Ignora autenticazione in Secure Web Appliance

Sommario

Introduzione

In questo documento viene descritta la procedura per concedere l'esenzione dall'autenticazione 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.

Autenticazione esente

L'esenzione dall'autenticazione per alcuni utenti o sistemi nell'SWA di Cisco può essere cruciale

per mantenere l'efficienza operativa e soddisfare requisiti specifici. In primo luogo, alcuni utenti o sistemi richiedono l'accesso ininterrotto a risorse o servizi critici che potrebbero essere ostacolati dai processi di autenticazione. Ad esempio, i sistemi automatizzati o gli account di servizio che eseguono aggiornamenti o backup regolari devono poter accedere senza difficoltà senza i ritardi o i potenziali errori introdotti dai meccanismi di autenticazione.

In alcuni casi, inoltre, il provider di servizi Web consiglia di non utilizzare un proxy per accedere al servizio. In questi casi, l'esenzione dell'autenticazione garantisce la conformità alle linee guida del provider e garantisce l'affidabilità del servizio. Inoltre, per bloccare efficacemente il traffico per alcuni utenti, spesso è necessario prima esentarli dall'autenticazione e poi applicare le opportune politiche di blocco. Questo approccio consente un controllo preciso sui permessi di accesso.

In alcuni casi, il servizio Web a cui si accede è attendibile e universalmente accettabile, ad esempio gli aggiornamenti di Microsoft. L'esenzione dell'autenticazione per tali servizi semplifica l'accesso per tutti gli utenti. Inoltre, vi sono situazioni in cui il sistema operativo o l'applicazione dell'utente non supporta il meccanismo di autenticazione configurato nell'SWA, che richiede un bypass per garantire la connettività.

Infine, i server con indirizzi IP fissi che non dispongono di accessi utente e dispongono di un accesso Internet sicuro e limitato non richiedono l'autenticazione, in quanto i modelli di accesso sono prevedibili e sicuri.

Esentando strategicamente l'autenticazione per questi casi, le organizzazioni possono bilanciare le esigenze di sicurezza con l'efficienza operativa.

Metodi per l'esenzione dell'autenticazione in Cisco SWA

L'esenzione dell'autenticazione nell'SWA può essere ottenuta tramite vari metodi, ognuno adattato a specifici scenari e requisiti. Di seguito sono riportati alcuni metodi comuni per configurare le esenzioni dall'autenticazione:

- Indirizzo IP o subnet mask: uno dei metodi più semplici consiste nell'esentare dall'autenticazione indirizzi IP specifici o intere subnet. Ciò è particolarmente utile per i server con indirizzi IP fissi o segmenti di rete attendibili che richiedono un accesso ininterrotto a Internet o alle risorse interne. Specificando questi indirizzi IP o subnet mask nella configurazione SWA, è possibile garantire che questi sistemi ignorino il processo di autenticazione.
- Porte proxy: è possibile configurare l'interfaccia SWA in modo che esenti il traffico in base a porte proxy specifiche. Ciò è utile quando alcune applicazioni o servizi utilizzano porte designate per la comunicazione. Identificando queste porte, è possibile configurare l'interfaccia SWA in modo che ignori l'autenticazione per il traffico su queste porte, garantendo un accesso senza problemi alle applicazioni o ai servizi pertinenti.
- Categorie URL: un altro metodo consiste nell'esentare l'autenticazione in base alle categorie URL. Possono includere sia categorie Cisco predefinite sia categorie URL personalizzate definite dall'utente in base alle esigenze specifiche dell'organizzazione. Ad esempio, se

alcuni servizi Web, come gli aggiornamenti Microsoft, sono considerati attendibili e accettabili a livello globale, è possibile configurare l'SWA in modo che ignori l'autenticazione per queste categorie di URL specifiche. In questo modo, tutti gli utenti possono accedere a questi servizi senza la necessità di autenticazione.

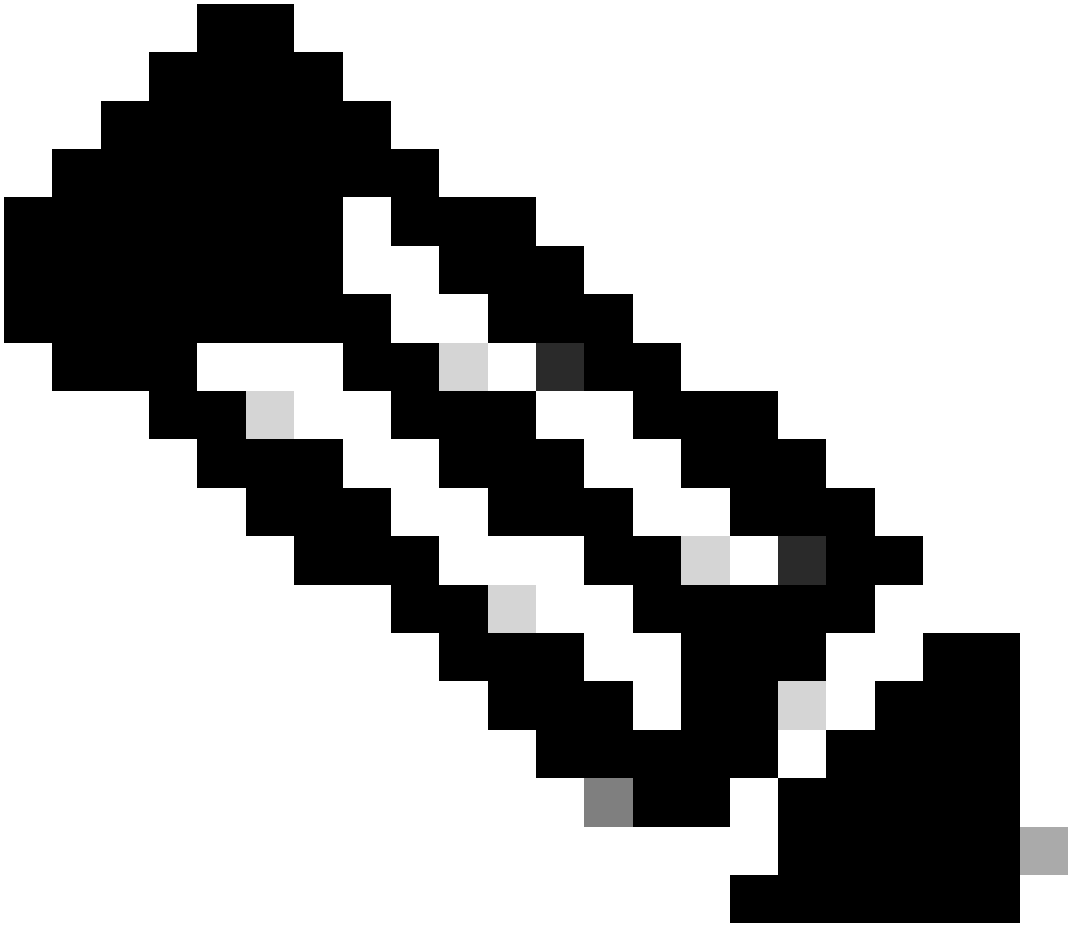
- Agenti utente: l'esenzione dell'autenticazione basata sugli agenti utente è utile quando si utilizzano applicazioni o dispositivi specifici che non supportano i meccanismi di autenticazione configurati. Identificando le stringhe degli agenti utente di queste applicazioni o dispositivi, è possibile configurare l'interfaccia SWA in modo che ignori l'autenticazione per il traffico proveniente da tali applicazioni o dispositivi, garantendo una connettività ottimale.

.

Passaggi per ignorare l'autenticazione

Per creare un profilo di identificazione da escludere dall'autenticazione, eseguire la procedura seguente:

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, scegliere la posizione in cui il profilo deve essere visualizzato nella tabella.

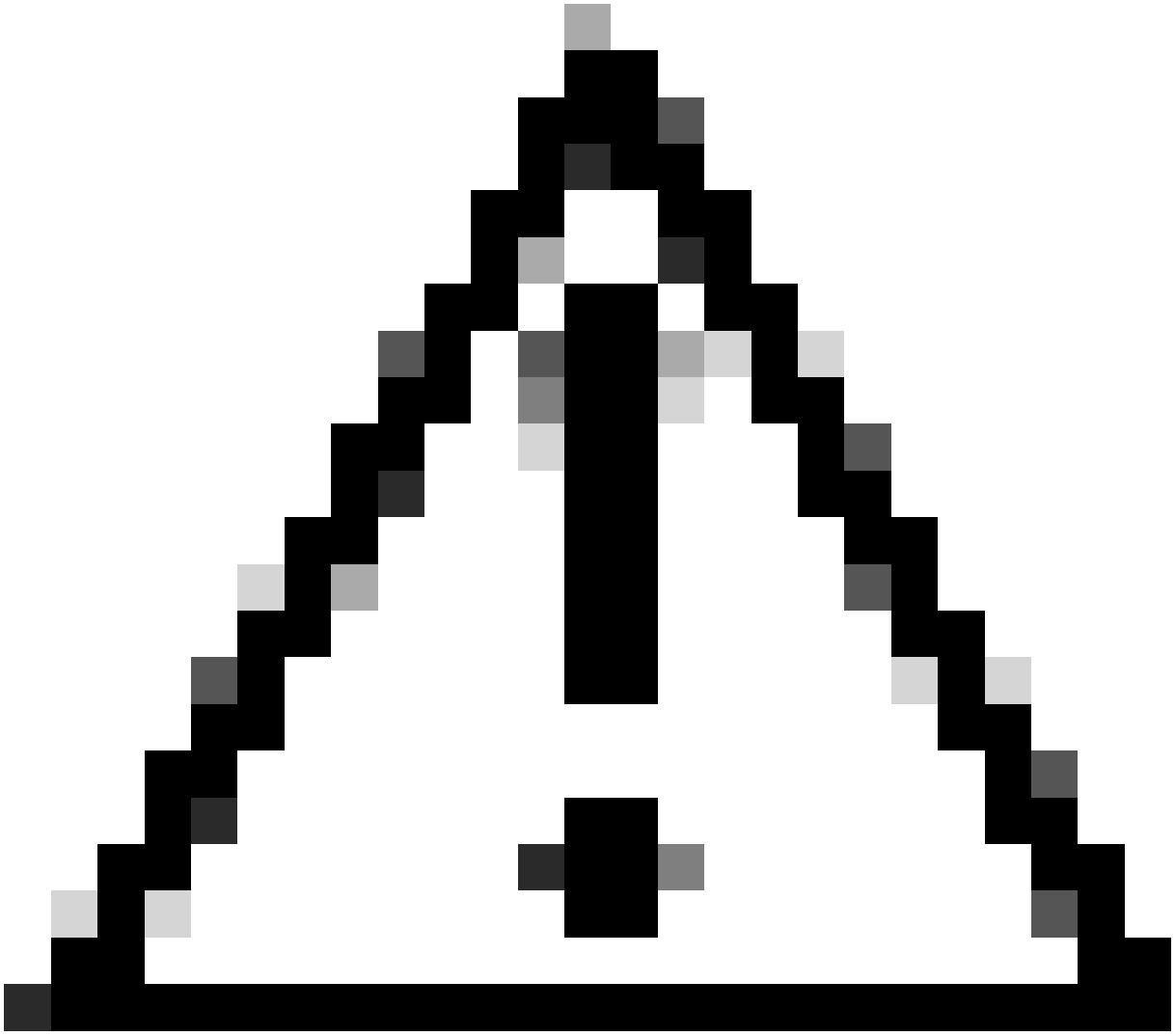


Nota: i profili di identificazione della posizione che non richiedono l'autenticazione vengono visualizzati in cima all'elenco. Questo approccio riduce il carico sull'SWA, riduce al minimo la coda di autenticazione e consente un'autenticazione più rapida per gli altri utenti.

Passaggio 7. Nella sezione Metodo di identificazione utente scegliere Esenzione da autenticazione/identificazione.

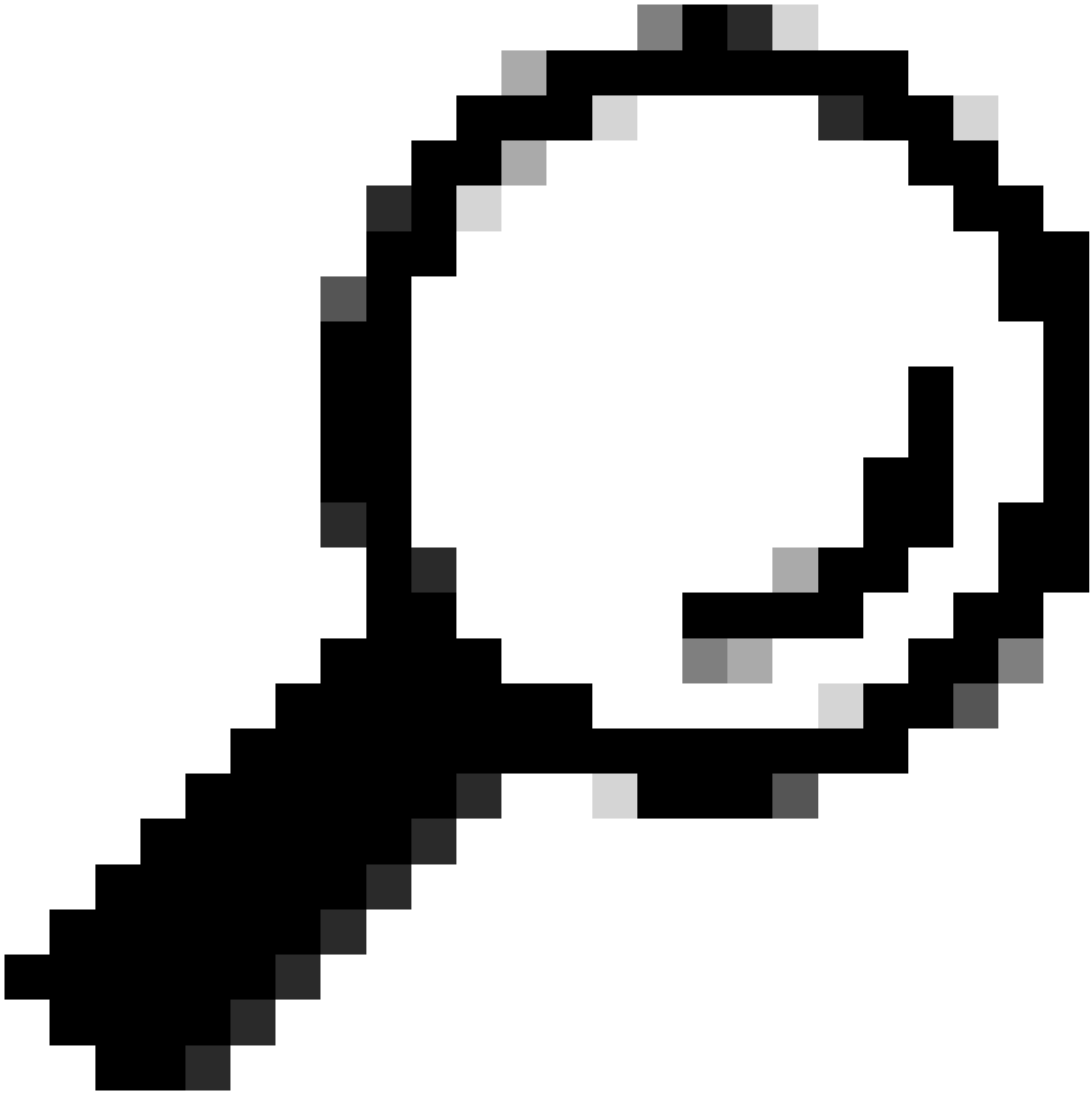
Passaggio 8. In Definisci membri per subnet immettere gli indirizzi IP o le subnet che devono essere applicati dal profilo di identificazione. È possibile utilizzare indirizzi IP, blocchi CIDR (Classless Inter-Domain Routing) e subnet.

Passaggio 9. (Facoltativo) Fare clic su Avanzate per definire ulteriori criteri di appartenenza, ad esempio porte proxy, categorie URL o agenti utente.



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.

Per ulteriori informazioni su come configurare la categoria di URL personalizzati, visitare: [Configure Custom URL Categories in Secure Web Appliance - Cisco]



Suggerimento: il criterio utilizza una logica AND, che indica che devono essere soddisfatte tutte le condizioni affinché il profilo ID corrisponda. Quando sono impostate le opzioni avanzate, è necessario soddisfare ogni singolo requisito affinché il criterio venga applicato.

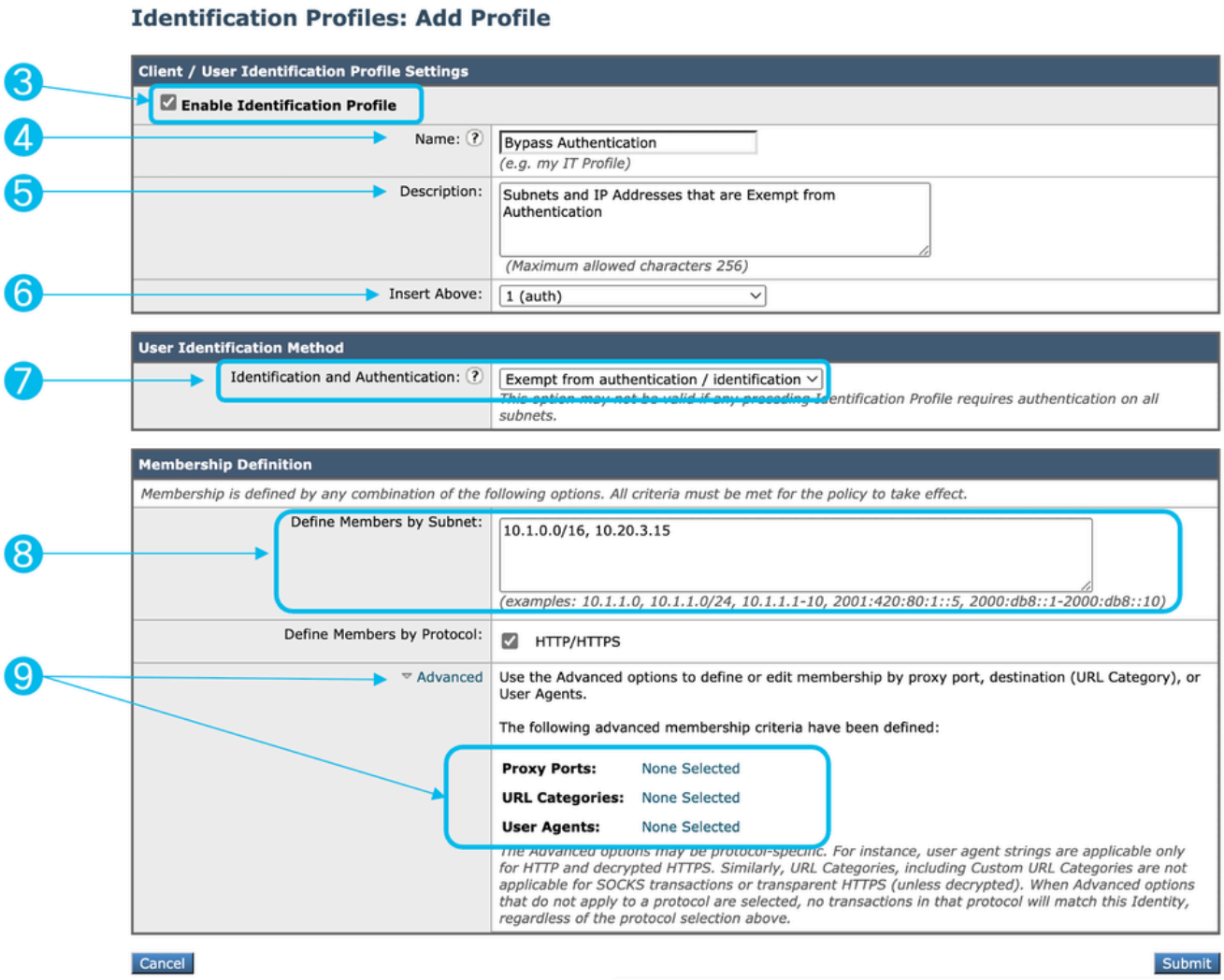


Immagine - Procedura per la creazione del profilo ID per ignorare l'autenticazione

Passaggio 10. Inviare e confermare le 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

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).