

URL-Filterung konfigurieren und überprüfen

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[Konfigurieren von Komponenten für eine URL-Filterrichtlinie](#)

[Erstellen von URL-Interessenslisten](#)

[Erstellen von Sicherheitsrichtlinien](#)

[Anwenden einer Sicherheitsrichtlinie auf ein Gerät](#)

[URL-Filterung ändern](#)

[URL-Filterung löschen](#)

[Überprüfung](#)

[Überwachen der URL-Filterung über die vManage-GUI](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

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

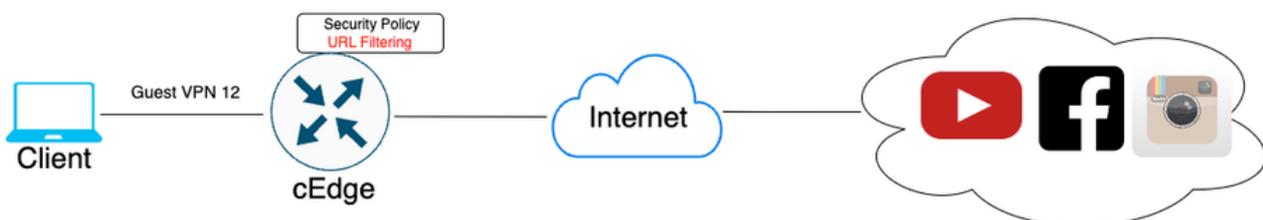
Dieses Dokument basiert auf den folgenden Software- und Hardwareversionen:

- 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

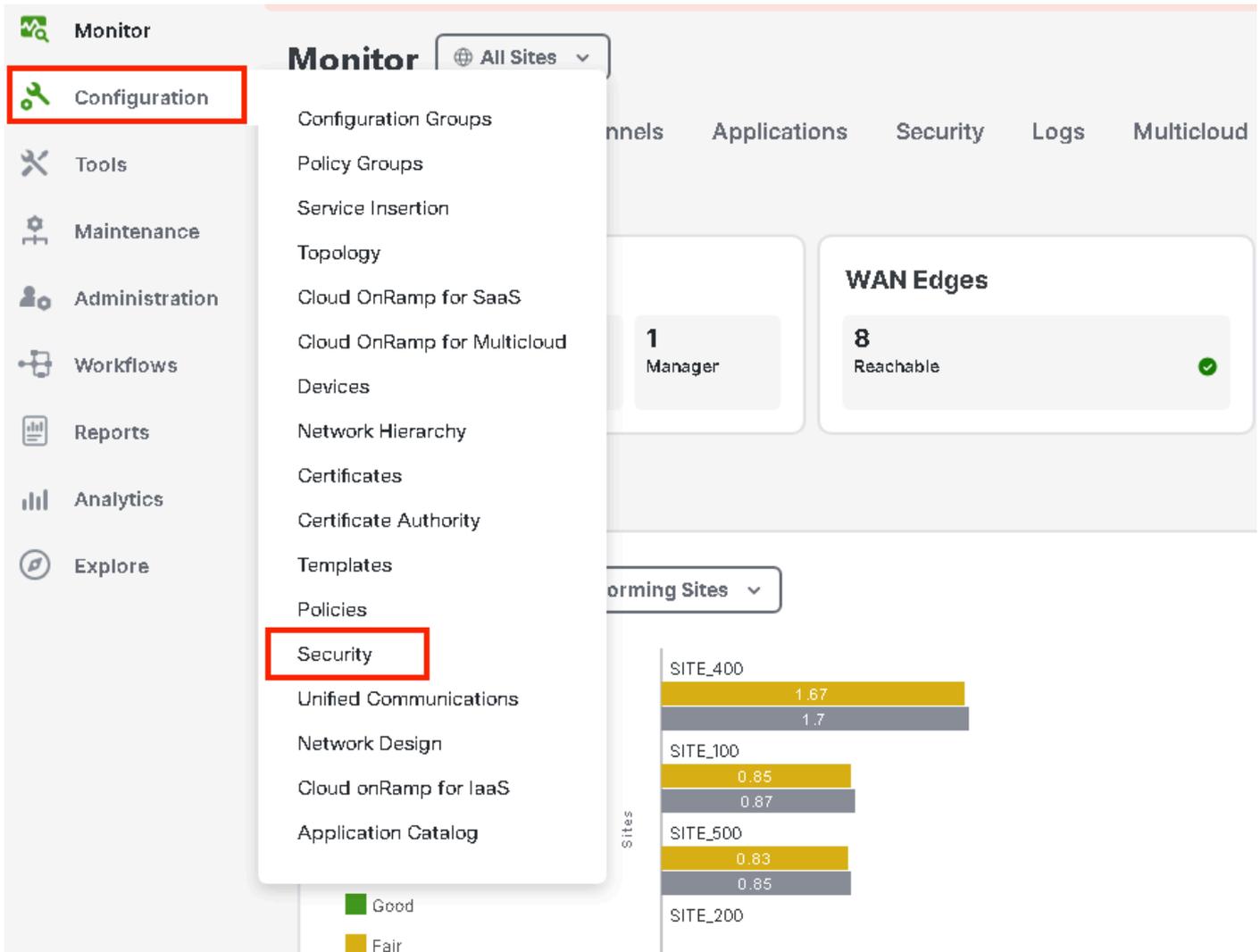
In diesem Artikel wird erläutert, wie die URL-Filterung so konfiguriert wird, dass bestimmter Client-HTTPS-Datenverkehr basierend auf Kategorie, Reputation oder nach Domänenblock-/Zulassungslisten blockiert bzw. zugelassen wird. Dabei gelten folgende Beispielanforderungen:

- 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).

Select a list type on the left and start creating your groups of interest

Application

Data Prefix

Domain

Signatures

Allow URL Lists

Block URL Lists

Zones

Port

Protocol

Rule Set

Geo Location

Object Group

Identity

New Allow URL List

Name	Entries	Reference Count	Update
No data available			

- 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.

Select a list type on the left and start creating your groups of interest

Application

Data Prefix

Domain

Signatures

Allow URL Lists

Block URL Lists

Zones

Port

Protocol

Rule Set

Geo Location

Object Group

New Allow URL List

Allow URL List Name*

Guest_Allow

Add Allow URL *

www.google.com, www.yahoo.com

Import

Add

Cancel



Hinweis: Sie können ein reguläres Muster für den Domännennamen 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).

Select a list type on the left and start creating your groups of interest

Application

Data Prefix

Domain

Signatures

Allow URL Lists

Block URL Lists

Zones

Port

Protocol

Rule Set

Geo Location

Object Group

Identity

New Block URL List

Name	Entries	Reference Count
------	---------	-----------------

- 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.

New Block URL List

Block URL List Name*

Guest_Block

Add Block URL

www.youtube.com,www.facebook.com,instagram.com

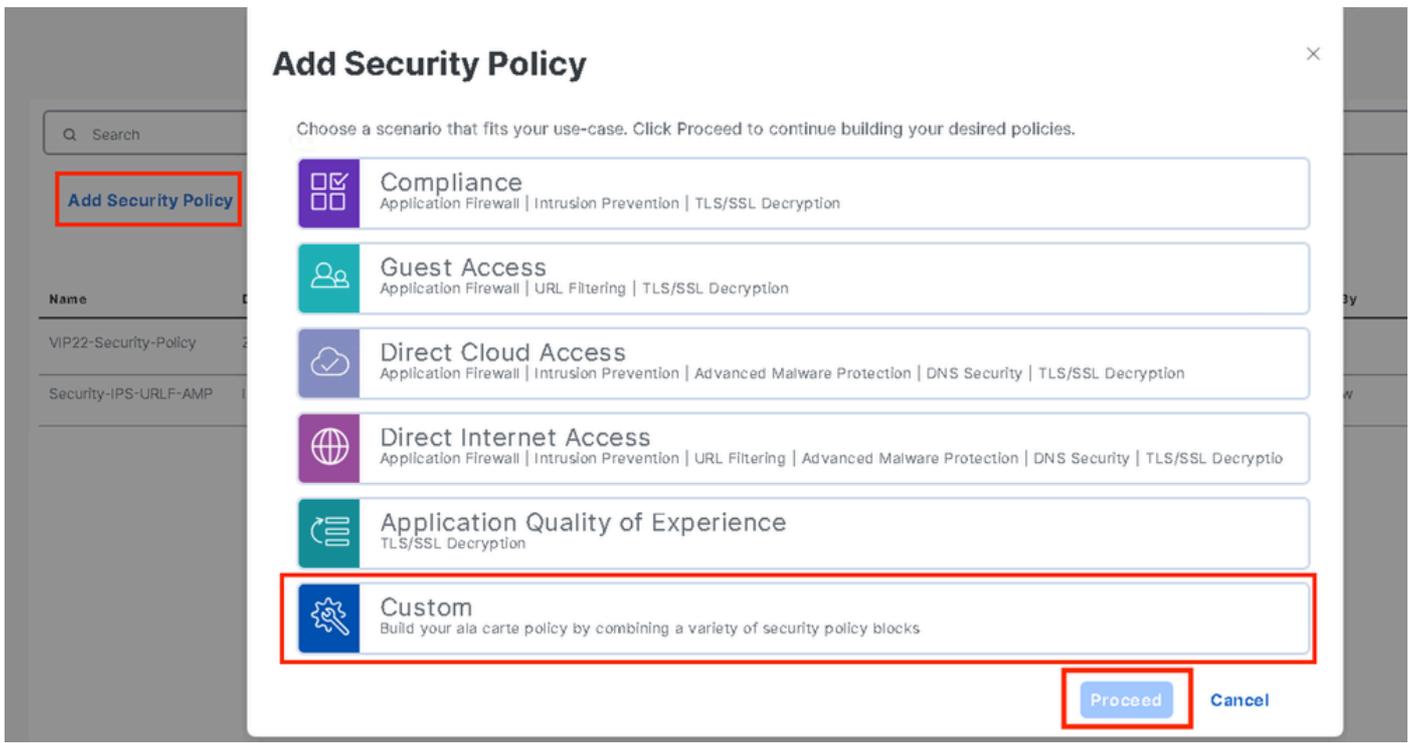
Import

Add Cancel

Erstellen von Sicherheitsrichtlinien

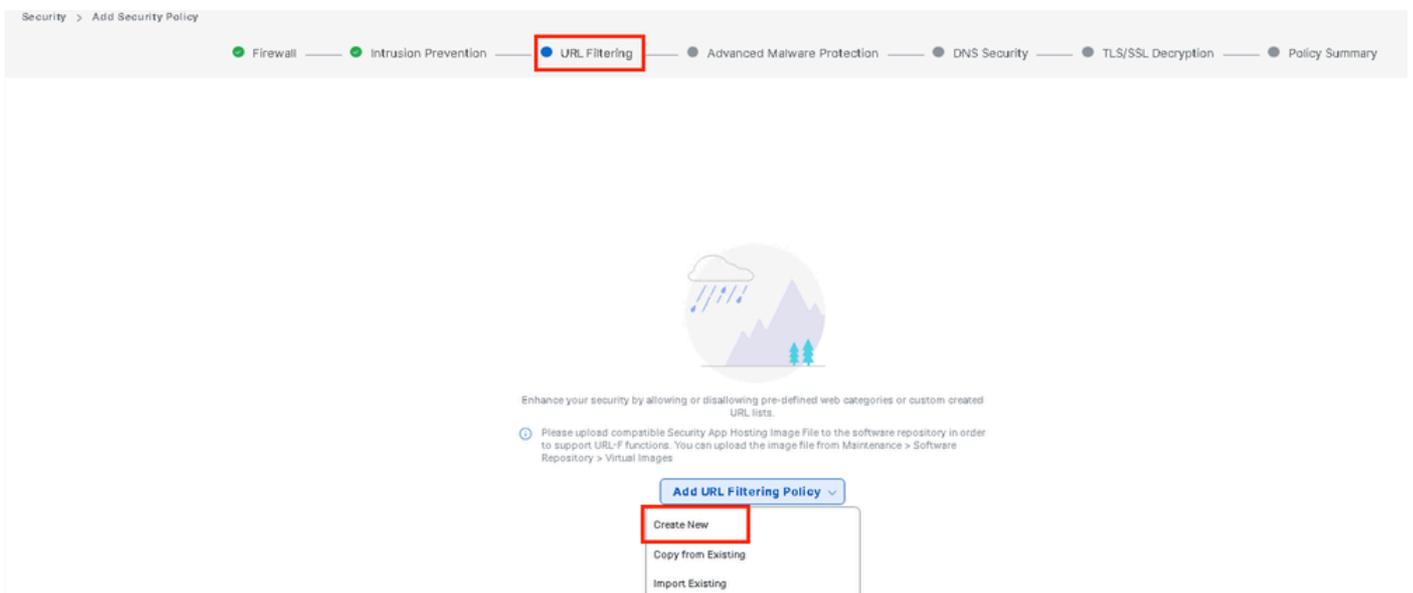
2. Navigieren Sie im Menü Cisco SD-WAN Manager zu Konfiguration > Sicherheit Klicken Sie auf Neue Sicherheitsrichtlinie hinzufügen. Der Assistent zum Hinzufügen von Sicherheitsrichtlinien

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.

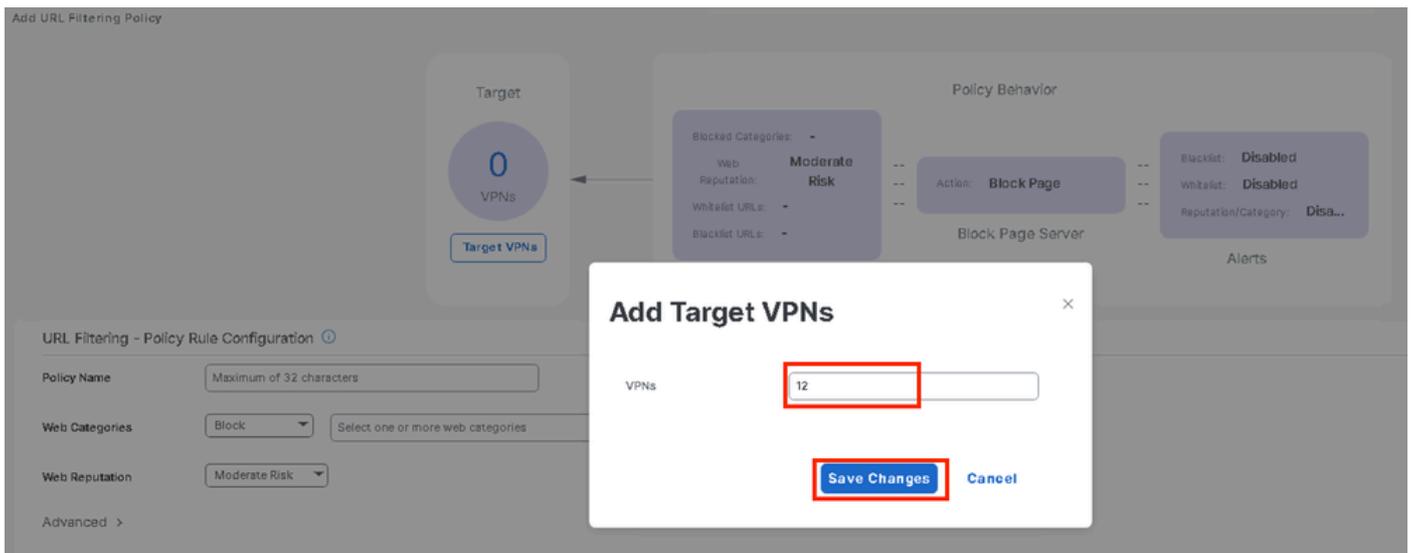


Hinweis: Wählen Sie unter Sicherheitsrichtlinie hinzufügen ein Szenario aus, das die URL-Filterung unterstützt (Gastzugriff, direkter Internetzugriff oder benutzerdefiniert).

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 "Sperrern" 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.

Add URL Filtering Policy

URL Filtering - Policy Rule Configuration

Policy Name: Guest_Access

Web Categories: Block (dropdown) | shocoin x | games x | oambino x | hackno x | abused-drugs

Web Reputation: Moderate Risk (dropdown)

Advanced >

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.

Advanced ▾

Whitelist URL List

Select a whitelist url list

Search

Guest_Allow

www\.google\.com
www\.yahoo\.com

New Allow URL List

Block Page Server

Block Page Content

Default Content Header

Content Body

Blacklist URL List

Select a blacklist url list

Search

Guest_Block

www\.youtube\.com
www\.facebook\.com
instagram.com

New Block URL List

Block Page Server

Block Page Content

Default Content Header

Content Body

Redirect URL ⓘ

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

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

URL Filtering - Policy Rule Configuration ⓘ

Advanced ▾

Whitelist URL List

Blacklist URL List

Block Page Server

Block Page Content

Default Content Header

Content Body

Redirect URL ⓘ

Alerts and Logs ⓘ

Alerts Blacklist Whitelist Reputation/Category

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.

● Firewall — ● Intrusion Prevention — ● URL Filtering — ● Advanced Malware Protection — ● DNS Security — ● TLS/SSL Decryption — ● Policy Summary

Provide a name and description for your security master policy and configure additional security settings. Click Save Policy to save the security master policy configuration.

Security Policy Name

Security Policy Description

Additional Policy Settings

Intrusion Prevention and/or URL Filtering and/or Advanced Malware Protection

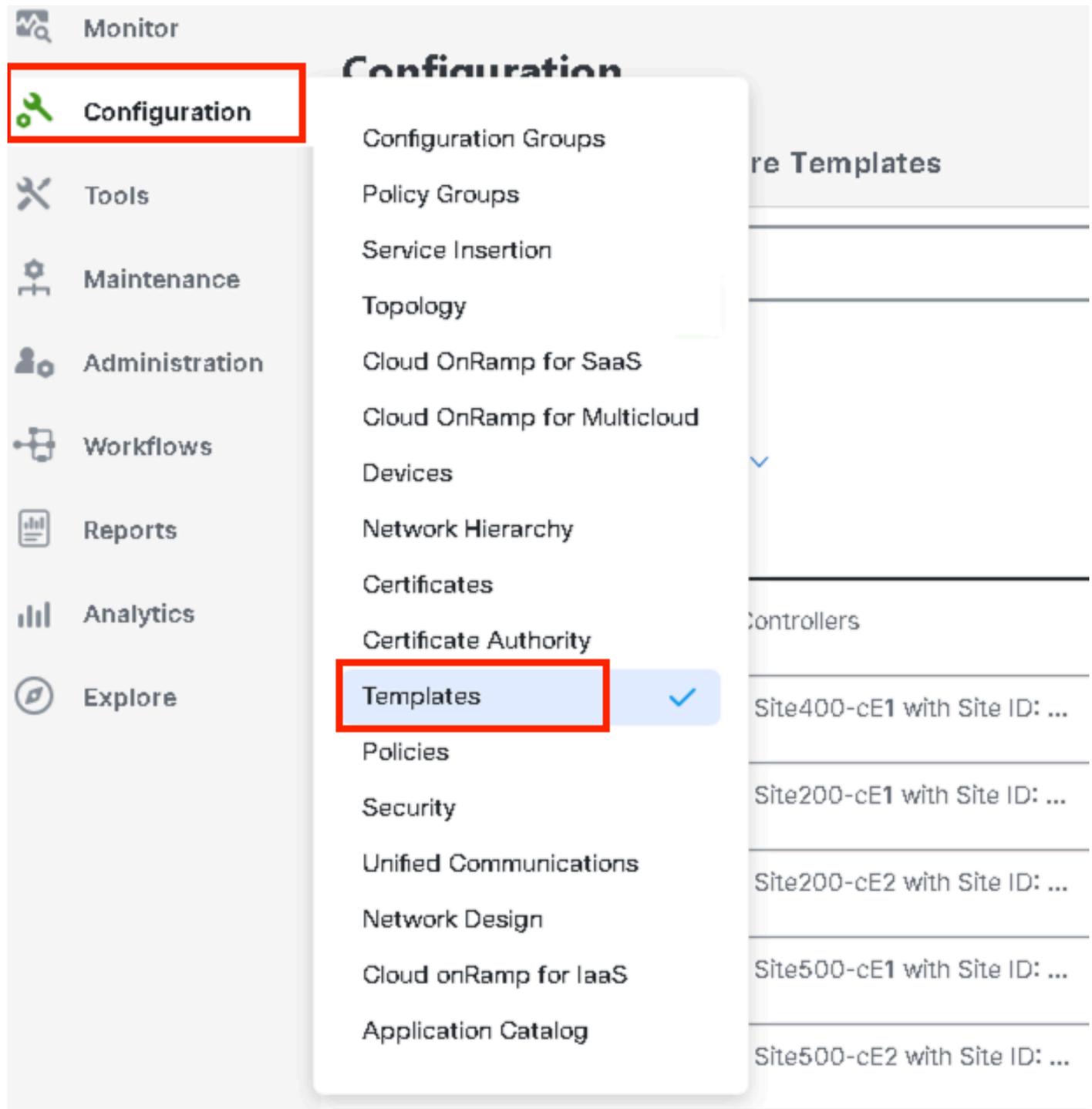
External Syslog Server VPN ⓘ Server IP

Failure Mode

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.

Configuration

Device Templates Feature Templates

Q 300 x Search

Create Template v

Template Type Non-Default v

Total Rows: 1 of 9

Name	Description	Type	Device Model ...	Device Role	Feature Templates	Draft Mode	Devices Attached	Updated By	Last Updated	common.TemplateStatus
fc862ea4-e57e-4616-8bc7-88d2d2978...	Device template of Site300-cE1 w...	Feature	C8000v	SDWAN Edge	25	Disabled	1	admin	24 Jul 2024 11...	In Sync

- Edit
- View
- Delete
- Copy
- Enable Draft Mode
- Attach Devices
- Detach Devices
- Export CSV
- Change Device Values

Klicken Sie auf Zusätzliche Vorlagen.

Configuration

Device Templates Feature Templates

Device Model* C8000v

Device Role* SDWAN Edge

Template Name* fc862ea4-e57e-4616-8bc7-88d2d2978089

Description* Device template of Site300-cE1 with Site ID: 300

Basic Information Transport & Management VPN Service VPN Cellular **Additional Templates** Switchport

- 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.

Policy VIP07_DPI_Visibility v

Probes Choose... v

Tenant Choose... v

Security Policy Guest_URL_Policy v

Container Profile * Factory_Default_UTD_Template v ⓘ

Switch Port + Switch Port v

Update Cancel

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.

The screenshot displays the vManage configuration interface for a device template. At the top, the 'Device Template' section shows 'fcB62ea4-e57e-4616-8...' and 'Total 1'. The 'Config Diff' button is highlighted in red. The 'Side by Side Diff' button is also highlighted in red. The 'Intent' button is visible on the right.

The 'Device list (Total: 1 devices)' section shows a search filter and a list of devices. One device is highlighted in blue: 'CBK-C18B1FE2-C89F-A311-DEA7-452A978B089A' with IP '10.1.1.130.1'. A 'Configure Devi...' button is below it.

The 'Local Configuration vs. New Configuration' section shows a table of configuration items:

Line	Local Configuration	New Configuration
1	1	system
2	2	ztp-status in-progress
3	3	device-model vedge-C8000V
4	4	gps-location latitude -23.60911
5	5	gps-location longitude -46.69768
6	6	system-ip 1.1.30.1
7	7	overlay-id 1
8	8	site-id 300
9	9	no transport-gateway enable
10	10	port-offset 0
11	11	control-session-pps 300
12	12	admin-tech-on-failure

The 'Side by Side Diff' view shows a comparison of configurations. The right pane is highlighted in green and contains the following configuration snippets:

```
389 parameter-map type regex Guest_Allow-wl_
390 pattern www.google.com
391 pattern www.yahoo.com
392 !
393 parameter-map type regex Guest_Block-bl_
394 pattern instagram.com
395 pattern www.facebook.com
396 pattern www.youtube.com
397 !
```

The bottom pane shows a more detailed configuration snippet, also highlighted in green:

```
444 web-filter block page profile block-Guest_Access
445 text Access to the requested page has been denied. Please contact your Network
Administrator
446 exit
447 web-filter url profile Guest_Access
448 alert blacklist categories-reputation whitelist
449 blacklist
450 parameter-map regex Guest_Block-bl_
451 exit
452 categories block
453 abused-drugs
454 gambling
455 games
456 hacking
457 shopping
458 exit
459 block page-profile block-Guest_Access
460 log level error
461 reputation
462 block-threshold moderate-risk
463 exit
464 whitelist
465 parameter-map regex Guest_Allow-wl_
466 exit
467 exit
468 utd global
469 exit
470 policy utd-policy-vrf-12
471 all-interfaces
472 vrf 12
473 web-filter url profile Guest_Access
474 exit
```

At the bottom, the 'Configure Devices' button is highlighted in red, along with 'Back' and 'Cancel' buttons.

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

Push Feature Template Configuration | ● Validation success

Total Task: 1 | Success: 1

Device Group (1)

Q Search Table

Status	Message	Chassis Number
● Success	Template successfully atta...	C8K-C16B1FE2-C89F-A311-DEA7-46...

View Logs

Host: Site300-cE1(1.1.30.1)
 Site ID: 300
 Device: C8000v
 Model:

[26-Jul-2024 13:55:55 PDT] Configuring device with feature template: fc862ee4-e57e-4616-8bc7-88d2d2978089

[26-Jul-2024 13:55:56 PDT] Checking and creating device in Manager

[26-Jul-2024 13:55:57 PDT] Generating configuration from template

[26-Jul-2024 13:56:06 PDT] Device is online

[26-Jul-2024 13:56:06 PDT] Updating device configuration in Manager

[26-Jul-2024 13:56:06 PDT] Sending configuration to device

[26-Jul-2024 13:56:12 PDT] Successfully notified device to pull configuration

[26-Jul-2024 13:56:14 PDT] Device has pulled the configuration

[26-Jul-2024 13:56:21 PDT] Device: Configured IOX

[26-Jul-2024 13:56:35 PDT] Device: Started IOX

[26-Jul-2024 13:56:58 PDT] Device: Successfully downloaded package for appid utd

[26-Jul-2024 13:57:40 PDT] Device: Successfully installed appid utd

[26-Jul-2024 13:59:07 PDT] Device: Verified appid utd in running state

[26-Jul-2024 13:59:07 PDT] Device: Successfully verified appids: utd

[26-Jul-2024 13:59:08 PDT] Device: Config applied successfully

[26-Jul-2024 13:59:08 PDT] Template successfully attached to device

URL-Filterung ändern

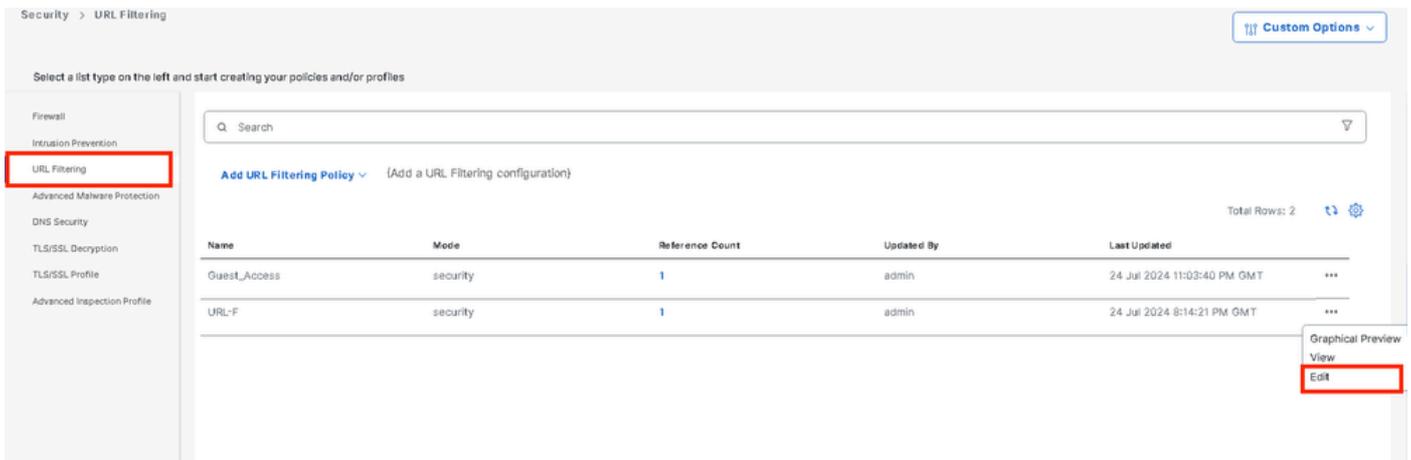
Um eine URL-Filterungsrichtlinie zu ändern, gehen Sie wie folgt vor:

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.

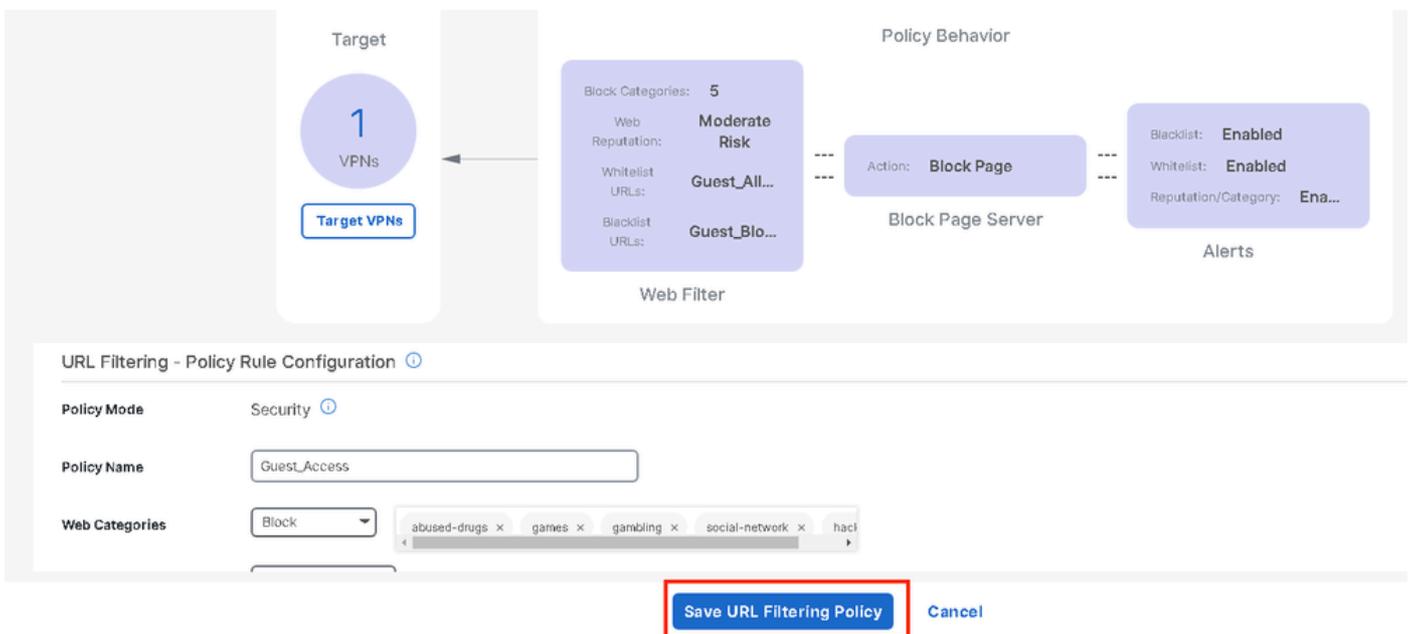
The screenshot shows the Cisco SD-WAN Manager interface. On the left is a navigation menu with 'Configuration' selected. The main area displays a table of security policies. A dropdown menu is open, showing 'Policies/Profiles' as the selected option, highlighted with a red box. Below the table, there are buttons for 'Add Security Policy' and 'Add Unified Security Policy'. The table has columns for Name, Description, Use Case, Policy Mode, Devices Attached, Device Templates/Config Groups, Updated By, and Last Updated.

Name	Description	Use Case	Policy Mode	Devices Attached	Device Templates/Config Groups	Updated By	Last Updated
VIP22-Security-Policy	ZBFW policy for DIA	Custom	security	0	0	admin	12 Apr 2024 9:32:39 PM

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.

Name	Description	Use Case	Policy Mode	Devices Attached	DeviceTemplates/ConfigGroups	Updated By	Last Updated
VIP22-Security-Policy	ZBFW policy for DIA	Custom	security	0	0	admin	12 Apr 2024 9:32:39 PM ...
Security-IPS-URLF-AMP	IPS, URL-F, AMP	Custom	security	0	0	admin	24 Jul 2024 8:49:01 PM ...
Guest_URL_Policy	Guest_URL_Policy	Custom	security	1	1	admin	24 Jul 2024 11:03:25 PM ...

- View
- Preview
- Edit
- Delete

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.

Firewall | Intrusion Prevention | **URL-Filterung** | Advanced Malware Protection | DNS Security | TLS/SSL Decryption | Policy Summary

Q Search

Total Rows: 1

Name	Type	Reference Count	Updated By	Last Updated
Guest_Access	urlfiltering	1	admin	24 Jul 2024 11:03:40 PM GMT

Graphical Preview
View
Edit
Detach

Preview **Save Policy Changes** Cancel

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.

The network is out of compliance due to licensing, please [click here](#) for more actions.

- Monitor
- Configuration
- Tools
- Maintenance
- Administration
- Workflows
- Reports
- Analytics
- Explore

Security

- Lists
- Policies/Profiles**
- Umbrella Registration
- Threat Grid API Key

Q Search

[Add Security Policy](#) [Add Unified Security Policy](#)

Total Rows: 3

Name	Description	Use Case	Policy Mode	Devices Attached	DeviceTemplates/ConfigGroups	Updated By	Last Updated
VIP22-Security-Policy	ZBFW policy for DIA	Custom	security	0	0	admin	12 Apr 2024 9:32:39 ...
Security-IPS-URLF-A...	IPS, URL-F, AMP	Custom	security	0	0	admin	24 Jul 2024 8:48:01 ...
GuestURL_Policy	Guest_URL_Policy	Custom	security	1	1	admin	25 Jul 2024 4:23:52 ...

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

Klicken Sie auf OK.

Security > URL Filtering

Custom Options

Select a list type on the left and start creating your policies and/or profiles

- Firewall
- Intrusion Prevention
- URL Filtering**
- Advanced Malware Protection
- DNS Security
- TLS/SSL Decryption
- TLS/SSL Profile
- Advanced Inspection Profile

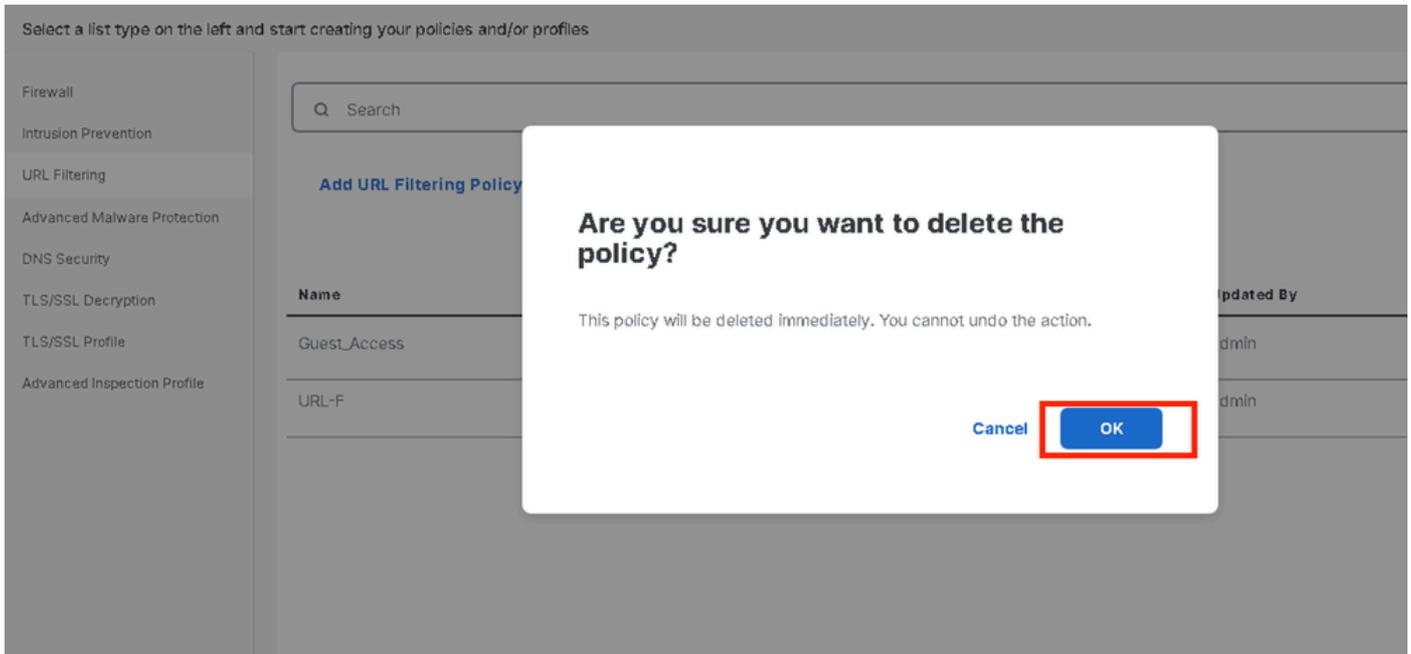
Q Search

[Add URL Filtering Policy](#) (Add a URL Filtering configuration)

Total Rows: 2

Name	Mode	Reference Count	Updated By	Last Updated
Guest_Access	security	0	admin	24 Jul 2024 11:03:40 PM GMT
URL-F	security	1	admin	24 Jul 2024 8:14:21 PM GMT

- Graphical Preview
- View
- Edit
- Delete**



Überprüfung

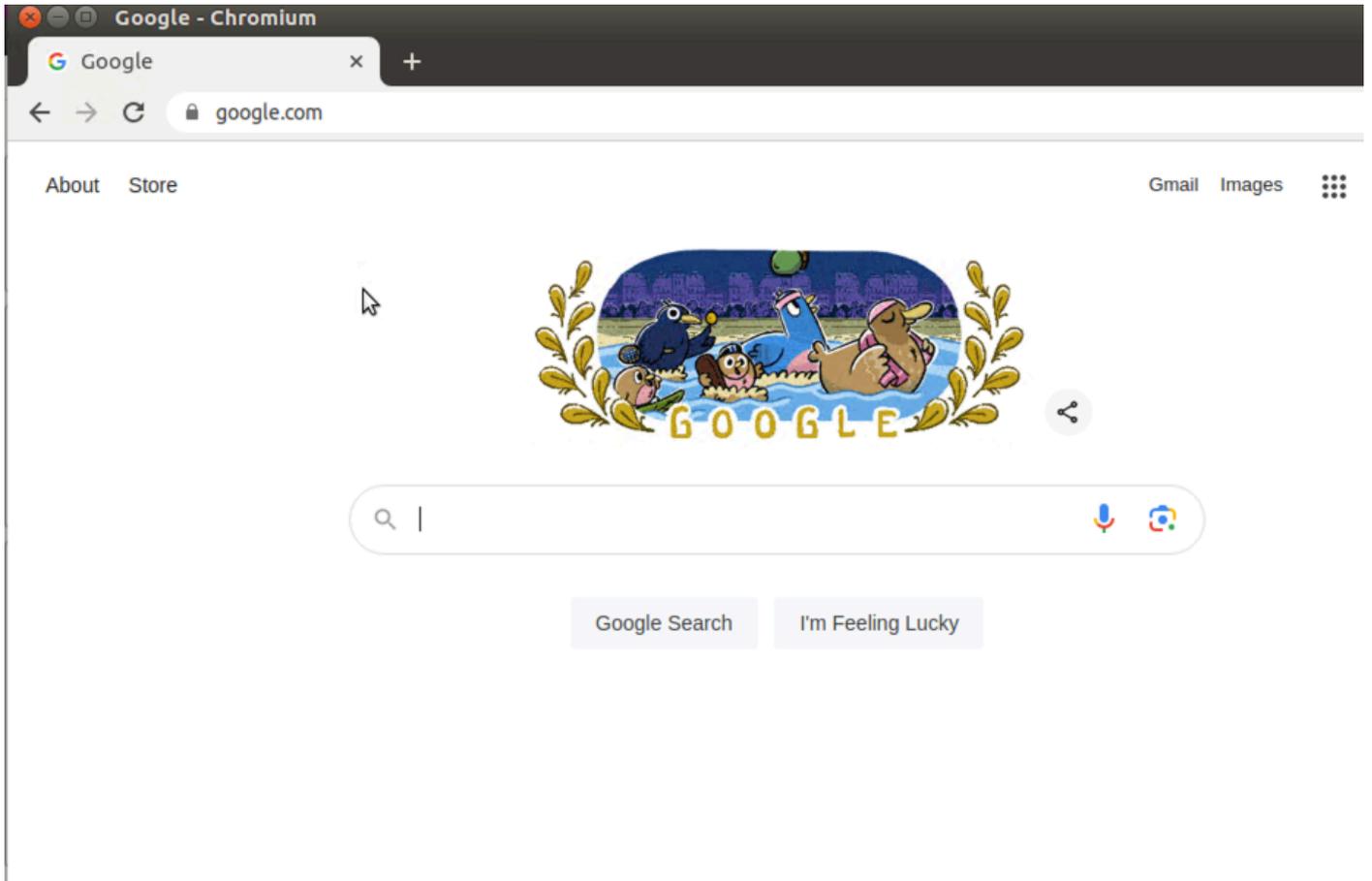
Überprüfen Sie, ob die Cisco UTD-Version installiert ist.

```
<#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

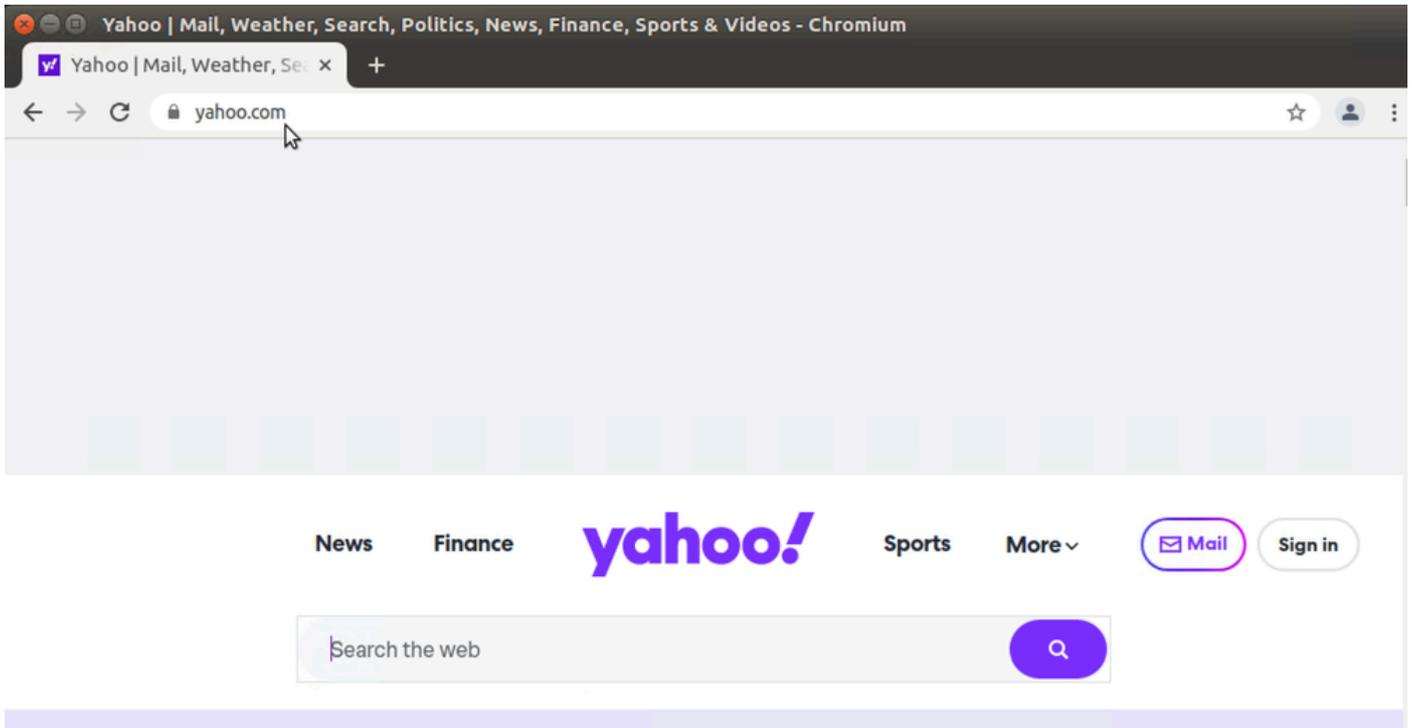
[**]

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

[**]

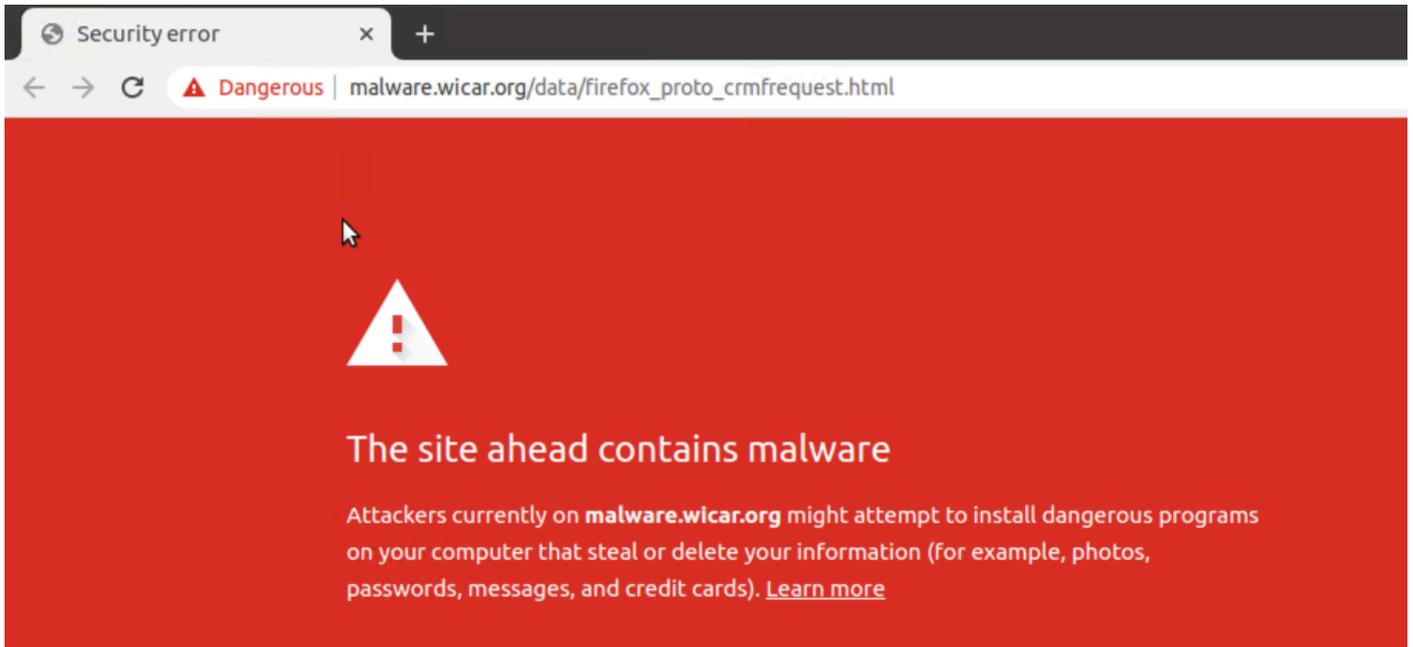
UTD WebFilter Allowlist

[**] [

URL: www.yahoo.com

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

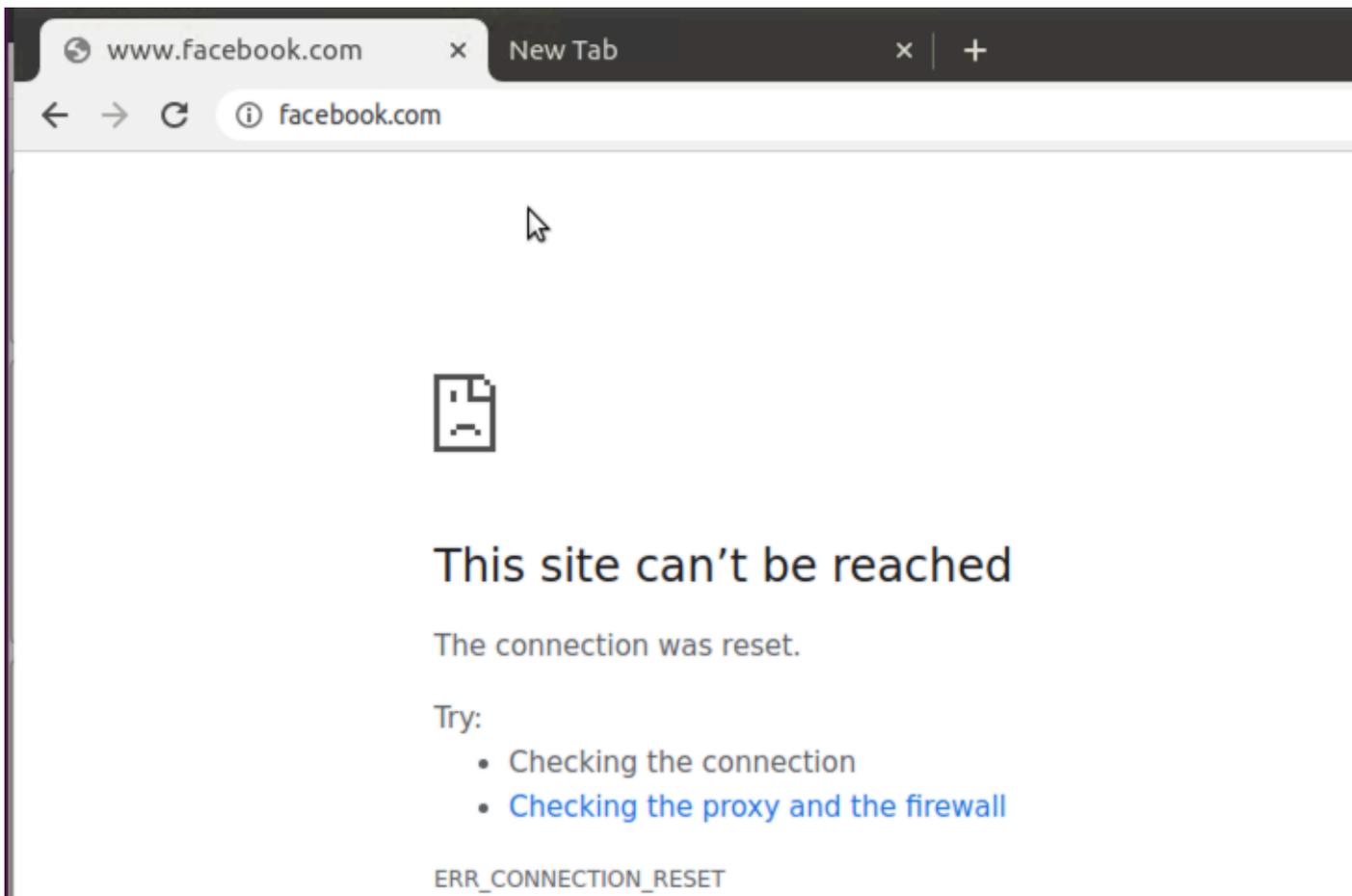
Wenn Sie auf dem Client-PC im Gast-VPN versuchen, Webseiten mit schlechten Reputationsbewertungen zu öffnen, oder wenn Sie aus einer der gesperrten Webkategorien stammen, verweigert die URL-Filterungs-Engine die HTTP-Anforderung.



<#root>

```
Site300-cE1#show utd engine standard logging events | in ma  
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 blacklist

[**] [

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

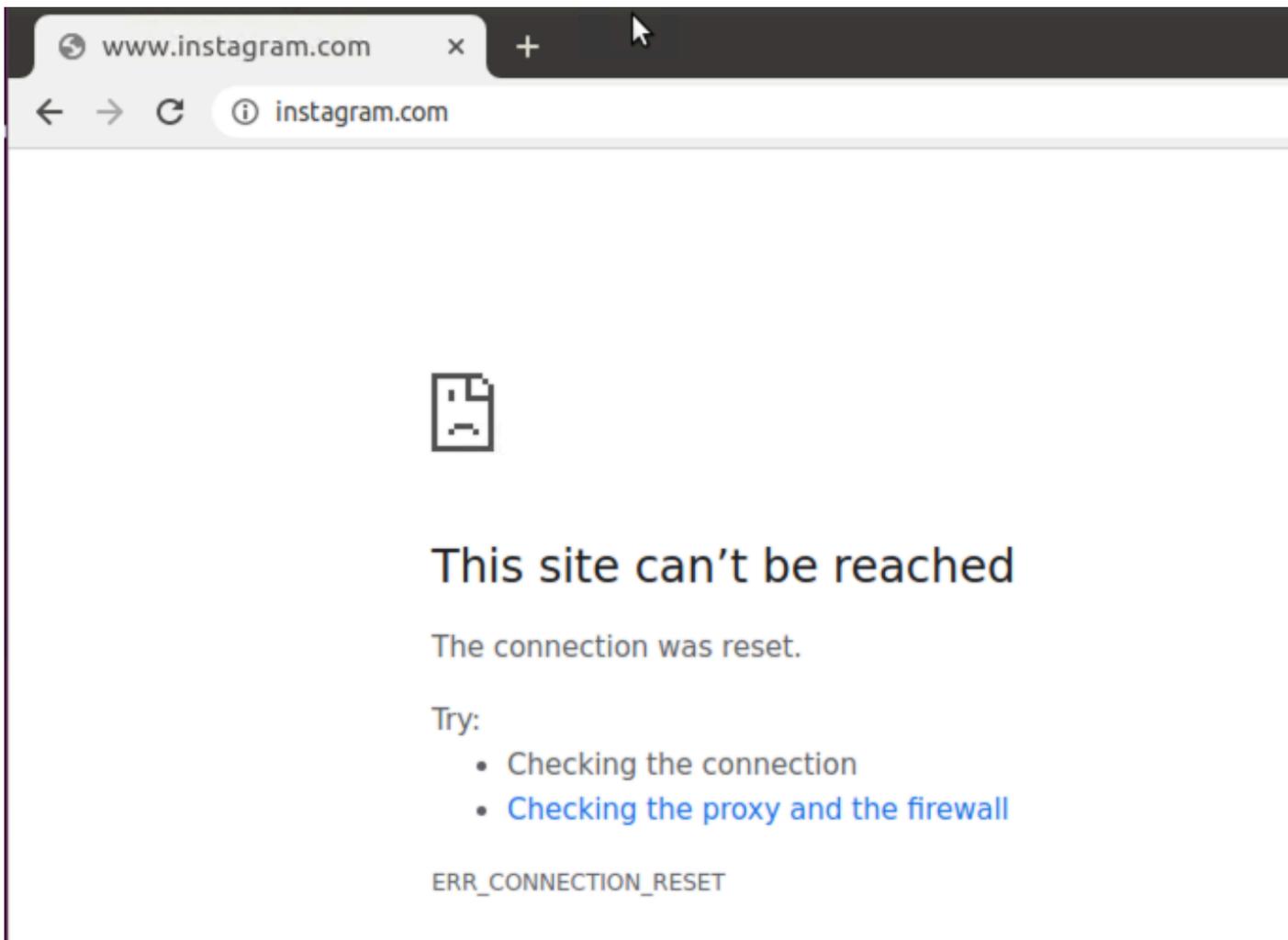
[**]

UTD WebFilter blacklist

[**] [

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 blacklist
[**] [
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 blacklist
[**] [
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

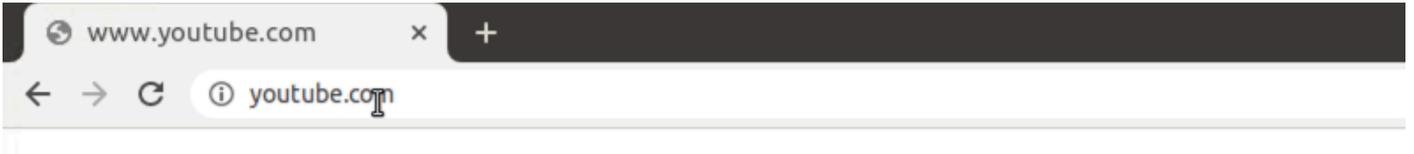
[**]

UTD WebFilter blocklist

[**] [

URL: www.instagram.com

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



This site can't be reached

The connection was reset.

Try:

- Checking the connection
- [Checking the proxy and the firewall](#)

ERR_CONNECTION_RESET

<#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 im Cisco SD-WAN Manager-Menü Überwachen > Geräte > Gerät auswählen aus.

The screenshot shows a network management interface. On the left, a sidebar menu is visible with the following items: Monitor (highlighted with a red box), Configuration, Tools, Maintenance, Administration, Workflows, Reports, Analytics, and Explore. A dropdown menu is open under 'Monitor', listing: Overview, Devices (highlighted with a red box and a blue checkmark), Tunnels, Applications, Security, VPN, Logs, Multicloud, SD-AVC Cloud Connector, and Compliance. The main content area shows a table with the following columns: Hostname, Device Model, Site Name, System IP, and Health. The table contains three rows of data:

Hostname	Device Model	Site Name	System IP	Health
vManage	Manager	SITE_1	1.1.1.1	✓
vBond	Validator	SITE_1	1.1.1.2	✓
vSmart-1	Controller	SITE_1	1.1.1.3	✓

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.

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.