

Blocca download file eseguibile in SWA

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Operazioni preliminari](#)

[Procedura di configurazione](#)

[Convalida del blocco delle estensioni dei file](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto il processo di configurazione di Secure Web Appliance (SWA) per bloccare il download di file eseguibili.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Accesso all'interfaccia grafica dell'SWA
- Accesso amministrativo all'SWA.

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.

Operazioni preliminari

Cisco SWA può bloccare in modo efficace il download di file eseguibili ispezionando il tipo MIME (Multipurpose Internet Mail Extensions) di contenuto Web. Identificando tipi di file quali application/x-msdownload, application/x-msi e altri tipi MIME correlati, SWA applica criteri che impediscono il recapito degli eseguibili agli utenti. Oltre al rilevamento del tipo MIME, SWA può utilizzare il filtro delle estensioni dei file, l'analisi basata sulla reputazione e le regole

personalizzate per rafforzare ulteriormente la protezione da download indesiderati o rischiosi. Queste funzionalità aiutano le organizzazioni a mantenere un ambiente di navigazione sicuro e a ridurre il rischio di infezioni da malware.



Suggerimento: SWA non è in grado di identificare il tipo MIME del file, a meno che il traffico non venga decrittografato.

application/octet-stream è un tipo MIME generico utilizzato per indicare che un file contiene dati binari. Non specifica la natura del file, quindi può essere utilizzato per qualsiasi file che non si adatta a un tipo MIME più specifico. Questo tipo viene in genere assegnato ai file eseguibili, ai programmi di installazione e ad altri file non di testo quando il server Web non è in grado di determinare un tipo più preciso.

Procedura di configurazione

Passaggio 1. Creare una categoria URL personalizzata per il sito Web.

Passaggio 1.1. Dalla GUI, passare a Web Security Manager e scegliere Categorie URL personalizzate ed esterne.

Passaggio 1.2. Fare clic su Aggiungi categoria per creare una nuova categoria di URL personalizzati.

Passaggio 1.3. Inserire il nome della nuova categoria.

Passaggio 1.4. Definire il dominio e/o i sottodomini del sito Web che si sta tentando di bloccare il traffico di caricamento (in questo esempio è cisco.local e tutti i relativi sottodomini).

Passaggio 1.5. Inviare le modifiche.

Custom and External URL Categories: Edit Category

The screenshot shows the 'Edit Custom and External URL Category' form. It has a dark header bar with the title. Below it, there are several input fields: 'Category Name' (with a red circle 1), 'Comments' (with a help icon), 'List Order' (set to 1), 'Category Type' (set to 'Local Custom Category'), and 'Sites' (with a help icon and a red circle 2, containing the text 'cisco.local, .cisco.local'). To the right of the 'Sites' field is a 'Sort URLs' button with a tooltip that says 'Click the Sort URLs button to sort all site URLs in Alpha-numerical order.' Below the 'Sites' field is an 'Advanced' section with a 'Regular Expressions' field (with a help icon) and a note: 'Enter one regular expression per line. Maximum allowed characters 2048.' At the bottom of the form are 'Cancel' and 'Submit' buttons.

Immagine - Crea categoria URL personalizzata



Suggerimento: Per ulteriori informazioni su come configurare le categorie URL personalizzate, visitare:

	 https://www.cisco.com/c/en/us/support/docs/security/secure-web-appliance-virtual/220557-configure-cu...
Passaggio 2. Decrittografare il traffico per l'URL	 Attenzione: La decrittografia di un numero elevato di URL può causare una riduzione delle prestazioni. Passaggio 2.1. Dalla GUI, passare a Web Security Manager e scegliere Decryption Policies (Criteri di decrittografia) Passaggio 2.2. Fare clic su Aggiungi criterio. Passaggio 2.3. EnterName per il nuovo criterio. Passaggio 2.4. (Facoltativo) Selezionare il profilo di identificazione a cui applicare il criterio.  Suggerimento: (Facoltativo) Se si desidera applicare il criterio a tutti gli utenti, anche se non sono autenticati, scegliere Tutti gli utenti (autenticati e non autenticati). Passaggio 2.5. Dalla sezione Definizione del membro dei criteri, fare clic su URL Categorieslinks (Categorie URL) per aggiungere la categoria URL personalizzata. Passaggio 2.6. Selezionare la categoria dell'URL creata nel Passaggio 1. Passaggio 2.7. Fare clic su Sottometti.

Decryption Policy: DecryptingTraffic

Policy Settings

☒ **Enable Policy**

Policy Name: (e.g. my IT policy)

Description:

Insert Above Policy:

Policy Expires: ☐ Set Expiration for Policy

On Date: MM/DD/YYYY
At Time: :

Policy Member Definition

Membership is defined by the combination of the following options. All criteria must be met for the policy to take effect.

Identification Profiles and Users:

All Identification Profiles

☒ All Authenticated Users
☐ Selected Groups and Users (?)

Groups: No groups entered
Users: No users entered
☐ All Users (authenticated and unauthenticated users)

☒ **Advanced**

Use the Advanced options to define or edit membership by proxy port, subnet, Time Range, destination (URL Category), or User Agents.
The following advanced membership criteria have been defined:

Proxy Ports: None Selected
Subnets: None Selected
Time Range: No Time Range Definitions Available (see Web Security Manager > Defined Time Ranges)
URL Categories:
User Agents: None Selected

Immagine - Crea criterio di decrittografia

Passaggio 2.8. Nella pagina Criteri di decrittografia, fare clic sul collegamento da Filtro URL per il nuovo criterio.

Decryption Policies

Policies						
Add Policy...						
Order	Group	URL Filtering	Web Reputation	Default Action	Clone Policy	Delete
1	DecryptingTraffic Identification Profile: All All identified users URL Categories: Category	Monitor: 1	(global policy)	(global policy)		
	Global Policy Identification Profile: All	Monitor: 107 Decrypt: 1	Enabled	Decrypt		
Edit Policy Order...						

Immagine - Selezionare il filtro URL

Passaggio 2.9. Choose Decrypt come azione per la categoria URL personalizzato.

Passaggio 2.10. Fare clic su Sottometti.

Decryption Policies: URL Filtering: DecryptingTraffic

Custom and External URL Category Filtering

These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.

Category	Category Type	Use Global Settings	Override Global Settings				
		Pass Through	Monitor	Decrypt	Drop	Quota-Based	Time-Based
Category	Custom (Local)	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)

	Immagine - Imposta decrittografia come azione
Passaggio 3. Bloccare i file eseguibili	Passaggio 3.1. Dalla GUI, passare a Web Security Manager e selezionare Access Policies (Policy di accesso). Passaggio 3.2. Fare clic su Aggiungi criterio. Passaggio 3.3. EnterName per il nuovo criterio. Passaggio 3.4. (Facoltativo) Selezionare il profilo di identificazione a cui applicare il criterio.  Suggerimento: (Facoltativo) Se si desidera applicare il criterio a tutti gli utenti, anche se non sono autenticati, scegliere Tutti gli utenti (autenticati e non autenticati). Passaggio 3.5. Dalla sezione Definizione membri dei criteri, fare clic sui collegamenti Categorie URL per aggiungere la categoria URL personalizzata. Passaggio 3.6. Selezionare la categoria dell'URL creata nel Passaggio 1. Passaggio 3.7. Fare clic su Sottometti. Access Policy: Block Exec Policy Settings ☒ Enable Policy Policy Name: Block Exec 1 (e.g. my IT policy) Description: (Maximum allowed characters 256) Insert Above Policy: 1 (Global Policy) Policy Expires: ☐ Set Expiration for Policy On Date: MM/DD/YYYY At Time: 00 : 00 Policy Member Definition Membership is defined by the combination of the following options. All criteria must be met for the policy to take effect. Identification Profiles and Users: All Identification Profiles ☒ All Authenticated Users ☐ Selected Groups and Users ? Groups: No groups entered Users: No users entered ☐ All Users (authenticated and unauthenticated users) 2 If the "All Users" option is selected, at least one Advanced membership option must also be selected. ☒ Advanced Use the Advanced options to define or edit membership by protocol, proxy port, subnet, Time Range, destination (URL Category), or User Agents. The following advanced membership criteria have been defined: Protocols: None Selected Proxy Ports: None Selected Subnets: None Selected Time Range: No Time Range Definitions Available (see Web Security Manager > Defined Time Ranges) URL Categories: Category 2 User Agents: None Selected Cancel Submit

Immagine - Criteri di accesso



Suggerimento: Ai fini della creazione di report, è consigliabile scegliere un nome diverso da qualsiasi altro criterio di accesso/decrittografia.

Passaggio 3.8. Nella pagina Criteri di accesso, verificare che l'azione Filtro URL sia impostata su Monitoraggio.

Passaggio 3.9. Nella pagina Criteri di accesso, fare clic sul collegamento da Oggetti per il nuovo criterio.

Access Policies

Policies									
Add Policy...									
Order	Group	Protocols and User Agents	URL Filtering	Applications	Objects	Anti-Malware and Reputation	HTTP ReWrite Profile	Clone Policy	Delete
1	Block Exec Identification Profile: All All identified users URL Categories: Category	(global policy)	Monitor: 1	Monitor: 325	(global policy)	(global policy)	(global policy)		
	Global Policy Identification Profile: All	No blocked items	Monitor: 108	Monitor: 325	No blocked items	Web Reputation: Enabled Secure Endpoint: Enabled Anti-Malware Scanning: Enabled	None		
Edit Policy Order...									

Immagine - Seleziona oggetti

Immagine - Selezionare il filtro URL

Passaggio 3.10. Dal menu a discesa scegliere Definisci impostazioni blocco oggetti personalizzati.

Access Policies: Objects: Block Exec

Edit Objects Blocking Settings

☒ Use Global Policy Objects Blocking Settings

☐ Define Custom Objects Blocking Settings

☐ Disable Object Blocking for this Policy

HTTP/HTTPS Max Download Size: No Maximum

FTP Max Download Size: No Maximum

Block Object Type

Not Defined

Custom MIME Types

Block Custom MIME Types: Not Defined

Cancel

Submit

Immagine - Definizione oggetti personalizzati

Passaggio 3.11. Fare clic su Codice eseguibile per selezionare i tipi di oggetti da bloccare.

Passaggio 3.12. Fare clic su Installatori per selezionare i tipi di oggetti da bloccare.

Passaggio 3.13. È inoltre possibile immettere i tipi MIME dei file

che si desidera bloccare nella sezione Tipi MIME personalizzati.

Access Policies: Objects: Block Exec

Edit Objects Blocking Settings

Define Custom Objects Blocking Settings

Objects Blocking Settings

Object Size

HTTP/HTTPS Max Download Size: ☐ 0 MB ☒ No Maximum

FTP Max Download Size: ☐ 0 MB ☒ No Maximum

Block Object Type

Object and MIME Type Reference

Archives

Inspectable Archives

Document Types

Executable Code

Installers

Media

P2P Metafiles

Web Page Content

Miscellaneous

Custom MIME Types

Object and MIME Type Reference

Block Custom MIME Types:

application/x-msdownload
application/x-msdos-program
application/x-msi

(Enter multiple entries on separate lines. Example: audio/x-mpeg3 or audio/* are valid entries. Maximum allowed characters 2048.)

Cancel Submit

Immagine - Configurazione degli oggetti da bloccare



Suggerimento: Per visualizzare l'elenco dei tipi MIME, fare clic su Riferimento a oggetti e tipi MIME.

Passaggio 3.14. Inoltare.

Passaggio 3.15. Eseguire il commit delle modifiche.

Convalida del blocco delle estensioni dei file

In questo esempio, quando un utente tenta di scaricare un file eseguibile, viene visualizzata la seguente pagina di avviso:

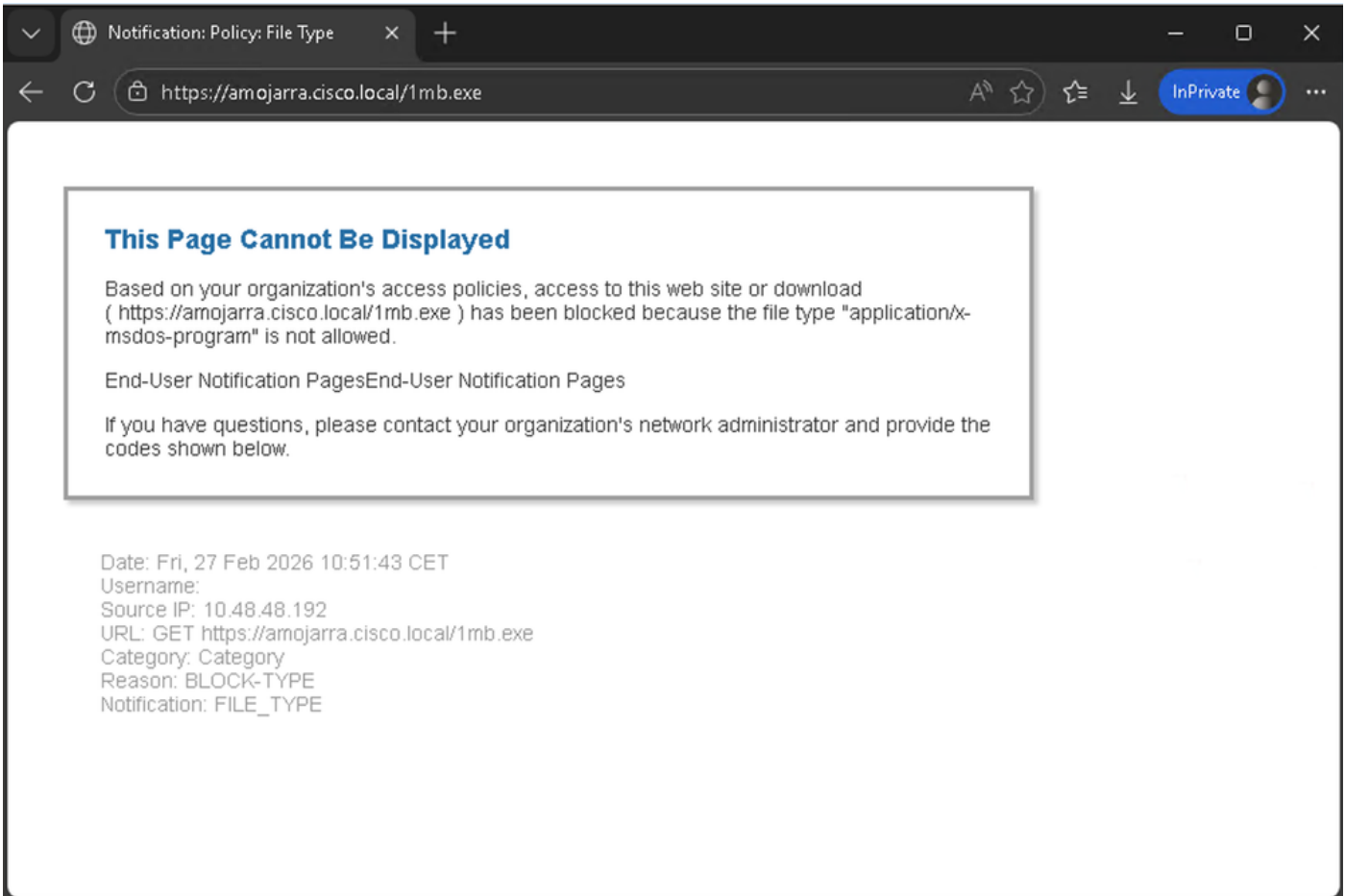


Immagine - Pagina Notifica di blocco

 **Suggerimento:** Per configurare la pagina Notifica utente finale (EUN), dalla GUI passare a Servizi di sicurezza e fare clic su Notifica utente finale e modificare la sezione Pagine di notifica utente finale.

Dai log degli accessi è possibile visualizzare due righe di log correlate al traffico.

La prima riga di registro è correlata al criterio di decrittografia (nome: DecryptingTraffic) che sta decrittografando il traffico. L'azione è DECRYPT_CUSTOMCAT

La seconda riga del log degli accessi è correlata ai criteri di accesso (Nome: Block_Exec) che è stato creato nel passo 1.3. L'azione è BLOCK_ADMIN_FILE_TYPE

Policy	Log degli accessi
Criterio di decrittografia	1772186569.823 182 10.48.48.192 TCP_MISS_SSL/200 39 CONNECT tunnel://amojarra.cisco.local:443/ - DIRECT/amojarra.cisco.local - DECRYPT_CUSTOMCAT_7- DecryptingTraffic-DefaultGroup-NONE-NONE-LAB_Access- NONE <"C_Cate",-,-,"-",-,-,-,"-,-,-,"-,-,-,"-,-,-,"- ",-,-,"-,-,"-,-,-,1.71,0,-,"-,-,-,"-,-,-,"-,-,-,-> -

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).