

Configurazione e verifica del filtro URL

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazione dei componenti per i criteri di filtro URL](#)

[Creazione di elenchi di interessi URL](#)

[Crea criterio di protezione](#)

[Applicare un criterio di protezione a un dispositivo](#)

[Modifica filtro URL](#)

[Eliminazione del filtro URL](#)

[Verifica](#)

[Monitoraggio del filtro URL dalla GUI vManage](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come configurare e verificare il filtro URL sui router Cisco IOS-XE® usando l'interfaccia utente di Cisco Catalyst Manager.

Prerequisiti

Caricare un'immagine virtuale compatibile con il software UTD con il codice Cisco IOS-XE corrente in vManage. Per istruzioni su come installare l'immagine virtuale di sicurezza UTD sui router cEdge, consultare la sezione Informazioni correlate.

Il router Cisco Edge deve essere in modalità vManaged con il modello preallegato.

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- La sovrapposizione Cisco SD-WAN richiama la configurazione iniziale.
- Configurazione del filtro URL nell'interfaccia utente di Cisco Catalyst Manager.

Componenti usati

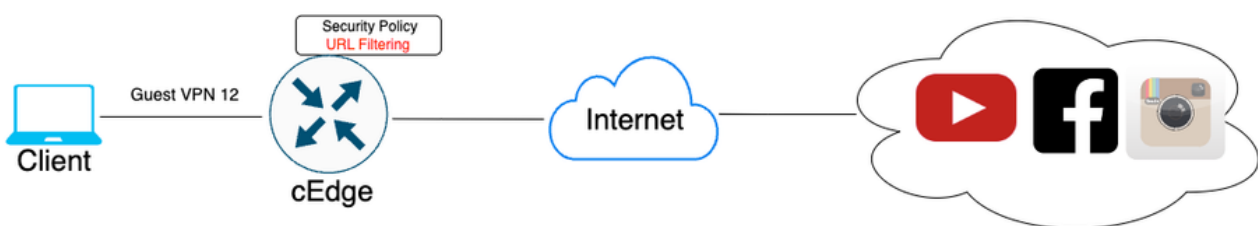
Questo documento si basa sulle seguenti versioni software e hardware:

- Cisco Catalyst SD-WAN Manager versione 20.14.1.
- Cisco Catalyst SD-WAN Controller versione 20.14.1.
- Cisco Edge Router versione 17.14.1.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Esempio di rete



Configurazione dei componenti per i criteri di filtro URL

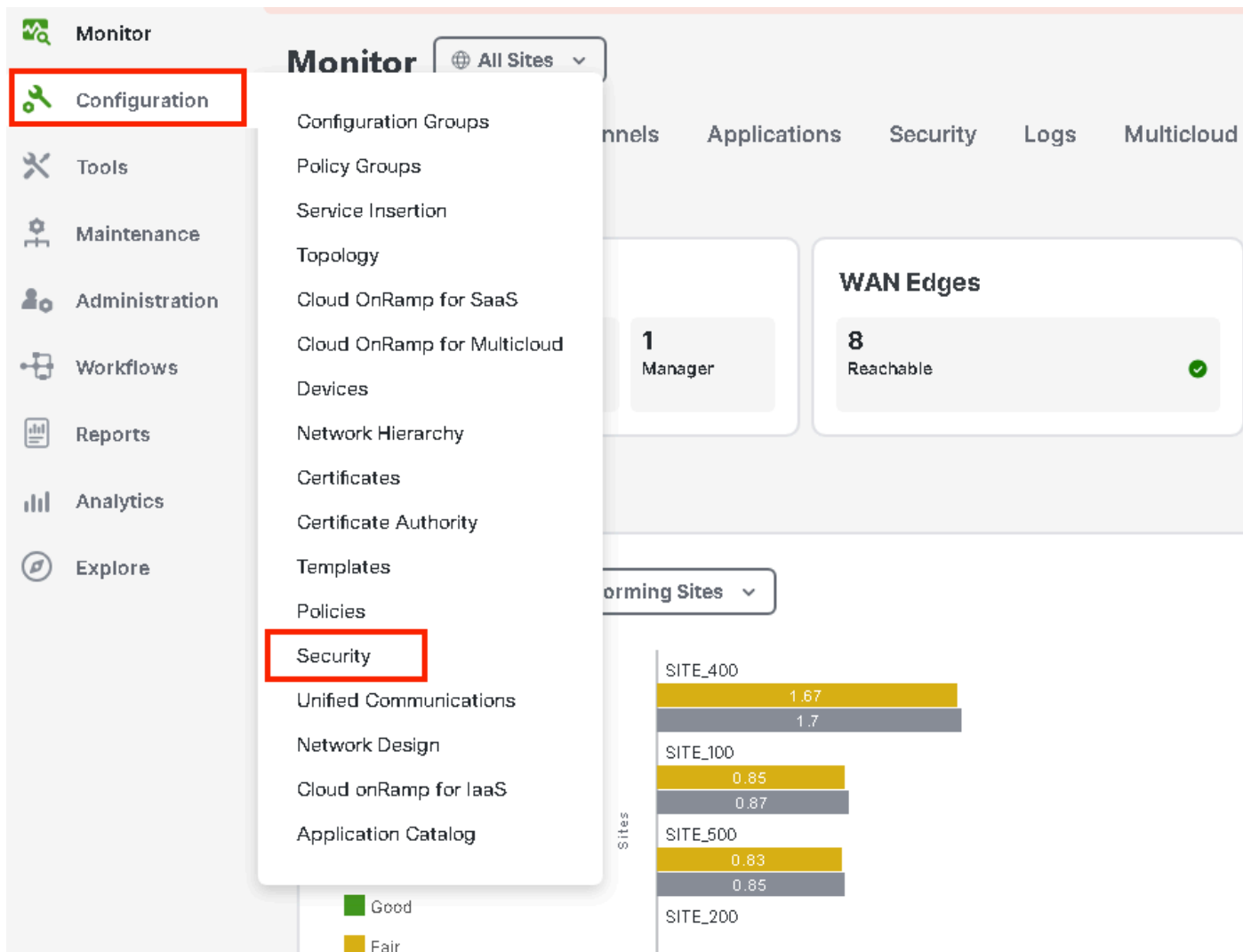
In questo articolo viene spiegato come configurare il filtro URL in modo da bloccare o consentire il traffico HTTPS di alcuni client in base alla categoria, alla reputazione o agli elenchi di domini bloccati o consentiti, a seconda dei requisiti di esempio:

- Blocca queste richieste HTTPS dai client nelle categorie Web VPN guest:
 - Giochi
 - Scommesse
 - Hacking
 - Droghe illegali
- Qualsiasi richiesta URL HTTPS a siti Web da client su VPN guest con una reputazione Web inferiore a 60 deve essere bloccata.
- Le richieste HTTP(s) ai siti Web dai client sulla VPN guest bloccano Facebook, Instagram e YouTube, consentendo al contempo l'accesso a google.com e yahoo.com.

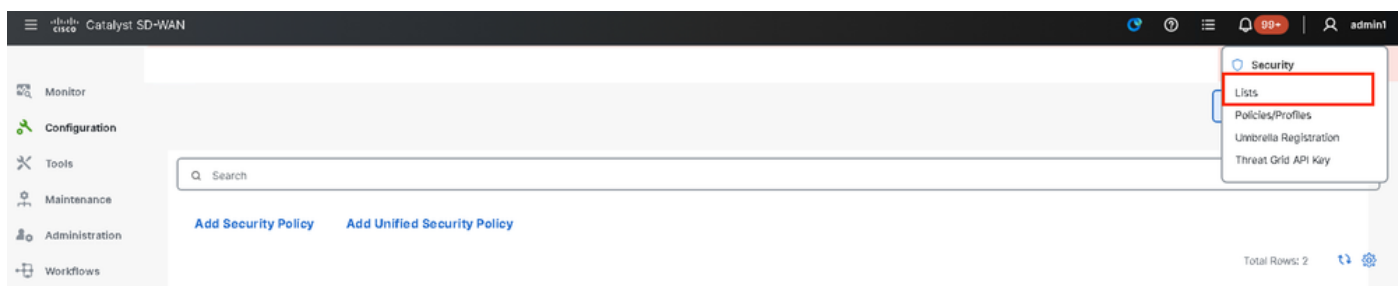
Per configurare il filtro URL:

Creazione di elenchi di interessi URL

1. Nel menu Cisco SD-WAN Manager, selezionare Configuration > Security tab nel pannello a sinistra.



Per creare o gestire Allowlist URL List o Blocklist URL List, selezionare Lists dal menu a discesa Custom Options nella parte superiore destra della pagina.



Fare clic su Consenti elenchi URL dal riquadro di sinistra e creare un nuovo elenco di URL consentiti.

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			

- Nel campo Nome elenco URL, immettere un nome elenco composto da un massimo di 32 caratteri (solo lettere, numeri, trattini e caratteri di sottolineatura).
- Nel campo URL, immettere gli URL da includere nell'elenco, separati da virgole. È inoltre possibile utilizzare il pulsante Importa per aggiungere elenchi da un percorso di archiviazione accessibile.
- Al termine, fare clic su Add (Aggiungi).

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](#)

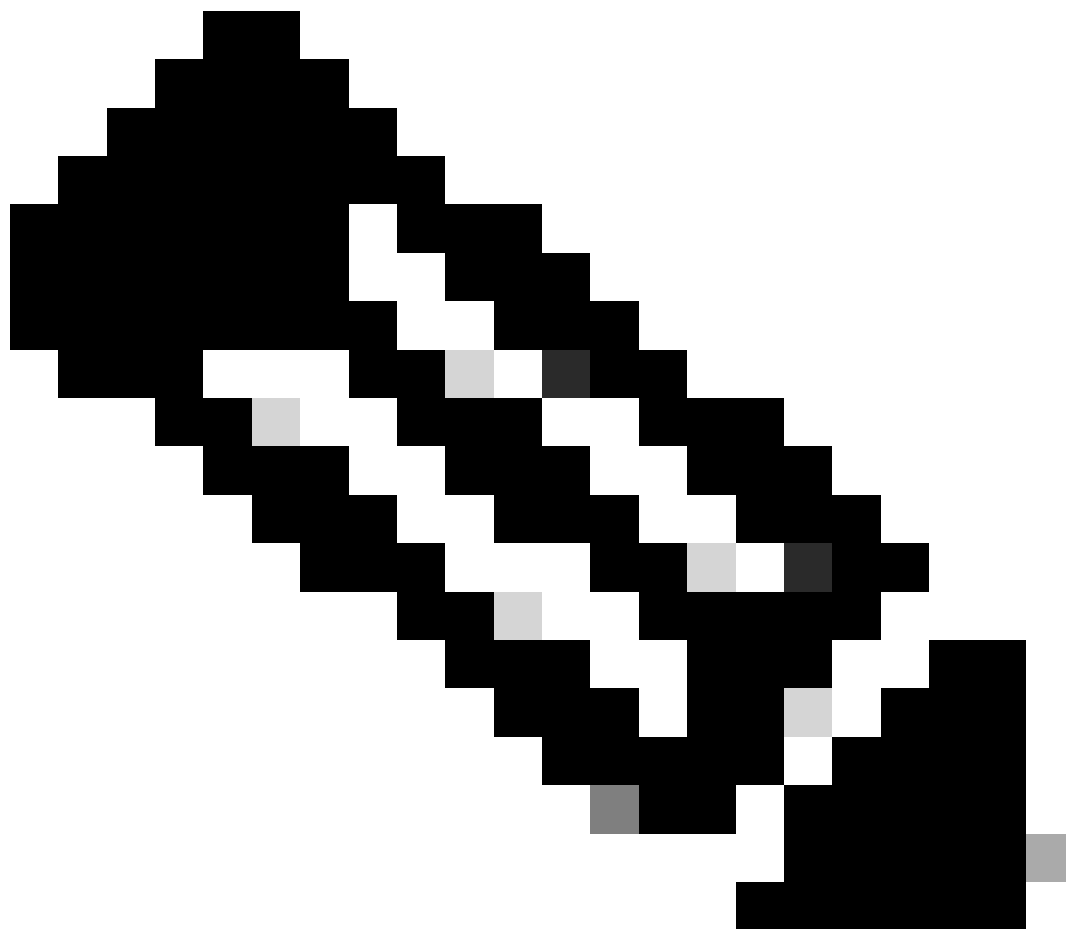
Allow URL List Name*

Guest_Allow

Add Allow URL *

www.google.com, www.yahoo.com

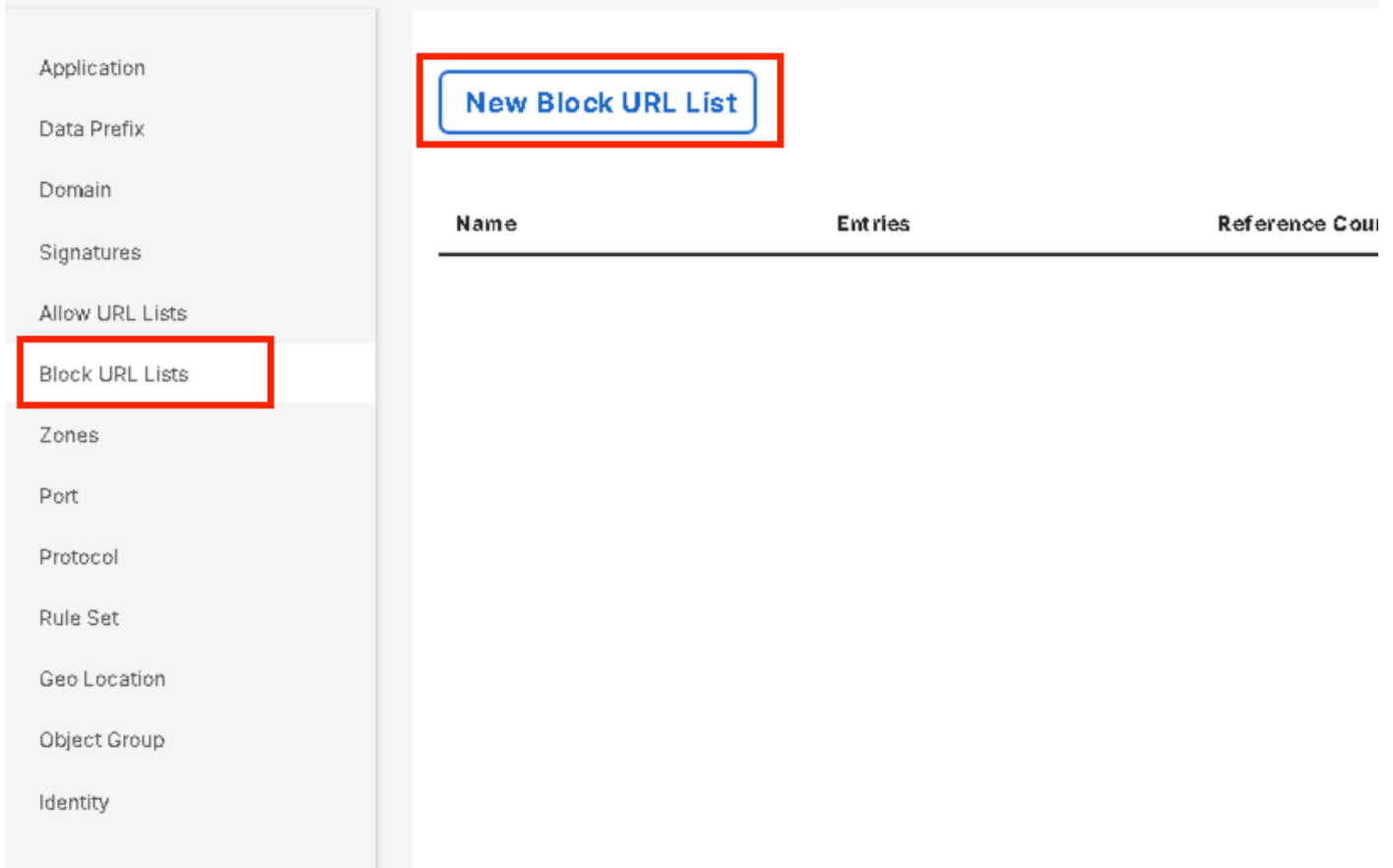
[Import](#)[Add](#)[Cancel](#)



Nota: è possibile utilizzare un modello regex per il nome di dominio negli elenchi Consenti e Blocca

Fare clic su Block URLs Lists dal riquadro di sinistra e creare New Block URL List.

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

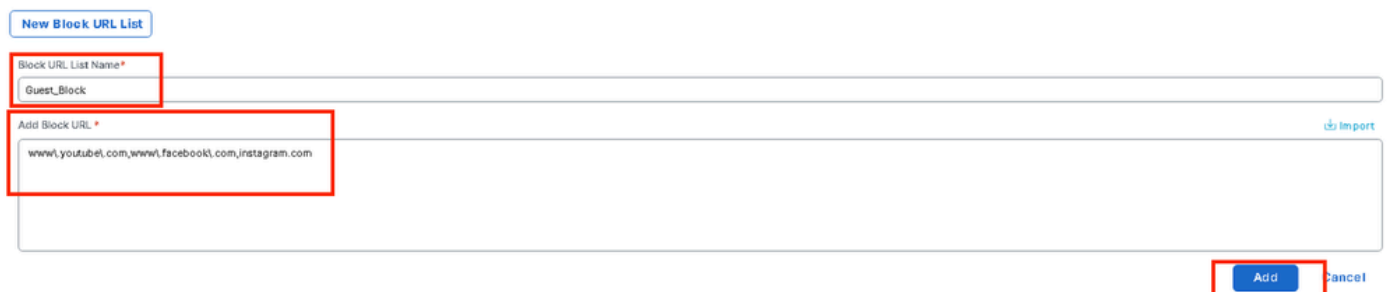
Object Group

Identity

New Block URL List

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

- Nel campo Nome elenco URL, immettere un nome elenco composto da un massimo di 32 caratteri (solo lettere, numeri, trattini e caratteri di sottolineatura)
- Nel campo URL, immettere gli URL da includere nell'elenco, separati da virgole. È inoltre possibile utilizzare il pulsante Importa per aggiungere elenchi da un percorso di archiviazione accessibile.
- Al termine, fare clic su Add (Aggiungi).



New Block URL List

Block URL List Name*

Guest_Block

Add Block URL

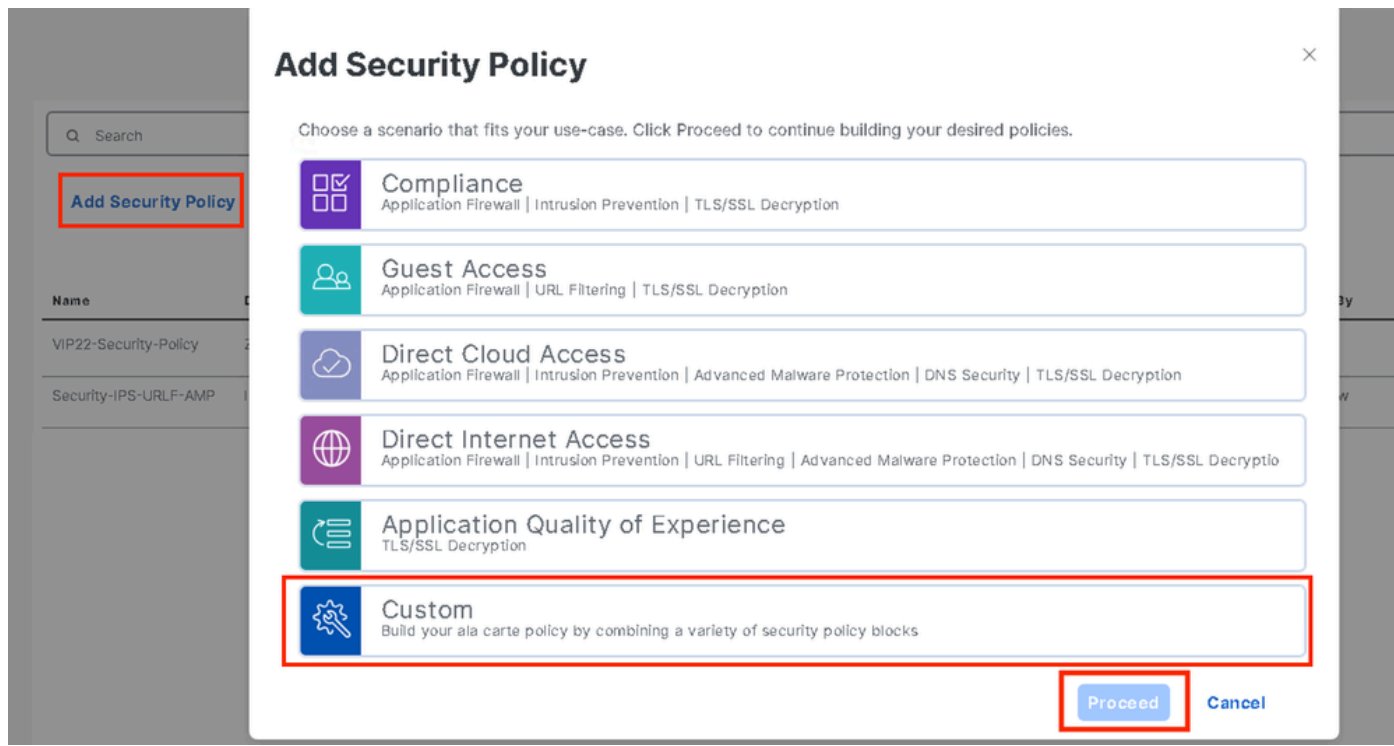
www.youtube.com,www.facebook.com,instagram.com

Add Cancel

Crea criterio di protezione

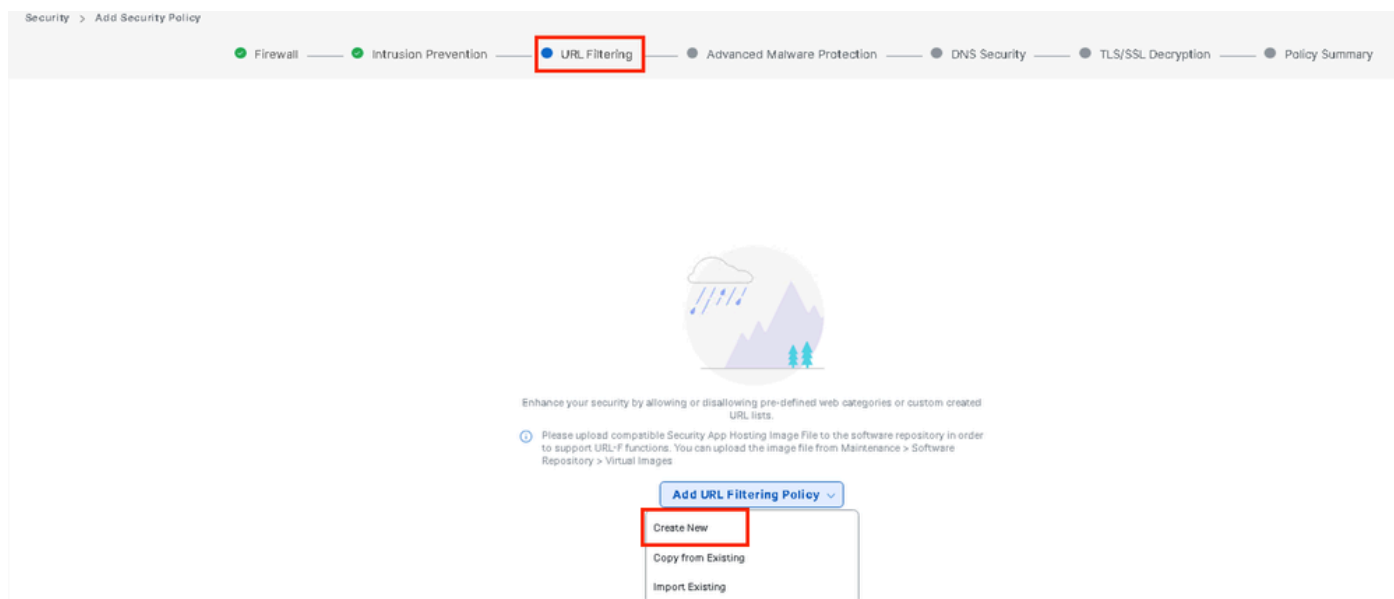
2. Dal menu Cisco SD-WAN Manager, selezionare Configuration > Security Fare clic su Add new security policy (Aggiungi nuovo criterio di sicurezza). Verrà aperta la procedura guidata Aggiungi

critero di protezione e verranno visualizzati vari scenari di utilizzo o verrà utilizzato il critero esistente presente nell'elenco. Selezionare custom, quindi fare clic su Continua per aggiungere un critero di filtro URL nella procedura guidata.

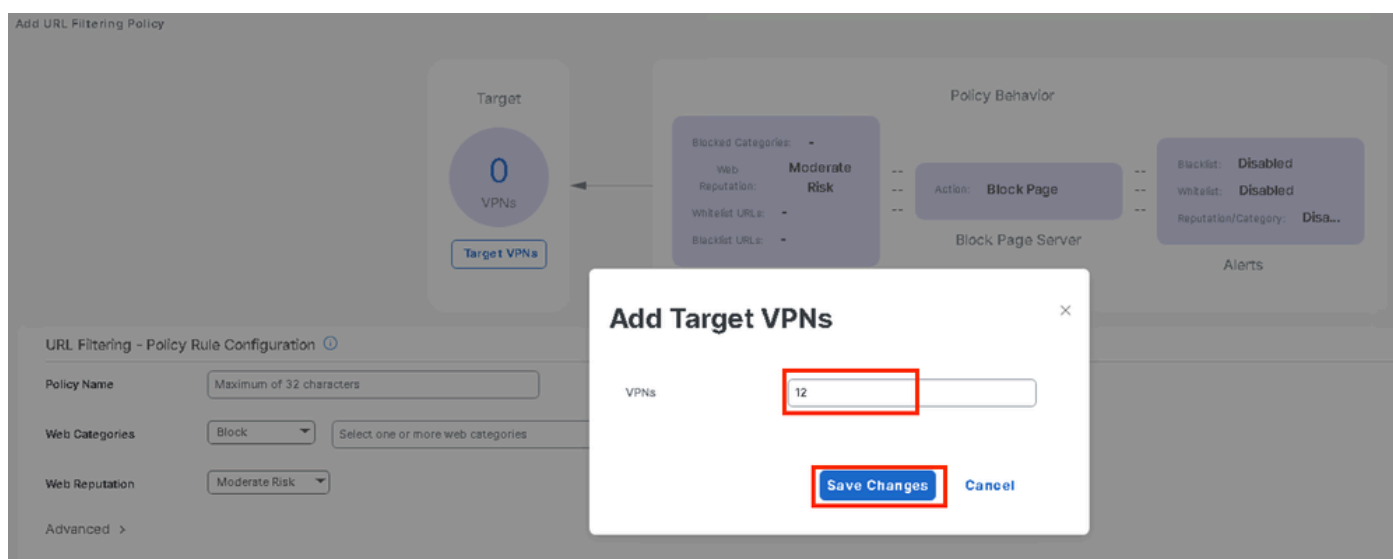


Nota: in Aggiungi critero di sicurezza scegliere uno scenario che supporti il filtro URL (Accesso guest, Accesso diretto a Internet o Personalizzato).

Nella procedura guidata Aggiungi critero di sicurezza, fare clic su Avanti finché non viene visualizzata la finestra del filtro URL. A questo punto, creare una policy di filtro URL scegliendo URL Filtering > Add URL Filtering Policy > Create New (Aggiungi policy di filtro URL > Crea nuovo). Fare clic su Avanti.



Fare clic su VPN di destinazione per aggiungere il numero richiesto di VPN nella procedura guidata Aggiungi VPN di destinazione.



- Immettere un nome per il criterio nel campo Nome criterio.
- Scegliere una di queste opzioni dall'elenco a discesa Categorie Web, selezionare Blocca e i siti Web corrispondenti alle categorie scelte vengono bloccati.

Blocca—Blocca i siti Web corrispondenti alle categorie selezionate.

Consenti: consente i siti Web corrispondenti alle categorie selezionate.

Scegliere una reputazione Web dal menu a discesa e impostare su Rischio moderato. Tutti gli URL la cui reputazione è pari o inferiore a 60 sono bloccati.

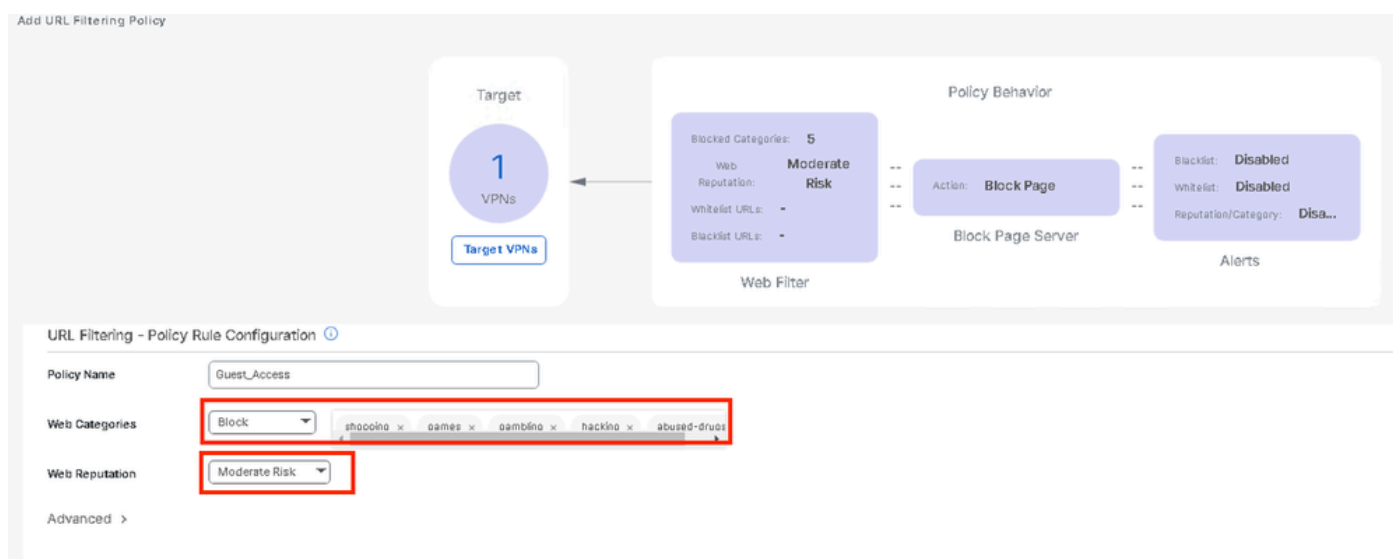
Rischio elevato: punteggio di reputazione compreso tra 0 e 20.

Sospetto: punteggio reputazione da 0 a 40.

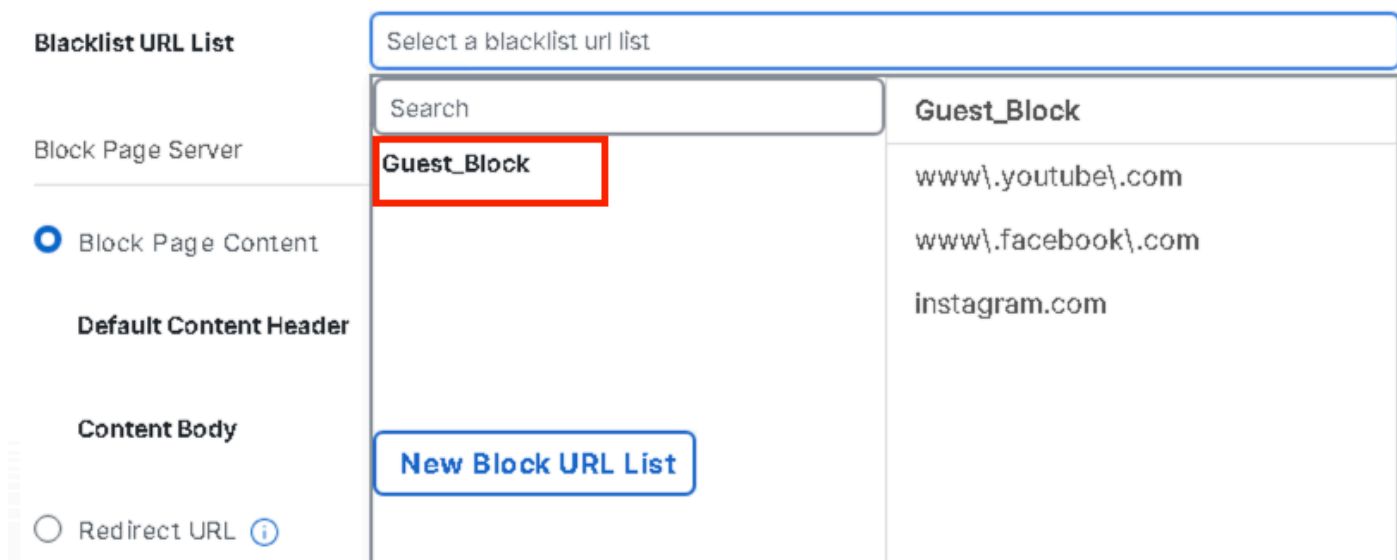
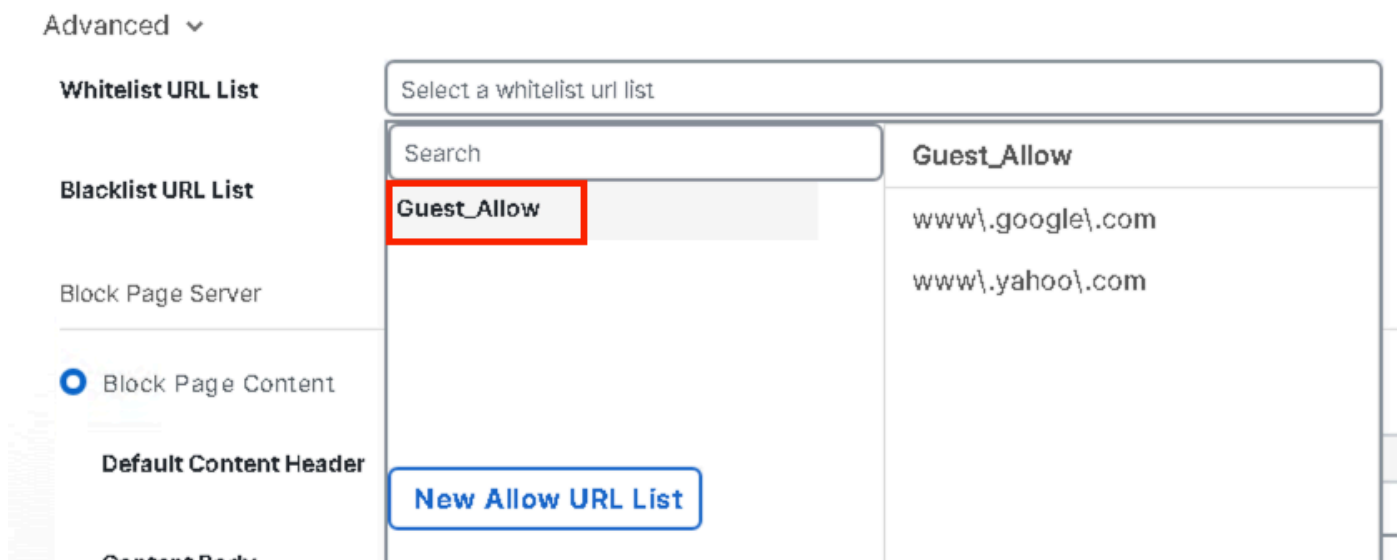
Rischio moderato: punteggio di reputazione da 0 a 60.

Basso rischio: punteggio di reputazione compreso tra 0 e 80.

Attendibile: punteggio di reputazione compreso tra 0 e 100.



Da Avanzate, scegliere gli elenchi esistenti o creare un nuovo elenco in base alle esigenze dal menu a discesa Elenco URL consentiti o Elenco URL bloccati.



Se necessario, modificare il corpo del contenuto in Blocca contenuto pagina e assicurarsi che tutti gli avvisi siano selezionati.

Per aggiungere un criterio di filtro URL, fare clic su Salva criterio di filtro URL.

URL Filtering - Policy Rule Configuration ⓘ

Advanced ▾

Whitelist URL List

Guest_Allow ×

Blacklist URL List

Guest_Block ×

Block Page Server

Block Page Content

Default Content Header

Access to the requested page has been denied

Content Body

Please contact your Network Administrator

Redirect URL ⓘ

Enter URL

Alerts and Logs ⓘ

Alerts



Blacklist



Whitelist



Reputation/Category

Save URL Filtering Policy

Cancel

Fare clic su Avanti finché non viene visualizzata la pagina Riepilogo criterio.

Immettere il nome del criterio di protezione e la descrizione del criterio di protezione nei campi corrispondenti.

● 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

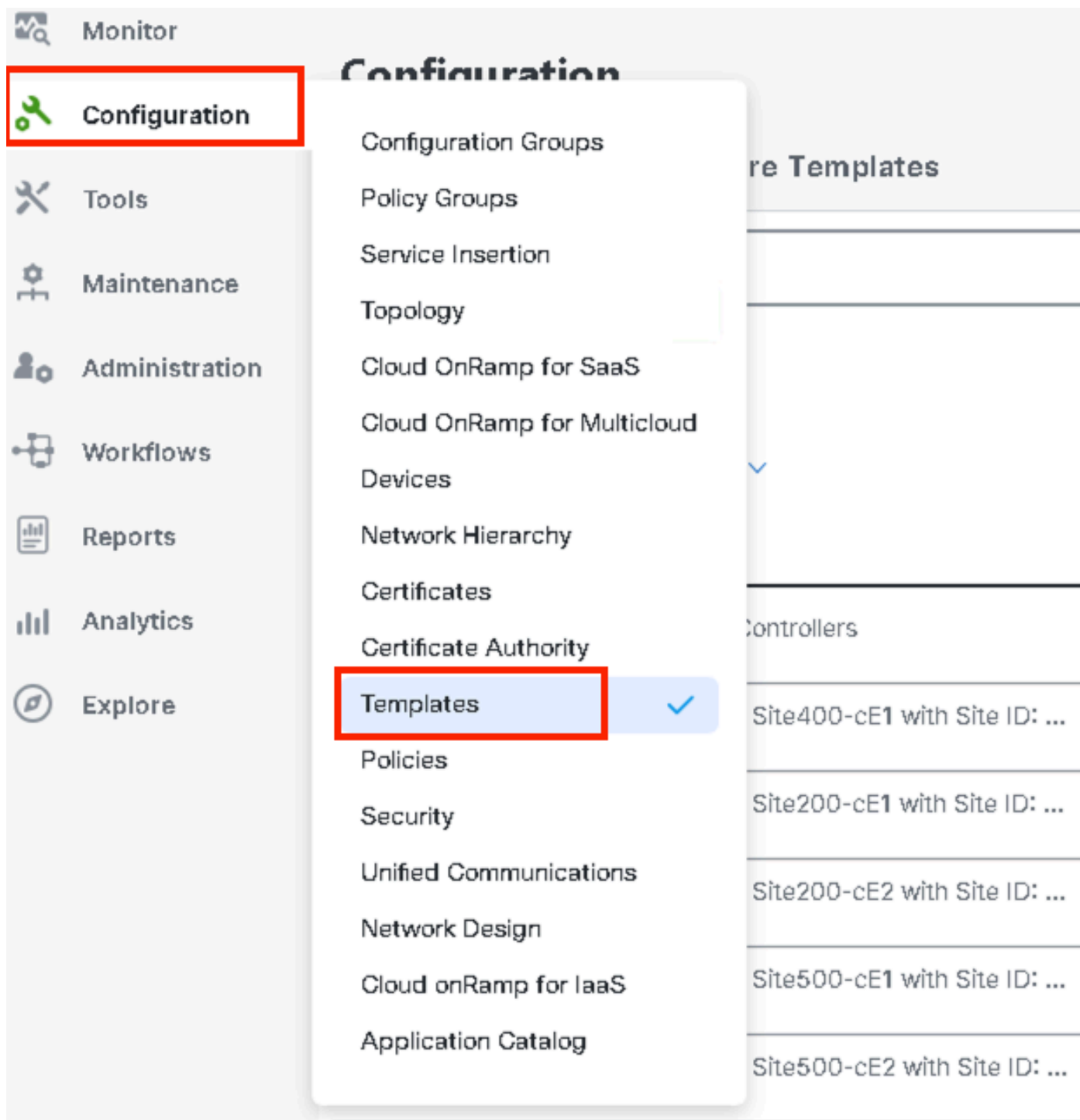
Failure Mode

Back Cancel

Applicare un criterio di protezione a un dispositivo

Per applicare un criterio di protezione a un dispositivo:

Dal menu Cisco SD-WAN Manager, scegliere Configurazione > Modelli.



Fare clic su Modelli di dispositivo e quindi su Modifica su modello di dispositivo.

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

Fare clic su Modelli aggiuntivi.

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

- Dall'elenco a discesa Criterio di sicurezza, scegliere il nome del criterio configurato in Guest_URL_Policy in precedenza e fare clic su Aggiorna.

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

Fare clic su device (Dispositivi), accertarsi che la configurazione sia corretta, quindi fare clic su

Config Diff (Differenza configurazione) e Side by Side Diff (Differenza configurazione affiancata).
 Fare clic su Configure Devices (Configura dispositivi).

The screenshot displays the vManage configuration interface. At the top, there are tabs for 'Config Preview' and 'Config Diff', with 'Config Diff' selected. To the right, there are buttons for 'Side by Side Diff' and 'Intent'. Below the tabs, the 'Local Configuration vs. New Configuration' section shows a list 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

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

At the bottom, there are buttons for 'Back', 'Configure Devices', and 'Cancel', with 'Configure Devices' highlighted.

vManage ha configurato correttamente il modello di dispositivo con i criteri di protezione e ha installato il pacchetto UTD sul dispositivo Edge.

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 apsid utd
 [26-Jul-2024 13:57:40 PDT] Device: Successfully installed apsid utd
 [26-Jul-2024 13:59:07 PDT] Device: Verified apsid utd in running state
 [26-Jul-2024 13:59:07 PDT] Device: Successfully verified apsid: utd
 [26-Jul-2024 13:59:08 PDT] Device: Config applied successfully
 [26-Jul-2024 13:59:08 PDT] Template successfully attached to device

Modifica filtro URL

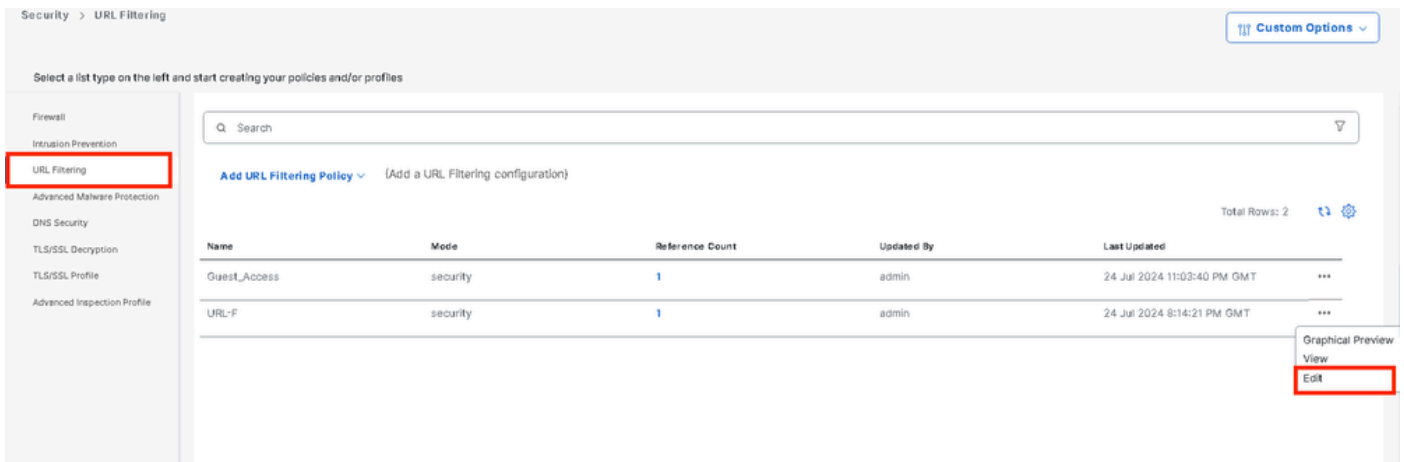
Per modificare un criterio di filtro URL, procedere come segue:

1. Dal menu Cisco SD-WAN Manager, scegliere Configurazione > Sicurezza.
2. Nella schermata Protezione, fare clic sul menu a discesa Opzioni personalizzate , quindi scegliere Criteri/Profili.

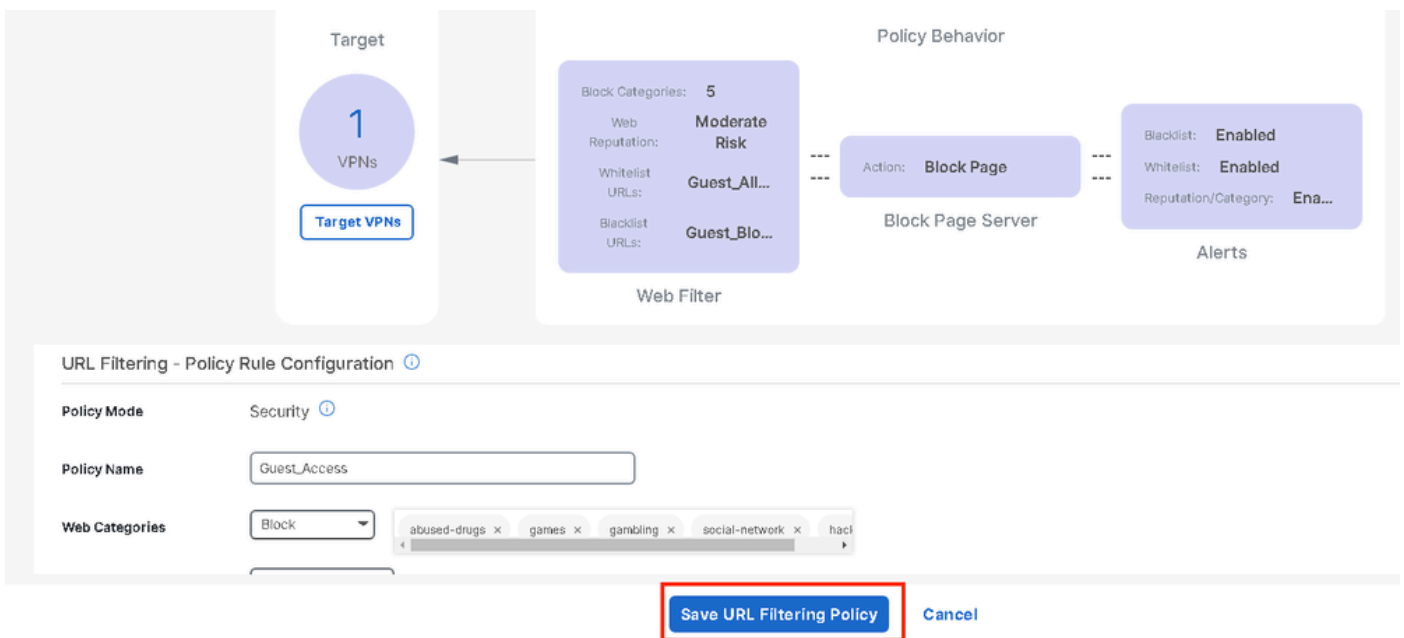
The screenshot shows the Cisco SD-WAN Manager interface. On the left is a navigation menu with 'Configuration' selected. On the right, a dropdown menu is open under 'Security', showing 'Policies/Profiles' highlighted with a red box. Below the menu is a search bar and a table of security policies.

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 8:32:38 PM ...

Fare clic su URL Filtering (Filtro URL) nella scheda a sinistra, per il criterio che si desidera modificare, fare clic su 3 punti (...)e scegliere Edit (Modifica).



Modificare il criterio come richiesto e fare clic su Salva criterio filtro URL.



Eliminazione del filtro URL

Per eliminare un criterio di filtro URL, è innanzitutto necessario scollegarlo dal criterio di sicurezza:

Dal menu Cisco SD-WAN Manager, scegliere Configurazione > Sicurezza.

Per scollegare il criterio di filtro URL dal criterio di protezione:

- Per il criterio di sicurezza che contiene il criterio di filtro URL, fare clic su 3 punti (...) quindi su Modifica.

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

Viene visualizzata la pagina Riepilogo criterio. Fare clic sulla scheda Filtro URL.

Per il criterio che si desidera eliminare, fare clic su 3 punti (...) quindi scegliere Disconnetti.

Fare clic su Salva modifiche criteri.

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

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

Per eliminare il criterio di filtro URL:

Nella schermata Security (Protezione), fare clic sul menu a discesa Custom Options (Opzioni personalizzate), selezionare Policies/Profiles (Criteri/profili), quindi selezionare URL Filtering (Filtro URL).

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 ...

Per il criterio che si desidera eliminare, fare clic su 3 punti (...) quindi su Elimina.

Fare clic su 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

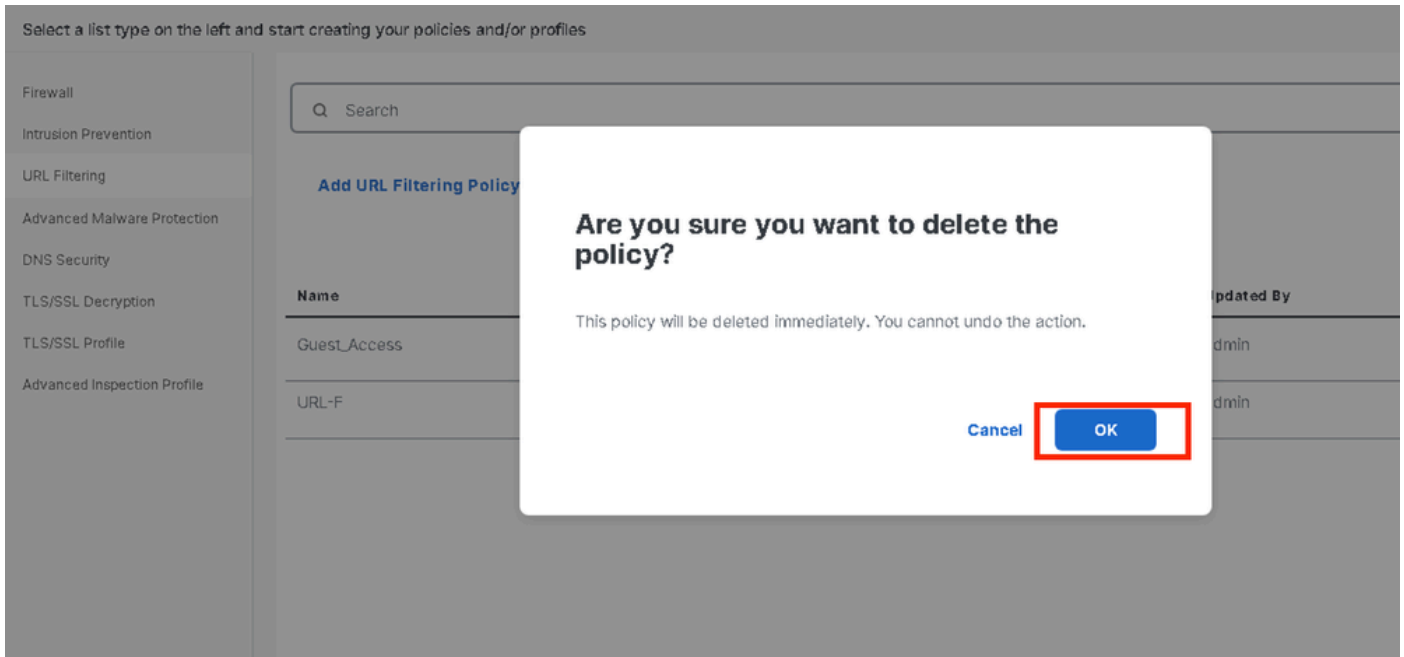
Q Search

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

Total Rows: 2

Name	Mode	Reference Count	Updated By	Last Updated
GuestAccess	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



Verifica

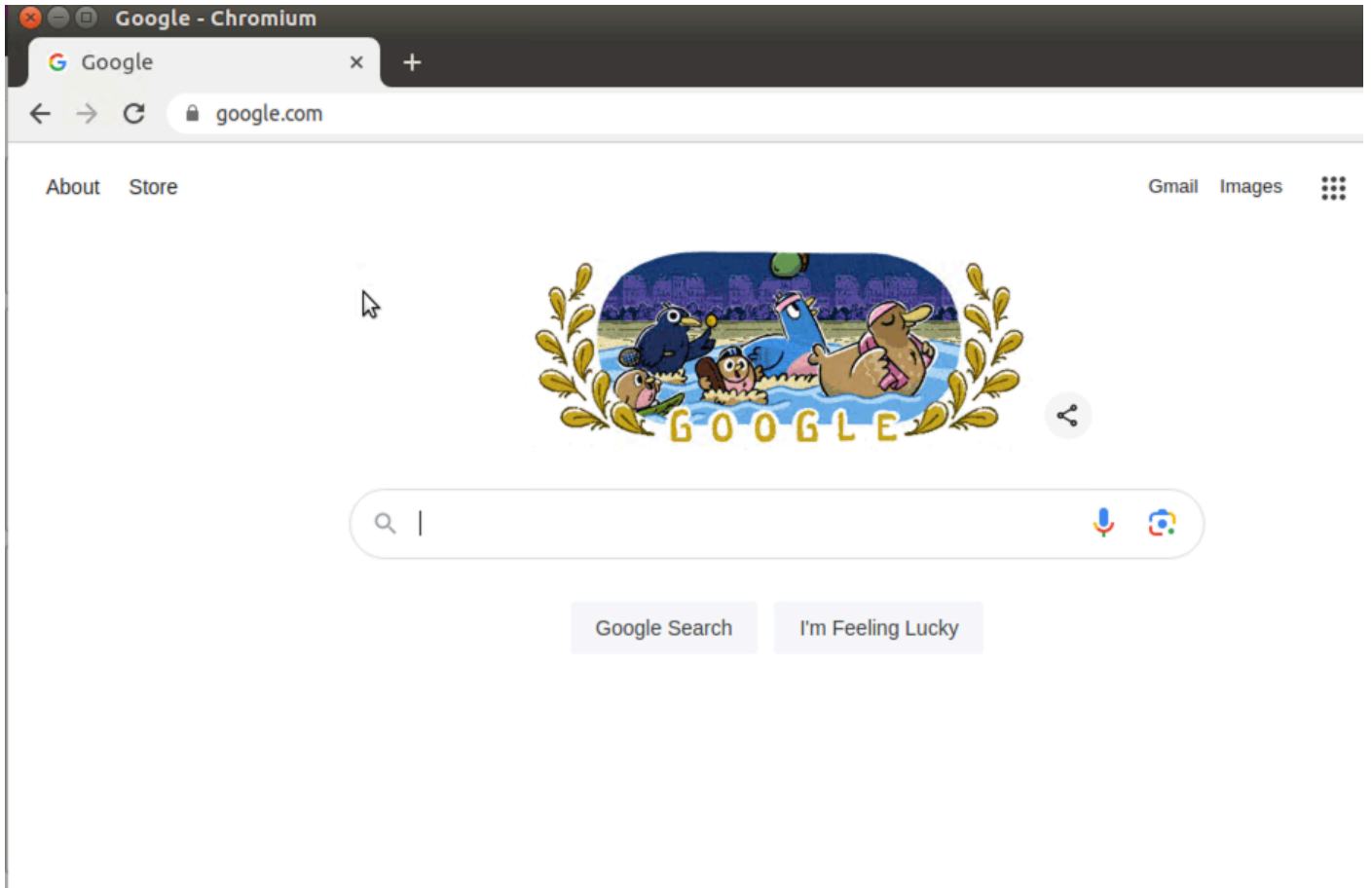
Verificare se è installata la versione UTD di Cisco.

```
<#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
```

Dal PC client sulla VPN per utenti guest, se si tenta di aprire google.com e yahoo.com, sono consentiti.



<#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

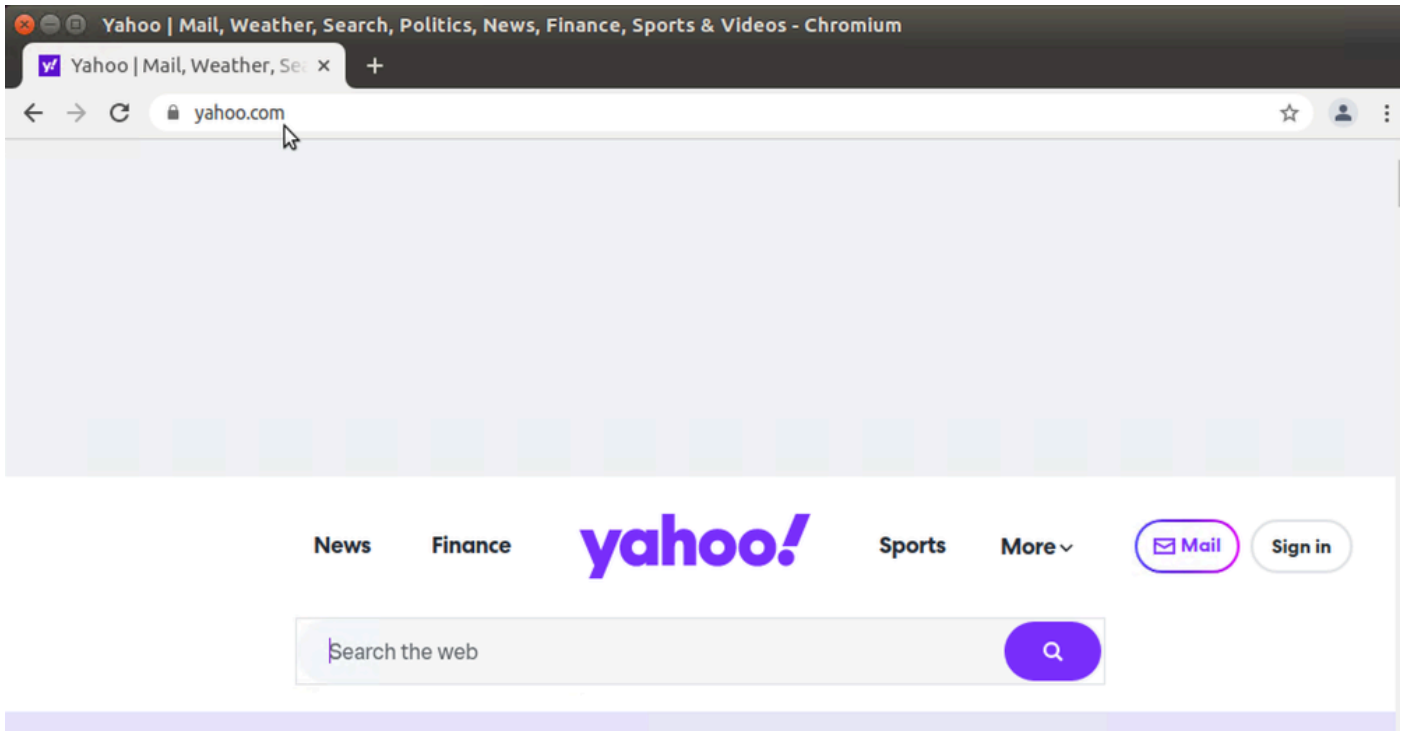
[**]

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

[**]

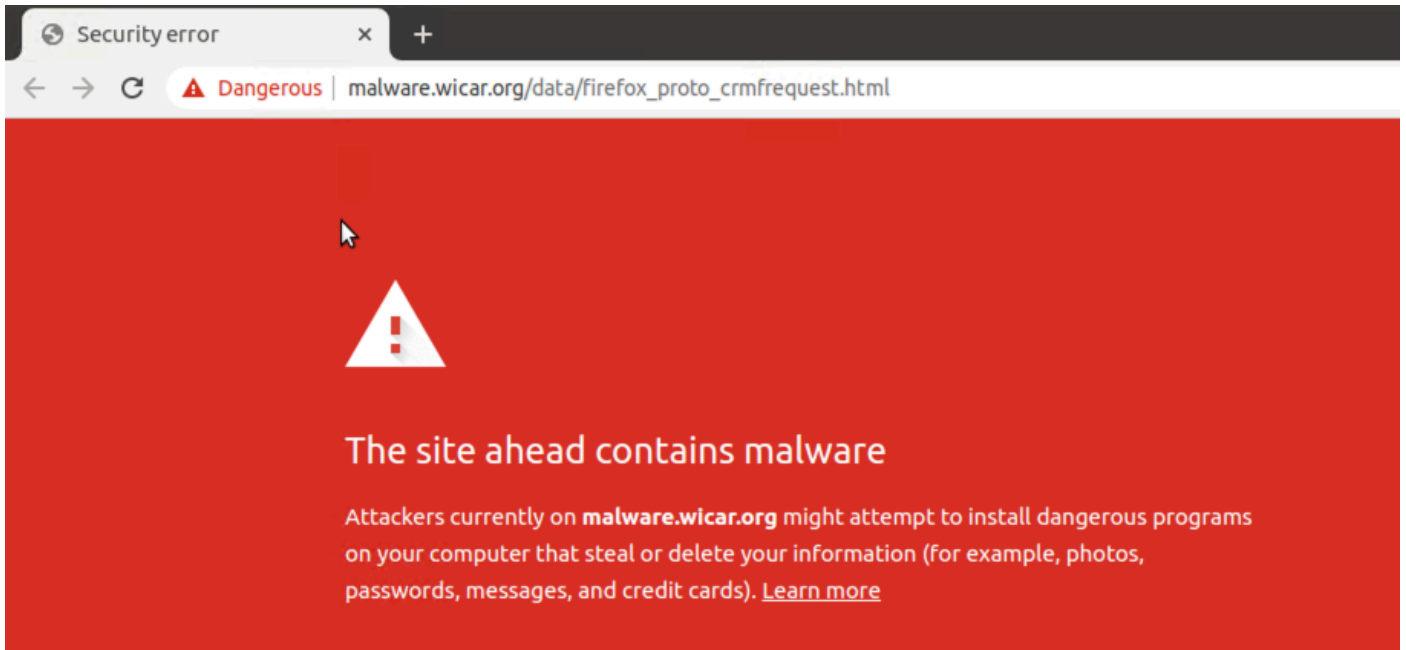
UTD WebFilter Allowlist

[**] [

URL: www.yahoo.com

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

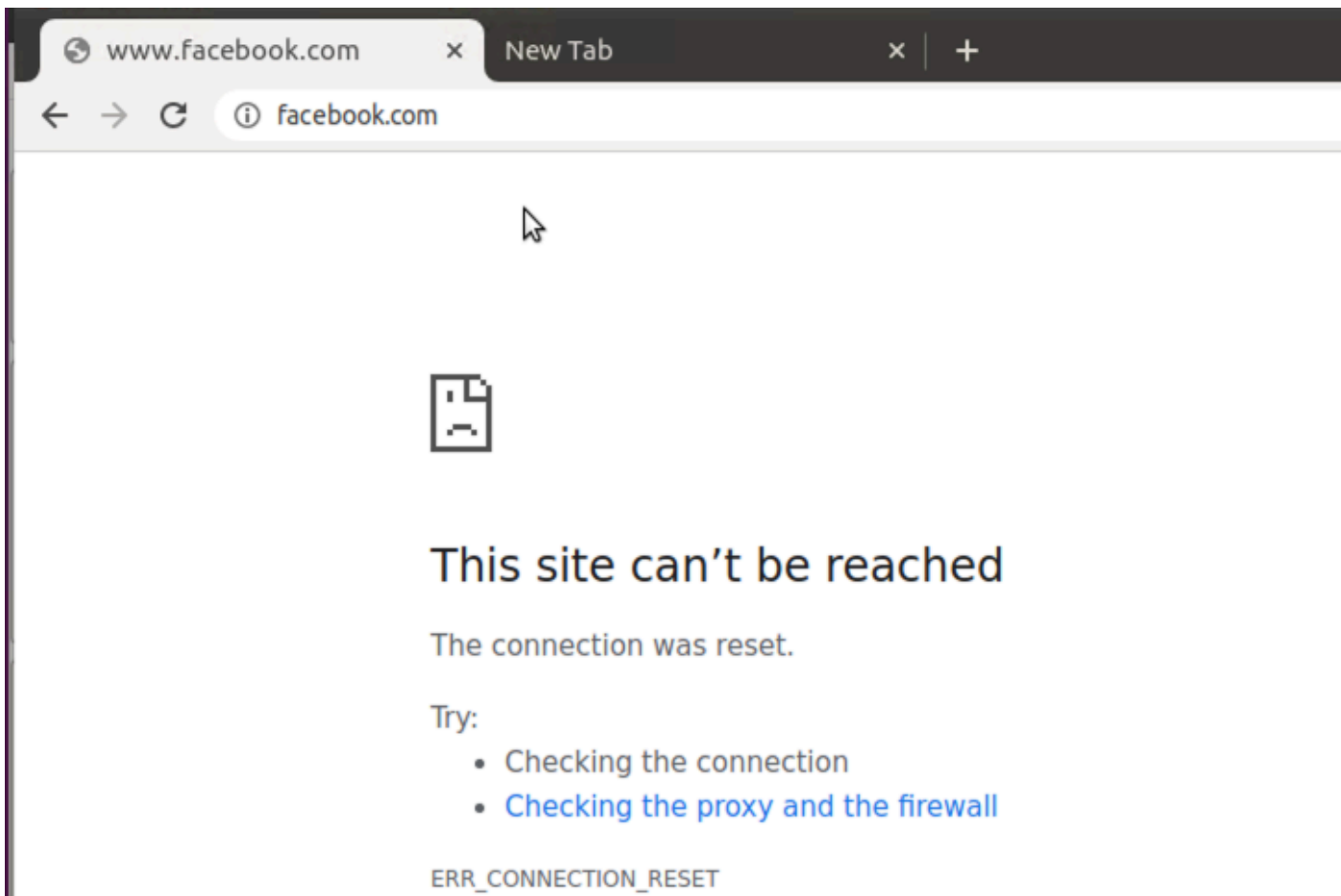
Dal PC client sulla VPN guest, se si cerca di aprire pagine Web con punteggi bassi o da una delle categorie Web bloccate, il motore di filtro URL rifiuta la richiesta HTTP.



<#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
```

Dal PC client situato sulla VPN per gli utenti guest, se si tenta di aprire facebook, instagram e youtube vengono bloccati.



<#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

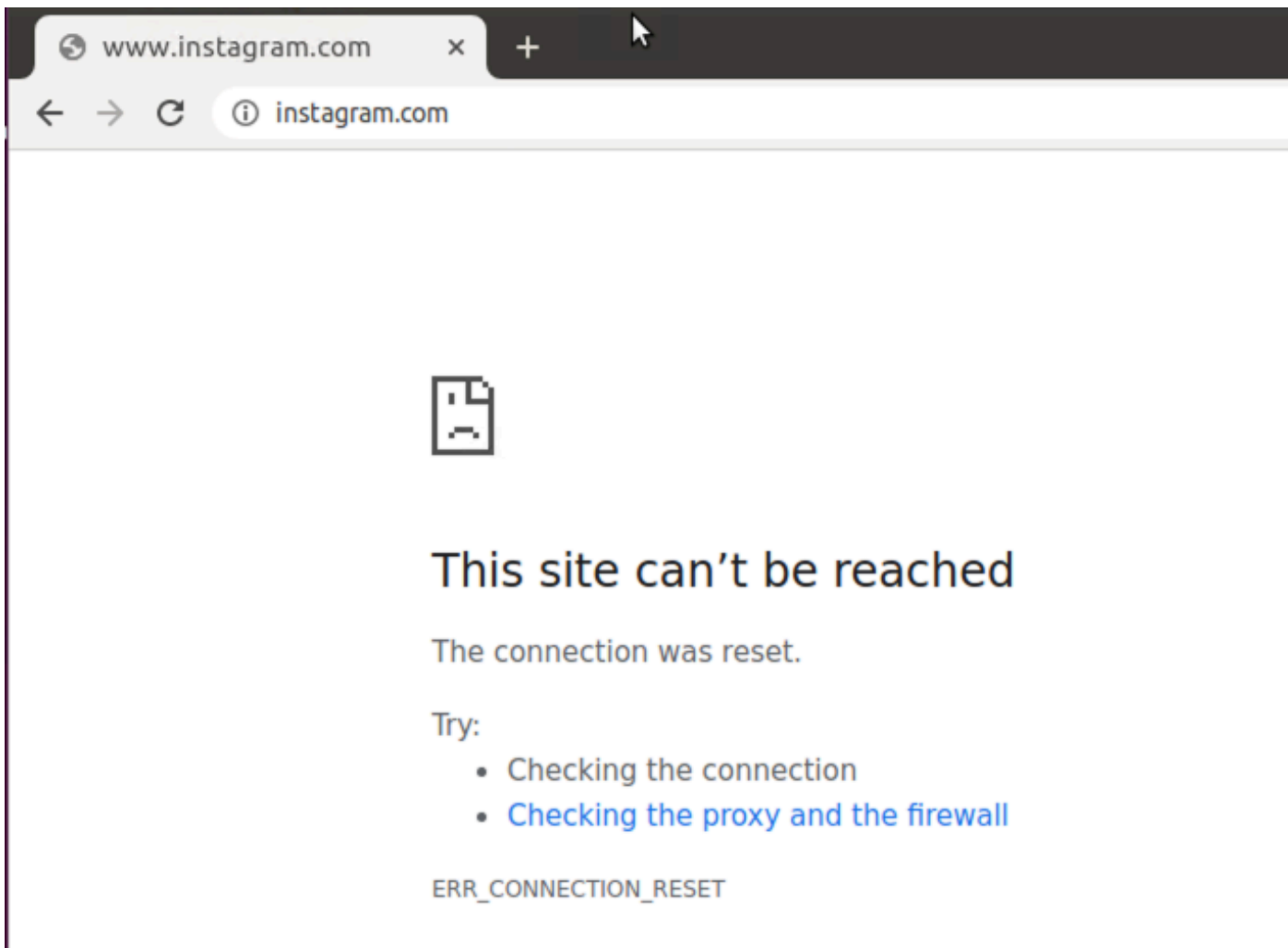
[**]

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

Monitoraggio del filtro URL dalla GUI vManage

La procedura seguente permette di monitorare il filtro URL in tempo reale o in modo cronologico per ciascun dispositivo, in base alle categorie Web.

Per monitorare gli URL bloccati o consentiti su un dispositivo Cisco IOS XE Catalyst SD-WAN:

1. Dal menu Cisco SD-WAN Manager, scegliere Monitor > Dispositivi > Seleziona dispositivo

The screenshot shows a navigation menu on the left with 'Monitor' highlighted. A dropdown menu is open under 'Monitor', with 'Devices' selected. The main content area displays a table of devices with the following 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. Nel riquadro sinistro, in Monitoraggio della sicurezza, fare clic su Filtro URL. Nel riquadro di destra vengono visualizzate le informazioni sul filtro URL.

- Fare clic su Bloccato. Viene visualizzato il conteggio delle sessioni su un URL bloccato.
- Fare clic su Consentito. Viene visualizzato il conteggio delle sessioni sugli URL consentiti.

Nota: lo stato della versione installata di UTD non può essere NON SUPPORTATO.

Verificare se UTD è in stato di esecuzione.

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

Lo stato di salute di Convalida UTD è in VERDE.

<#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

Verificare che la funzionalità del filtro URL sia abilitata.

<#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

Per visualizzare i log del filtro URL, eseguire il comando `show utd engine standard logging events url-filtering`.

```
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
```

Nota: eseguire il comando `clear utd engine standard logging events` per cancellare i vecchi eventi.

Controlla i pacchetti in entrata/uscita nel contenitore UTD e ritarda la ricerca.

```
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
```

Informazioni correlate

- [Guida alla configurazione della sicurezza di Cisco Catalyst SD-WAN](#)
- [Installa immagine virtuale di sicurezza UTD su router cEdge](#)
- [Risoluzione dei problemi relativi alla gestione dei percorsi di dati tramite UTD e filtro URL](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).