Blocca il traffico in Secure Web Appliance

Sommario

Introduzione

In questo documento viene descritta la procedura per bloccare il traffico in Secure Web Appliance (SWA).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Amministrazione della SWA.

Cisco raccomanda:

- SWA fisico o virtuale installato.
- Accesso amministrativo all'interfaccia grafica (GUI) 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.

Blocco del traffico

Bloccare il traffico nell'SWA è un passo cruciale per garantire la sicurezza della rete, mantenere la conformità con le politiche interne e proteggere il sistema da attività dannose. Di seguito sono riportati alcuni dei motivi più comuni per bloccare il traffico:

Motivi del blocco per origine

- Inondazioni da parte di uno o più utenti: quando uno o più utenti generano traffico eccessivo, può sovraccaricare la rete, con conseguente riduzione delle prestazioni e possibili interruzioni del servizio.
- Accesso alle risorse non attendibili da parte delle applicazioni (agenti utente): alcune applicazioni potrebbero tentare di accedere a risorse non attendibili o potenzialmente dannose. Il blocco di questi agenti utente consente di prevenire violazioni della sicurezza e perdite di dati.
- Limitazione dell'accesso a Internet per intervalli IP specifici: è possibile che ad alcuni indirizzi o intervalli IP venga impedito l'accesso a Internet a causa di policy di protezione o per impedire utilizzi non autorizzati.
- Comportamento sospetto: per proteggere la rete, è necessario bloccare il traffico che presenta modelli o comportamenti insoliti che potrebbero indicare attività dannose o minacce alla sicurezza.

Motivi del blocco per destinazione

- Conformità con le Politiche aziendali interne: le organizzazioni spesso dispongono di politiche che limitano l'accesso a determinati siti web o risorse online per garantire la produttività e la conformità con i requisiti legali o normativi.
- Siti non attendibili: il blocco dell'accesso a siti Web ritenuti non attendibili o potenzialmente dannosi consente di proteggere gli utenti da phishing, malware e altre minacce online.
- Comportamento dannoso: i siti noti per l'hosting di contenuti dannosi o per l'esecuzione di attività dannose devono essere bloccati per evitare incidenti relativi alla sicurezza e violazioni dei dati.

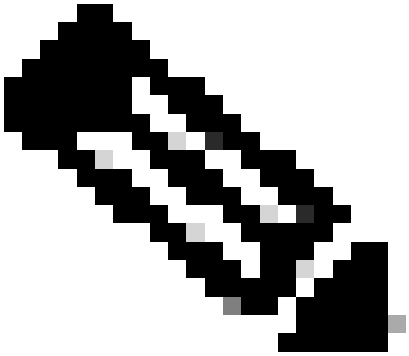
.

Passi per bloccare il traffico

In generale, per bloccare il traffico in SWA sono previste tre fasi principali:

- Creare un profilo di identificazione per gli utenti.
- Blocca il traffico HTTPS nel criterio di decrittografia.
- Bloccare il traffico HTTP nei criteri di accesso.

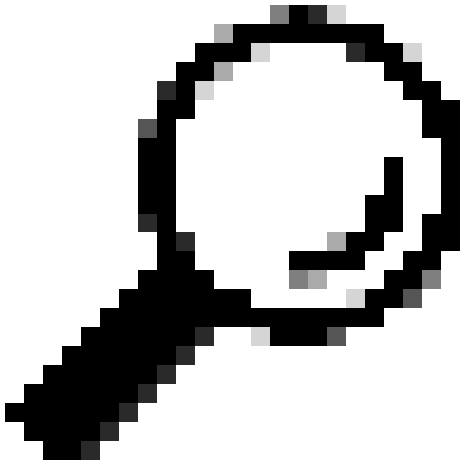
Stadi	Impedisci a utenti specifici di accedere a qualsiasi sito Web	Impedisci a utenti specifici di accedere a determinati siti Web

Categoria URL personalizzato	Non applicabile.	Creare una categoria URL personalizzata per i siti a cui si intende bloccare l'accesso. Per maggiori informazioni, visitare: Configurazione di categorie URL personalizzate in Secure Web Appliance - Cisco
Profilo di identificazione	Passaggio 1. Dalla GUI, selezionare Web Security Manager, quindi fare clic su Profili di identificazione. Passaggio 2. Fare clic su Aggiungi profilo per aggiungere un profilo. Passaggio 3. Utilizzare la casella di controllo Abilita profilo di identificazione per abilitare o disabilitare rapidamente il profilo senza eliminarlo. Passaggio 4. Assegnare un nome di profilo univoco. Passaggio 5. (Facoltativo) Aggiungere Una Descrizione. Passaggio 6. Dall'elenco a discesa Inserisci sopra, scegliere dove visualizzare il profilo nella tabella. Passaggio 7. Nella sezione Metodo di identificazione utente scegliere Esenzione da autenticazione/identificazione. Passaggio 8. In Definisci membri per subnet immettere gli indirizzi IP o le subnet che devono essere applicati dal profilo di identificazione. È possibile utilizzare indirizzi IP, blocchi CIDR (Classless Inter-Domain Routing) e subnet.	 Nota: per bloccare l'accesso a determinati siti Web per tutti gli utenti, non è necessario creare un profilo ID separato. Questa funzionalità può essere gestita in modo efficiente tramite le Regole di accesso e decrittografia globali. Passaggio 1. Dalla GUI, selezionare Web Security Manager, quindi fare clic su Profili di identificazione. Passaggio 2. Fare clic su Aggiungi profilo per aggiungere un profilo. Passaggio 3. Utilizzare la casella di controllo Abilita profilo di identificazione per abilitare o disabilitare rapidamente il profilo senza eliminarlo. Passaggio 4. Assegnare un nome di profilo univoco. Passaggio 5. (Facoltativo) Aggiungere Una Descrizione.

		Passaggio 6. Dall'elenco a discesa Inserisci sopra, scegliere dove visualizzare il profilo nella tabella. Passaggio 7. Nella sezione Metodo di identificazione utente scegliere Esenzione da autenticazione/identificazione. Passaggio 8. In Definisci membri per subnet immettere gli indirizzi IP o le subnet che devono essere applicati dal profilo di identificazione. È possibile utilizzare indirizzi IP, blocchi CIDR (Classless Inter-Domain Routing) e subnet. Passaggio 9. Fare clic su Advanced (Avanzate) e aggiungere la categoria URL a cui si desidera bloccare l'accesso.
Criterio di decrittografia	Passaggio 1. Dalla GUI, selezionare Web Security Manager, quindi fare clic su Decryption Policy (Criterio di decrittografia). Passaggio 2. Fare clic su Aggiungi criterio per aggiungere un criterio di decrittografia. Passaggio 3. Utilizzare la casella di controllo Abilita criterio per abilitare il criterio. Passaggio 4. Assegnare un nome di criterio univoco. Passaggio 5. (Facoltativo) Aggiungere Una Descrizione. Passaggio 6. Dall'elenco a discesa Inserisci sopra criterio scegliere il primo criterio. Passaggio 7. In Profili di identificazione e utenti scegliere il profilo di identificazione creato nei passi precedenti.	Passaggio 1. Dalla GUI, selezionare Web Security Manager, quindi fare clic su Decryption Policy (Criterio di decrittografia). Passaggio 2. Fare clic su Aggiungi criterio per aggiungere un criterio di decrittografia. Passaggio 3. Utilizzare la casella di controllo Abilita criterio per abilitare il criterio. Passaggio 4. Assegnare un nome di criterio univoco. Passaggio 5. (Facoltativo) Aggiungere Una Descrizione. Passaggio 6. Dall'elenco a discesa Inserisci sopra criterio scegliere il primo criterio. Passaggio 7. In Profili di identificazione e utenti scegliere il profilo di identificazione creato nei passi precedenti.

Passaggio 8. Invia.

Passaggio 9. Nella pagina Criteri di decrittografia, in Filtro URL, fare clic sul collegamento associato al nuovo criterio di decrittografia.

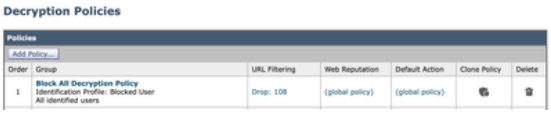


Suggerimento: poiché si bloccano tutte le categorie URL, è possibile ottimizzare il criterio rimuovendo le categorie URL personalizzate e utilizzando solo le categorie URL predefinite. In questo modo si riduce il carico di elaborazione sull'interfaccia SWA evitando l'ulteriore passaggio di abbinare gli URL alle categorie URL personalizzate.

Passaggio 10. Selezionare Elimina come azione per ciascuna categoria di URL.

Passaggio 11. Nella stessa pagina, scorrere l'elenco fino a URL non classificati, quindi selezionare Drop (Elimina) dall'elenco a discesa.

Passaggio 12. Invia.



Passaggio 8. Invia.

Passaggio 9. Nella pagina Criteri di decrittografia, in Filtro URL, fare clic sul collegamento associato al nuovo criterio di decrittografia.

Passaggio 10. Selezionare Elimina come azione per la categoria URL personalizzato creata per i siti Web bloccati.

Passaggio 11. Fare clic su Invia.

Immagine - Blocca alcuni URL nel criterio di decrittografia

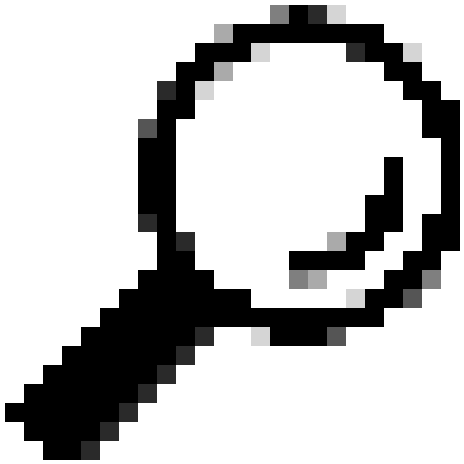
	Immagine - Criterio di decrittografia per bloccare tutto il sito Web per determinati utenti	
Criteri di accesso	Passaggio 1. Dalla GUI, selezionare Web Security Manager, quindi fare clic su Access Policy (Criteri di accesso). Passaggio 2. Fare clic su Aggiungi criterio per aggiungere un criterio di accesso. Passaggio 3. Utilizzare la casella di controllo Abilita criterio per abilitare il criterio. Passaggio 4. Assegnare un nome di criterio univoco. Passaggio 5. (Facoltativo) Aggiungere Una Descrizione. Passaggio 6. Dall'elenco a discesa Inserisci sopra criterio scegliere il primo criterio. Passaggio 7. In Profili di identificazione e utenti scegliere il profilo di identificazione creato nei passi precedenti. Passaggio 8. Invia. Passaggio 9. Nella pagina Criteri di accesso, in Protocolli e agenti utente, fare clic sul collegamento associato a questi nuovi criteri di accesso. Passaggio 10. Nell'elenco a discesa Modifica impostazioni protocolli e agenti utente scegliere Definisci impostazioni personalizzate. Passaggio 11. Dentro Protocolli a blocchi: selezionare casella di controllo per entrambi FTP su HTTP e HTTP. Passaggio 12. Dentro Porte CONNECT HTTP, rimuovere ogni numero di porta per bloccare tutte le	Passaggio 1. Dalla GUI, selezionare Web Security Manager, quindi fare clic su Access Policy (Criteri di accesso). Passaggio 2. Fare clic su Aggiungi criterio per aggiungere un criterio di accesso. Passaggio 3. Utilizzare la casella di controllo Abilita criterio per abilitare il criterio. Passaggio 4. Assegnare un nome di criterio univoco. Passaggio 5. (Facoltativo) Aggiungere Una Descrizione. Passaggio 6. Dall'elenco a discesa Inserisci sopra criterio scegliere il primo criterio. Passaggio 7. In Profili di identificazione e utenti scegliere il profilo di identificazione creato nei passi precedenti. Passaggio 8. Invia. Passaggio 9. Nella pagina Criteri di accesso, in Filtro URL, fare clic sul collegamento associato al nuovo criterio di accesso Passaggio 10. Selezionare Blocca come azione per la categoria URL personalizzato creata per i siti Web bloccati. Passaggio 11. Invia. Passaggio 12. Eseguire il commit delle modifiche.  Immagine - Blocca alcuni URL nei criteri di accesso

porte.

Immagine - Blocco di protocolli e porte di connessione nei criteri di accesso

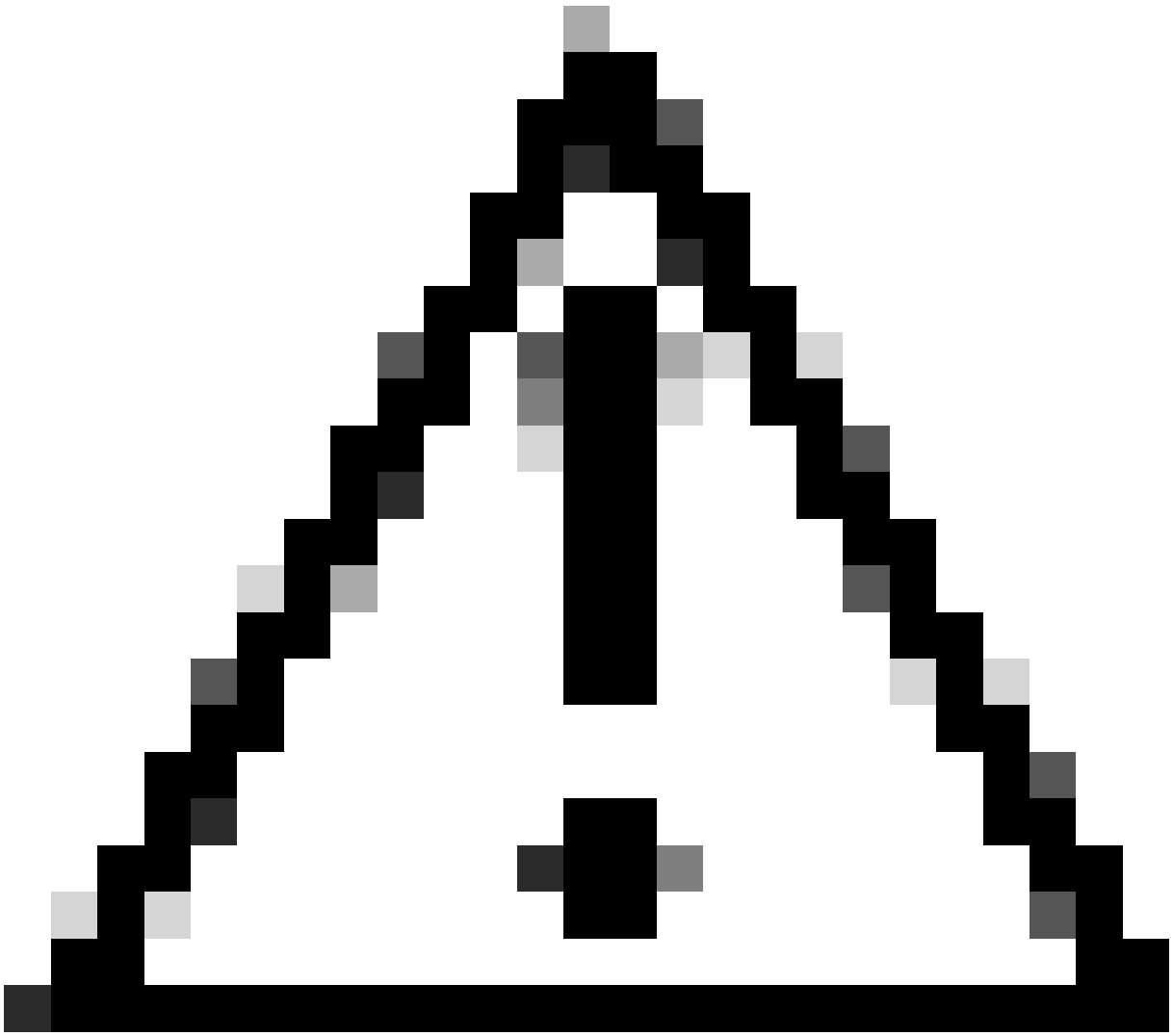
Passaggio 13. Invia.

Passaggio 14. (Facoltativo) Nella pagina Criteri di accesso, in Filtro URL, fare clic sul collegamento associato al nuovo criterio di accesso e selezionare Blocca come azione per ciascuna categoria di URL e URL non classificati, quindi inviati.



Suggerimento: poiché si bloccano tutte le categorie URL, è possibile ottimizzare il criterio rimuovendo le categorie URL personalizzate e utilizzando solo le categorie URL predefinite. In questo modo si riduce il carico di elaborazione sull'interfaccia SWA evitando l'ulteriore passaggio di abbinare gli URL alle categorie URL

	personalizzate. Passaggio 16. Eseguire il commit delle modifiche.  Immagine- Criteri di accesso per bloccare tutti i siti	



Attenzione: nella distribuzione proxy trasparente, SWA non può leggere gli agenti utente o l'URL completo per il traffico HTTPS a meno che il traffico non venga decrittografato. Di conseguenza, se si configura il profilo di identificazione utilizzando gli agenti utente o una categoria di URL personalizzati con espressioni regolari, questo traffico non corrisponde

al profilo di identificazione.

Blocco dei siti mediante espressioni regolari nella distribuzione proxy trasparente

In una distribuzione proxy trasparente, se si intende bloccare una categoria di URL personalizzati che presenta la condizione Espressioni regolari, ad esempio per bloccare l'accesso ad alcuni canali YouTube, è possibile eseguire la procedura seguente:

Passaggio 1. Creare una categoria URL personalizzata per il sito principale. In questo esempio: YouTube.com.

Passaggio 2. Creare un criterio di decrittografia, assegnare questa categoria di URL personalizzati e impostare l'azione su Decrittografa.

Passaggio 3. Creare un criterio di accesso, assegnare la categoria URL personalizzato alle espressioni regolari (in questo esempio la categoria URL personalizzato per i canali YouTube) e impostare l'azione su Blocca.

Informazioni correlate

- Guida per l'utente di AsyncOS 15.0 per Cisco Secure Web Appliance - GD (General Deployment) - Classify End-Users for Policy Application [Cisco Secure Web Appliance] - Cisco
- Configurazione di categorie URL personalizzate in Secure Web Appliance - Cisco
- Come esentare il traffico di Office 365 dall'autenticazione e dalla decrittografia su Cisco Web Security Appliance (WSA) - Cisco

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).