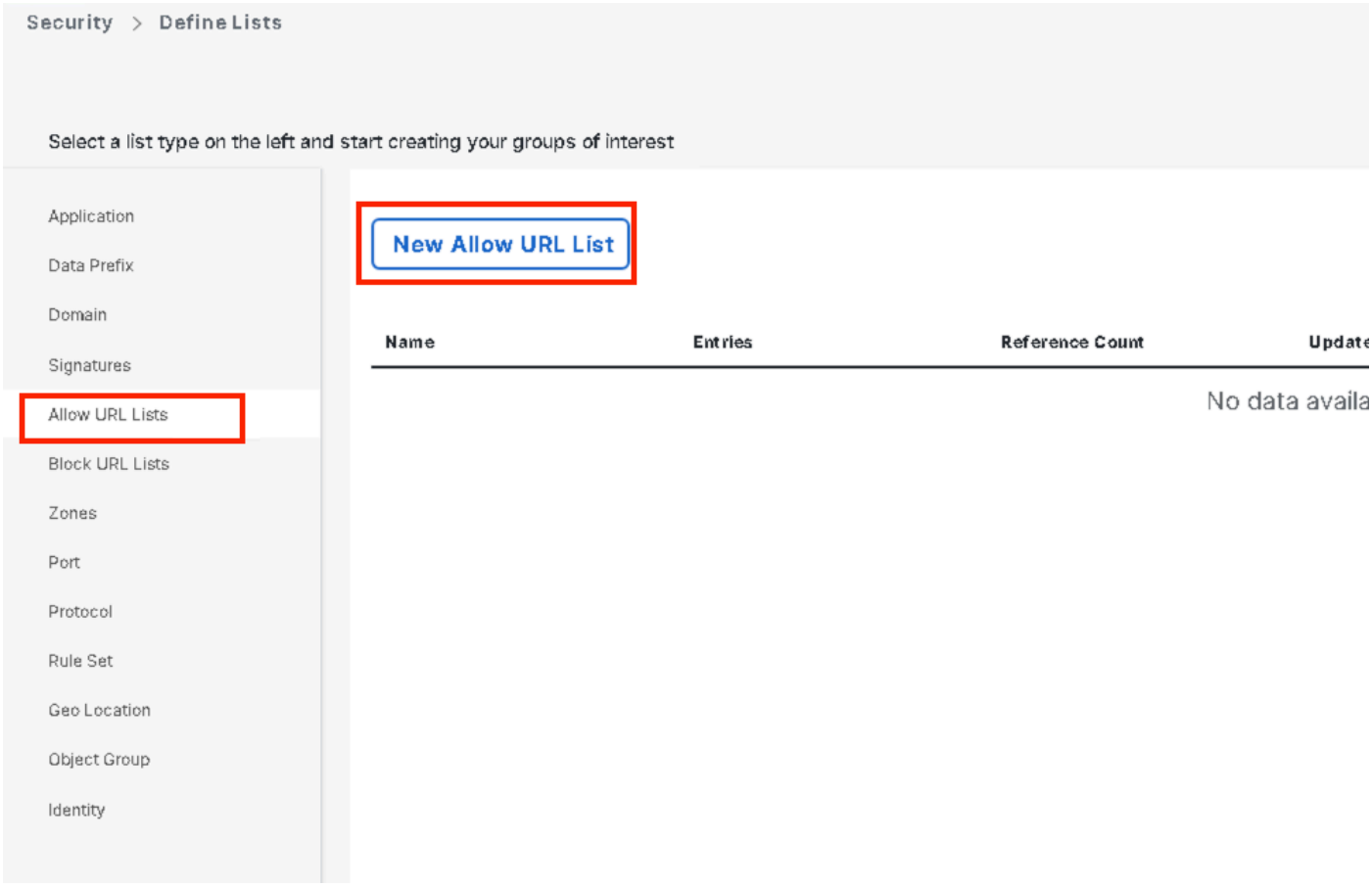
1. Navigieren Sie im Menü Cisco SD-WAN Manager im linken Bereich zur Registerkarte Configuration > Security (Konfiguration > Sicherheit).



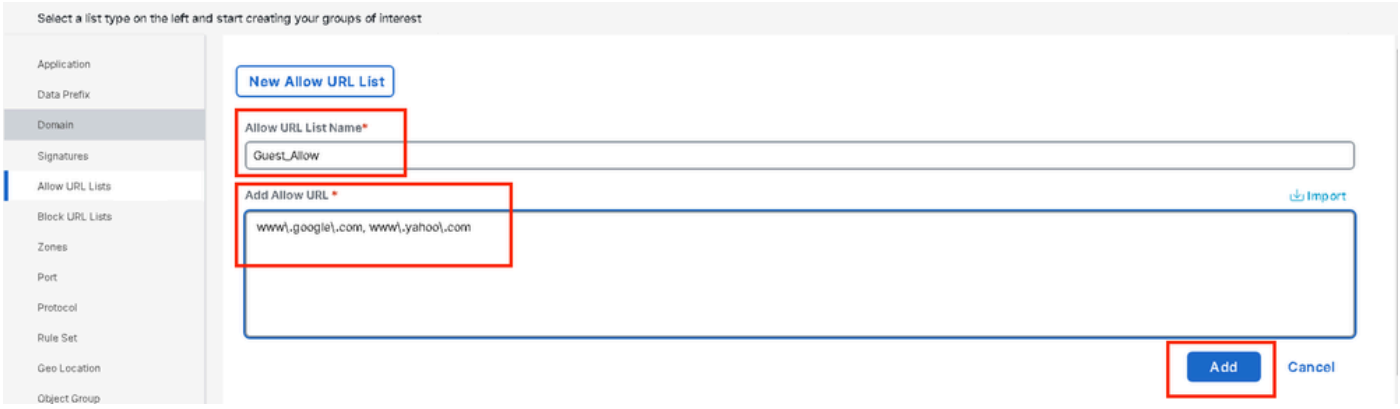
Um eine Liste mit zulässigen URLs oder eine Liste mit gesperrten URLs zu erstellen oder zu verwalten, wählen Sie Listen aus dem Dropdown-Menü Benutzerdefinierte Optionen oben rechts auf der Seite aus.

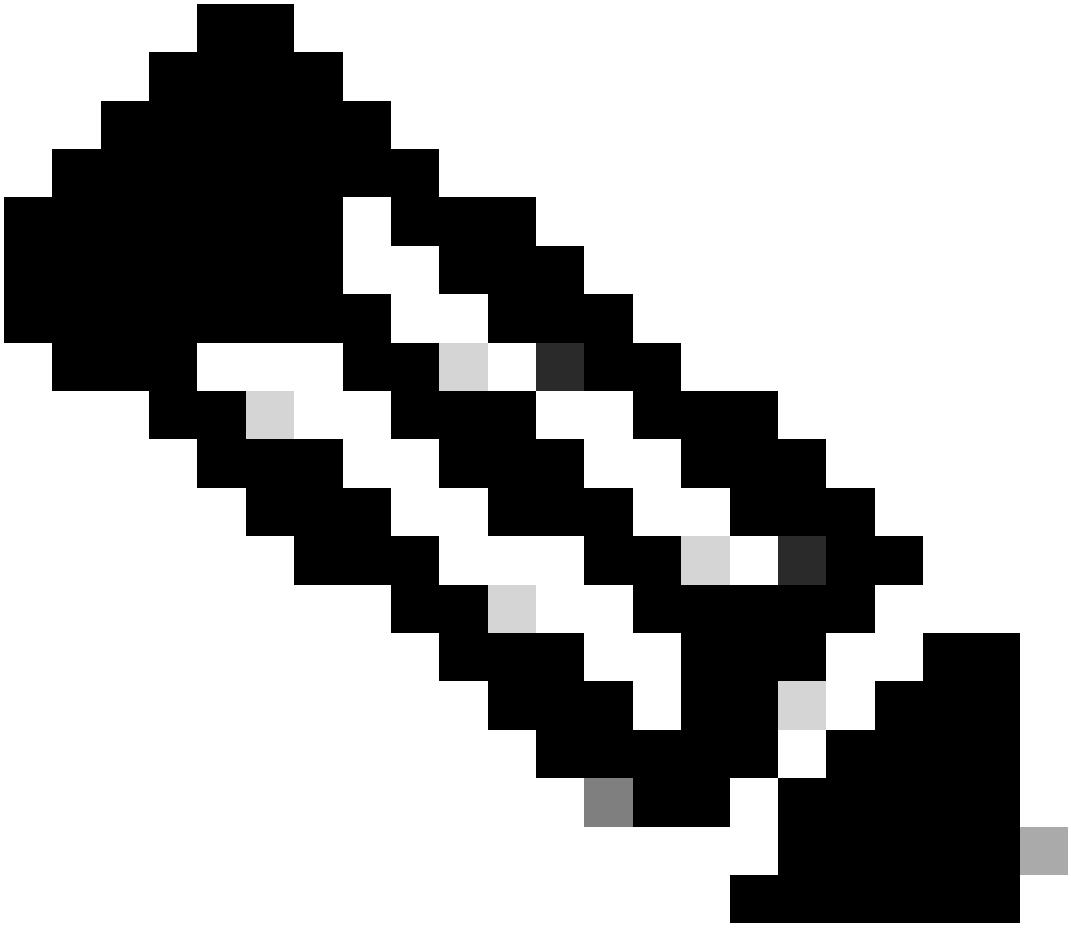


Klicken Sie im linken Bereich auf Allow URLs Lists (URL-Listen zulassen), und erstellen Sie New Allow URL List (Neue URL-Liste zulassen).



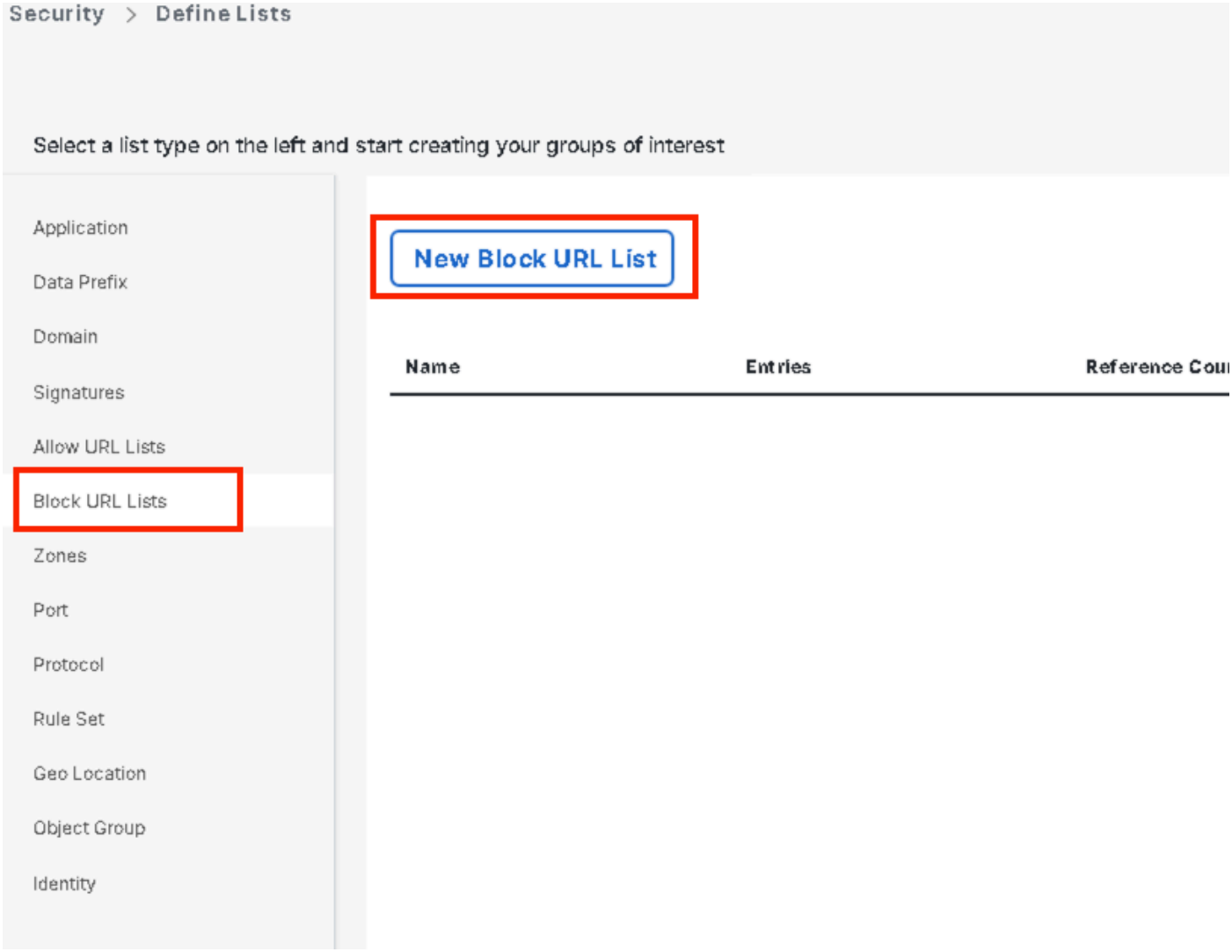
- Geben Sie im Feld Name der URL-Liste einen Listennamen mit bis zu 32 Zeichen ein (nur Buchstaben, Ziffern, Bindestriche und Unterstriche).
- Geben Sie im Feld URL die URLs ein, die in die Liste aufgenommen werden sollen, getrennt durch Kommas. Sie können auch die Schaltfläche Importieren verwenden, um Listen von einem zugänglichen Speicherort hinzuzufügen.
- Klicken Sie abschließend auf Hinzufügen.



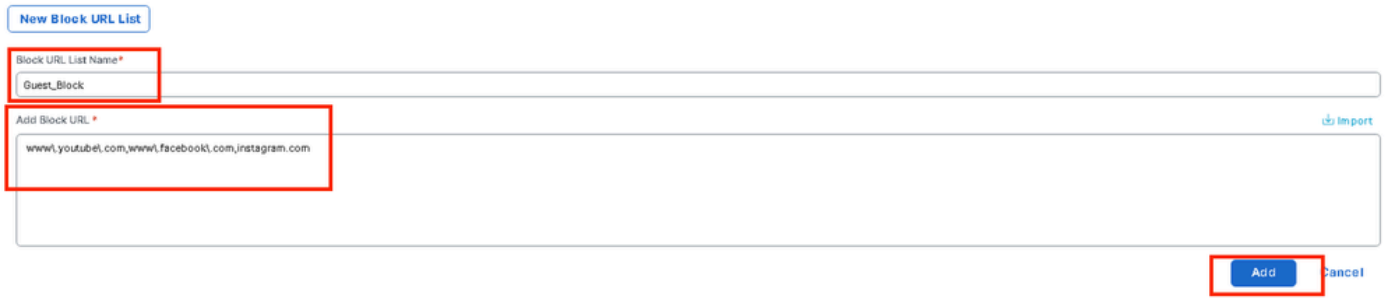


Hinweis: Sie können ein reguläres Muster für den Domänennamen in Listen für Zulassen und Sperren verwenden.

Klicken Sie im linken Bereich auf Block URLs Lists (URL-Listen blockieren), und erstellen Sie New Block URL List (Neue URL-Liste blockieren).



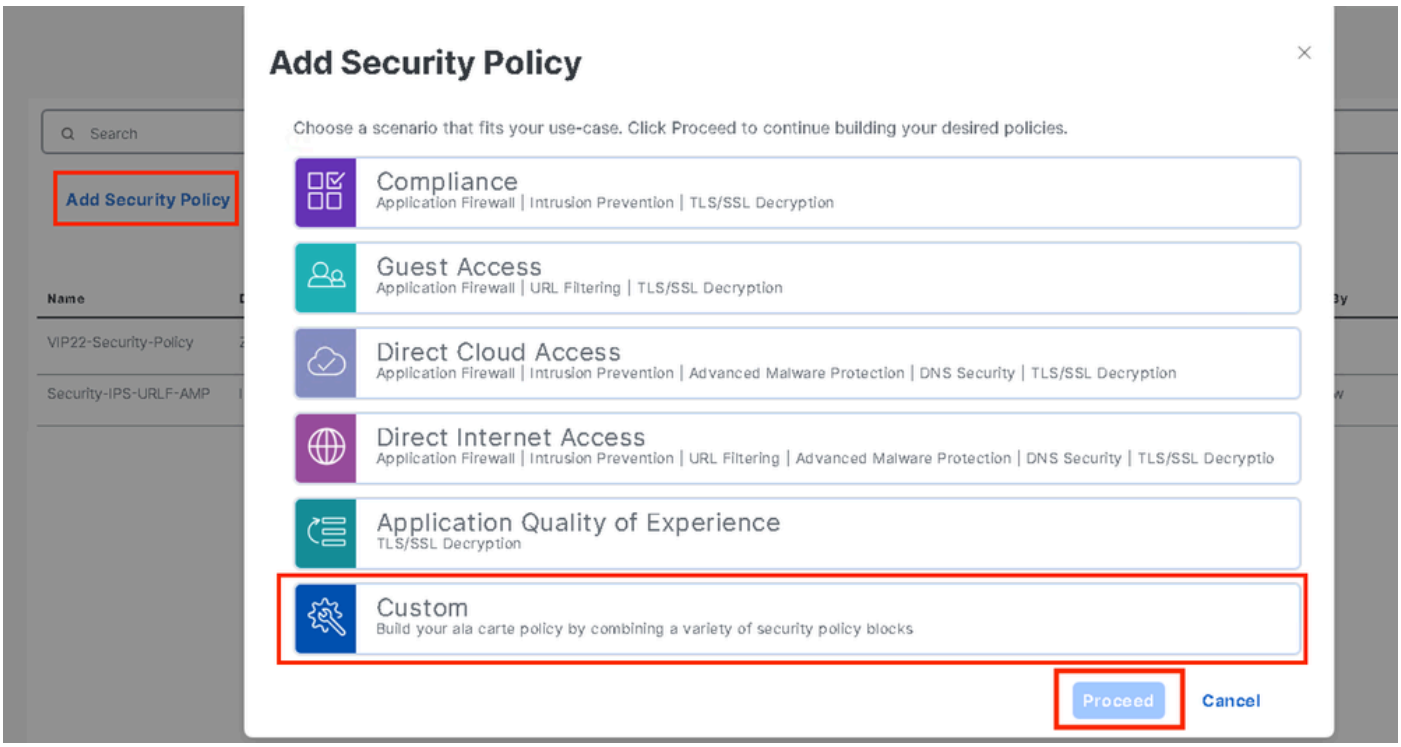
- Geben Sie im Feld Name der URL-Liste einen Listennamen mit bis zu 32 Zeichen ein (nur Buchstaben, Ziffern, Bindestriche und Unterstriche).
- Geben Sie im Feld URL die URLs ein, die in die Liste aufgenommen werden sollen, getrennt durch Kommas. Sie können auch die Schaltfläche Importieren verwenden, um Listen von einem zugänglichen Speicherort hinzuzufügen.
- Klicken Sie abschließend auf Hinzufügen.



Erstellen von Sicherheitsrichtlinien

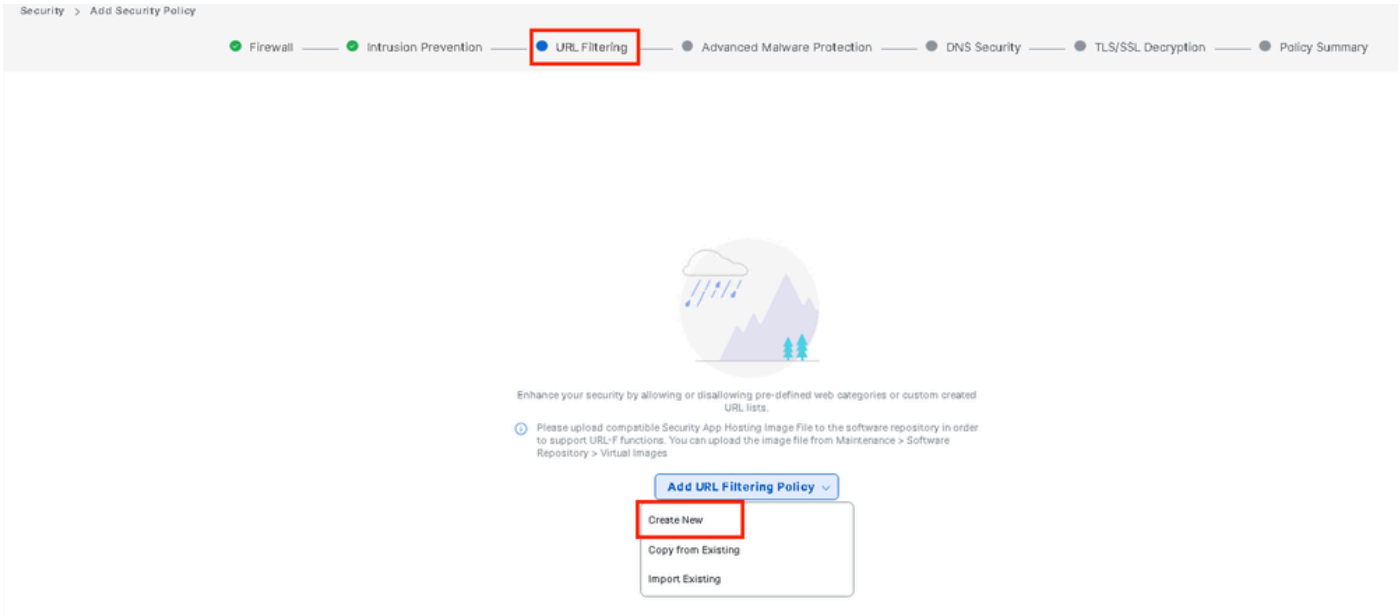
2. Navigieren Sie im Menü Cisco SD-WAN Manager zu Konfiguration > Sicherheit Klicken Sie auf Neue Sicherheitsrichtlinie hinzufügen. Der Assistent zum Hinzufügen von Sicherheitsrichtlinien

wird geöffnet, und es werden verschiedene Anwendungsfälle angezeigt, oder es wird eine vorhandene Richtlinie aus der Liste verwendet. Wählen Sie Benutzerdefiniert aus, und klicken Sie auf Proceed (Fortfahren), um eine URL-Filterrichtlinie im Assistenten hinzuzufügen.

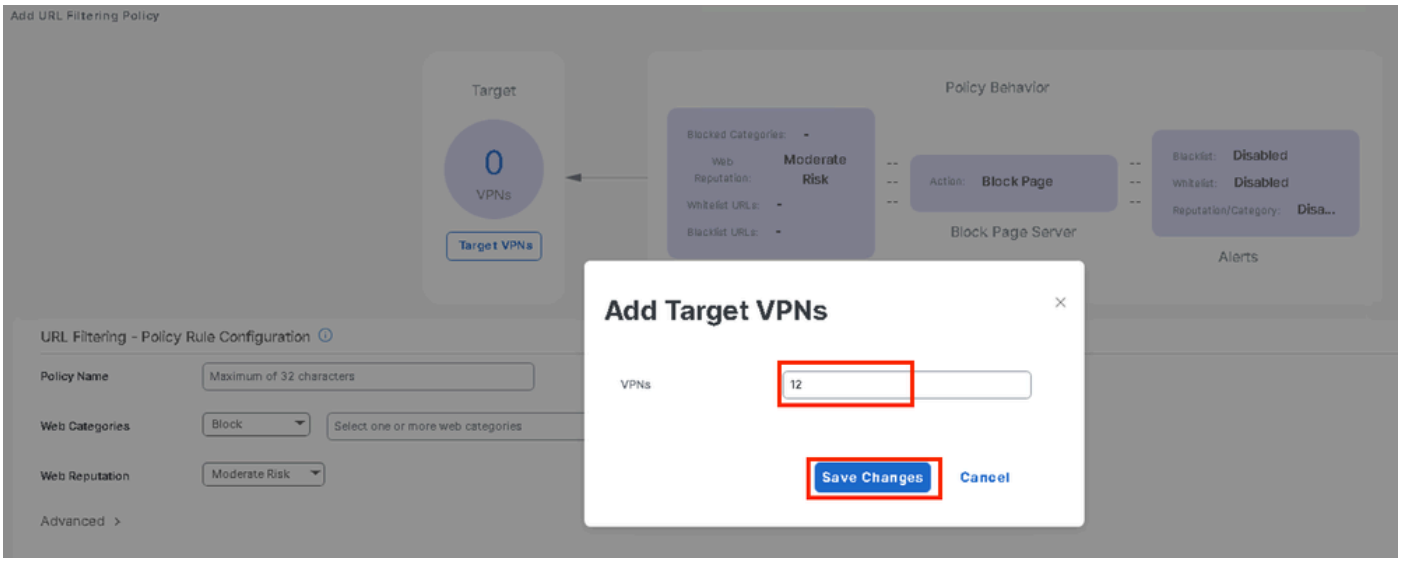


Hinweis: Wählen Sie unter Sicherheitsrichtlinie hinzufügen ein Szenario aus, das die URL-Filterung unterstützt (Gastzugriff, direkter Internetzugriff oder benutzerdefiniert).

Klicken Sie im Sicherheitsrichtlinien-Assistenten auf Weiter, bis das Fenster URL-Filterung angezeigt wird. Erstellen Sie jetzt eine URL-Filterungsrichtlinie, indem Sie zu URL-Filterung > URL-Filterungsrichtlinie hinzufügen > Neu erstellen wechseln. Klicken Sie auf Next (Weiter).



Klicken Sie auf Ziel-VPNs, um die erforderliche Anzahl von VPNs im Assistenten zum Hinzufügen von Ziel-VPNs hinzuzufügen.

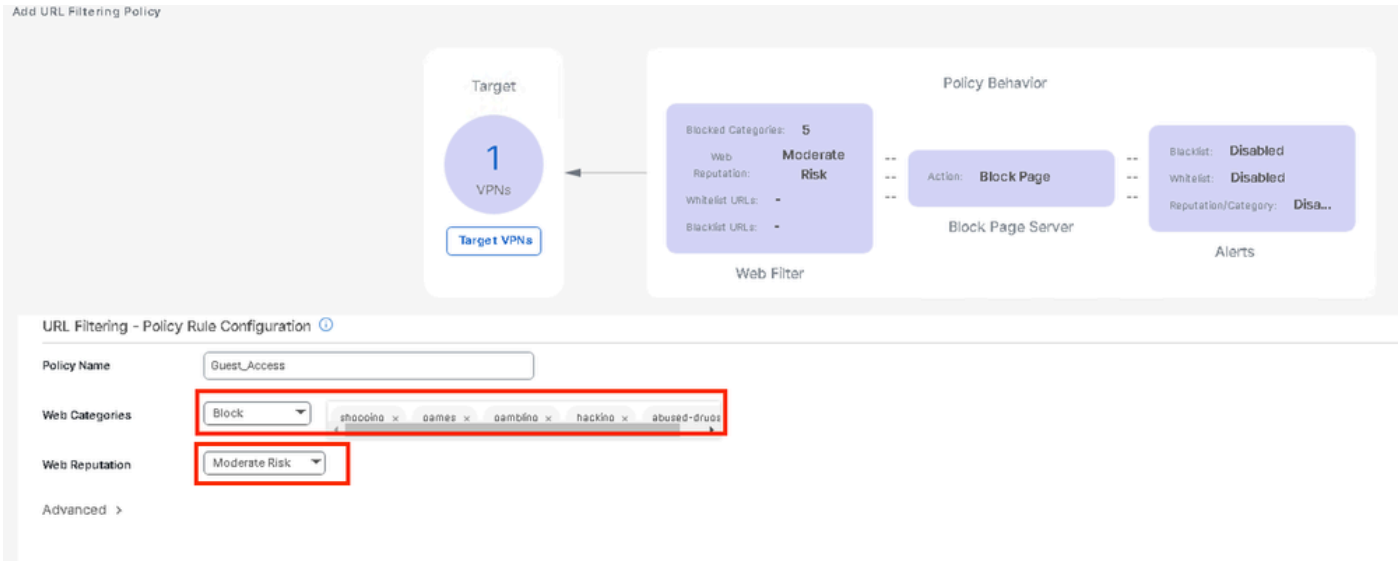


- Geben Sie im Feld Policy Name (Richtlinienname) einen Richtliniennamen ein.
- Wählen Sie im Dropdown-Menü "Webkategorien" eine der folgenden Optionen aus, und wählen Sie "Sperren" aus. Die Websites, die den ausgewählten Kategorien entsprechen, sind gesperrt.

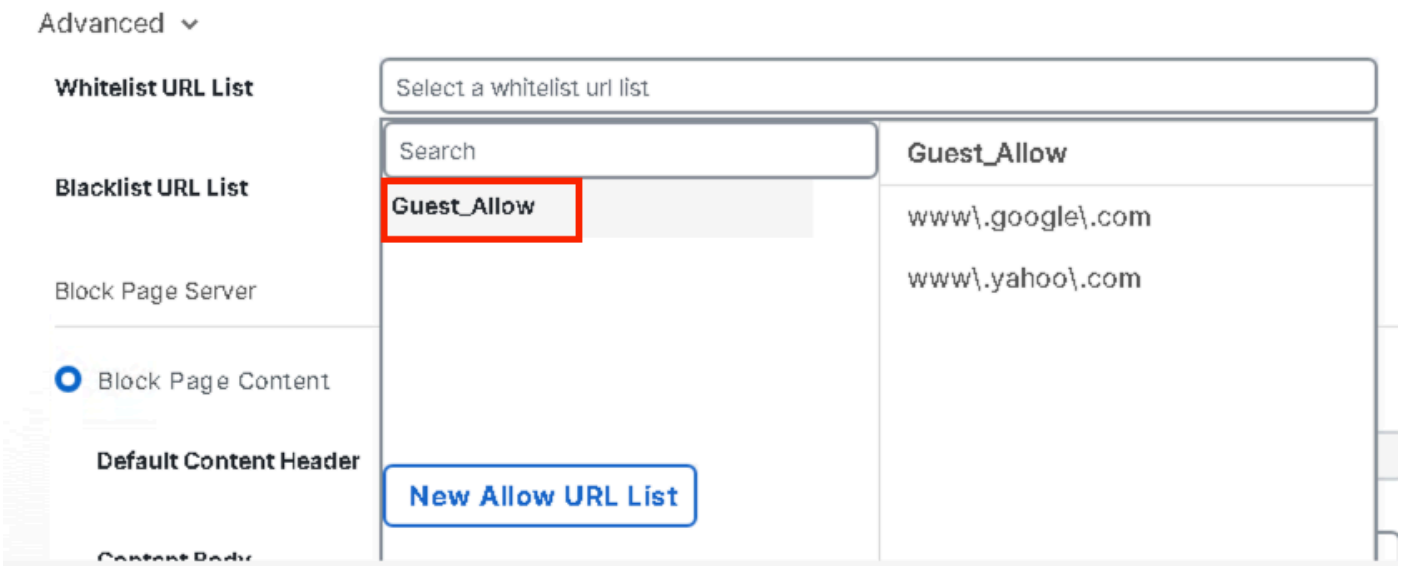
    Blockieren: Blockiert Websites, die den von Ihnen ausgewählten Kategorien entsprechen.
    Zulassen: Websites zulassen, die den von Ihnen ausgewählten Kategorien entsprechen.

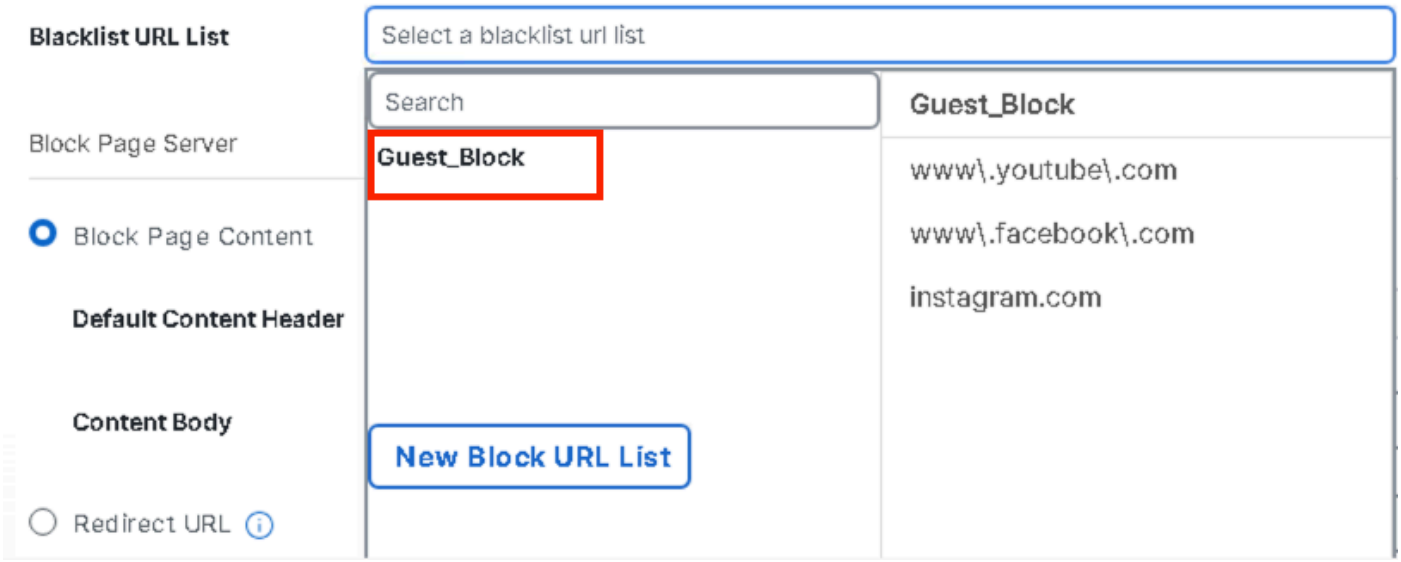
Wählen Sie im Dropdown-Menü eine Webreputation aus, und legen Sie die Option "Moderates Risiko" fest. URLs mit einer Reputationsbewertung von mindestens 60 werden blockiert.

Hohes Risiko: Reputationsbewertung von 0 bis 20.
Verdächtig: Reputationsbewertung von 0 bis 40.
Moderates Risiko: Reputationswert von 0 bis 60.
Geringes Risiko: Reputationsbewertung von 0 bis 80.
Vertrauenswürdig: Reputationswert von 0 bis 100.



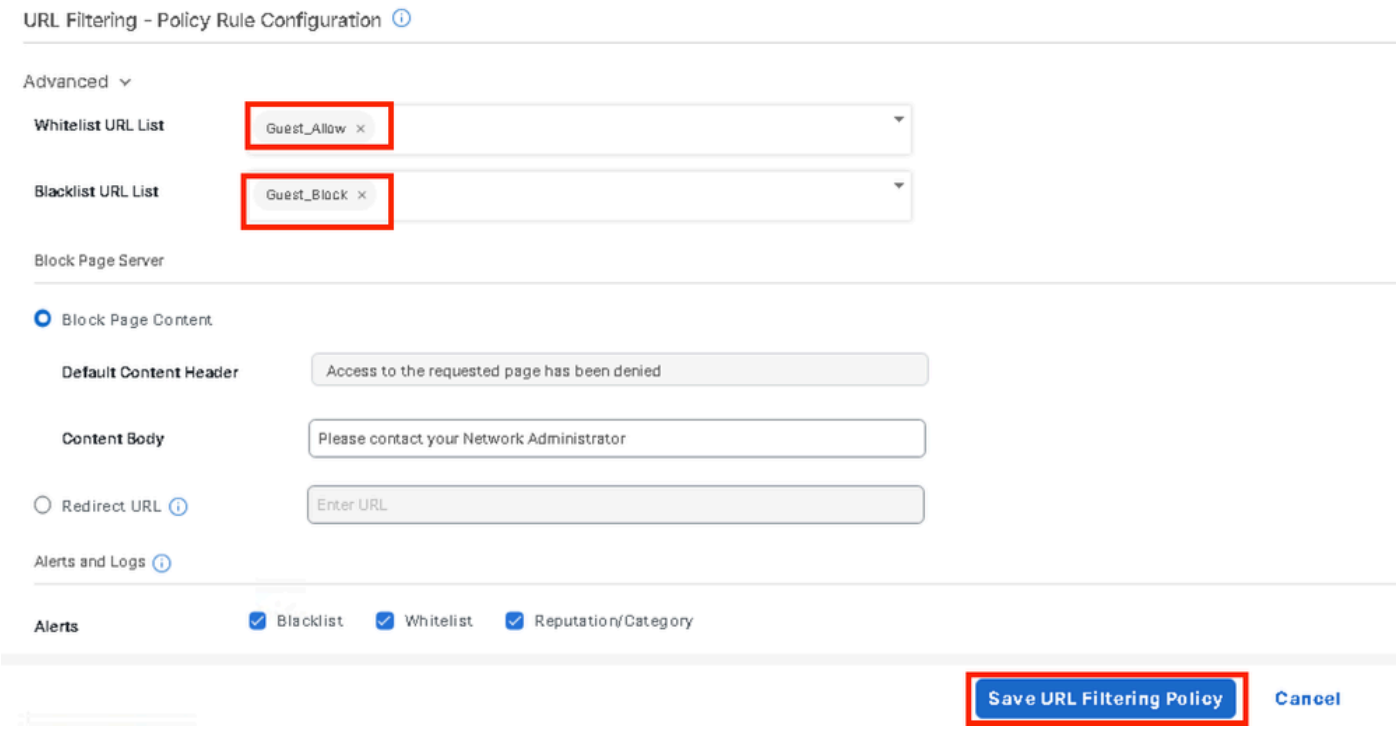
Wählen Sie unter Erweitert vorhandene Listen aus, oder erstellen Sie eine neue Liste nach Bedarf im Dropdown-Menü Liste der zulässigen URLs oder Sperrliste der URL-Liste.





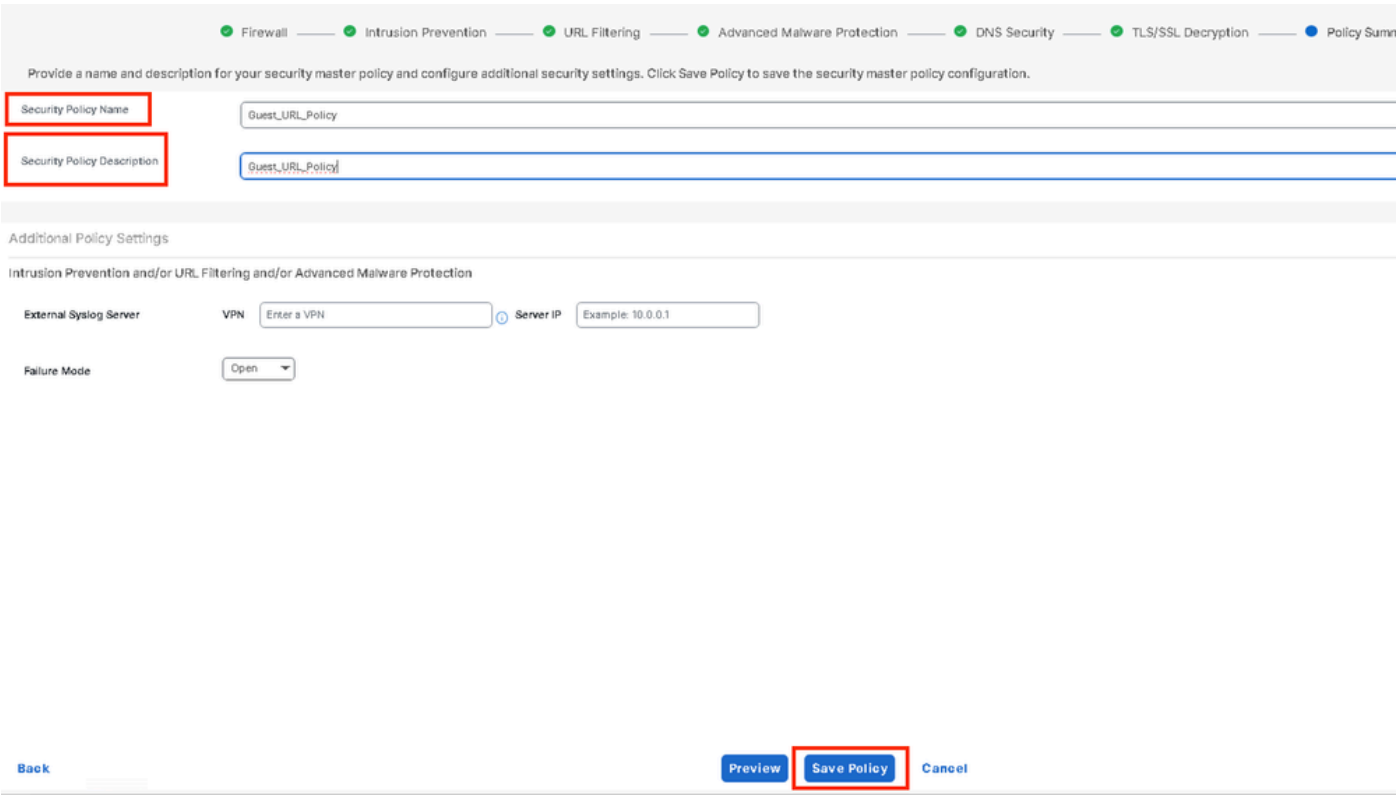
Ändern Sie ggf. den Textkörper unter Seiteninhalt blockieren, und stellen Sie sicher, dass alle Warnmeldungen ausgewählt sind.

Klicken Sie auf URL-Filterrichtlinie speichern, um eine URL-Filterrichtlinie hinzuzufügen.



Klicken Sie auf Weiter, bis die Seite "Richtlinienübersicht" angezeigt wird.

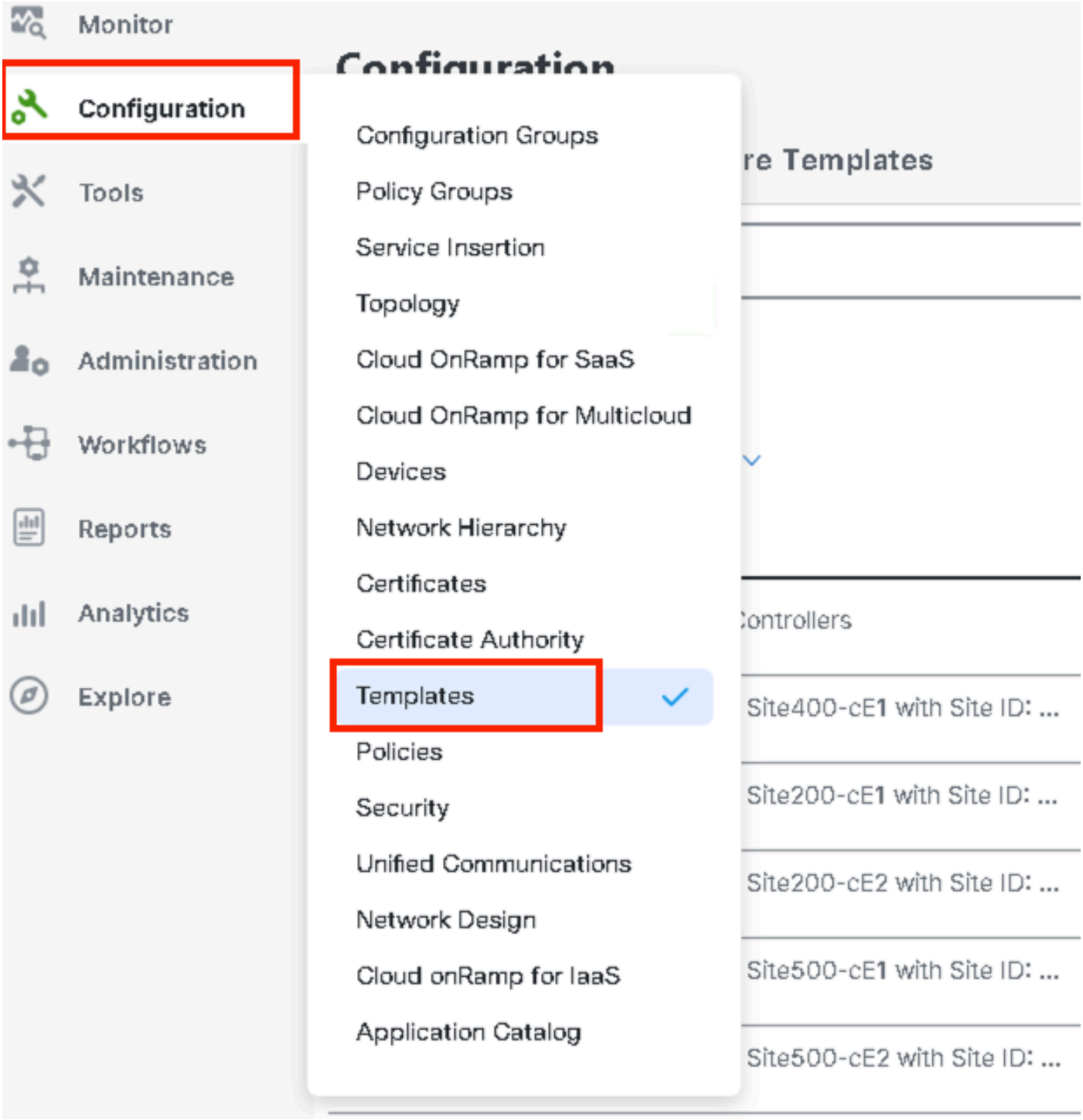
Geben Sie den Namen der Sicherheitsrichtlinie und die Beschreibung der Sicherheitsrichtlinie in die entsprechenden Felder ein.



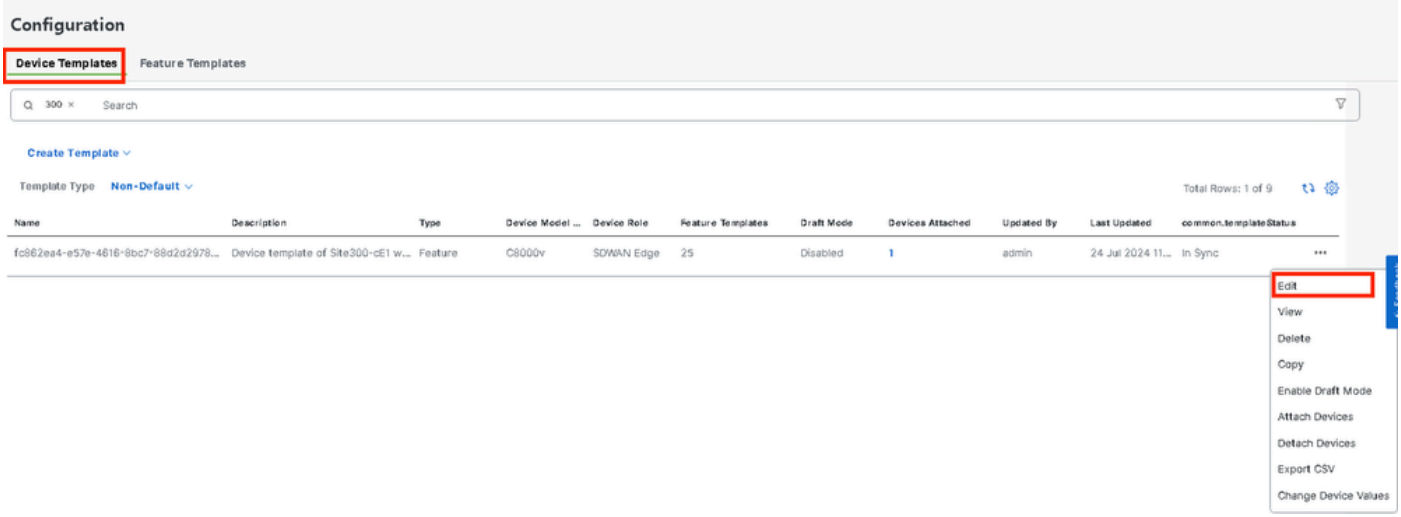
Anwenden einer Sicherheitsrichtlinie auf ein Gerät

So wenden Sie eine Sicherheitsrichtlinie auf ein Gerät an:

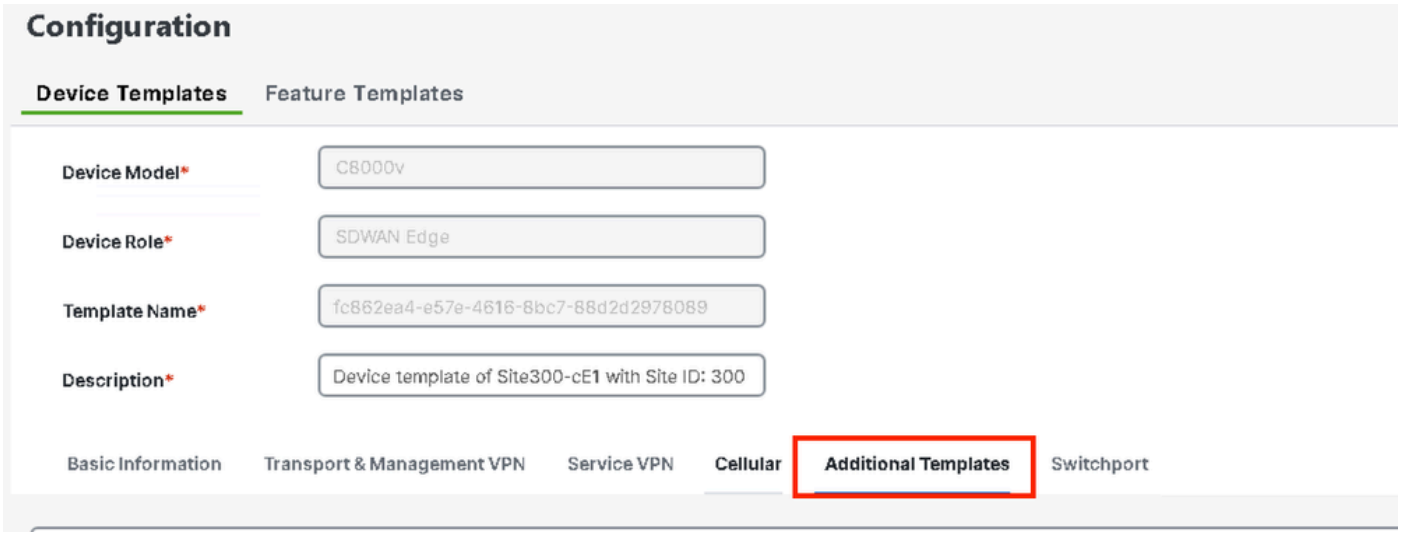
Wählen Sie im Menü Cisco SD-WAN Manager die Option Configuration > Templates (Konfiguration > Vorlagen).



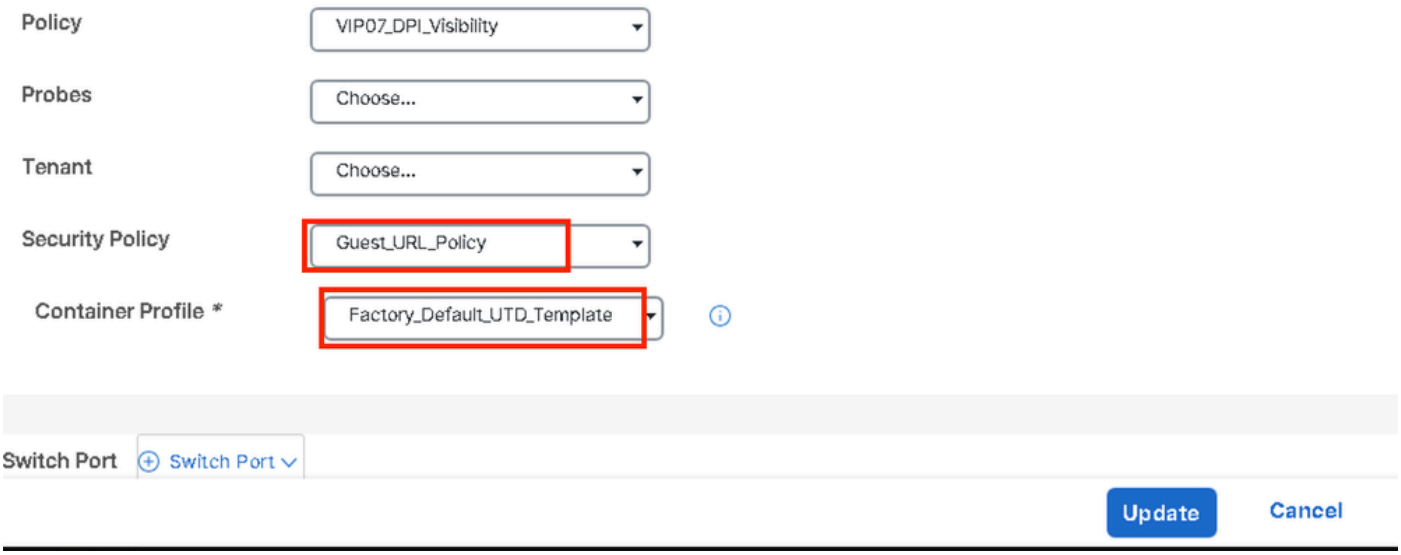
Klicken Sie auf Gerätevorlagen und dann auf Bearbeiten auf Gerätevorlage.



Klicken Sie auf Zusätzliche Vorlagen.

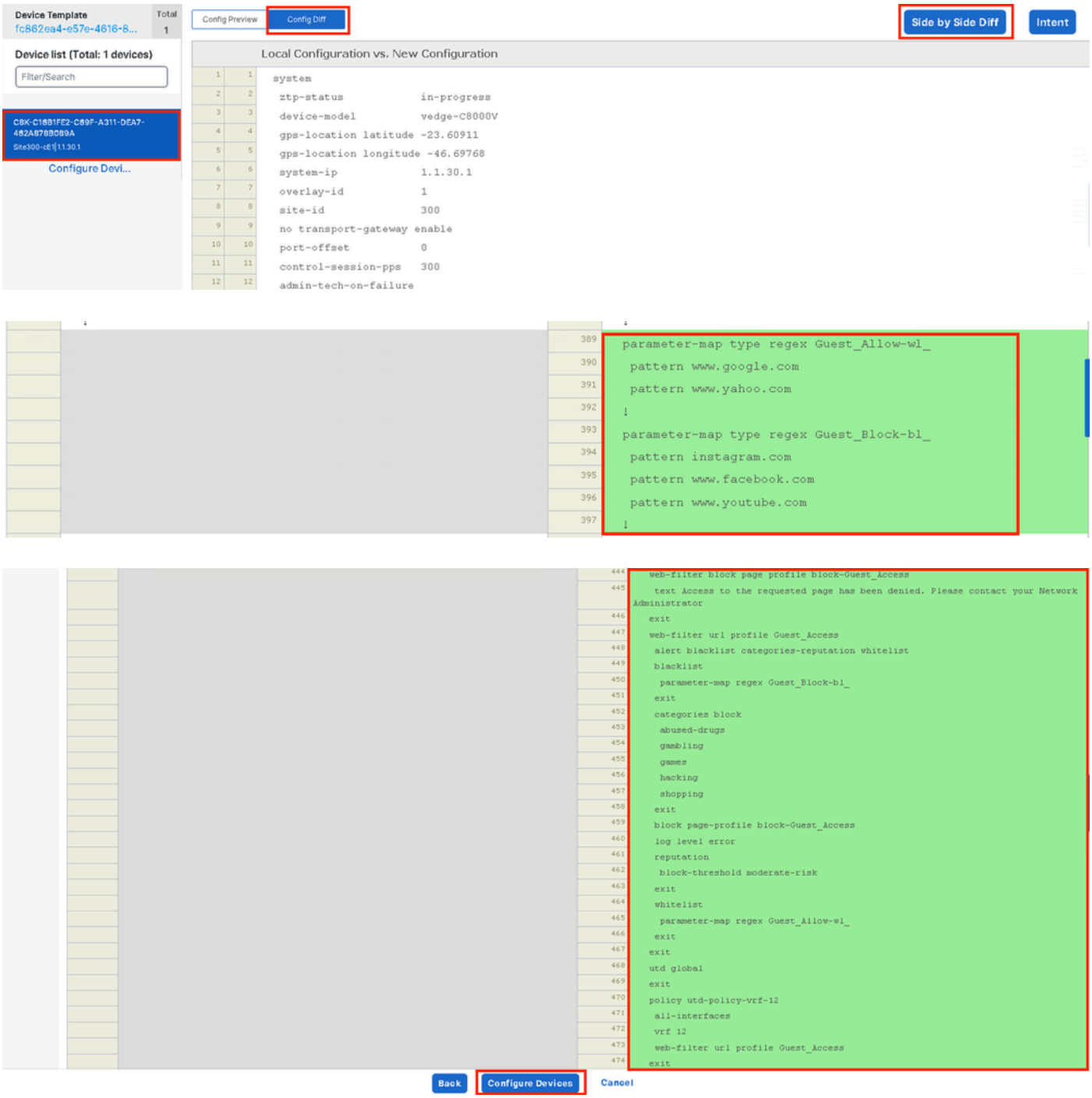


- Wählen Sie aus der Dropdown-Liste Sicherheitsrichtlinie den Namen der Richtlinie aus, die Sie zuvor unter Guest_URL_Policy konfiguriert haben, und klicken Sie auf Aktualisieren.

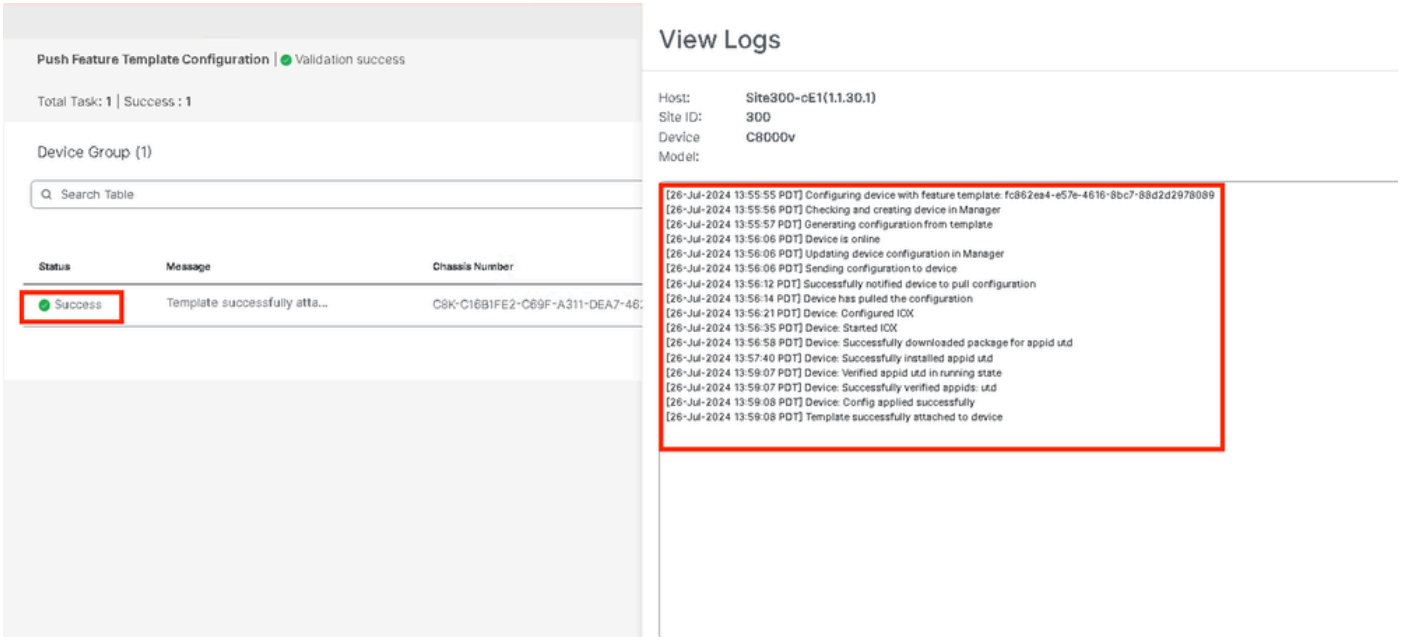


Klicken Sie auf die Geräte, und vergewissern Sie sich, dass die Konfiguration korrekt ist. Klicken

Sie dann auf Config Diff (Konfigurationsdiff) und Side by Side Diff (Nebeneinander-Diff). Klicken Sie auf Geräte konfigurieren.



vManage hat die Gerätevorlage erfolgreich mit der Sicherheitsrichtlinie konfiguriert und das UTD-Paket auf dem Edge-Gerät installiert.

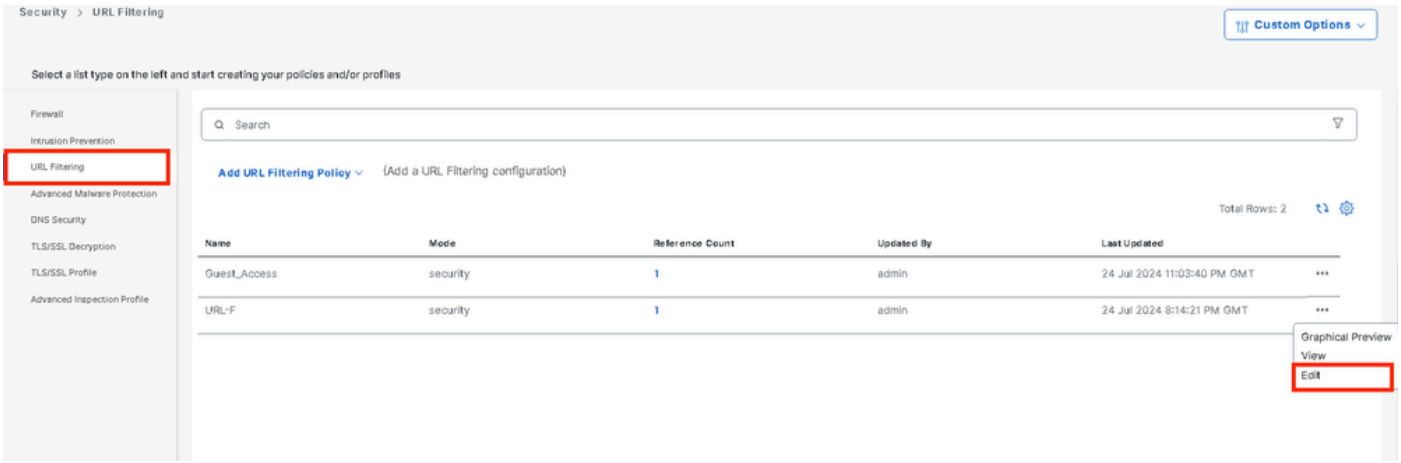


URL-Filterung ändern

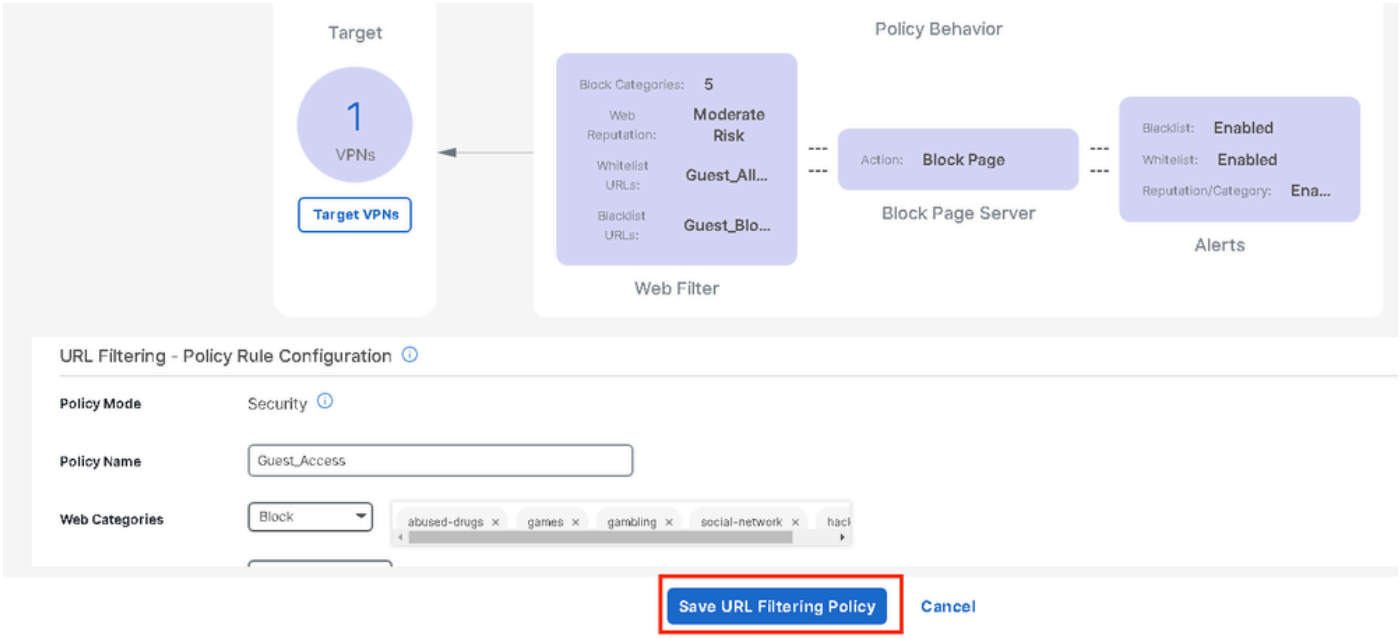
Um eine URL-Filterungsrichtlinie zu ändern, gehen Sie wie folgt vor:

1. Wählen Sie im Menü Cisco SD-WAN Manager die Option Configuration > Security (Konfiguration > Sicherheit).
2. Klicken Sie im Bildschirm Sicherheit auf das Dropdown-Menü Benutzerdefinierte Optionen, und wählen Sie Richtlinien/Profile aus.

Klicken Sie auf der linken Registerkarte auf URL-Filterung, um die gewünschte Richtlinie zu ändern, klicken Sie auf 3 Punkte (...) und wählen Sie Bearbeiten aus.



Ändern Sie die Richtlinie nach Bedarf, und klicken Sie auf Save URL Filtering Policy (URL-Filterrichtlinie speichern).



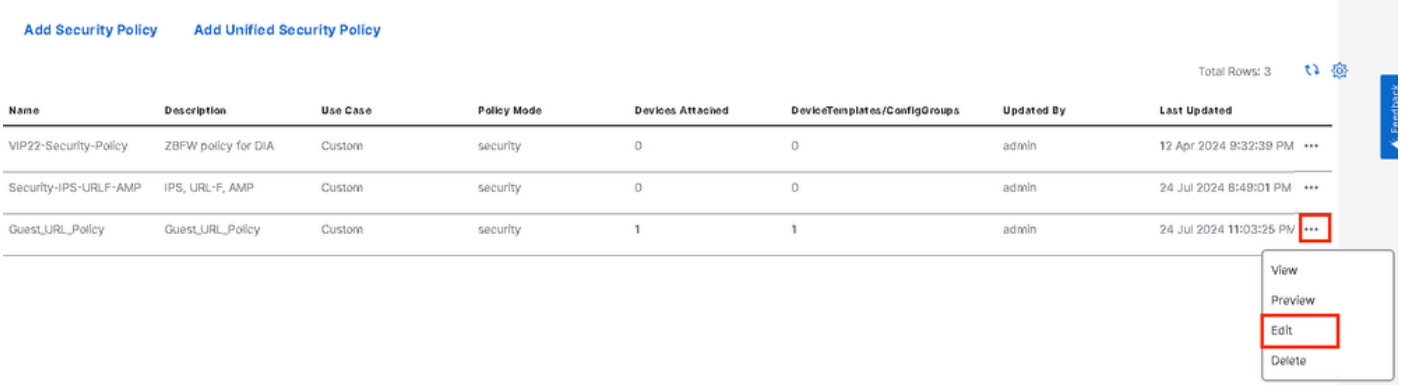
URL-Filterung löschen

Um eine URL-Filterrichtlinie zu löschen, müssen Sie diese zuerst von der Sicherheitsrichtlinie trennen:

Wählen Sie im Menü Cisco SD-WAN Manager Configuration > Security.

So trennen Sie die URL-Filterrichtlinie von der Sicherheitsrichtlinie:

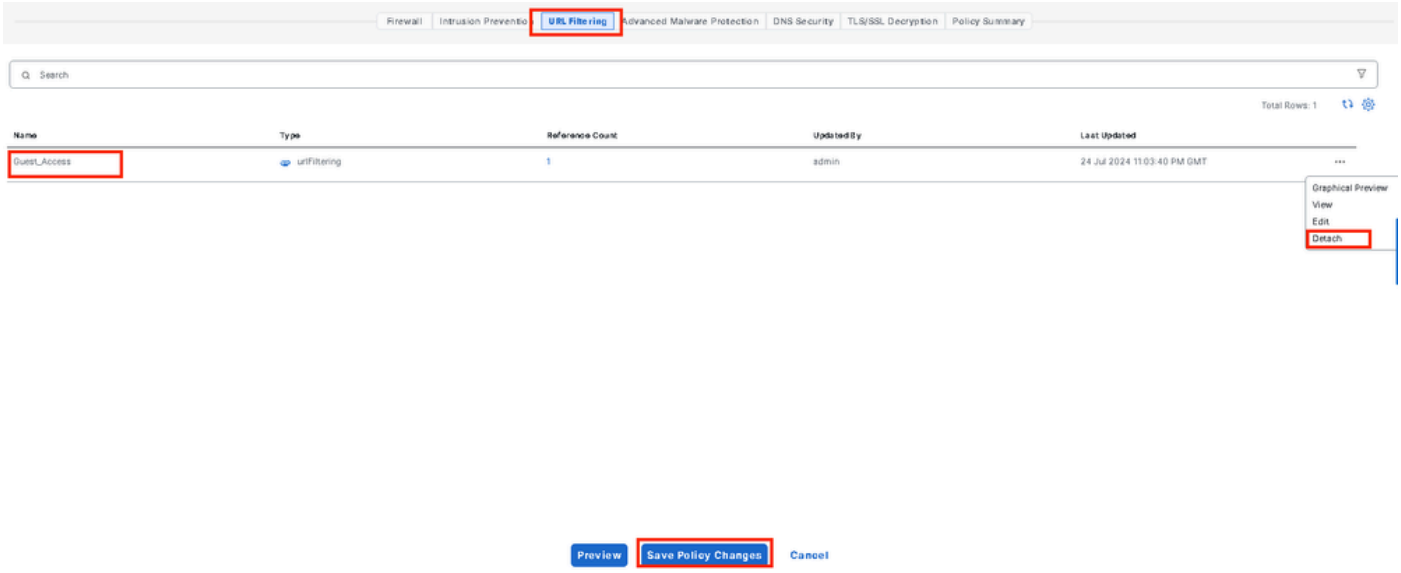
- Klicken Sie für die Sicherheitsrichtlinie, die die URL-Filterrichtlinie enthält, auf 3 Punkte (...) und dann auf Bearbeiten.



Die Seite "Policy Summary" (Richtlinienübersicht) wird angezeigt. Klicken Sie auf die Registerkarte URL-Filterung.

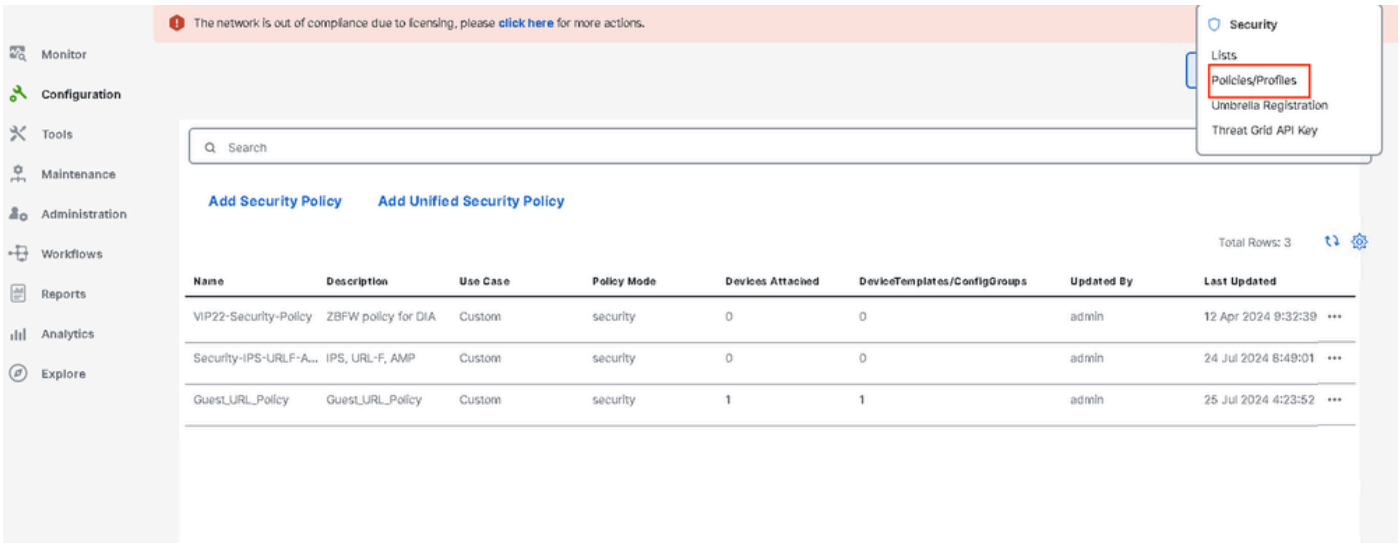
Klicken Sie für die Richtlinie, die Sie löschen möchten, auf 3 Punkte (...), und wählen Sie dann Trennen.

Klicken Sie auf Richtlinienänderungen speichern.



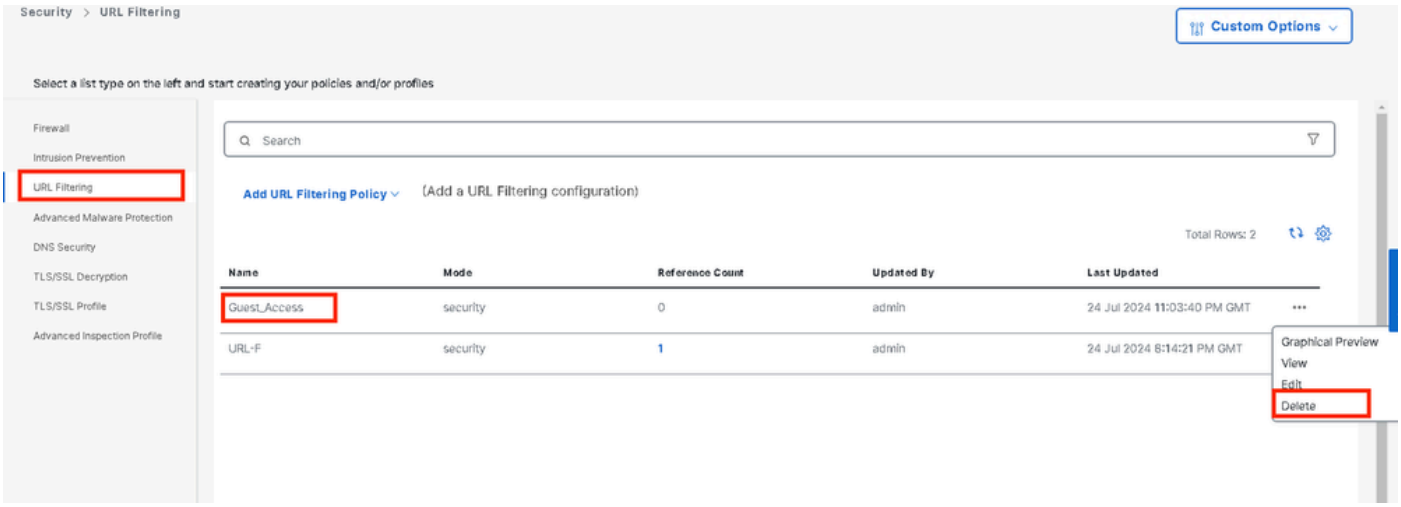
So löschen Sie die URL-Filterrichtlinie:

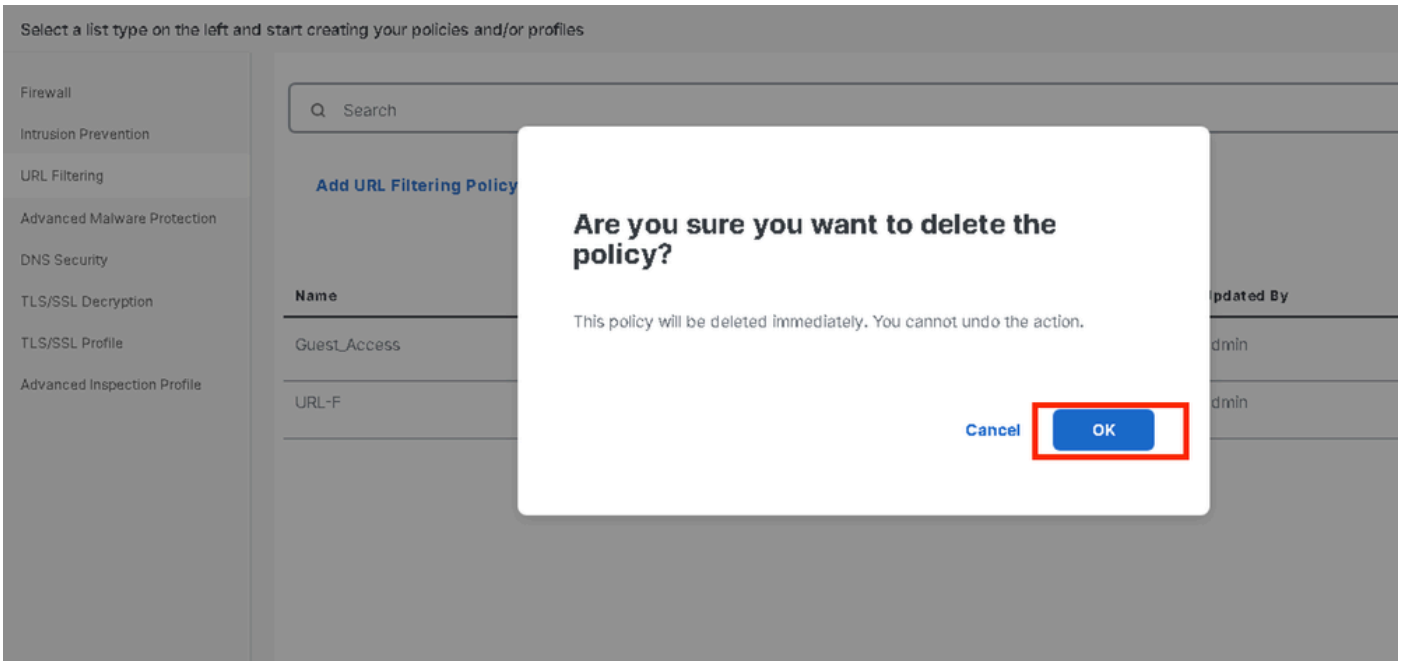
Klicken Sie auf dem Bildschirm Sicherheit auf das Dropdown-Menü Benutzerdefinierte Optionen, wählen Sie Richtlinien/Profile und dann URL-Filterung.



Klicken Sie für die Richtlinie, die Sie löschen möchten, auf 3 Punkte (...), und klicken Sie dann auf Löschen.

Klicken Sie auf OK.





Überprüfung

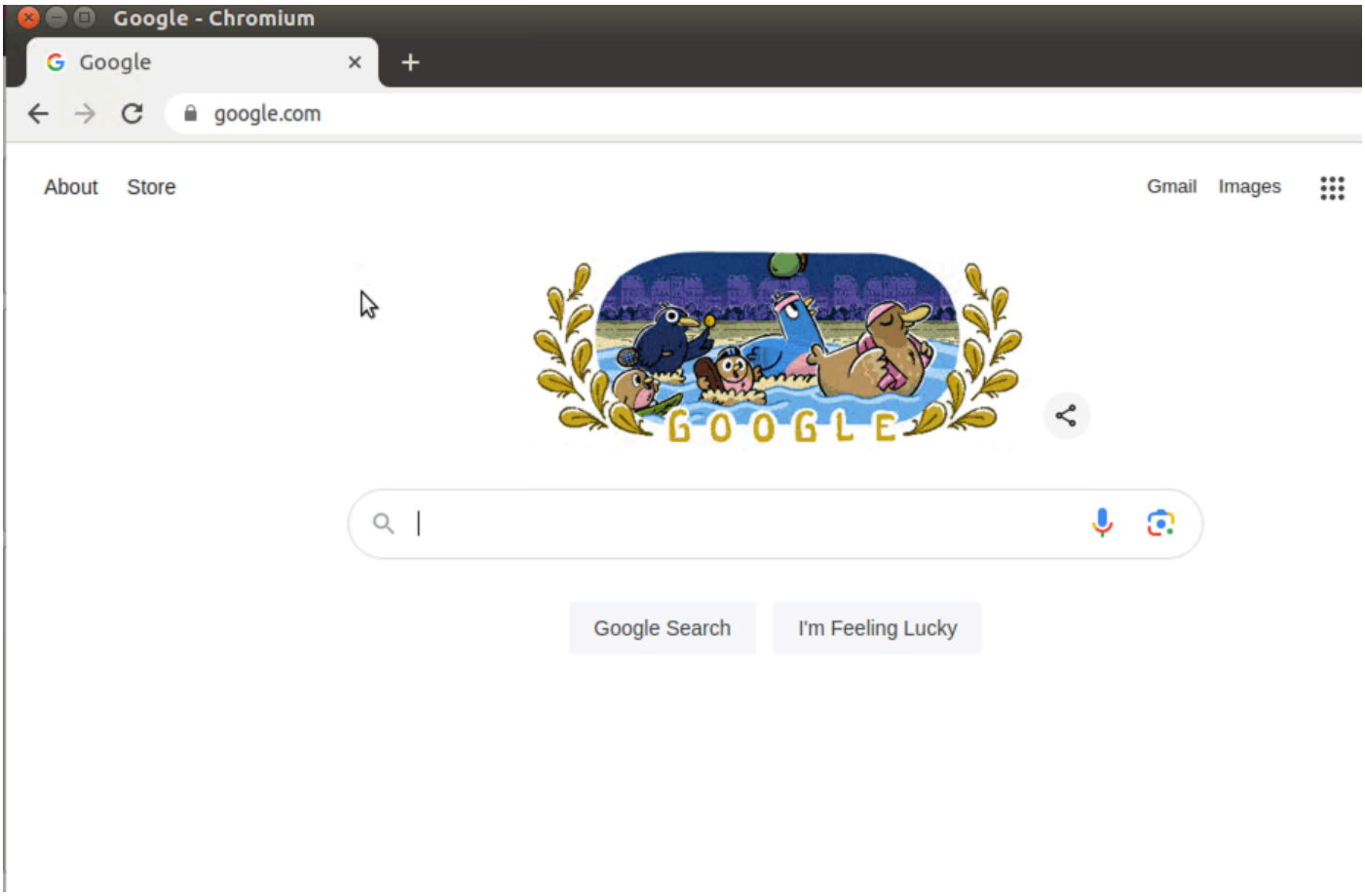
Überprüfen Sie, ob die Cisco UTD-Version installiert ist.

<#root>

```
Site300-cE1#show utd engine standard version
UTD Virtual-service Name: utd
IOS-XE Recommended UTD Version: 1.0.2_SV3.1.67.0_XE17.14
IOS-XE Supported UTD Regex: ^1\.0\.([0-9]+)_SV(.*)_XE17.14$
UTD Installed Version:
```

1.0.2_SV3.1.67.0_XE17.14

Wenn Sie versuchen, google.com und yahoo.com zu öffnen, sind diese vom Client-PC im Gast-VPN aus zulässig.



<#root>

```
Site300-cE1#show utd engine standard logging events | in google
2024/07/24-13:22:38.900508 PDT [**] [Hostname: site300-ce1] [**] [System_IP: x.x.x.x] [**] [Instance_ID
```

Pass

[**]

UTD WebFilter Allowlist

[**] [

URL: www.google.com

```
] [VRF: 12] {TCP} 10.32.1.10:55310 -> 142.250.189.196:443
2024/07/24-13:24:03.429964 PDT [**] [Hostname: site300-ce1] [**] [System_IP: x.x.x.x] [**] [Instance_ID
```

Pass

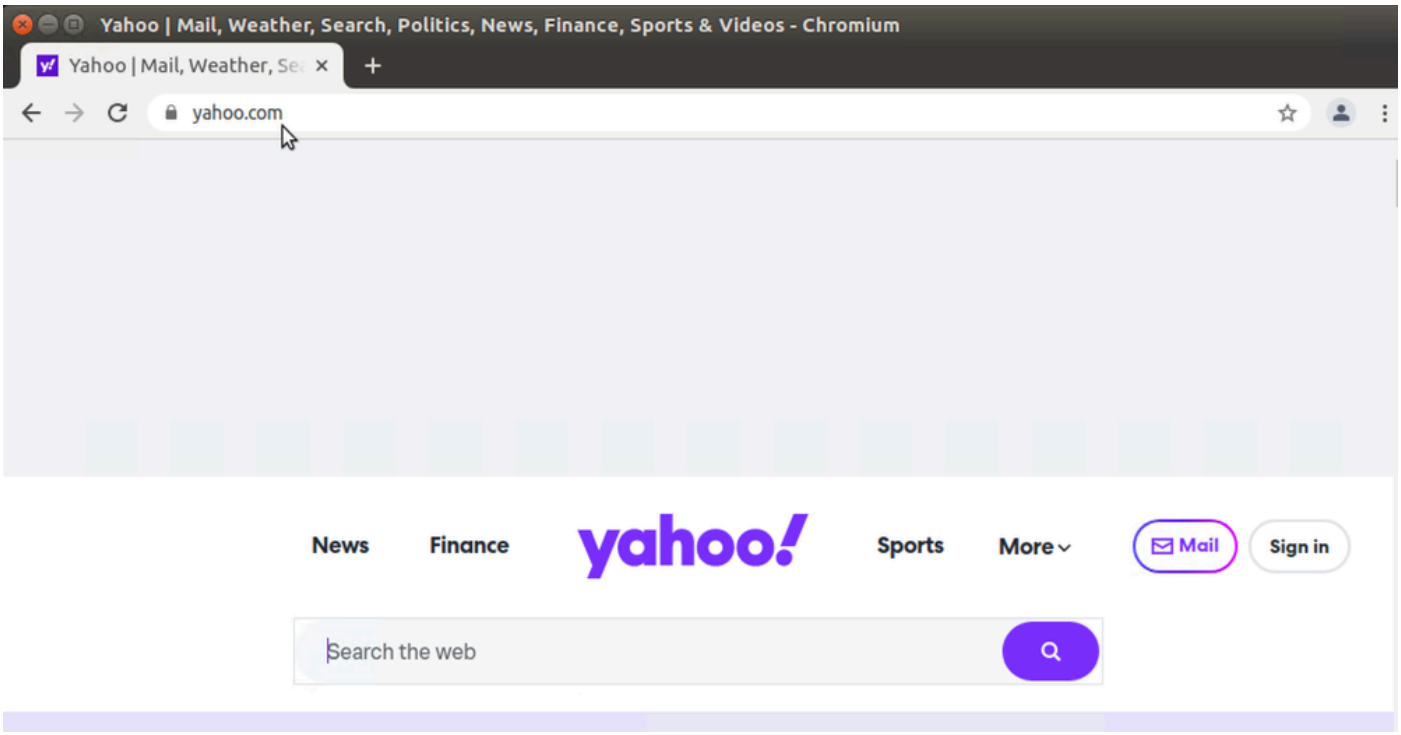
[**]

UTD WebFilter Allowlist

[**] [

URL: www.google.com

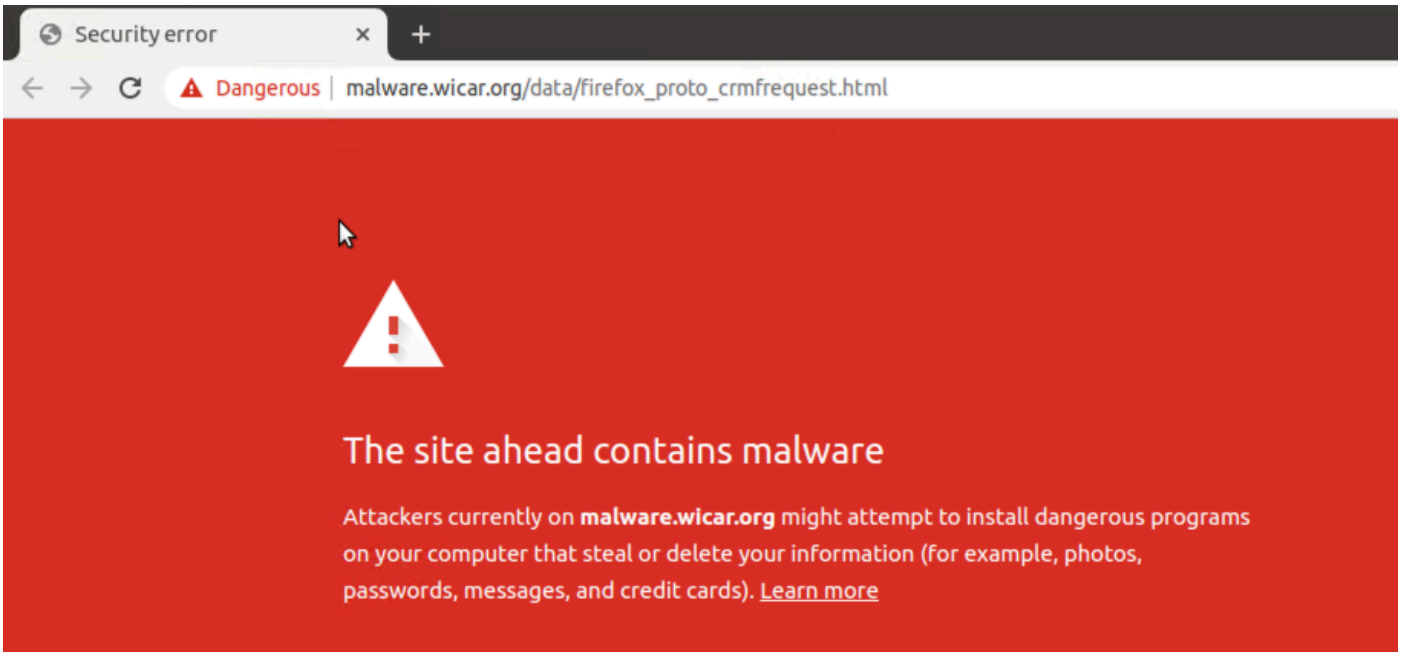
```
] [VRF: 12] {TCP} 10.32.1.10:55350 -> 142.250.189.196:443
```



<#root>

```
Site300-cE1#show utd engine standard logging events | in yahoo
2024/07/24-13:20:45.238251 PDT [**] [Hostname: site300-ce1] [**] [System_IP: x.x.x.x] [**] [Instance_ID

Pass [

**]

UTD WebFilter Allowlist

 [**] [

URL: www.yahoo.com

] [VRF: 12] {TCP} 10.32.1.10:48714 -> 69.147.88.8:443
2024/07/24-13:20:45.245446 PDT [**] [Hostname: site300-ce1] [**] [System_IP: x.x.x.x] [**] [Instance_ID

Pass

 [**]

UTD WebFilter Allowlist

 [**] [

URL: www.yahoo.com

] [VRF: 12] {TCP} 10.32.1.10:48716 -> 69.147.88.8:443
```

Wenn Sie auf dem Client-PC im Gast-VPN versuchen, Webseiten mit schlechten Reputationsbewertungen zu öffnen, oder wenn Sie aus einer der gesperrten Webkategorien stammen, verweigert die URL-Filterungs-Engine die HTTP-Anforderung.



<#root>

```
Site300-cE1#show utd engine standard logging events | in mal
2024/07/24-13:32:18.475318 PDT [**] [Hostname: site300-ce1] [**] [System_IP: x.x.x.x] [**] [Instance_ID
```

Drop

[**]

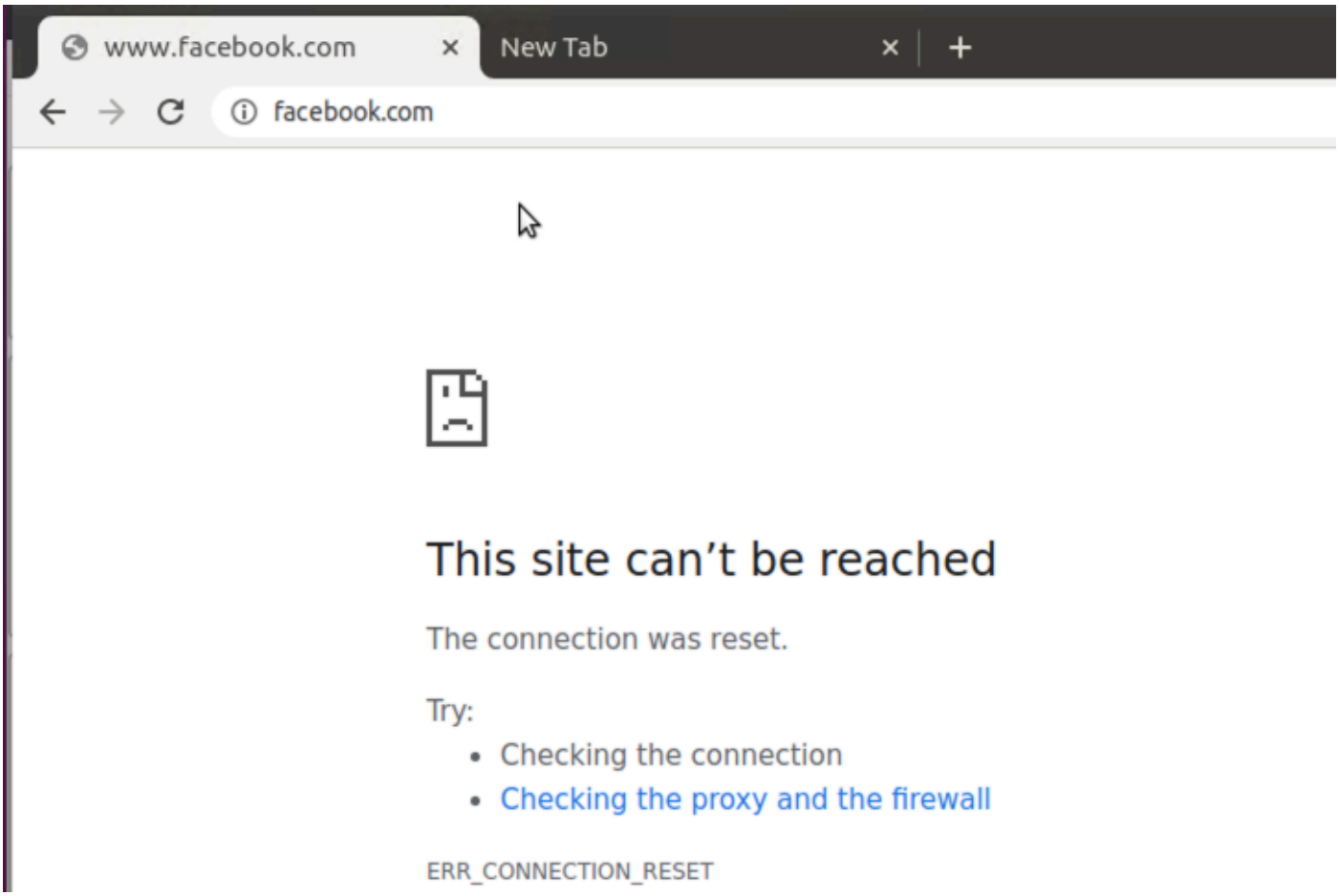
UTD WebFilter Category/Reputation

[**] [

URL: malware.wicar.org/data/firefox_proto_crmfrequest.html

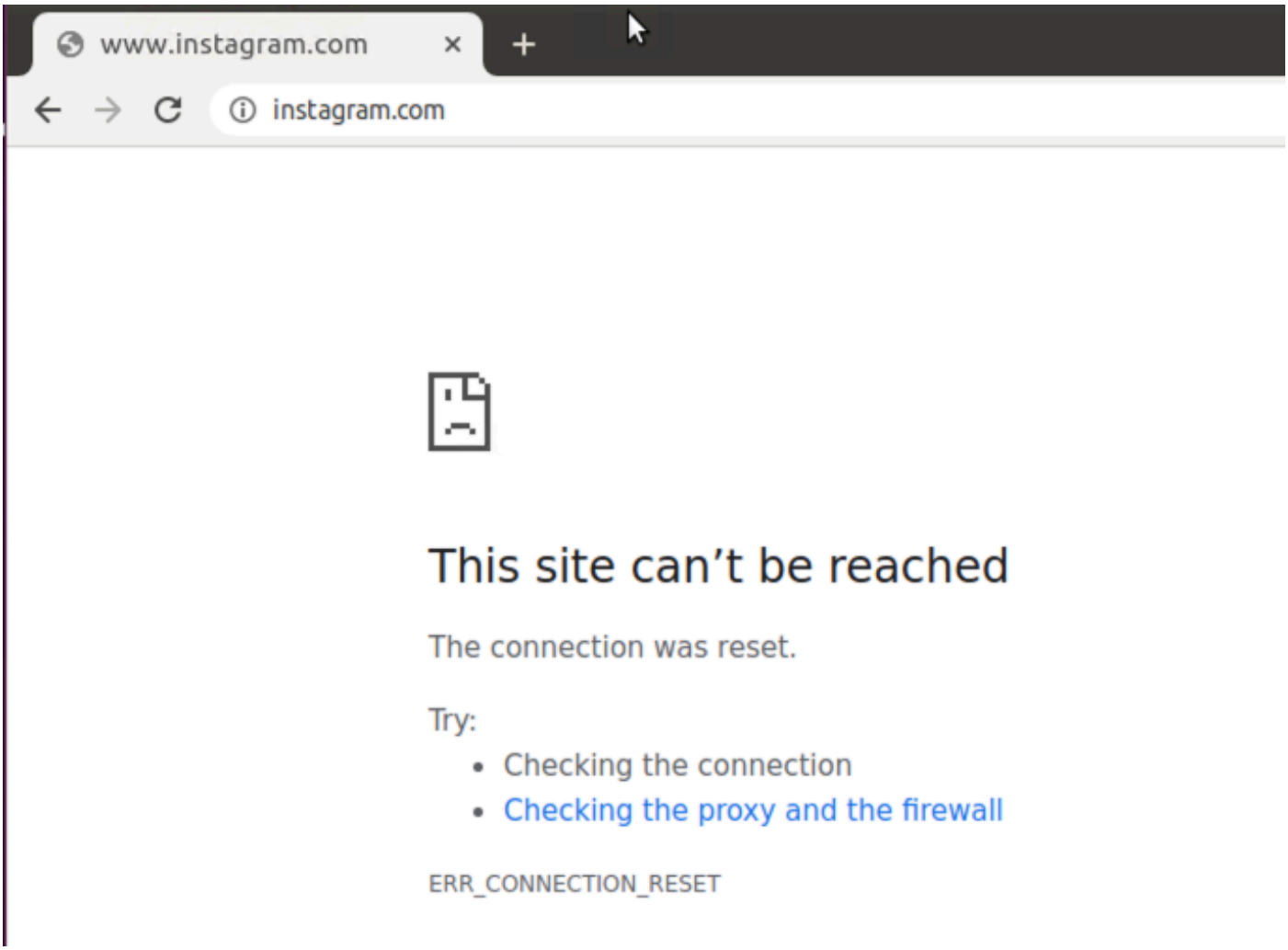
```
] ** [Category: Malware Sites] ** [Reputation: 10] [VRF: 12] {TCP} 10.32.1.10:40154 -> 208.94.116.246:8
```

Wenn Sie versuchen, Facebook zu öffnen, werden Instagram und YouTube vom Client-PC auf dem Gast-VPN blockiert.



<#root>

```
Site300-cE1#show utd engine standard logging events | in face
2024/07/24-13:05:25.622746 PDT [**] [Hostname: site300-ce1] [**] [System_IP: x.x.x.x] [**] [Instance_ID

Drop

 [**]

UTD WebFilter blocklist

 [**] [

URL: www.facebook.com

] [VRF: 12] {TCP} 10.32.1.10:55872 -> 157.240.22.35:443
2024/07/24-13:05:25.638612 PDT [**] [Hostname: site300-ce1] [**] [System_IP: x.x.x.x] [**] [Instance_ID

 Drop

 [**]

UTD WebFilter blocklist

 [**] [

URL: www.facebook.com

] [VRF: 12] {TCP} 10.32.1.10:55876 -> 157.240.22.35:443
```



<#root>

```
Site300-cE1#show utd engine standard logging events | in insta
2024/07/24-13:09:07.027559 PDT [**] [Hostname: site300-ce1] [**] [System_IP: x.x.x.x] [**] [Instance_ID

 Drop

 [**]

UTD WebFilter blocklist

 [**] [

URL: www.instagram.com

] [VRF: 12] {TCP} 10.32.1.10:58496 -> 157.240.22.174:443
2024/07/24-13:09:07.030067 PDT [**] [Hostname: site300-ce1] [**] [System_IP: x.x.x.x] [**] [Instance_ID

Drop

 [**]

UTD WebFilter blocklist

 [**] [

URL: www.instagram.com

] [VRF: 12] {TCP} 10.32.1.10:58498 -> 157.240.22.174:443
2024/07/24-13:09:07.037384 PDT [**] [Hostname: site300-ce1] [**] [System_IP: x.x.x.x] [**] [Instance_ID
```

Drop

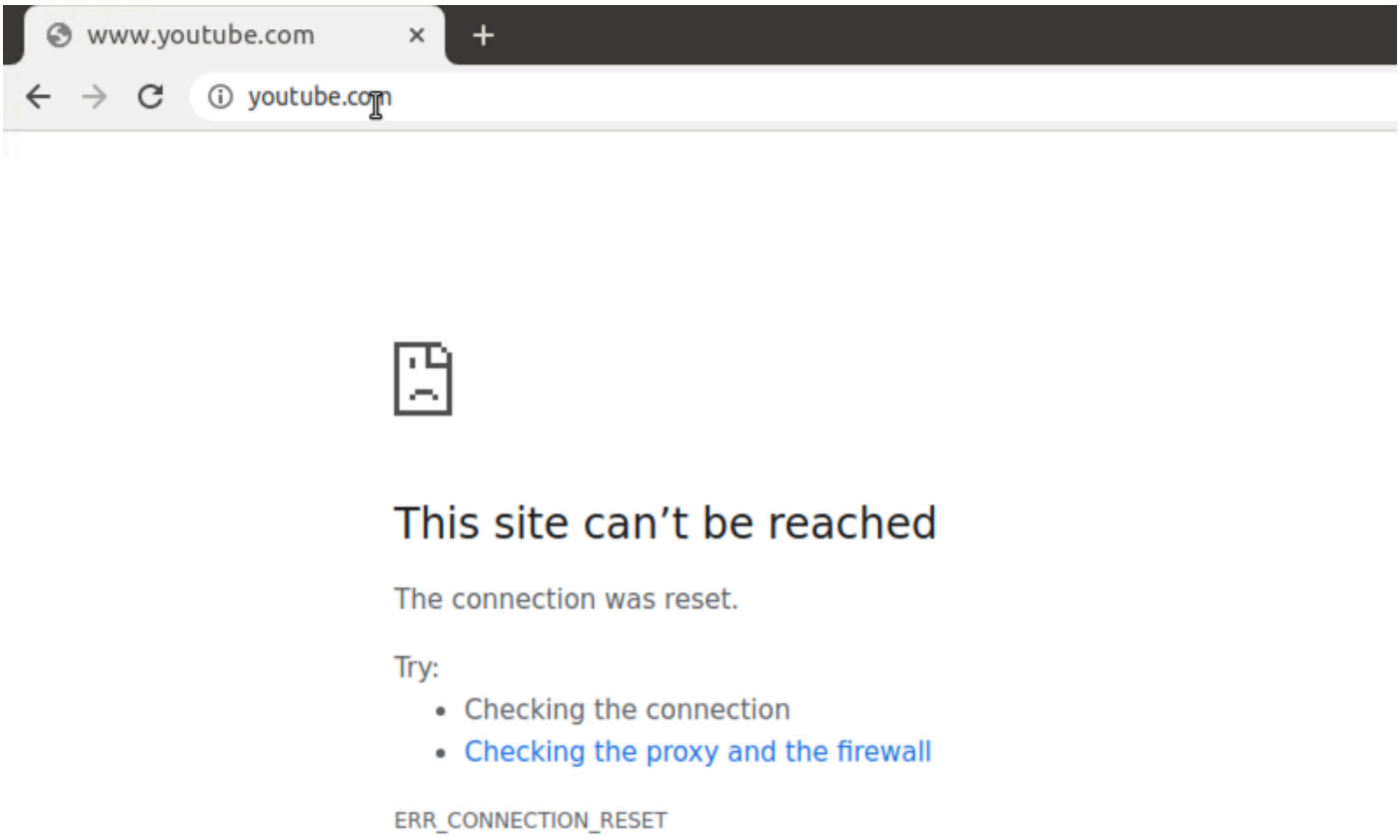
[**]

UTD WebFilter blocklist

[**] [

URL: www.instagram.com

] [VRF: 12] {TCP} 10.32.1.10:58500 -> 157.240.22.174:443



<#root>

Site300-cE1#show utd engine standard logging events | in youtube
2024/07/24-13:10:01.712501 PDT [**] [Hostname: site300-ce1] [**] [System_IP: x.x.x.x] [**] [Instance_ID

Drop

[**]

UTD WebFilter blocklist

[**] [

URL: www.youtube.com

] [VRF: 12] {TCP} 10.32.1.10:54292 -> 142.250.72.206:443
2024/07/24-13:10:01.790521 PDT [**] [Hostname: site300-ce1] [**] [System_IP: x.x.x.x] [**] [Instance_ID

Drop

[**]

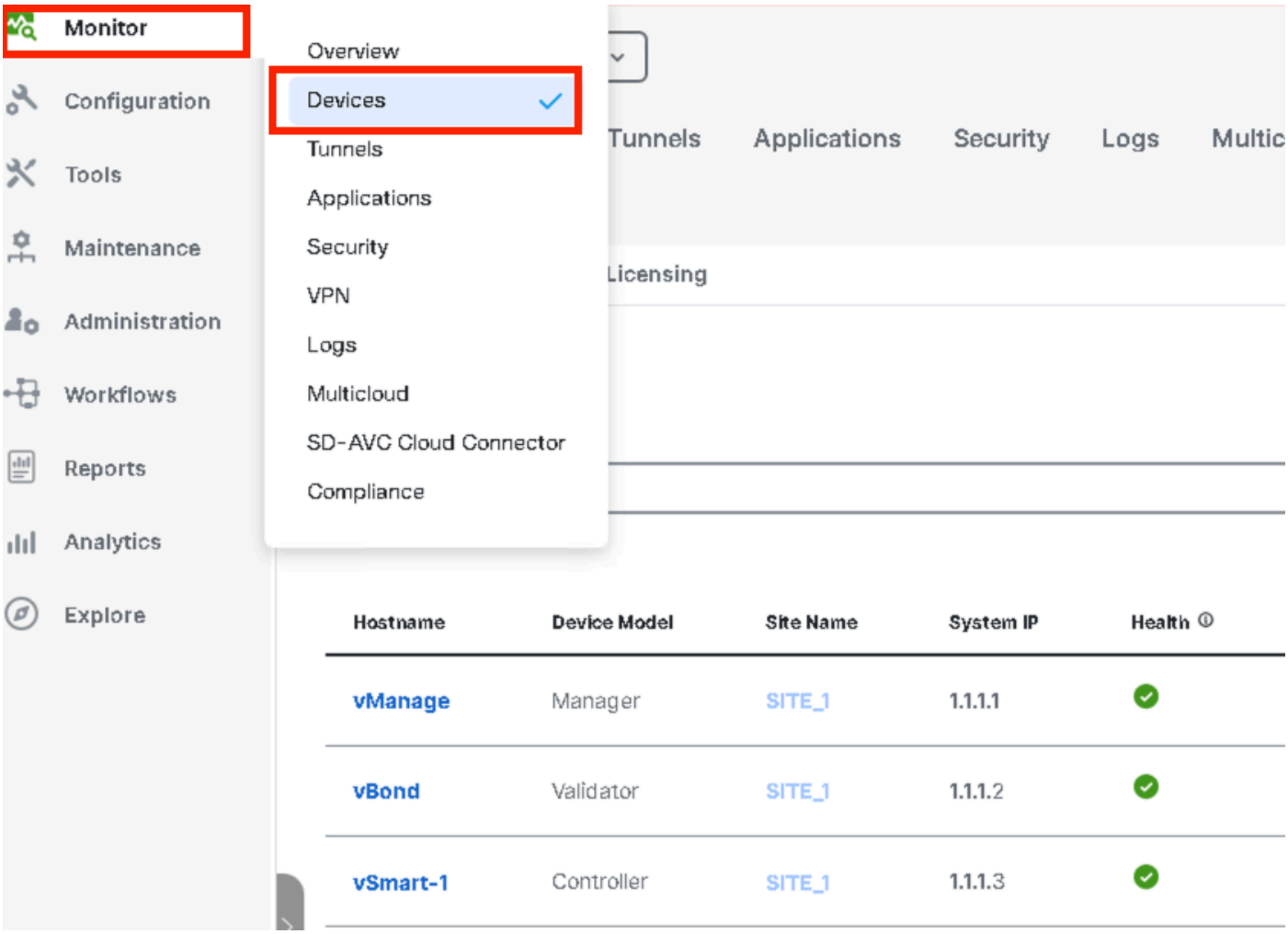
```
UTD WebFilter blocklist

 [**] [

URL: www.youtube.com

] [VRF: 10] {TCP} 10.30.1.10:37988 -> 142.250.72.206:443
2024/07/24-13:11:11.400417 PDT [**] [Hostname: site300-ce1] [**] [System_IP: x.x.x.x] [**] [Instance_ID

Drop

 [**]

UTD WebFilter blocklist

 [**] [

URL: www.youtube.com

] [VRF: 12] {TCP} 10.32.1.10:54352 -> 142.250.72.206:443
```

Überwachen der URL-Filterung über die vManage-GUI

Mit diesen Schritten können Sie die URL-Filterung für jedes Gerät nach Webkategorien in Echtzeit oder historisch überwachen.

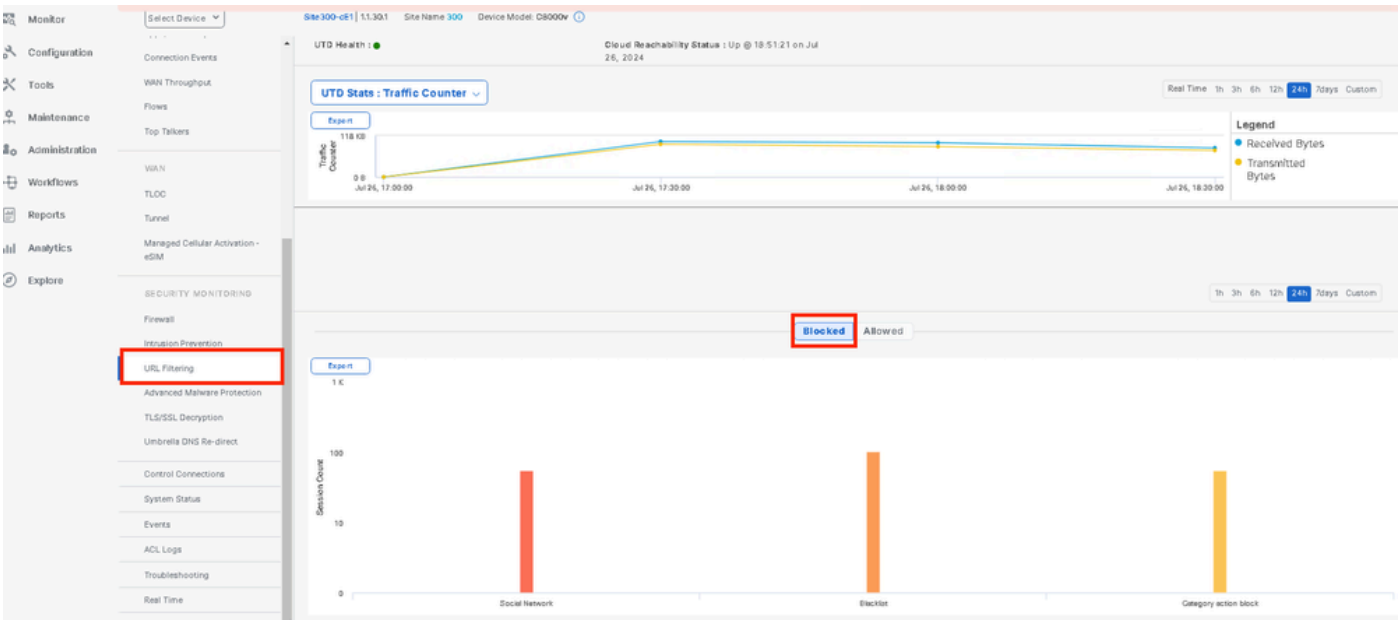
So überwachen Sie die URLs, die auf einem Cisco IOS XE Catalyst SD-WAN-Gerät blockiert oder zugelassen werden:

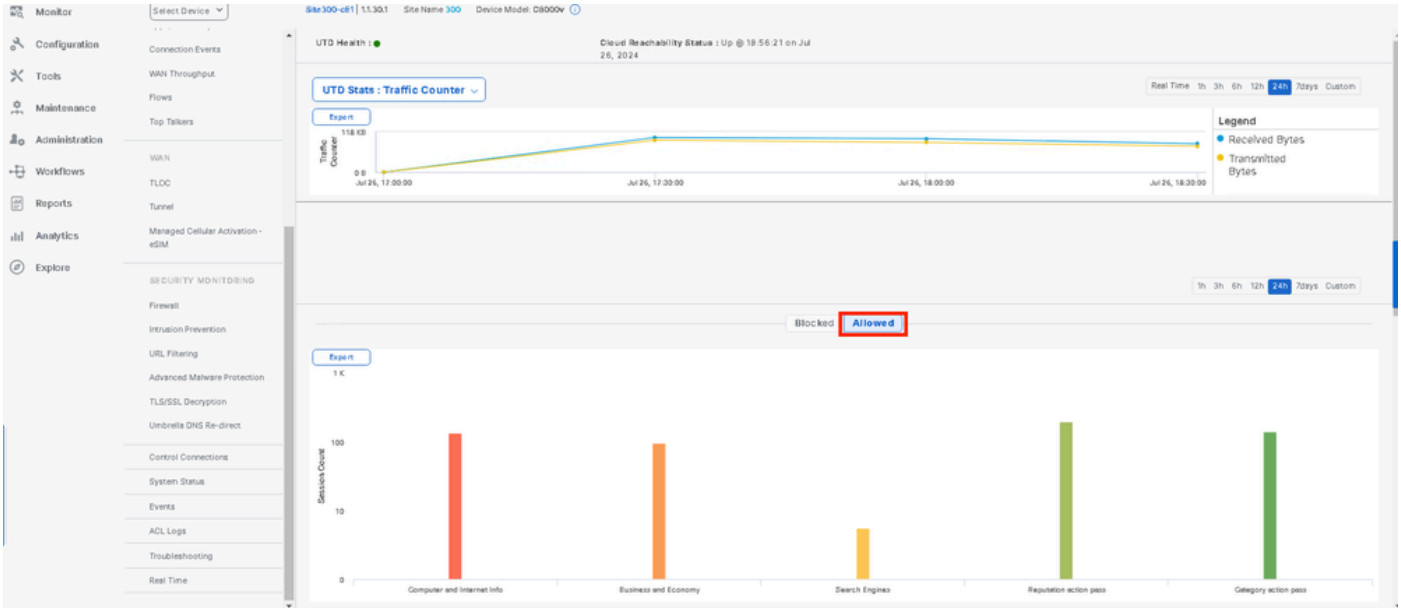
1. Wählen Sie imCisco SD-WAN Manager-Menü Überwachen > Geräte > Gerät auswählen aus.



2. Klicken Sie im linken Bereich unter Sicherheitsüberwachung auf URL-Filterung. Die URL-Filterungsinformationen werden im rechten Bereich angezeigt.

- Klicken Sie auf Blockiert. Die Sitzungsanzahl für eine gesperrte URL wird angezeigt.
- Klicken Sie auf Zulässig. Die Sitzungsanzahl für zulässige URLs wird angezeigt.





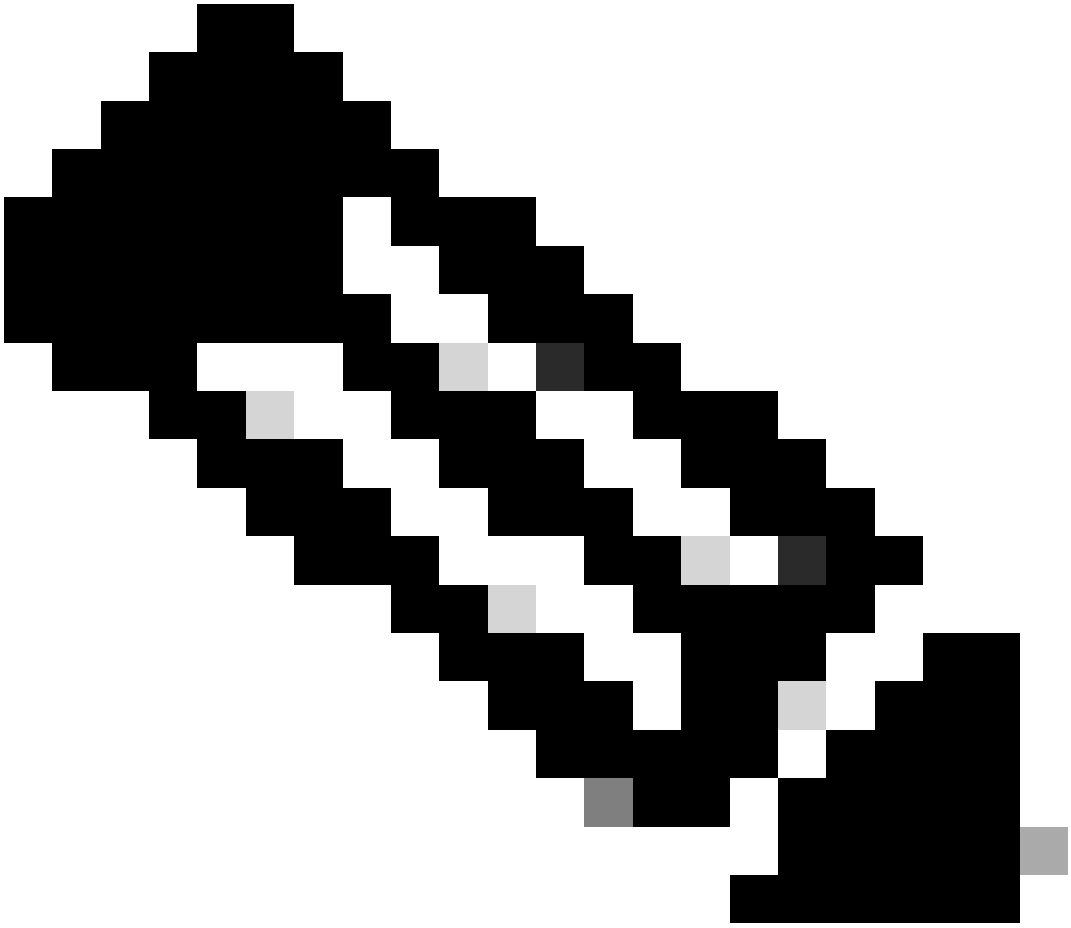
Fehlerbehebung

Überprüfen Sie, ob die unterstützte UTD-Version installiert ist:

<#root>

```
Site300-cE1#show utd engine standard version
UTD Virtual-service Name: utd
IOS-XE Recommended UTD Version: 1.0.2_SV3.1.67.0_XE17.14
IOS-XE Supported UTD Regex: ^1\.0\.([0-9]+)_SV(.*)_XE17.14$
UTD Installed Version:
```

1.0.2_SV3.1.67.0_XE17.14 <<<<<<<<<<<<<<<<



Hinweis: Die installierte UTD-Version darf nicht den Status UNSUPPORTED aufweisen.

Überprüfen Sie, ob UTD den Status "running" aufweist.

```
Site300-cE1#show app-hosting list
App id                                   State
---------------------------------------------------------
utd                                      RUNNING
```

Validierung des UTD-Heidestatus ist GRÜN.

<#root>

```
Site300-cE1#show utd engine standard status
Engine version       : 1.0.2_SV3.1.67.0_XE17.14
Profile              : Cloud-Low
```

```
System memory        :
              Usage  : 11.70 %
              Status : Green
Number of engines    : 1

Engine        Running    Health     Reason
======================================================
Engine(#1):
```

Yes   Green   None

```
======================================================
Overall system status: Green
Signature update status:
=========================
Current signature package version: 29.0.c
Last update status: None
Last successful update time: None
Last failed update time: None
Last failed update reason: None
Next update scheduled at: None
Current status: Idle
```

Überprüfen Sie, ob die URL-Filterungsfunktion aktiviert ist.

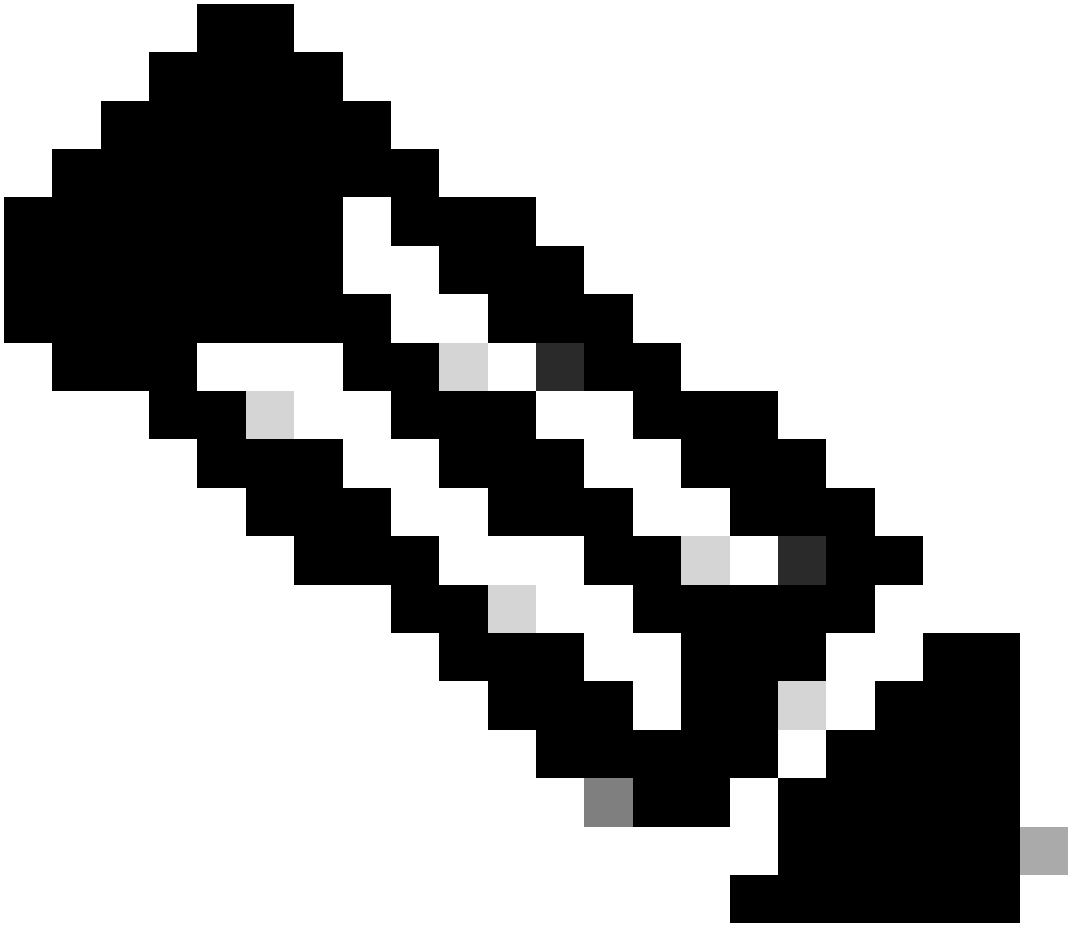
<#root>

```
Site300-cE1#show platform hardware qfp active feature utd config
Global configuration
  NAT64: disabled
  Drop pkts: disabled
  Multi-tenancy: enabled
  Data plane initialized: yes
  TLS Decryption Policy: disabled
  Divert controller mode: enabled
  Unified Policy mode: disabled
  SN threads: 12

  CFT inst_id 0 feat id 4 fo id 4 chunk id 19

  Max flows: 165000
  SN Health: channel: Threat Defense : Green
  SN Health: channel: Service : Down

  Flow-logging Information:
  ------------------------
   State                  : disabled



  Context Id: 3, Name: 3 : 12

   Ctx Flags: (0xc50001)
        Engine: Standard
        State            : Enabled
        SN Redirect Mode : Fail-open, Divert
        Threat-inspection: Not Enabled
```

```
        Domain Filtering : Not Enabled

URL Filtering    : Enabled

        File Inspection  : Not Enabled
        All Interfaces   : Enabled
```

Um die URL-Filterungsprotokolle anzuzeigen, führen Sie den Befehl show utd engine standard logging events url-filter aus.

```
Site300-cE1#show utd engine standard logging events url-filtering
2024/07/24-20:36:58.833237 PDT [**] [Hostname: site300-ce1] [**] [System_IP: x.x.x.x] [**] [Instance_ID
2024/07/24-20:37:59.000400 PDT [**] [Hostname: site300-ce1] [**] [System_IP: x.x.x.x] [**] [Instance_ID
2024/07/24-20:37:59.030787 PDT [**] [Hostname: site300-ce1] [**] [System_IP: x.x.x.x] [**] [Instance_ID
2024/07/24-20:38:59.311304 PDT [**] [Hostname: site300-ce1] [**] [System_IP: x.x.x.x] [**] [Instance_ID
2024/07/24-20:38:59.343273 PDT [**] [Hostname: site300-ce1] [**] [System_IP: x.x.x.x] [**] [Instance_ID
```



Hinweis: Führen Sie den Befehl clear utd engine standard logging events aus, um alte Ereignisse zu löschen.

Ein-/Ausgangspakete in UTD-Container prüfen, Suche verzögern.

```
Site300-cE1#show utd engine standard statistics url-filtering vrf name 12 internal

UTM Preprocessor URLF Statistics
--------------------------------
URL Filter Requests Sent:                  50
URL Filter Response Received:              50
blocklist Hit Count:                       27
Allowlist Hit Count:                       0
Reputation Lookup Count:                   50
Reputation Action Block:                   0
Reputation Action Pass:                    50
Reputation Action Default Pass:            0
Reputation Action Default Block:           0
Reputation Score None:                     0
```

```
Reputation Score Out of Range:              0
Category Lookup Count:                      50
Category Action Block:                      15
Category Action Pass:                       35
Category Action Default Pass:               0
Category Action Default Block:              0
Category None:                              0
Category Out of Range:                      0

UTM Preprocessor URLF Internal Statistics
-----------------------------------------
Total Packets Received:                     1335
SSL Packet Count:                           56
HTTP Header Count:                          22
Action Drop Flow:                           69
Action Reset Session:                       0
Action Block:                               42
Action Pass:                                503
Action Offload Session:                     0
Invalid Action:                             0
No UTM Tenant Persona:                      0
No UTM Tenant Config:                       0
URL Lookup Response Late:                   150
URL Lookup Response Very Late:              21
URL Lookup Response Extremely Late:         0
URL Lookup Response Status Invalid:         0
Response Does Not Match Session:            0
No Response When Freeing Session:           0
First Packet Not From Initiator:            0
No HTTP Header:                             0
Invalid Action:                             0
Send Error Fail Open Count:                 0
Send Error Fail Close Count:                0
Lookup Error Fail Open Count:               0
Lookup Error Fail Close Count:              0
Lookup Timeout Fail Open Count:             0
Lookup Timeout Fail Close Count:            0
```

Zugehörige Informationen

- Cisco Catalyst SD-WAN - Sicherheitskonfigurationsleitfaden
- Installation des virtuellen UTD Security Images auf cEdge-Routern
- Fehlerbehebung bei Datenpfadbehandlung durch UTD und URL-Filterung

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.