

Definizione di categorie URL personalizzate in WSA

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Consenti URL](#)

[Crea un nuovo URL personalizzato](#)

[Modifica criteri di accesso globale](#)

[Blocca URL](#)

[Crea un nuovo URL personalizzato](#)

[Modifica criteri di accesso globale](#)

Introduzione

In questo documento viene descritto come definire le categorie di URL personalizzate da utilizzare in Web Security Appliance (WSA).

Contributo di Shikha Grover e modificato da Yeraldin Sanchez, Cisco TAC Engineers.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze di base di Cisco Web Security Appliance

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

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.

Premesse

La categoria a cui appartiene un URL è determinata da un database di categorie di filtro. Web Security Appliance raccoglie informazioni e gestisce un database separato per ciascun motore di filtro URL. I database delle categorie di filtro ricevono periodicamente aggiornamenti dal server di aggiornamento Cisco e vengono gestiti da Cisco TALOS. Talos, Security Intelligence and Research Group di Cisco, segue costantemente un'ampia serie di attributi per valutare le conclusioni relative a un determinato host.

In alcuni casi può essere necessario classificare un URL, un dominio o un indirizzo IP in modo diverso e personalizzare la classificazione in base alla propria casella. A tale scopo, è possibile utilizzare le categorie URL personalizzate.

Quando il motore di filtro URL confronta una categoria URL con l'URL di una richiesta client, prima valuta l'URL con le categorie URL personalizzate incluse nel gruppo di criteri. Se l'URL nella richiesta non corrisponde a una categoria personalizzata inclusa, il motore di filtro URL lo confronta con le categorie URL predefinite.

Configurazione

Consenti URL

Se si considera attendibile il sito Web, è possibile consentirlo eseguendo il processo seguente.

Crea un nuovo URL personalizzato

1. Per creare una nuova categoria URL personalizzata, selezionare **GUI > Web Security Manager > Custom URL Categories > Add Custom Category Name** (Aggiungi categoria personalizzata): URL consentiti.
2. Aggiungere i siti che si desidera controllare nella sezione dei siti (company.com..company.com).

Custom and External URL Categories: Edit Category

Edit Custom and External URL Category	
Category Name:	<input type="text" value="Allowed URLs"/>
Comments: (?)	<input type="text"/>
List Order:	<input type="text" value="1"/>
Category Type:	Local Custom Category
Sites: (?)	<input type="text" value="company.com, .company.com"/> <small>(e.g. 10.0.0.1, 2001:420:80:1::5, example.com.)</small>
	<input type="button" value="Sort URLs"/> <small>Click the Sort URLs button to sort all site URLs in Alpha-numerical order.</small>
Advanced	Regular Expressions: (?) <input type="text"/> <small>Enter one regular expression per line.</small>
<input type="button" value="Cancel"/>	<input type="button" value="Submit"/>

3.
4. Si noti che "domain.com" corrisponderà solo a "domain.com", non a www.domain.com o a "host.domain.com". Per consentire l'accesso a un sito e a tutti i sottodomini, sono necessarie due voci nella sezione "Siti": ". domain.com, dominio.com".
5. Fare clic su **Invia**.

Modifica criteri di accesso globale

1. Aprire **Web Security Manager > Criteri di accesso > Criteri globali > Filtro URL**.
2. Fare clic su **Seleziona categorie personalizzate**.
3. Fare clic sulla freccia a discesa **URL consentiti**, scegliere **Includi nei criteri** e fare clic su **Applica**.
4. Selezionare la casella **Consenti**.
5. Fare clic su **Invia** e **Conferma modifiche**.

Access Policies: URL Filtering: Global Policy

Category	Category Type	Block	Redirect	Allow	Monitor	Warn	Quota-based	Time-based
Allowed URLs	Custom (Local)	Select all						

Blocca URL

Se non si considera attendibile il sito Web, è possibile bloccarlo eseguendo la procedura seguente.

Crea un nuovo URL personalizzato

1. Per creare una nuova categoria URL personalizzata, selezionare **GUI > Web Security Manager > Custom URL Categories > Add Custom Category Name** (Aggiungi categoria personalizzata): URL bloccati.
2. Aggiungere i siti che si desidera controllare nella sezione dei siti (company.com, .company.com).

Custom and External URL Categories: Edit Category

Category Name:

Comments:

List Order:

Category Type: Local Custom Category

Sites: [Sort URLs](#)
Click the Sort URLs button to sort all site URLs in Alpha-numerical order.

(e.g. 10.0.0.1, 2001:420:80:1::5, example.com.)

Advanced: Regular Expressions:
Enter one regular expression per line.

3. Si noti che "domain.com" corrisponderà solo a "domain.com", non a www.domain.com o a "host.domain.com". Per bloccare un sito e tutti i sottodomini, sono necessarie due voci nella sezione "Siti": ". domain.com, dominio.com".
4. Fare clic su **Invia**.

Modifica criteri di accesso globale

1. Aprire **Web Security Manager** > **Criteri di accesso** > **Criteri globali** > **Filtro URL**.
2. Fare clic su **Seleziona categorie personalizzate...**
3. Fare clic sulla freccia dell'elenco a discesa **URL bloccati**, scegliere **Includi nei criteri** e fare clic su **Applica**.
4. Selezionare la casella **Blocco**.
5. Fare clic su **Invia** e **conferma modifiche**.

Access Policies: URL Filtering: Global Policy

Custom and External URL Category Filtering		Block	Redirect	Allow	Monitor	Warn	Quota-Based	Time-Based
Category	Category Type	Select all	Select all	Select all	Select all	Select all		
 Blocked URLs	Custom (LOCK)	<input checked="" type="checkbox"/>						

Select Custom Categories...

Nota: le modifiche di cui sopra possono essere apportate a qualsiasi politica di accesso e non solo alla politica globale. La stessa procedura può essere applicata ai criteri di decrittografia.

Consultare questa [guida](#) per un caso di utilizzo ampiamente diffuso.