Ignora traffico aggiornamenti Microsoft in Secure Web Appliance

Sommario

Introduzione

In questo documento viene descritto come ignorare il traffico degli aggiornamenti Microsoft in Secure Web Appliance (SWA).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Amministrazione della SWA.

Cisco consiglia di installare i seguenti strumenti:

- SWA fisico o virtuale
- 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.

Aggiornamenti Microsoft

Gli aggiornamenti Microsoft sono patch essenziali, aggiornamenti per la sicurezza e miglioramenti delle funzionalità rilasciati da Microsoft per i sistemi operativi e le applicazioni software. Questi aggiornamenti sono fondamentali per mantenere la sicurezza, la stabilità e le prestazioni dei computer e dei dispositivi di rete. Garantiscono la protezione dei sistemi da vulnerabilità, la risoluzione dei bug e l'integrazione di nuove funzionalità o miglioramenti nel software.

L'impatto degli aggiornamenti Microsoft sui server proxy, ad esempio Cisco SWA, può essere significativo. Questi aggiornamenti spesso implicano il download di file di grandi dimensioni o di numerosi file di piccole dimensioni, che possono occupare una notevole quantità di larghezza di banda e di risorse di elaborazione sul proxy. Ciò può causare congestione, rallentamento delle prestazioni di rete e un aumento del carico sull'infrastruttura proxy, con un potenziale impatto sull'esperienza complessiva dell'utente e su altre operazioni di rete critiche.

Ignorare il traffico di Microsoft Update dal proxy può essere un modo sicuro ed efficace per gestire queste problematiche. Poiché gli aggiornamenti Microsoft provengono da server Microsoft attendibili, consentire a questo traffico di ignorare il proxy può contribuire a ridurre il carico sul server proxy senza compromettere la sicurezza della rete. In questo modo, gli aggiornamenti essenziali vengono distribuiti in modo efficiente, preservando al contempo le risorse proxy per altre attività di sicurezza e di filtro dei contenuti. È tuttavia importante implementare tali configurazioni di bypass con attenzione per mantenere la sicurezza complessiva della rete e la conformità con le policy organizzative.

Ignora aggiornamenti Microsoft

Se si sta valutando la possibilità di evitare l'inoltro del traffico degli aggiornamenti Microsoft, esistono due approcci principali

1. Bypass: questa operazione implica la configurazione della rete per reindirizzare il traffico in modo che non raggiunga mai il dispositivo SWA.
2. Pass-through: questa operazione implica la configurazione dell'SWA in modo che non decrittografi né esegua la scansione del traffico degli aggiornamenti Microsoft, consentendone il passaggio attraverso il proxy senza ispezione.

Aggirare il traffico nell'SWA

Per evitare il traffico degli aggiornamenti Microsoft nelle reti dotate di SWA, l'approccio varia a seconda della configurazione dell'installazione proxy:

Tipo di distribuzione	Aggirare il traffico
Distribuzione trasparente	È possibile reindirizzare il traffico degli aggiornamenti

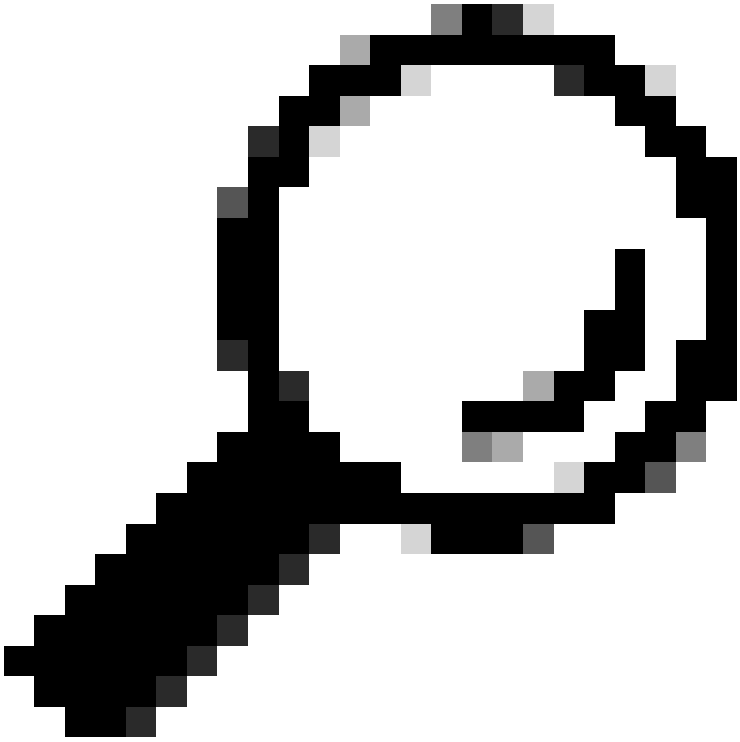
	Microsoft sul router o sugli switch di livello 4 responsabili dell'inoltro del traffico al server proxy.
	È possibile configurare le impostazioni di bypass direttamente nell'interfaccia grafica (GUI) SWA.
Distribuzione esplicita	Per evitare che il traffico di Microsoft Updates raggiunga il SWA, è necessario configurare il bypass all'origine. Ciò significa esentare gli URL rilevanti sui computer client per garantire che il traffico non venga reindirizzato al dispositivo SWA.

Se bypassare un traffico specifico richiede un'ampia riprogettazione della rete e non è fattibile, un approccio alternativo è configurare l'SWA in modo che passi attraverso alcuni tipi di traffico. A tal fine, è possibile impostare l'SWA in modo che non decripti né esegua la scansione del traffico designato, consentendo al proxy di passare attraverso il proxy senza ispezione. Questo metodo garantisce l'efficienza della distribuzione del traffico essenziale, riducendo al minimo l'impatto sulle prestazioni della rete e sulle risorse proxy.

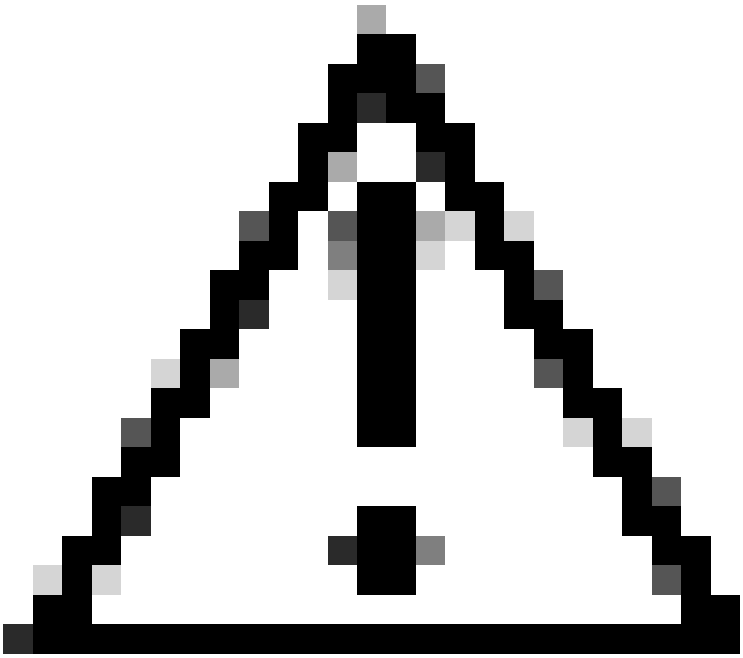
Passthrough di aggiornamenti Microsoft

I traffici di aggiornamenti Microsoft sono suddivisi in quattro fasi principali:

Fase	Passi
1. Creare una categoria URL personalizzata per gli URL di Microsoft Update	Passaggio 1.Dalla GUI, selezionare Web Security Manager, quindi fare clic su Categorie URL personalizzate ed esterne. Passaggio 2. Fare clic su Aggiungi categoria per aggiungere una categoria URL personalizzata. Passaggio 4. Assegnare un CategoryName univoco. Passaggio 5. (Facoltativo) Aggiungere Una Descrizione. Passaggio 6. Da Ordine elenco, scegliere la prima categoria da posizionare in alto. Passaggio 7. Dall'elenco a discesa Category Typedrop, scegliere Local Custom Category (Categoria personalizzata locale). Passaggio 8. Aggiungere gli URL di Microsoft Update nella sezione Siti.



Suggerimento: è possibile controllare l'elenco degli aggiornamenti Microsoft da questo collegamento: [Passaggio 2 - Configurazione di WSUS | Microsoft Learn]



Attenzione: non copiare/incollare gli URL come sono nei documenti Microsoft. Formattarli correttamente come formato SWA. Per ulteriori informazioni,

	visitare: Configure Custom URL Categories in Secure Web Appliance - Cisco Passaggio 9. Invia.
2. Creare un profilo di identificazione per esentare il traffico degli aggiornamenti Microsoft dall'autenticazione	Passaggio 10.Dalla GUI, selezionare Web Security Manager e fare clic su Profili di identificazione. Passaggio 11. Fare clic su Aggiungi profilo per aggiungere un profilo. Passaggio 12.Utilizzare la casella di controllo Abilita profilo di identificazione per abilitare o disabilitare rapidamente il profilo senza eliminarlo. Passaggio 13. Assegnare un profileName univoco. Passaggio 14. (Facoltativo) Aggiungere Una Descrizione. Passaggio 15.Dall'elenco a discesa Inserisci, scegliere la posizione in cui visualizzare il profilo nella tabella. Passaggio 16. Nella sezione Metodo di identificazione utente, scegliere Esenzione da autenticazione/identificazione. Passaggio 17.Nella finestra Definisci membri per subnet, se si desidera passare attraverso il traffico Microsoft per alcuni utenti specifici, immettere gli indirizzi IP o le subnet applicabili oppure lasciare vuoto questo campo per includere tutti gli indirizzi IP. Passaggio 18. Dalla sezione Advanced, scegliere Custom URL Categories (Categorie URL personalizzate). Passaggio 19. Aggiungere la categoria URL personalizzata creata per gli aggiornamenti Microsoft. Passaggio 20. Selezionate Fatto (Done). Passaggio 21. Invia.
3. Creare un criterio di decrittografia per il passaggio del traffico degli aggiornamenti Microsoft	Passaggio 22.Dalla GUI, selezionare Web Security Manager, quindi fare clic su Criterio di decrittografia. Passaggio 23. Fare clic su Aggiungi criterio per aggiungere un criterio di decrittografia. Passaggio 24.Utilizzare la casella di controllo Abilita criterio

	per abilitare questo criterio. Passaggio 25. Assegnare un PolicyName univoco. Passaggio 26. (Facoltativo) Aggiungere Una Descrizione. Passaggio 27.Dall'elenco a discesa Inserisci sopra criterio, scegliere il primo criterio. Passaggio 28.Da Profili di identificazione e utenti, scegliere il Profilo di identificazione creato nei passaggi precedenti. Passaggio 29. Invia. Passaggio 30. Nella pagina Criteri di decrittografia, in Filtro URL, fare clic sul collegamento associato a questo nuovo criterio di decrittografia. Passaggio 32.SelectPassThrough come categoria di azioni per gli URL degli aggiornamenti Microsoft. Passaggio 32. Invia.
4. Creare un criterio di accesso per consentire il traffico degli aggiornamenti Microsoft	Passaggio 3.Dalla GUI, selezionare Web Security Manager, quindi fare clic su Access Policy (Policy di accesso). Passaggio 34. Fare clic su Aggiungi criterio per aggiungere un criterio di accesso. Passaggio 35.Utilizzare la casella di controllo Abilita criterio per abilitare questo criterio. Passaggio 36. Assegnare un PolicyName univoco. Passaggio 37. (Facoltativo) Aggiungere Una Descrizione. Passaggio 38.Dall'elenco a discesa Inserisci sopra criterio, scegliere il primo criterio. Passaggio 39.Da Profili di identificazione e utenti, scegliere il Profilo di identificazione creato nei passaggi precedenti. Passaggio 40. Invia. Passaggio 9. Nella pagina Criteri di accesso, in Filtro URL, fare clic sul collegamento associato al nuovo criterio di accesso Passaggio 10. Selezionare Consenti l'azione per la categoria URL personalizzato creata per gli aggiornamenti Microsoft. Passaggio 11. Invia. Passaggio 12. Eseguire il commit delle modifiche.

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
- Uso delle best practice di Secure Web Appliance - Cisco
- Bypass Authentication in Secure Web Appliance - 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).