

Configurazione della catena di proxy tra Secure Web Appliance e Umbrella SWG

Sommario

[Introduzione](#)

[Panoramica](#)

[Configurazione dei criteri di Secure Web Appliance](#)

[Per la distribuzione di proxy trasparente](#)

[Configurazione dei criteri Web SWG in Umbrella Dashboard](#)

Introduzione

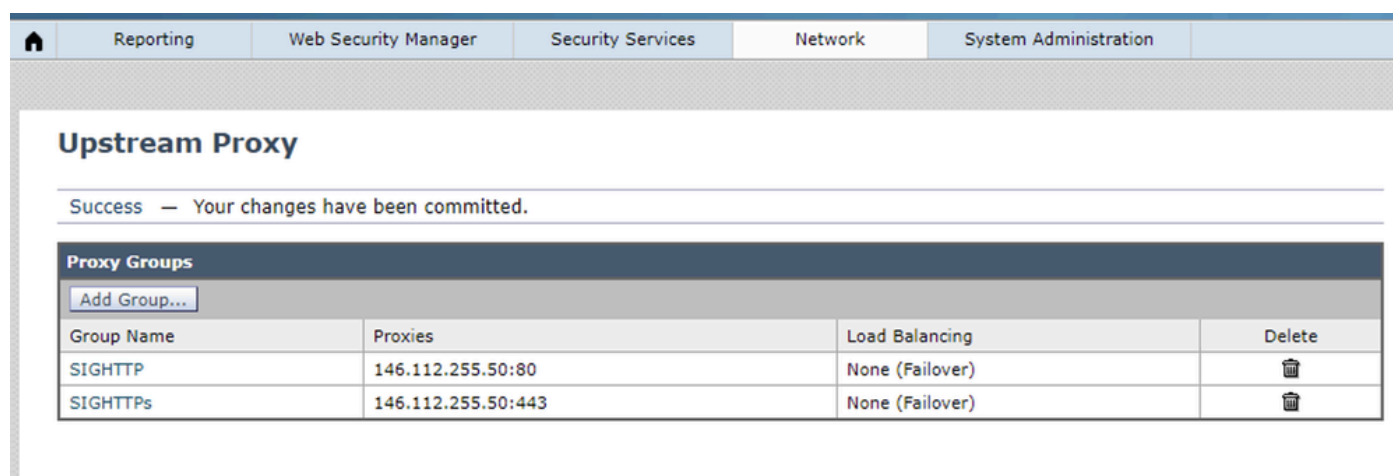
In questo documento viene descritto come configurare la catena di proxy tra Secure Web Appliance e Umbrella Secure Web Gateway (SWG).

Panoramica

Umbrella SIG supporta la catena di proxy e può gestire tutte le richieste HTTP/HTTP dal server proxy downstream. Questa è una guida completa per l'implementazione della catena di proxy tra [Cisco Secure Web Appliance \(in precedenza Cisco WSA\)](#) e [Umbrella Secure Web Gateway \(SWG\)](#), compresa la configurazione per Secure Web Appliance e SWG.

Configurazione dei criteri di Secure Web Appliance

1. Configurare i collegamenti HTTP e HTTP SWG come proxy upstream tramite Rete>Proxy upstream.



Group Name	Proxies	Load Balancing	Delete
SIGHTTP	146.112.255.50:80	None (Failover)	
SIGHTTPs	146.112.255.50:443	None (Failover)	

360079596451

2. Creare un criterio di bypass tramite Web Security Manager>Criterio di routing per instradare

direttamente tutti gli URL suggeriti a Internet. Tutti gli URL ignorati sono disponibili nella documentazione: [Guida per l'utente di Cisco Umbrella SIG: Gestisci concatenamento proxy](#)

- Creare innanzitutto una nuova "Categoria personalizzata" passando a Gestione sicurezza Web>Categorie URL personalizzate ed esterne come mostrato di seguito. Il criterio di bypass si basa sulla "Categoria personalizzata".

Home	Reporting	Web Security Manager	Security Services	Network	System Administration
------	-----------	----------------------	-------------------	---------	-----------------------

Custom and External URL Categories: Edit Category

Edit Custom and External URL Category

Category Name:	ProxyChainBypassList		
List Order:	1		
Category Type:	Local Custom Category		
Sites: ?	.cisco.com, .isrg.trustid.ocsp.identrust.com, .login.microsoftonline.com, .ocsp.int-x3.letsencrypt.org, .okta.com, .oktacdn.com, .opendns.com, .pingidentity.com, .secure.aadcdn.microsoftonline-p.com, .umbrella.com (e.g. 10.0.0.1, 2001:420:80:1::5, example.com.)		Sort URLs Click the Sort URLs button to sort all site URLs in Alpha-numerical order.
Advanced	Regular Expressions: ? Enter one regular expression per line.		

CancelSubmit

360050592552

- Creare quindi un nuovo criterio di bypass passando a Web Security Manager>Criterio di routing. Verificare che questo criterio sia il primo, in quanto Secure Web Appliance corrisponde al criterio in base all'ordine del criterio.

Reporting Web Security Manager Security Services Network System Administration

Routing Policy: BypassProxyChain

Policy Settings

☒ **Enable Policy**

Policy Name: (e.g. my IT policy)

Description:

Insert Above Policy:

Policy Member Definition

Membership is defined by the combination of the following options. All criteria must be met for the policy to take effect.

Identification Profiles and Users:

If "All Identification Profiles" is selected, at least one Advanced membership option must also be selected.

☒ **Advanced**

Use the Advanced options to define or edit membership by protocol, proxy port, subnet, Time Range, destination (URL Category), or User Agents.

The following advanced membership criteria have been defined:

Protocols:

Proxy Ports:

Subnets:

Time Range:

URL Categories:

User Agents:

360050703131

3. Creare un nuovo criterio di routing per tutte le richieste HTTP.

- Nella definizione dei membri dei criteri di routing di Secure Web Appliance, le opzioni di protocollo sono HTTP, FTP su HTTP, FTP nativo e "Tutti gli altri" mentre è selezionata l'opzione "Tutti i profili di identificazione". Poiché non è disponibile alcuna opzione per gli HTTP, creare il criterio di routing per le singole richieste HTTP dopo aver implementato il criterio di routing per tutte le richieste HTTP.

Reporting Web Security Manager Security Services Network System Administration

Routing Policies: Policy "SIGALLHTTP": Membership by Protocol

Advanced Membership Definition: Protocols

Policy membership can be defined to apply to one or more protocols. Leave all protocols unselected if membership by protocol is not desired.

Protocols: ☒ HTTP

☐ FTP over HTTP

☐ Native FTP

☐ All others

Note: Policy membership by HTTPS is not available when the HTTPS proxy is enabled.

360050592772

Reporting Web Security Manager Security Services Network System Administration

Routing Policy: SIGALLHTTP

Policy Settings

☒ Enable Policy

Policy Name: (e.g. my IT policy)

Description:

Insert Above Policy:

Policy Member Definition

Membership is defined by the combination of the following options. All criteria must be met for the policy to take effect.

Identification Profiles and Users:

If "All Identification Profiles" is selected, at least one Advanced membership option must also be selected.

Use the Advanced options to define or edit membership by protocol, proxy port, subnet, Time Range, destination (URL Category), or User Agents.

The following advanced membership criteria have been defined:

Protocols: HTTP
 Proxy Ports: None Selected
 Subnets: None Selected
 Time Range: No Time Range Definitions Available (see Web Security Manager > Defined Time Ranges)
 URL Categories: None Selected
 User Agents: None Selected

Cancel Submit

360050589572

4. Creare il criterio di instradamento per le richieste HTTP in base al "Profilo di identificazione". Prestare attenzione alla sequenza del "Profilo di identificazione" definito, poiché l'appliance Web sicura corrisponde all'"Identificazione" per la prima corrispondenza. Nell'esempio, il profilo di identificazione "win2k8" è un'identità interna basata su IP.

Reporting Web Security Manager Security Services Network System Administration

Identification Profiles

Client / User Identification Profiles				
Add Identification Profile...				
Order	Transaction Criteria	Authentication / Identification Decision	End-User Acknowledgement	Delete
1	win2k8 Subnets: 192.168.0.212 Protocols: HTTP/HTTPS	Exempt from Authentication / User Identification	(global profile)	

360050703971

Reporting Web Security Manager Security Services Network System Administration

Routing Policy: Win2k8HTTps

Policy Settings

☒ Enable Policy

Policy Name: (e.g. my IT policy)

Description:

Insert Above Policy:

Policy Member Definition

Membership is defined by the combination of the following options. All criteria must be met for the policy to take effect.

Identification Profiles and Users:

Identification Profile	Authorized Users and Groups	
win2k8	No authentication required	Add Identification Profile

☒ Advanced

Use the Advanced options to define or edit membership by protocol, proxy port, subnet, Time Range, destination (URL Category), or User Agents. The following advanced membership criteria have been defined:

Protocols: HTTP/HTTPS/FTP over HTTP in Identification Profile win2k8
Proxy Ports: None Selected
Subnets: None Selected
Time Range: No Time Range Definitions Available (see Web Security Manager > Defined Time Ranges)
URL Categories: None Selected
User Agents: None Selected

"Protocols" can't be selected for the individual "Identification Profile"

360050700091

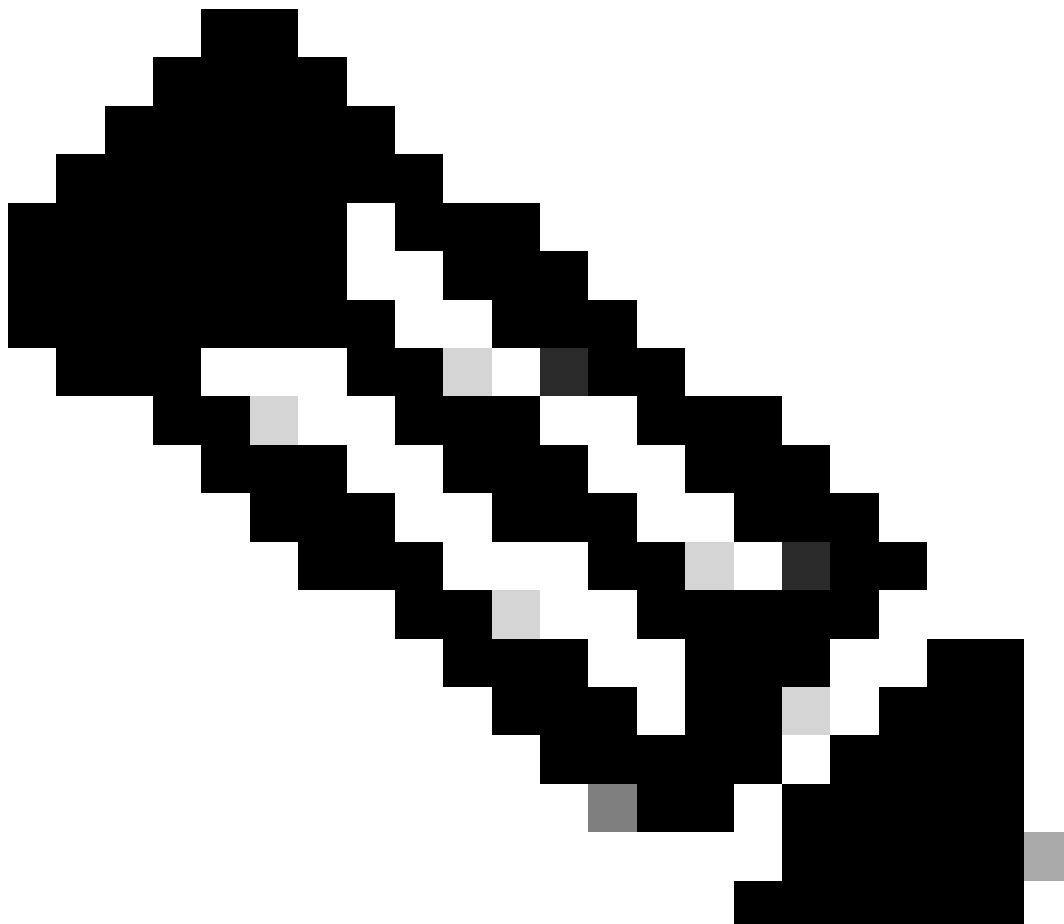
5. Configurazioni finali per i criteri di routing di Secure Web Appliance:

- È importante ricordare che Secure Web Appliance valuta le identità e i criteri di accesso utilizzando un approccio di elaborazione delle regole "top-down". Ciò significa che la prima corrispondenza effettuata in qualsiasi momento dell'elaborazione determina l'azione eseguita da Secure Web Appliance.
- Inoltre, le identità vengono valutate per prime. Quando l'accesso di un client corrisponde a un'identità specifica, Secure Web Appliance controlla tutti i criteri di accesso configurati per utilizzare l'identità corrispondente all'accesso del client.

Routing Policies

Routing Definitions			
Add Policy...			
Order	Members	Routing Destination	Delete
1	BypassProxyChain Identification Profile: All URL Categories: ProxyChainBypassList	Direct Connection	
2	SIGALLHTTPs (disabled) Identification Profile: All Protocols: All others	SIGHTTPs proxy.sig.umbrella.com:443	
3	SIGALLHTTP Identification Profile: All Protocols: HTTP	SIGHTTP proxy.sig.umbrella.com:80	
4	Win2k8HTTPs Identification Profile: win2k8 All identified users	SIGHTTPs proxy.sig.umbrella.com:443	
5	Win2016ProxyChainHTTPs Identification Profile: Win2016 All identified users	SIGHTTPs proxy.sig.umbrella.com:443	

360050700131



Nota: La configurazione dei criteri indicata è applicabile solo per la distribuzione di proxy esplicito.

Per la distribuzione di proxy trasparente

Nel caso di HTTPS trasparente, AsyncOS non ha accesso alle informazioni nelle intestazioni client. Pertanto, AsyncOS non può applicare i criteri di routing se un criterio di routing o un profilo di identificazione si basa sulle informazioni contenute nelle intestazioni dei client.

1. Le transazioni HTTPS reindirizzate in modo trasparente corrispondono ai criteri di routing solo se:
 - Per il gruppo di criteri di routing non sono stati definiti criteri di appartenenza ai criteri quali la categoria URL, l'agente utente e così via.
 - Per il profilo di identificazione non sono stati definiti criteri di appartenenza ai criteri quali la categoria URL, l'agente utente e così via.
2. Se per un profilo di identificazione o un criterio di routing è stata definita una categoria URL personalizzata, tutte le transazioni HTTPS trasparenti corrisponderanno al gruppo di criteri di routing predefinito.
3. Evitare per quanto possibile di configurare i criteri di routing con tutti i profili di identificazione, in quanto ciò potrebbe causare la corrispondenza delle transazioni HTTPS trasparenti con il gruppo di criteri di routing predefinito.

1. X-Forwarded-For Header

- per implementare il criterio Web basato su IP interno in SWG. Assicurarsi di abilitare l'intestazione "X-Forwarded-For" in Secure Web Appliance tramite Security Services > Proxy Settings.

Home

Reporting

Web Security Manager

Security Services

Network

System Administration

Proxy Settings

Web Proxy Settings

Basic Settings

Proxy:	Enabled
HTTP Ports to Proxy:	80, 3128
Caching:	Disabled Clear Cache
Proxy Mode:	Transparent
IP Spoofing:	Not Enabled

Advanced Settings

Persistent Connection Timeout:	Client Side: 300 Seconds Server Side: 300 Seconds
In-Use Connection Timeout:	Client Side: 300 Seconds Server Side: 300 Seconds
Simultaneous Persistent Connections:	Server Maximum Number: 2000
Generate Headers:	X-Forwarded-For: Send Request Side VIA: Send Response Side VIA: Send
Use Received Headers:	Identification of Client IP Addresses using X-Forwarded-For: Disabled
Range Request Forwarding:	Disabled

Edit Settings...

360050700111

2. Certificato radice attendibile per la decrittografia HTTP.

- Se la decrittografia HTTP è abilitata in Criteri Web nel dashboard Umbrella, scaricare "Cisco Root Certificate" dal dashboard Umbrella> Distribuzioni> Configurazione e importarlo nei certificati radice attendibili di Secure Web Appliance.

Manage Trusted Root Certificates

Custom Trusted Root Certificates

[Import...](#)

Trusted root certificates are used to determine whether HTTPS sites' signing certificates should be trusted based on their chain of certificate authorities. Certificates imported here are added to the trusted root certificate list. Add certificates to this list in order to trust certificates with signing authorities not recognized on the Cisco list.

Certificate	Expiration Date	On Cisco List	Delete
▸ Cisco Umbrella Root CA	Jun 28 15:37:53 2036 GMT	No	

[Cancel](#)[Submit](#)

Cisco Trusted Root Certificate List (332 entries, 0 overridden)

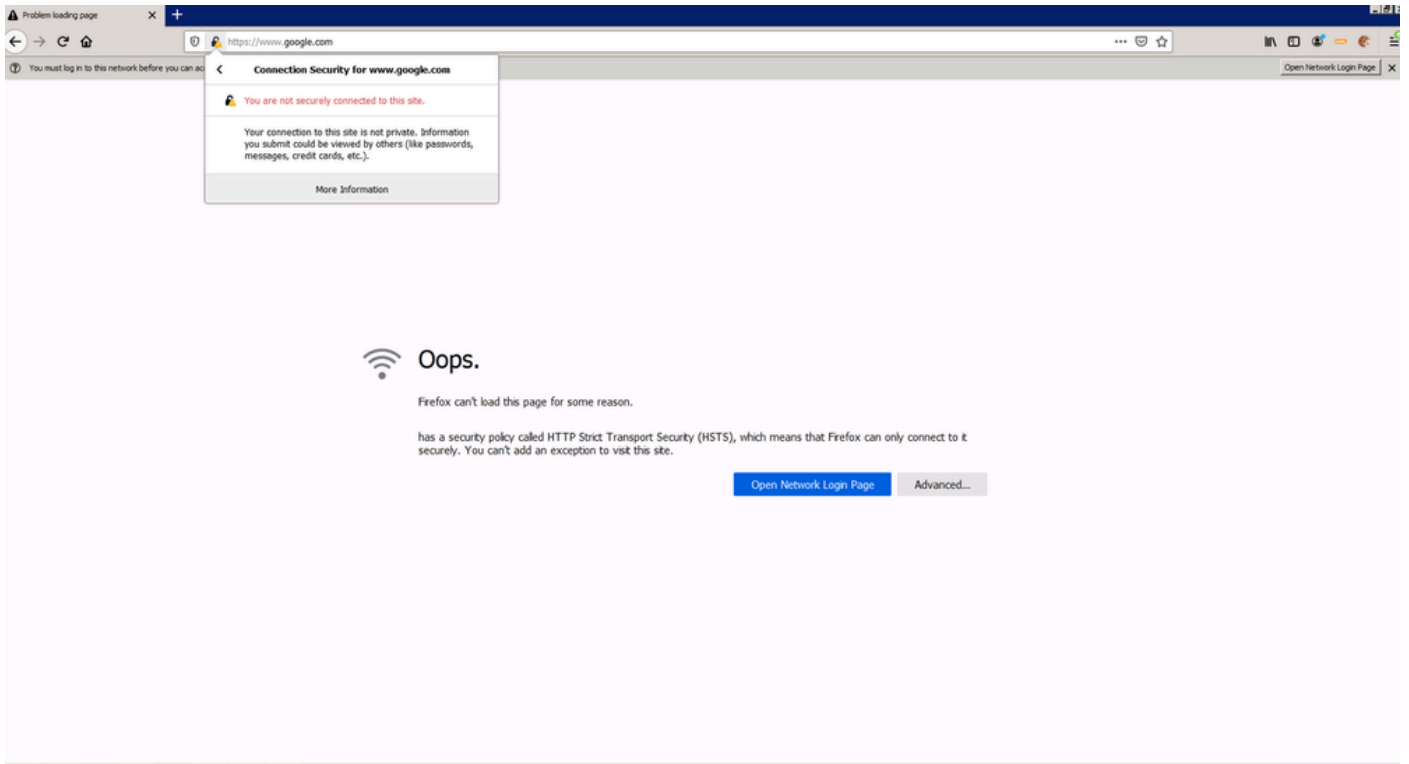
This list displays the certificates representing trust root certificate authorities recognized by Cisco. Expand items in this list to view certificate details or download.

Use the checkboxes to override entries. If an entry on the list is overridden, it will not be treated as a trusted root certificate authority.

Certificate	Expiration Date	Override Trust ?
▸ (c) 1998 VeriSign, Inc. - For authorized use only	Aug 1 23:59:59 2028 GMT	☐
▸ A-Trust-nQual-03	Jul 23 08:38:29 2025 GMT	☐
▸ A-Trust-Qual-02	Jul 1 09:23:33 2024 GMT	☐
▸ A-Trust-Root-05	Sep 20 11:24:11 2023 GMT	☐
▸ AAA Certificate Services	Dec 31 23:59:59 2028 GMT	☐

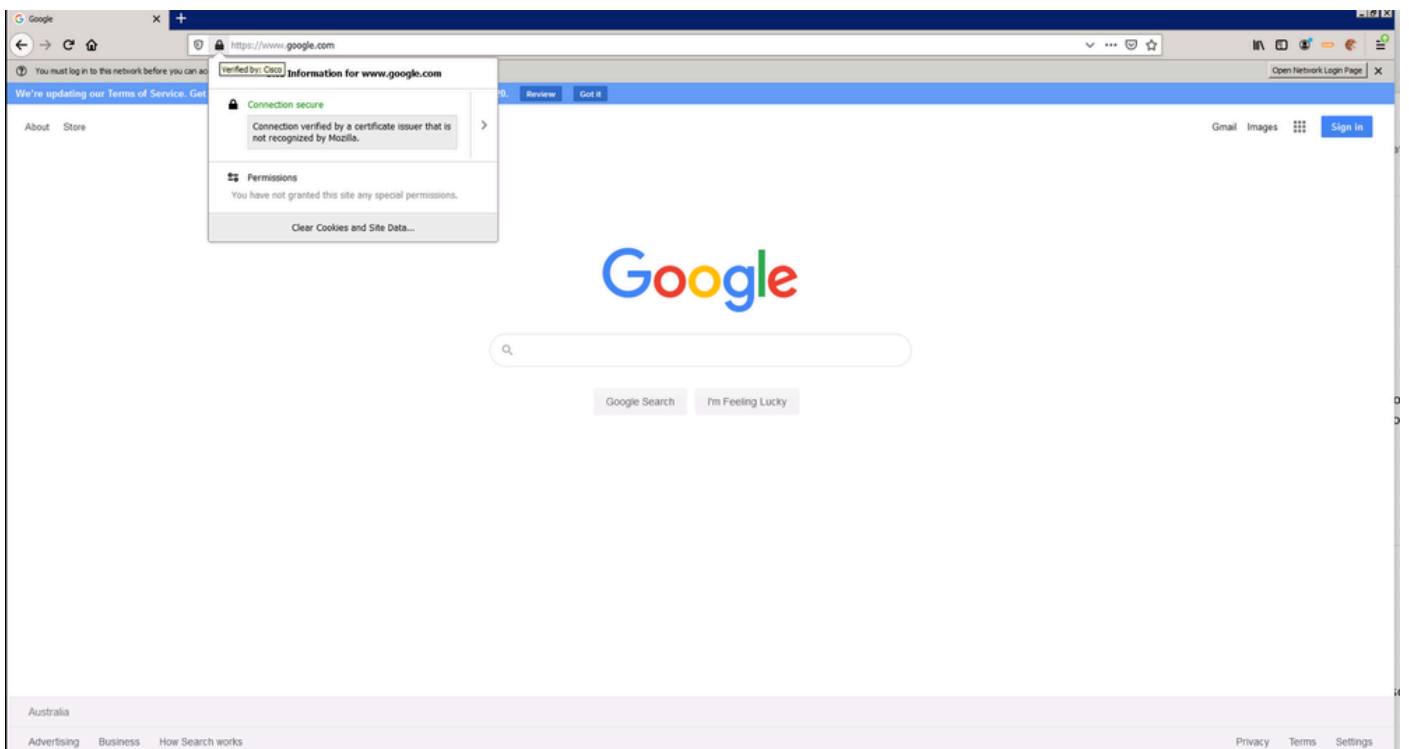
360050589612

- Se il "Certificato radice Cisco" non è stato importato in Secure Web Appliance mentre la decrittografia HTTP è abilitata in SWG Web Policy, l'utente finale riceve un errore simile a quello riportato nell'esempio seguente:
 - "Oops. (browser) non è in grado di caricare la pagina per qualche motivo. dispone di un criterio di protezione denominato HTTP Strict Transport Security (HSTS), il che significa che (browser) può connettersi a esso solo in modo sicuro. Impossibile aggiungere un'eccezione per visitare questo sito."
 - "La connessione al sito non è sicura."



360050700171

- Questo è un esempio di HTTP decriptati da Umbrella SWG. Il certificato è verificato dal "Certificato radice Cisco" denominato "Cisco".



360050700191

Configurazione dei criteri Web SWG in Umbrella Dashboard

SWG Web Policy basato su IP interno:

- Assicurarsi di abilitare l'intestazione "X-Forwarded-For" (Inoltro X-Per) in Secure Web Appliance, in quanto SWG si basa su tale intestazione per identificare l'IP interno.
- Registrare l'indirizzo IP in uscita di Secure Web Appliance in Distribuzione > Reti.
- Creare un IP interno del computer client in Distribuzione > Configurazione > Reti interne. Selezionare l'indirizzo IP di uscita di Secure Web Appliance registrato (passaggio 1) dopo aver selezionato "Mostra reti".
- Creare un nuovo criterio Web basato sull'indirizzo IP interno creato nel passaggio 2.
- Assicurarsi che l'opzione "Abilita SAML" sia disabilitata nei criteri Web.

Criteri Web SWG basati su utente/gruppo AD:

- Verificare che tutti gli utenti e i gruppi di Active Directory siano predisposti per il dashboard Umbrella.
- Creare un nuovo criterio Web basato sull'indirizzo IP in uscita registrato di Secure Web Appliance con l'opzione "Abilita SAML" abilitata.
- Creare un altro nuovo criterio Web basato sull'utente/gruppo AD con l'opzione "Abilita SAML" disabilitata. È inoltre necessario che questo criterio Web venga posizionato prima del criterio Web creato al passaggio 2.

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).