Configurare il proxy upstream in Secure Web Appliance

Sommario

Introduzione

In questo documento viene descritto come configurare il proxy upstream in Secure Web Appliance (SWA).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Amministrazione della SWA.
- Protocolli di rete e proxy di base.

Cisco consiglia di installare i seguenti strumenti:

- SWA fisico o virtuale

- Accesso amministrativo all'interfaccia grafica (GUI) SWA
- Accesso amministrativo all'interfaccia CLI (Command Line Interface) 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.

Configurazione del proxy upstream

Per configurare un proxy upstream in SWA, attenersi alla seguente procedura.

Passi	Passi
Passaggio 1. (Facoltativo) Creazione di una categoria URL personalizzata per gli URL Nota: Se si desidera definire il proxy upstream per tutto il traffico, è possibile ignorare questo passaggio.	Passaggio 1.1.Dalla GUI, selezionare Web Security Manager, quindi fare clic su Categorie URL personalizzate ed esterne. Passaggio 1.2.Fare clic su Aggiungi categoria per aggiungere una categoria URL personalizzata. Passaggio 1.3. Assegnare un CategoryName univoco. Passaggio 1.4. (Facoltativo) Aggiungere Una Descrizione. Passaggio 1.5. Da Ordine elenco, scegliere la prima categoria da posizionare in alto. Passaggio 1.6. Dall'elenco a discesa Category Typedrop, scegliere Local Custom Category (Categoria personalizzata locale). Passaggio 1.7. Aggiungere gli URL desiderati nella sezione Siti. Passaggio 1.8. Inviare.

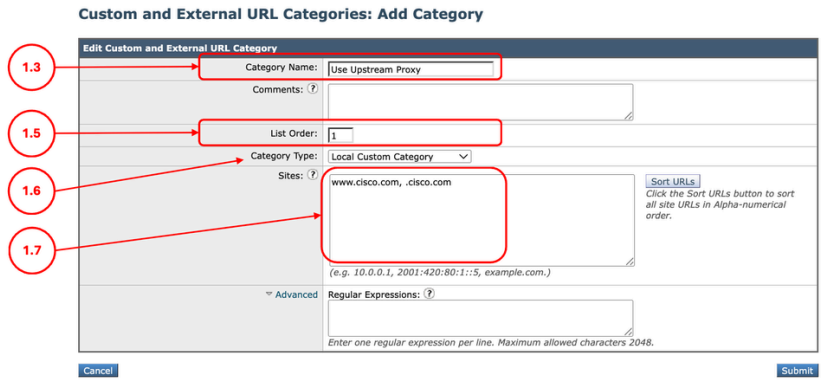


Immagine - Creazione di una categoria URL personalizzata

Passaggio 2. (Facoltativo) Creare un profilo di identificazione per utilizzare il proxy upstream

Nota: Se si desidera definire il proxy upstream per tutto il traffico, è possibile ignorare questo passaggio.

Passaggio 2.1.Dalla GUI, selezionare Web Security Manager e fare clic su Profili di identificazione.
Passaggio 2.2.Fare clic su Aggiungi profilo per aggiungere un profilo.
Passaggio 2.3.Utilizzare la casella di controllo Abilita profilo di identificazione per abilitare o disabilitare rapidamente il profilo senza eliminarlo.
Passaggio 2.4. Assegnare un profileName univoco.
Passaggio 2.5. (Facoltativo) Aggiungere Una Descrizione.
Passaggio 2.6.Dall'elenco a discesa Inserisci sopra, scegliere la posizione in cui visualizzare il profilo nella tabella.

Passaggio 2.7. Se si desidera non autenticare gli utenti che utilizzano questo criterio, nella sezione Metodo di identificazione utente scegliere Esente da autenticazione/identificazione, altrimenti configurare i parametri di autenticazione.

Passaggio 2.8.In Definisci membri per subnet, lasciare vuoto questo campo per includere tutti gli indirizzi IP dei client a meno che non si desideri passare attraverso il traffico per determinati indirizzi IP.

Passaggio 2.9. (Facoltativo: se è necessario utilizzare un proxy upstream per utenti specifici che accedono a determinati siti Web, completare questo passaggio.) Dalla sezione Advanced, scegliere Custom URL Categories (Categorie URL personalizzate), quindi Add the Custom URL Category (Aggiungi categoria URL personalizzata) creata nel passo 1

Passaggio 2.10. Inoltra.

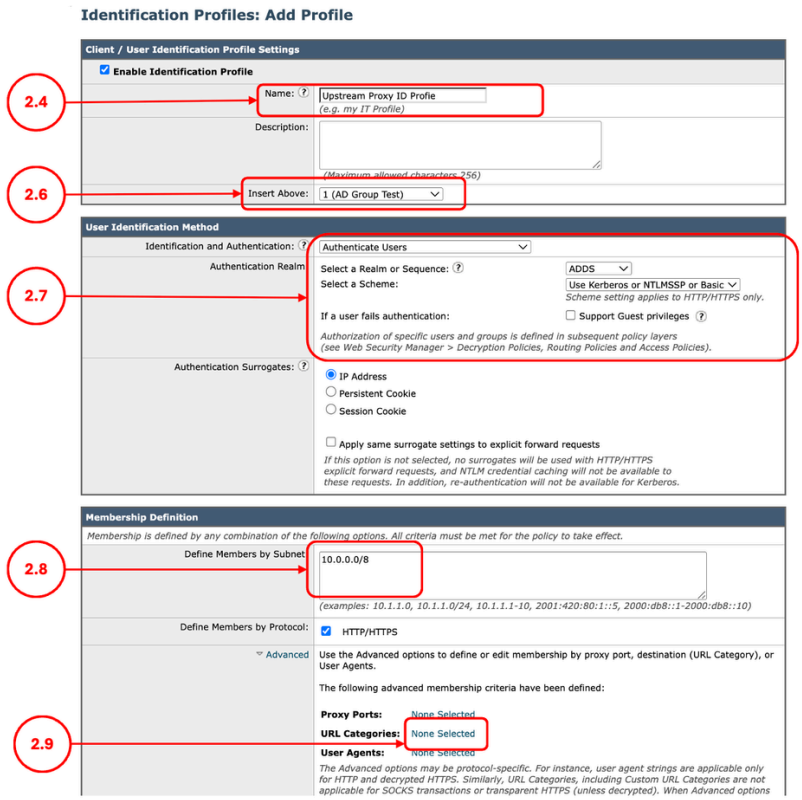
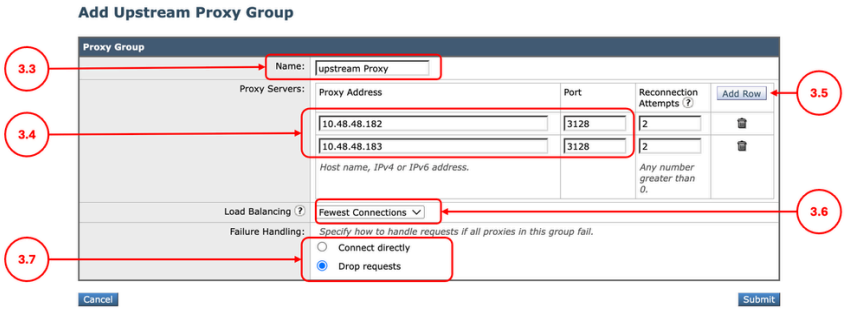


Immagine - Creazione di un profilo di identificazione

Passaggio 3. Creazione del proxy upstream	Passaggio 3.1.Dalla GUI, selezionare Network, quindi fare clic su Upstream Proxy. Passaggio 3.2. Fare clic su Aggiungi gruppo. Passaggio 3.3.Assegnare un UNIQUEName. Passaggio 3.4. Definire l'indirizzo proxy e il numero di porta. Passaggio 3.5. (Facoltativo) Se si dispone di più proxy upstream, fare clic su Aggiungi riga per definire il proxy successivo. Passaggio 3.6. (Facoltativo) Se sono stati immessi più proxy upstream dalla sezione Bilanciamento del carico, definire il metodo di bilanciamento del carico desiderato. • Nessuno (failover): il proxy Web indirizza le transazioni a un proxy esterno nel gruppo. Tenta di connettersi ai proxy nell'ordine in cui sono elencati. Se non è possibile raggiungere un proxy, il proxy Web tenta di connettersi a quello successivo nell'elenco. • Meno connessioni: il proxy Web tiene traccia del numero di richieste attive con i diversi proxy nel gruppo e indirizza una transazione al proxy che attualmente sta servendo il minor numero di connessioni. • Basato su hash:utilizzato meno di recente. Il proxy

	Web indirizza una transazione al proxy che ha ricevuto una transazione meno di recente se tutti i proxy sono attivi. Questa impostazione è simile alla funzione round robin, con la differenza che il proxy Web prende in considerazione anche le transazioni ricevute da un proxy come membro di un gruppo di proxy diverso. In altre parole, se un proxy è elencato in più gruppi di proxy, è meno probabile che l'opzione "utilizzata meno di recente" sovraccarichi il proxy. • Round robin: il proxy Web esegue il ciclo delle transazioni equamente tra tutti i proxy del gruppo nell'ordine elencato. Passaggio 3.7. Scegliere l'opzione Gestione errori dipende dai criteri interni. • Connetti direttamente:invia le richieste direttamente ai server di destinazione. • Elimina richieste:ignora le richieste senza inoltrarle. Passaggio 3.8. Inoltrare.  Immagine - Aggiungi gruppo proxy upstream
Passaggio 4. (Facoltativo) Caricare il certificato di decrittografia Nota: Se il proxy upstream non sta decrittografando il traffico o il relativo server CA è già considerato attendibile nell'area SWA, è possibile ignorare questo passaggio	Passaggio 4.1.Dalla GUI, selezionare Rete, quindi fare clic su Gestione certificati. Passaggio 4.2. Dalla sezione Gestione certificati, fare clic su Gestisci certificati radice attendibili.

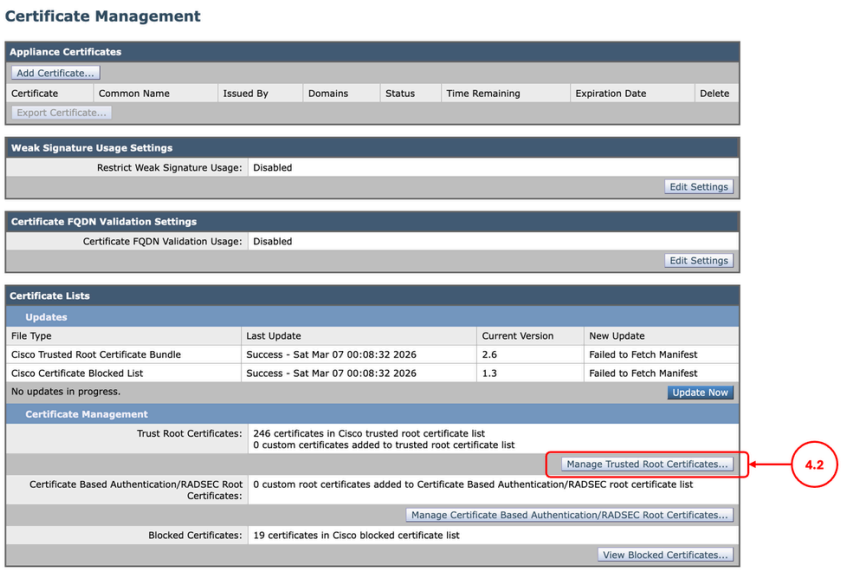


Immagine - Gestisci certificato radice attendibile

Passaggio 4.3. Sottomettere e confermare le modifiche.

> ⚠ Attenzione: se sono richiesti certificati CA radice e intermedi, caricare prima il certificato CA radice, quindi fare clic su Invia e conferma. Al termine del commit, importare il certificato CA intermedio e inviare di nuovo ed eseguire il commit delle modifiche.

Passaggio 5. Configurare i criteri di routing

Passaggio 5.1. Dalla GUI, selezionare Web Security Manager e fare clic su Criteri di routing.

Passaggio 5.2. (Facoltativo) Se si desidera utilizzare il proxy upstream per utenti o siti Web specifici, fare clic su Aggiungi criterio, quindi selezionare il profilo di identificazione creato nel passaggio 2.

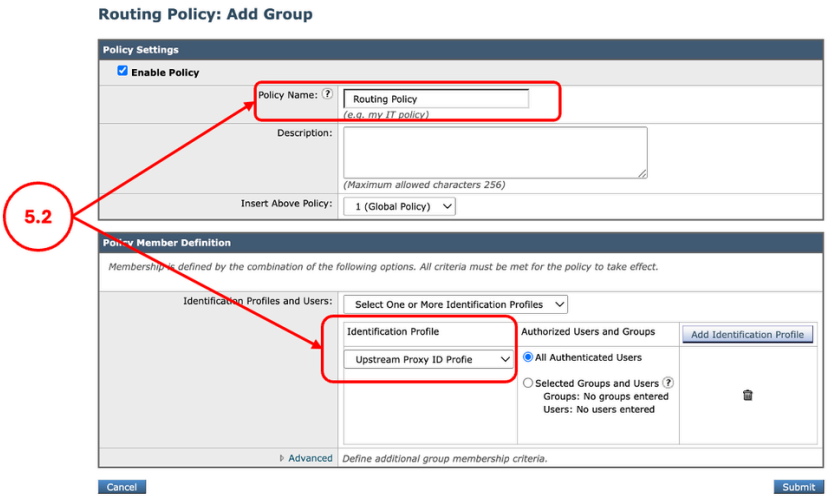


Immagine - Aggiunta del profilo ID ai criteri di routing

Passaggio 5.3. Per le condizioni desiderate, in cui si desidera utilizzare il proxy upstream, fare clic sul collegamento Destinazione di routing e selezionare il gruppo di proxy upstream creato nel passaggio 3.

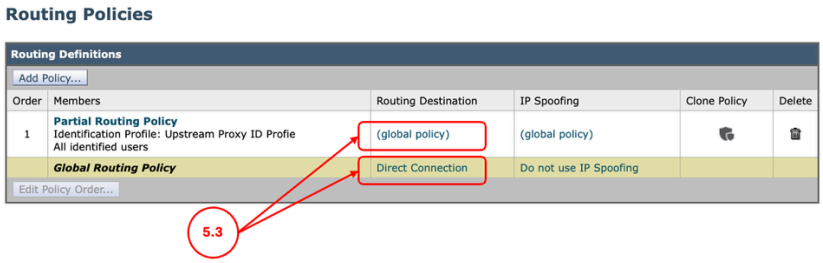


Immagine - Configurazione della destinazione di instradamento

Nota: Se si desidera che tutto il traffico utilizzi il proxy upstream, dal criterio di routing globale selezionare il proxy upstream desiderato.

Passaggio 5.4. Sottomettere e confermare le modifiche.

Passaggio 6. (Facoltativo) Configurazione delle impostazioni di timeout di mancata risposta del proxy upstream

Suggerimento: si consiglia di non modificare questi valori a meno che non se ne conosca il comportamento e l'impatto potenziale.

Passaggio 6.1. Accedere alla CLI ed eseguire advancedproxyconfig

Passaggio 6.2. Selezionare VARIE

Passaggio 6.3. Premere Invio finché non viene visualizzato il messaggio Enter minimum idle timeout per il controllo del proxy upstream che non risponde (in secondi). è possibile configurare la quantità minima di tempo, in modo che SWA attenda di riprovare il proxy a monte precedentemente dichiarato malato. Il valore predefinito è 10 secondi.

Passaggio 6.4. Premere Invio per procedere all'impostazione successiva. Quando si definisce il timeout massimo di inattività per il controllo di un proxy upstream non rispondente, si noti che se questo valore di timeout viene raggiunto prima che sia esaurito il numero configurato di tentativi di riconnessione (passaggio 3), il proxy upstream viene considerato offline.

Passaggio 6.7. Continuare a premere Invio fino a uscire dalla procedura guidata ed eseguire il commit per salvare le modifiche.

Registrazione

Log accessi

Nei log degli accessi, il traffico instradato al proxy upstream viene visualizzato come DEFAULT_PARENT seguito dal nome del proxy upstream. di seguito è riportato un esempio:

```
1775659642.780 462 10.20.3.15 TCP_MISS_SSL/200 129 CONNECT tunnel://www.cisco.com:443/ "AMOJARRA\amojar
```

Log proxy

Dai log proxy è possibile verificare lo stato dei proxy a monte.

Suggerimento: È possibile filtrare per peer per esaminare i log correlati al proxy upstream.

Di seguito sono riportati alcuni esempi, poiché i tentativi di riconnessione eseguiti nel passaggio 3 sono stati configurati due volte, dopo due errori di connessione al proxy upstream, il proxy upstream viene dichiarato e SWA rimuove questo proxy upstream dall'elenco fino al riavvio del processo proxy.

```
Thu Apr  2 13:52:35 2026 Info: PROX_CONNTRACK : 940 : [15968:0] Peer-upstream 10.48.48.182:3128 was hea
Thu Apr  2 13:52:36 2026 Info: PROX_CONNTRACK : 940 : [15968:0] Peer 10.48.48.182:3128 was sick, now he
...
Thu Apr  2 13:59:37 2026 Info: PROX_CONNTRACK : 60 : [71197:0] Peer 10.48.48.183:3128 remains sick afte
Thu Apr  2 13:59:39 2026 Warning: PROX_CONNTRACK : 70 : [71197:0] Peer-upstream 10.48.48.183:3128 decla
```

Nota: Se il proxy upstream non risponde alle richieste SYN di TCP, non restituisce un codice di risposta HTTP o restituisce una risposta HTTP 504 (Timeout gateway), il proxy upstream viene considerato non disponibile e lo stato del proxy viene modificato da Integro a Malato.

Suggerimento: Il proxy a monte viene considerato integro se restituisce un'intestazione VIA.

Informazioni correlate

- Guida per l'utente di AsyncOS 15.0 per Cisco Secure Web Appliance
- 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
- Blocca il traffico in Secure Web Appliance
- Blocca il traffico di caricamento in Secure Web Appliance
- Blocca download file eseguibile in SWA
- Ignora traffico aggiornamenti Microsoft in Secure Web Appliance
- 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).