Blocca il traffico di caricamento in Secure Web Appliance

Sommario

Introduzione

In questo documento viene descritto il processo di blocco del traffico di caricamento su alcuni siti Web in Secure Web Appliance (SWA).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

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

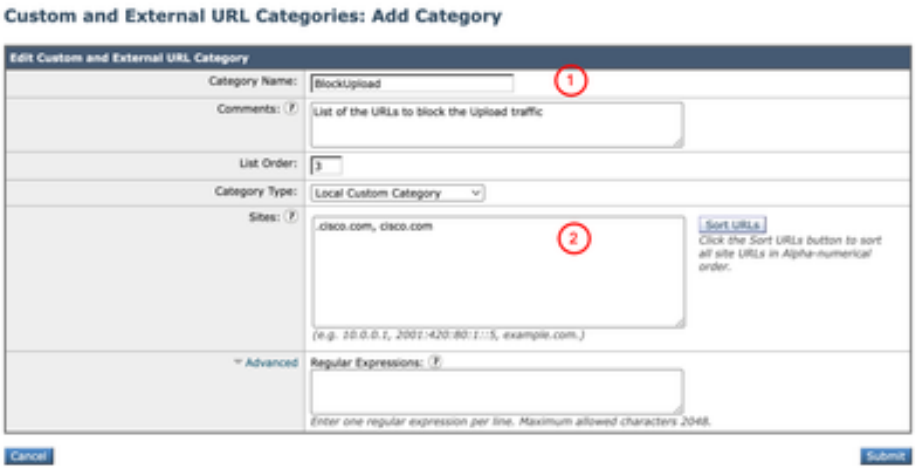
Componenti usati

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.

Procedura di configurazione

Passaggio 1. Creare una	Passaggio 1.1. Dalla GUI, passare a Web Security Manager e

categoria URL personalizzata per il sito Web.	scegliere Categorie URL personalizzate ed esterne. Passaggio 1.2. Fare clic su Add Category 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 cisco.com e tutti i relativi sottodomini). Passaggio 1.5.Sottomettere le modifiche.  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-custom-url-categories-in-secur.html
Passaggio 2. Decrittografare il traffico per l'URL	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. Immettere il nome del nuovo criterio. Passaggio 2.4. (Facoltativo) Selezionare il profilo di identificazione a cui applicare il criterio. Passaggio 2.5. Dalla sezione Definizione membri dei criteri, fare clic sui collegamenti 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.

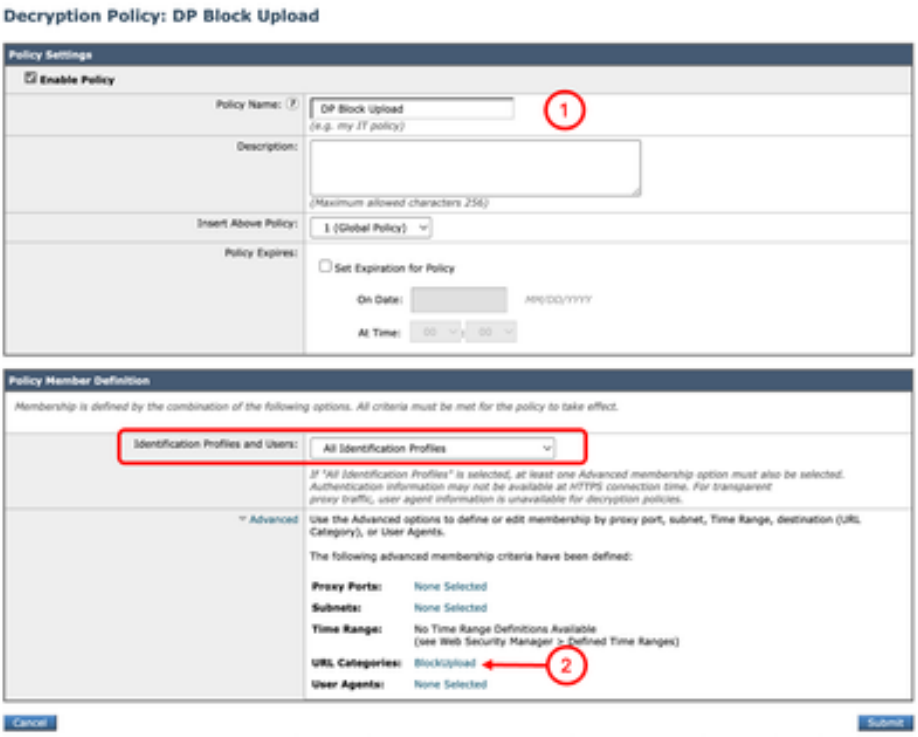


Immagine - Crea criterio di decrittografia

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

Immagine - Selezionare il filtro URL

Passaggio 2.9. Scegliere Decrittografa come azione per Categoria URL personalizzato.

Passaggio 2.10. Fare clic su Sottometti.

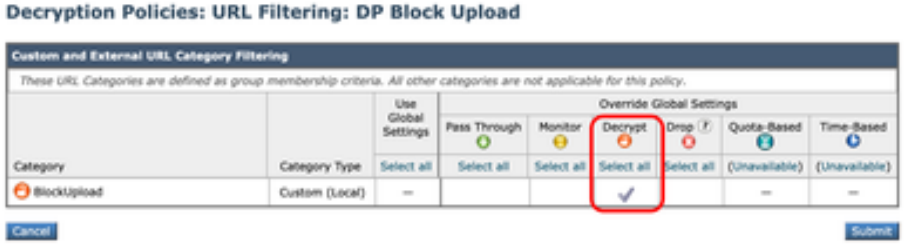


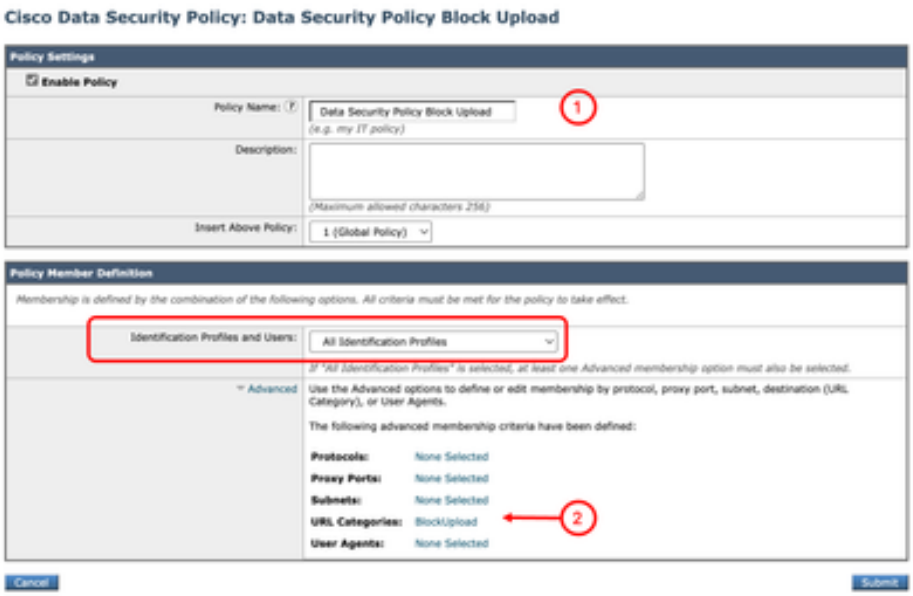
	Immagine - Imposta decrittografia come azione
Passaggio 3. Blocco del traffico di caricamento	Passaggio 3.1. Dalla GUI, passare a Web Security Manager e scegliere Cisco Data Security. Passaggio 3.2. Fare clic su Aggiungi criterio. Passaggio 3.3. Immettere il nome del nuovo criterio. Passaggio 3.4. (Facoltativo) Selezionare il profilo di identificazione a cui applicare il criterio. 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.  Immagine - Policy di sicurezza dei dati Cisco 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 Criterio di sicurezza data di Cisco, fare clic sul collegamento dal filtro URL per il nuovo criterio.

Immagine - Selezionare il filtro URL

Passaggio 3.9. Scegliere Blocca come azione per Categoria URL personalizzata.

Passaggio 3.10. Fare clic su Sottometti.

Immagine - Blocca caricamento

Passaggio 3.11. Eseguire il commit delle modifiche.

Report e log

Log

È possibile visualizzare i log relativi al traffico di caricamento dalla CLI scegliendo idsdataloss_logs come nome di log predefinito per i log di sicurezza dei dati.

Per accedere ai log, attenersi alla procedura descritta di seguito.

Passaggio 1. Accedere alla CLI

Passaggio 2. Digitare grep e premere Invio.

Passaggio 3. Trovare e digitare il numero associato a idsdataloss_logs:

- Tipo: "Registri di sicurezza dei dati"
- Recupero: FTP Poll e premere Invio.

Passaggio 4. (Facoltativo) Immettere l'espressione regolare per grep filtrare le ventole in base alle parole chiave oppure premere Invio, per visualizzare tutti i log

Passaggio 5. (Facoltativo) Non applicare la distinzione tra maiuscole e minuscole alla ricerca? [Y]> Se si selezionano parole chiave nel passaggio 4, è possibile scegliere se il filtro non fa distinzione tra maiuscole e minuscole.

Passaggio 6. (Facoltativo) Cercare le righe non corrispondenti? [N]>Se è necessario filtrare tutti i log ad eccezione delle parole chiave selezionate definite nel passo 4, è possibile utilizzare questa sezione, altrimenti premere Invio.

Passaggio 7. (Facoltativo) Definire la coda dei log? [N]> Se è necessario visualizzare i log attivi, digitare Y e premere Invio. In caso contrario, premere Invio per visualizzare tutti i registri disponibili.

Passaggio 8. (Facoltativo) Impaginare l'output? [N]> Se è necessario visualizzare i risultati per pagina, è possibile digitare Y e premere Invio, altrimenti premere Invio per utilizzare il valore predefinito [N].

Creazione di report

È possibile generare un report di tracciamento Web per visualizzare i report del traffico di caricamento bloccato in base al nome del criterio Cisco Data Security.

Per generare i rapporti, effettuare le operazioni riportate di seguito.

Passaggio 1. Dalla GUI, selezionare Reporting e scegliere Tracciamento Web.

Passaggio 2. Scegliere l'intervallo di tempo desiderato.

Passaggio 3. Fare clic sul collegamento Avanzate per cercare le transazioni utilizzando criteri avanzati.

Passaggio 4. Nella sezione Criterio, selezionare Filtra per criterio e digitare il nome della protezione dei dati Cisco creata in precedenza.

Passaggio 5. Fare clic su Cerca per esaminare il report.

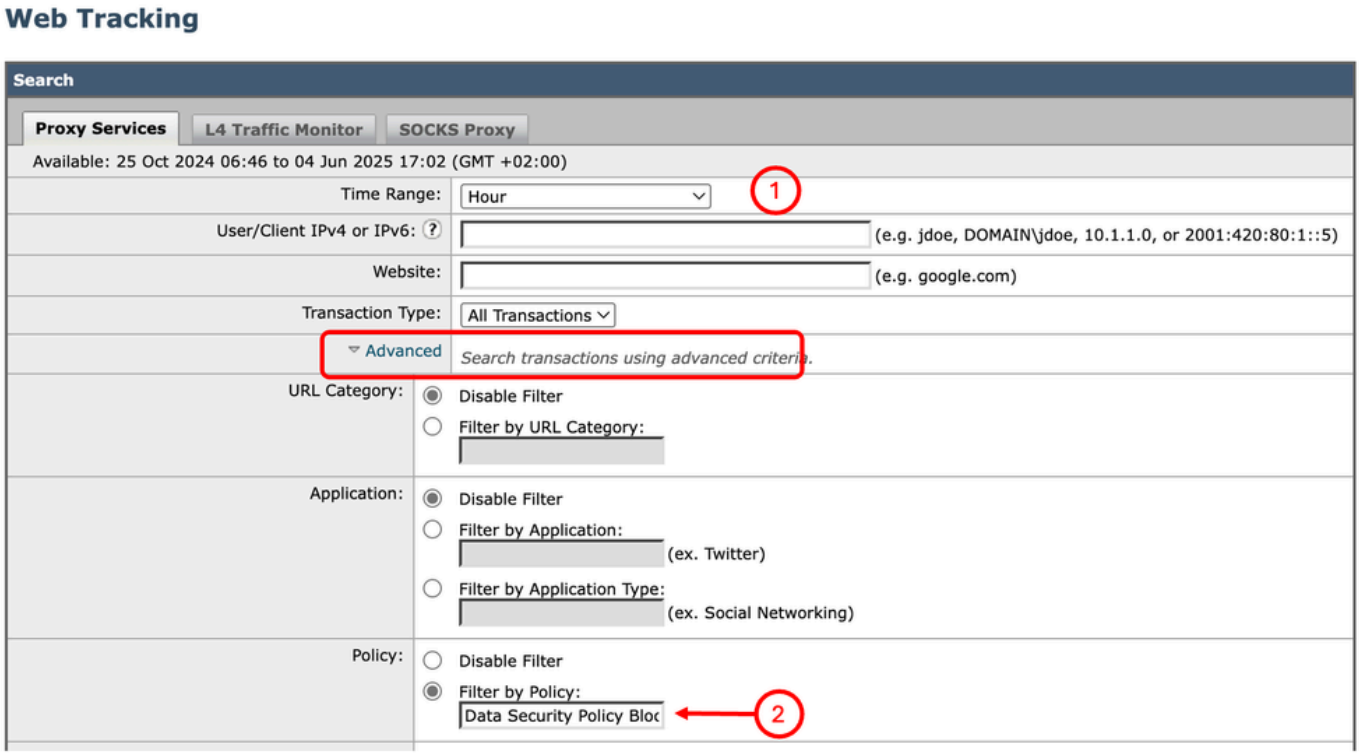


Immagine - Filtraggio dei report di verifica Web

Informazioni correlate

- Guida per l'utente di AsyncOS 15.2 per Cisco Secure Web Appliance
- Guida all'installazione di Cisco Secure Email e Web Virtual Appliance
- Configurazione di categorie URL personalizzate in Secure Web Appliance - Cisco
- Utilizzare le procedure ottimali per Secure Web Appliance
- Configurare il firewall per Secure Web Appliance
- Configura certificato di decrittografia in Appliance Web sicura
- Configurazione e risoluzione dei problemi di SNMP in SWA
- Configurazione dei log di push SCP in Secure Web Appliance con Microsoft Server
- Abilita canale/video YouTube specifico e blocca resto di YouTube in SWA
- Informazioni sul formato HTTPS Accesslog in Secure Web Appliance
- Accesso ai registri protetti di Web Appliance
- Ignora autenticazione in Secure Web Appliance
- Blocca il traffico in Secure Web Appliance
- Ignora traffico aggiornamenti Microsoft in Secure Web Appliance

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).