

Ignorare il traffico in Secure Web Appliance

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Diversi tipi di bypass](#)

[Procedure di bypass SWA per tipo di distribuzione](#)

[Ignorare il traffico nella distribuzione esplicita](#)

[Configurazione file PAC](#)

[Configurazione browser \(Microsoft Edge, Internet Explorer, Google Chrome\)](#)

[Configurazione browser \(Mozilla FireFox\)](#)

[Configurazione browser \(Apple Safari\)](#)

[Configurazione di Criteri di gruppo](#)

[Ignora traffico in TransparentDeployment](#)

[Impostazione bypass SWA](#)

[Reindirizzamento del traffico dal router WCCP/PBR](#)

[Configurazione di pass-through e autorizzazione del traffico in SWA](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritta la procedura per ignorare il traffico 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

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.

Diversi tipi di bypass

In SWA, esistono tre diversi concetti che consentono di evitare che un traffico raggiunga il file SWA, che dipende dalla distribuzione del proxy (distribuzione esplicita o trasparente), o che venga analizzato e analizzato dal file SWA. Di seguito è riportata una breve panoramica di questi tre concetti:

- **Ignora:** Impostazione che impedisce al traffico di raggiungere il dispositivo SWA, riducendo l'utilizzo della scheda di interfaccia di rete (NIC, Network Interface Card) ed eliminando la necessità di una sessione tra l'utente e l'accessorio.
- **Pass-through:** Questa configurazione impedisce al servizio SWA di decrittografare il traffico HTTPS. Ciononostante, la SWA continua a facilitare due sessioni distinte: una tra il client e l'SWA e una seconda tra l'SWA e il server Web.
- **Consenti:** Impostazione della policy di accesso in cui il traffico HTTP o decrittografato ignora l'ispezione da parte dei motori SWA interni, ad esempio AMP, Sophos, WebRoot e il filtro dell'applicazione. In questo caso, nell'SWA sono ancora in uso due sessioni.

Type	Applies to	Transparent Deployment	Explicit Deployment	Configuration Path	Logging	Number of Sessions	Description
Bypass from SWA	HTTPS & HTTP	✓	✗	GUI > Web Security Manager > Bypass Settings	Bypasslogs	1	SWA routes the traffic to configured gateway (Layer 3 redirection)
Bypass from WCCP Router	HTTPS & HTTP	✓	✗	WCCP Router	No Logs on SWA	0	Traffic Redirects to the Gateway from Router
Bypass from PAC	HTTPS & HTTP	✗	✓	From the PAC file	No Logs on SWA	0	Requests are not sent to the proxy.
Bypass from Browser	HTTPS & HTTP	✗	✓	From the Browser or Group Policy	No Logs on SWA	0	Requests are not sent to the proxy.
Pass Through	HTTPS & HTTP	✓	✓	GUI > Web Security Manager > Decryption Policy	Accesslogs	2	SWA does not decrypt the traffic and sends the same ClientHello to the web server.
Allow	Decrypted Traffic & HTTP	✓	✓	GUI > Web Security Manager > Access Policy	Accesslogs	2	SWA does not Scan the traffic with its scanning engines, such as AMP, Sophos, WebRoot, AVC and ...

Immagine - Grafico di confronto

Procedure di bypass SWA per tipo di distribuzione

Le procedure di bypass variano a seconda del modello di distribuzione del proxy. Di seguito è riportata una breve panoramica di ciascun tipo:

- Distribuzione esplicita: I client sono configurati manualmente per indirizzare il traffico al proxy.
- Installazione trasparente: L'infrastruttura di rete reindirizza automaticamente il traffico al proxy, senza richiedere alcuna configurazione sul lato client.

Ignorare il traffico nella distribuzione esplicita

Per evitare il traffico nella distribuzione esplicita, è necessario configurare il client in modo che non inoltri la richiesta Web per gli URL desiderati all'SWA. Come mostrato nel diagramma di rete, parte del traffico va direttamente al firewall o al gateway predefinito per ignorare l'interfaccia SWA (percorso numero 2).

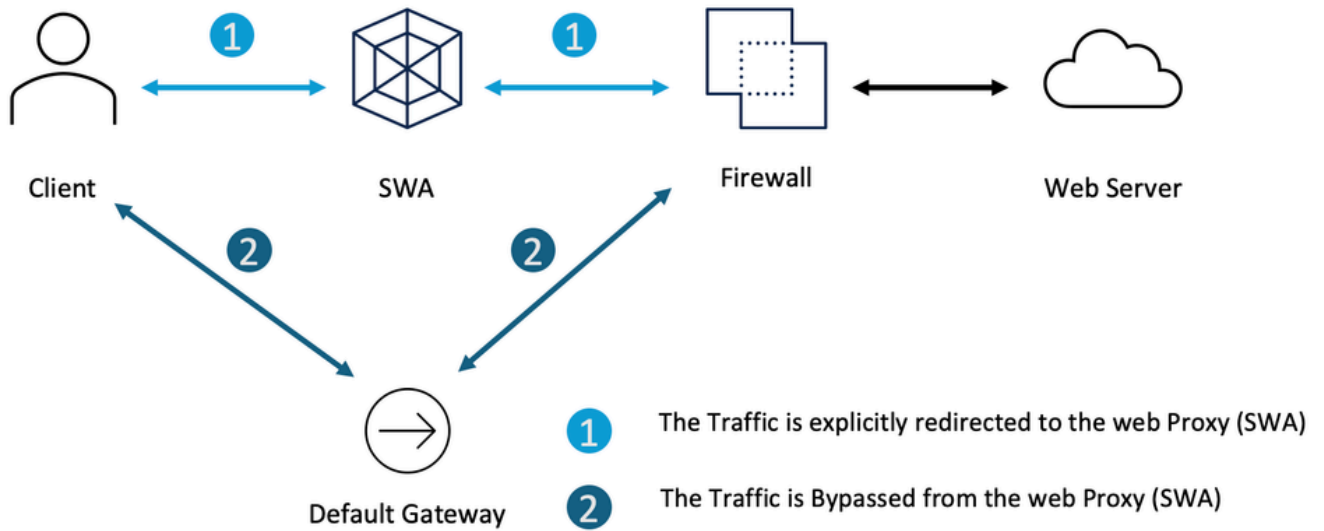



Immagine - Ignorare il traffico nella distribuzione esplicita

A seconda della distribuzione proxy esplicita, è possibile esentare alcuni URL dal reindirizzamento all'SWA.

Configurazione proxy esplicita	Procedura per escludere gli URL dal raggiungimento dell'SWA
Configurazione file PAC	<p>A seconda di come è stato configurato il file PAC, è possibile definire l'elenco di eccezioni e impostare l'azione su DIRECT.</p> <p>Di seguito sono riportati alcuni esempi per evitare che l'indirizzo IP privato raggiunga lo SWA</p> <pre>var resolved_ip = dnsResolve(host); if (isInNet(resolved_ip, "10.0.0.0", "255.0.0.0") isInNet(resolved_ip, "172.16.0.0", "255.240.0.0") isInNet(resolved_ip, "192.168.0.0", "255.255.0.0") isInNet(resolved_ip, "127.0.0.0", "255.255.255.0")) return "DIRECT";</pre> <p>Questo è un esempio di come evitare il traffico diretto a www.cisco.com per il reindirizzamento del SWA</p> <pre>if (localHostOrDomainIs(host, "www.cisco.com")) return "DIRECT";</pre> <p>In questo esempio vengono ignorati tutti i sottodomini di cisco.com dal</p>

	<p>reindirizzamento del file SWA</p> <pre>if (dnsDomainIs(host, ".cisco.com")) return "DIRECT";</pre> <hr/> <p> Nota: Poiché il file PAC non è un prodotto Cisco, le informazioni vengono fornite per tua comodità. Per ulteriore assistenza, contattare il fornitore del software.</p> <hr/>
<p>Configurazione browser (Microsoft Edge, Internet Explorer, Google Chrome)</p>	<p>Passaggio 1. Nel menu Start, digitare "Opzioni Internet" e premere Invio</p> <p>Passaggio 2. Passare alla scheda Connessioni e fare clic su Impostazioni LAN</p> <p>Passaggio 3. Fare clic su Advanced</p> <p>Passaggio 4. Definire gli URL desiderati nella sezione Eccezioni.</p>

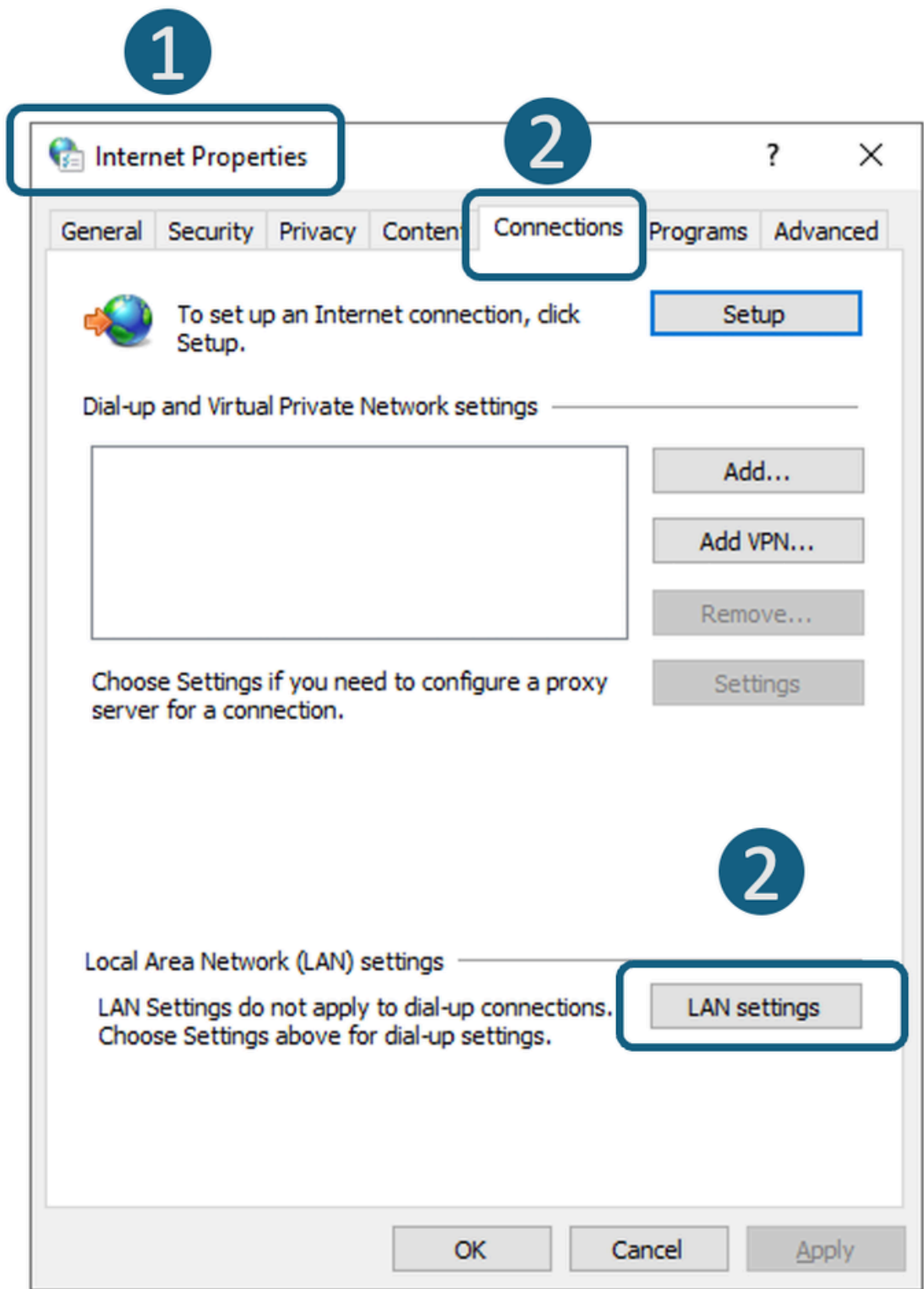
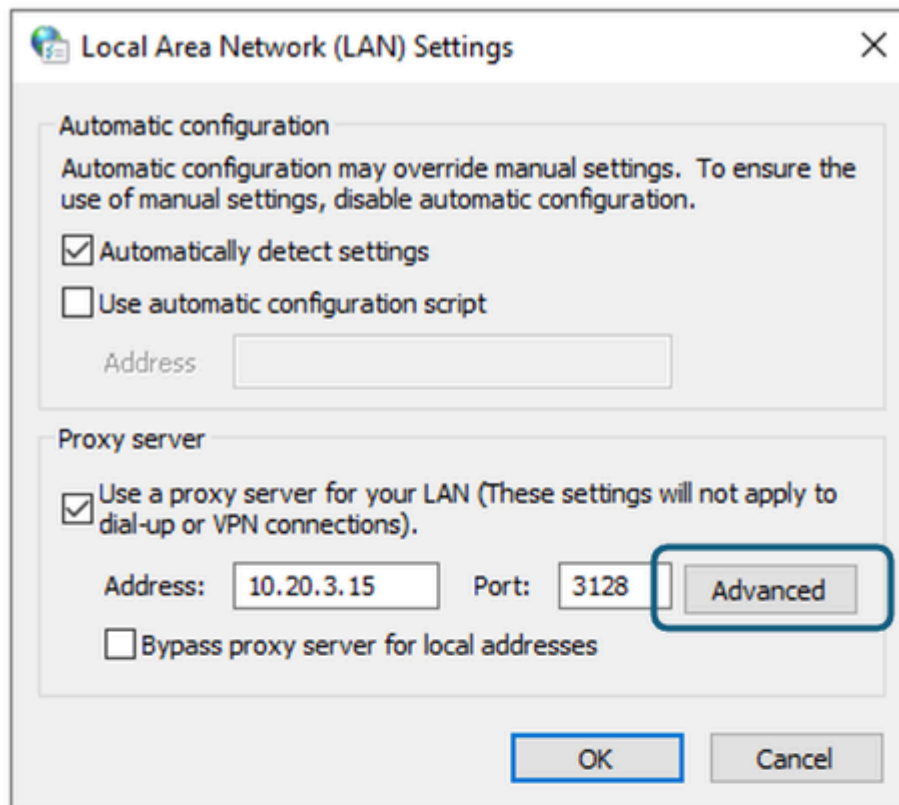
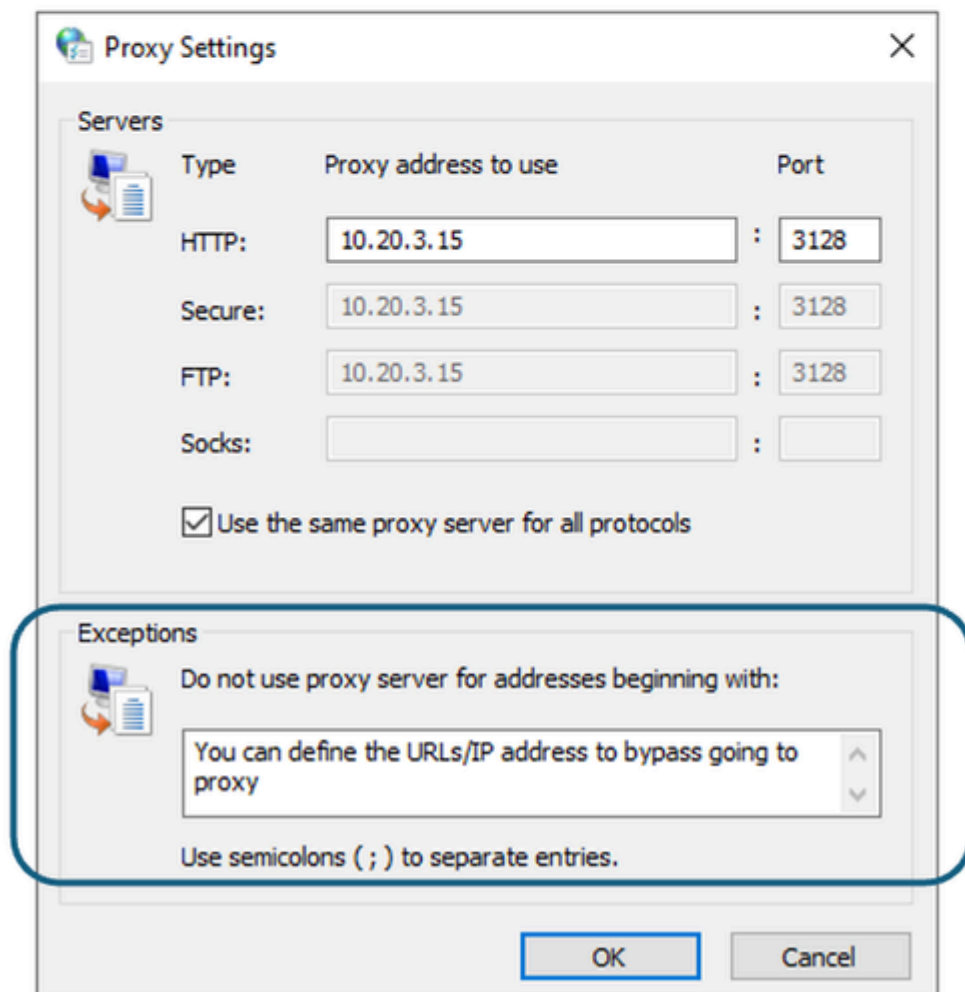


Immagine - Passa alle impostazioni LAN



3



4

Configurazione browser (Mozilla FireFox)

Passaggio 1. Nell'angolo in alto a destra, fare clic sul menu a tre barre e selezionare Settings.

Passaggio 2. Nella barra di ricerca, digitare proxy.

Passaggio 3. Definire gli URL desiderati nella sezione Nessun proxy per.

The screenshot shows the 'Connection Settings' dialog box in Firefox. The 'Manual proxy configuration' option is selected. The HTTP Proxy is set to 10.20.3.15 on port 3128, and the 'Also use this proxy for HTTPS' checkbox is checked. The HTTPS Proxy is also set to 10.20.3.15 on port 3128. The SOCKS Host is empty, and the SOCKS version is set to v5. The 'Automatic proxy configuration URL' is set to https://prod.radkit-cloud.cisco.com/pac?port=4000. A red box highlights the 'No proxy for' section, which contains a text input field with the placeholder text 'You can define the URLs/IP address to bypass going to proxy'. A red circle with the number '3' is next to this section. Below the input field, there is an example: '.mozilla.org, .net.nz, 192.168.1.0/24' and a note: 'Connections to localhost, 127.0.0.1/8, and ::1 are never proxied.' There are also checkboxes for 'Do not prompt for authentication if password is saved', 'Proxy DNS when using SOCKS v4', and 'Proxy DNS when using SOCKS v5' (which is checked). 'Cancel' and 'OK' buttons are at the bottom right.

Immagine - Definizione delle eccezioni in Fire Fox

Configurazione browser (Apple Safari)

Passaggio 1. Nell'angolo in alto a sinistra, fare clic sull'icona Apple e scegliere Impostazioni di sistema.

Passaggio 2. Dal pannello di sinistra passare a Rete e selezionare l'interfaccia di rete che si sta utilizzando per accedere a Internet.

Passaggio 3. Fare clic su Dettagli.

Passaggio 4. Dal pannello sinistro, selezionare Proxy.

Passaggio 5. Definire gli URL desiderati nella sezione Ignora impostazioni proxy.

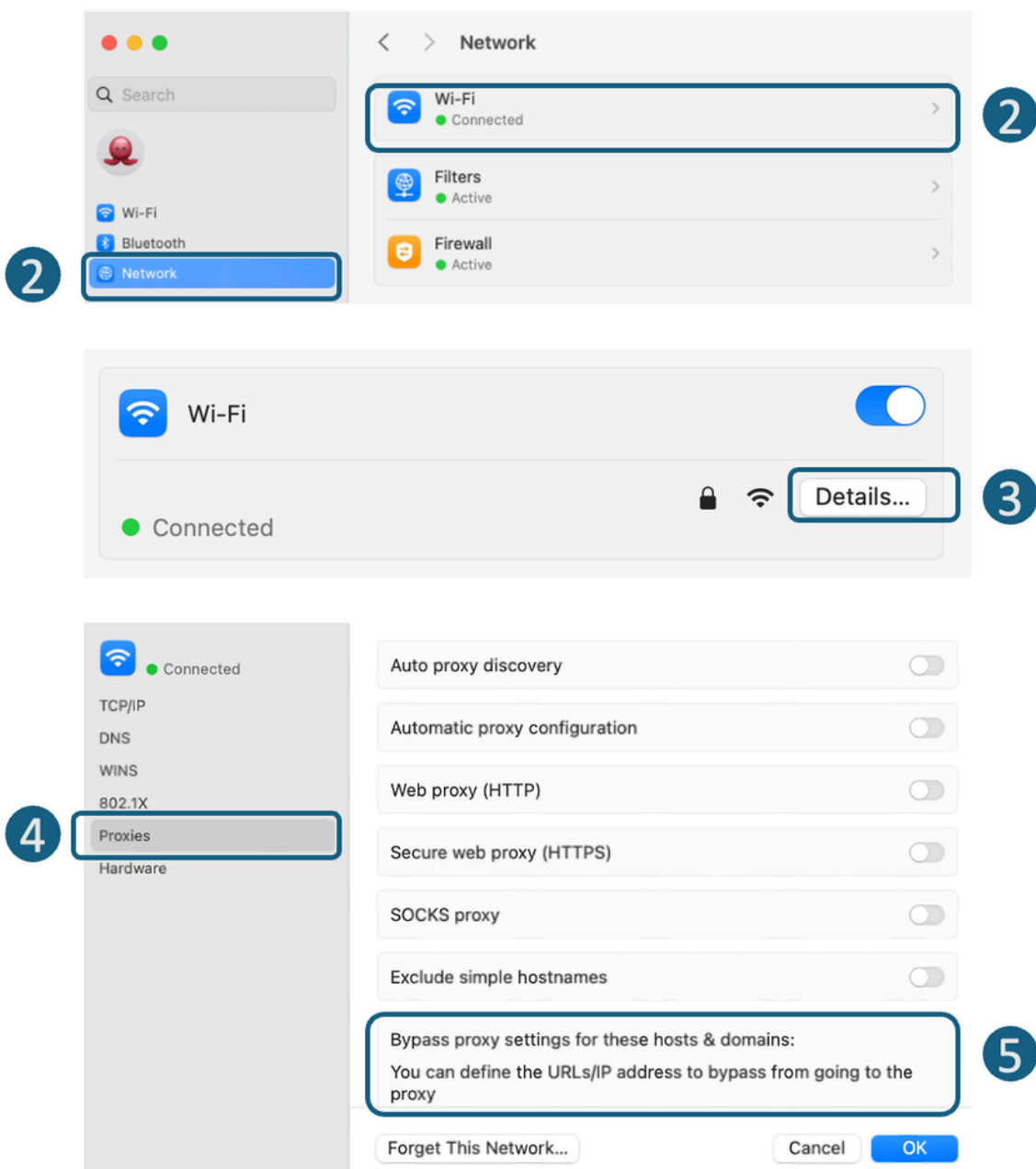


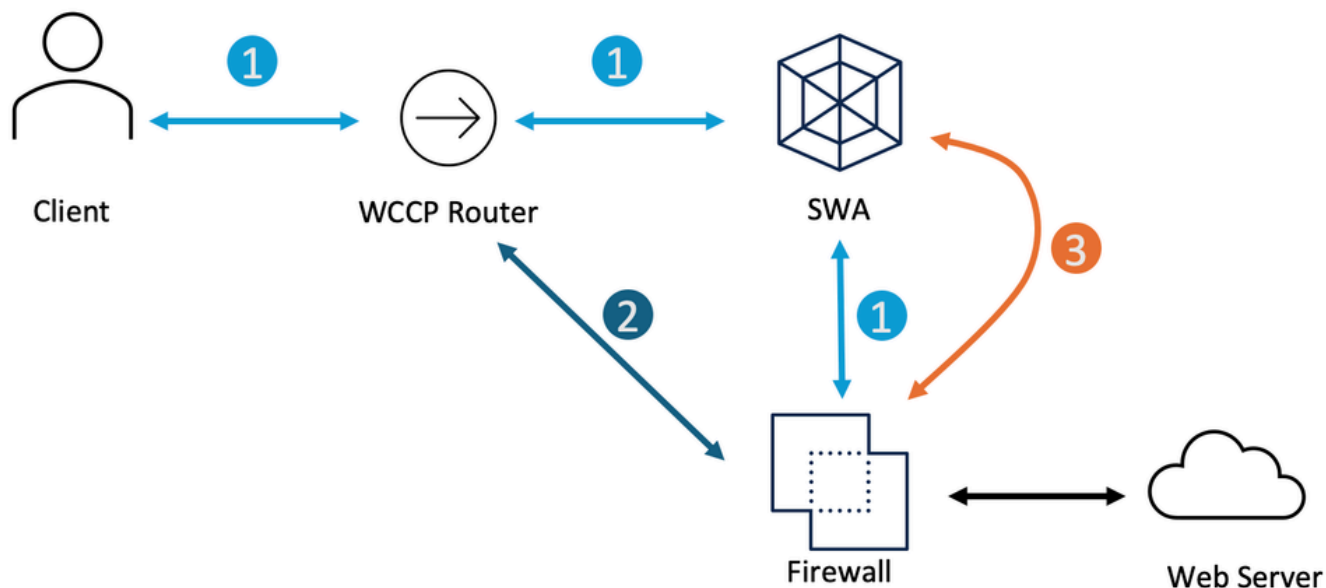
Immagine - Definizione delle eccezioni in Fire Fox

Configurazione di Criteri di gruppo

A seconda della configurazione dei Criteri di gruppo per il push delle impostazioni proxy, è possibile definire l'elenco di eccezioni.

Ignorare il traffico nella distribuzione trasparente

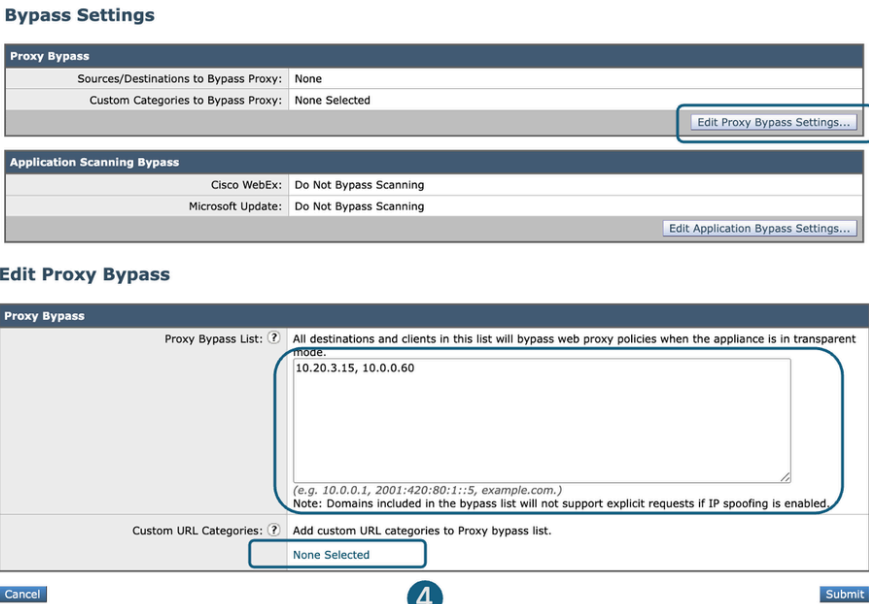

È possibile ignorare il traffico in una distribuzione trasparente utilizzando le impostazioni WCCP router o SWA Bypass. SWA Bypass agisce sul layer 3, indirizzando il traffico al gateway predefinito e ignorando completamente l'accessorio, impedendo l'elaborazione e la creazione di sessioni separate.



- 1** The Traffic is Transparently redirected to the SWA
- 2** The Traffic is Redirected from the WCCP Router, to not go to the SWA
- 3** The Traffic is Bypassed in the SWA as a layer 3 traffic and routes to the SWA Default Gateway

Immagine - Ignorare il traffico nella distribuzione trasparente

Distribuzione del proxy trasparente di traffico ignorata	Istruzioni per evitare il traffico proveniente dal raggiungimento dell'SWA
Impostazione bypass SWA	<p>Passaggio 1. Dalla GUI, Scegliere Web Security Manager.</p> <p>Passaggio 2. Selezionare Bypass Settings.</p> <p>Passaggio 3. Fare clic su Edit Proxy Bypass Settings.</p> <p>Passaggio 4. È possibile immettere l'URL, l'indirizzo IP o aggiungere una categoria URL personalizzata all'elenco.</p> <p>Passaggio 5. Sottomettere e confermare le modifiche.</p>

	 <p>Immagine - Configurazione impostazioni bypass</p> <p> Suggerimento: Il traffico ignorato con queste impostazioni non viene registrato nei log degli accessi e può essere visualizzato nei log Bypass.</p>
Reindirizzamento del traffico dal router WCCP/PBR	È possibile configurare l'indirizzo IP di origine o di destinazione nel WCCP o nel PBR (Policy Based Router) in modo che alcuni traffici non vengano reindirizzati al SWA.

Configurazione di pass-through e autorizzazione del traffico in SWA

Se il traffico colpisce l'SWA e per ridurre il carico dell'SWA a causa di problemi di privacy non si desidera che il traffico di alcuni URL venga ispezionato dall'SWA, attenersi alla seguente procedura.

Passi	Passi
Passaggio 1. Creare una categoria URL personalizzata per gli URL.	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.

Custom and External URL Categories: Add Category

1.3 Category Name: No Proxy URL

1.5 List Order: 1

1.6 Category Type: Local Custom Category

1.7 Sites: www.cisco.com

Sort URLs
Click the Sort URLs button to sort all site URLs in Alpha-numerical order.

(e.g. 10.0.0.1, 2001:420:80:1::5, example.com.)

Advanced Regular Expressions: ?
Enter one regular expression per line. Maximum allowed characters 2048.

Cancel Submit

Immagine - Creazione di una categoria URL personalizzata

Passaggio 2. Creare un profilo di identificazione per escludere il traffico dall'autenticazione.

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

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. Dalla sezione Avanzate, scegliere Categorie URL personalizzate.

Identification Profiles: Add Profile

Client / User Identification Profile Settings

Enable Identification Profile

Name: (e.g. my IP Profile)

Description:

(Maximum allowed characters 256)

Insert Above:

User Identification Method

Identification and Authentication: (This option may not be valid if any preceding Identification Profile requires authentication on all subnets.)

Membership Definition

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

Define Members by Subnet:

(examples: 10.1.1.0, 10.1.1.0/24, 10.1.1.1-10, 2001:420:80:1::5, 2000:db8::1-2000:db8::10)

Define Members by Protocol: HTTP/HTTPS

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

The following advanced membership criteria have been defined:

Proxy Ports:

URL Categories: (circled 2.9)

User Agents:

The Advanced options may be protocol-specific. For instance, user agent strings are applicable only for HTTP and decrypted HTTPS. Similarly, URL Categories, including Custom URL Categories are not applicable for SOCKS transactions or transparent HTTPS (unless decrypted). When Advanced options that do not apply to a protocol are selected, no transactions in that protocol will match this Identity, regardless of the protocol selection above.

Immagine - Aggiungi profilo di identificazione

Passaggio 2.10. Aggiungere la categoria URL personalizzata creata nel passaggio 1.

Passaggio 2.11. Fare clic su Fine.

Passaggio 2.12. Inoltra.

Passaggio 3. Creare un criterio di decrittografia per il passaggio del traffico.

Passaggio 3.1. Dalla GUI, selezionare Web Security Manager, quindi fare clic su Criterio di decrittografia.

Passaggio 3.2. Fare clic su Aggiungi criterio per aggiungere un criterio di decrittografia.

Passaggio 3.3. Utilizzare la casella di controllo Abilita criterio per abilitare questo criterio.

Passaggio 3.4. Assegnare un PolicyName univoco.

Passaggio 3.5. (Facoltativo) Aggiungere Una Descrizione.

Passaggio 3.6. Dall'elenco a discesa Inserisci sopra criterio, scegliere il primo criterio.

Passaggio 3.7. Da Profili di identificazione e utenti, scegliere

il Profilo di identificazione creato nel Passaggio 2.

Passaggio 3.8. Inoltrare.

Decryption Policy: Add Group

Policy Settings

Enable Policy

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

Description:

Insert Above Policy:

Policy Expires: Set Expiration for Policy

On Date: MM/DD/YYYY

At Time: :

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	<input type="button" value="Add Identification Profile"/>
<input type="text" value="No Auth ID"/>	No authentication required	<input type="button" value="Add Identification Profile"/>

Define additional group membership criteria.

Immagine - Creazione di un criterio di decrittografia

Passaggio 3.9. Nella pagina Criteri di decrittografia, in Filtro URL, fare clic sul collegamento associato a questo nuovo criterio di decrittografia.

Decryption Policies

Success — The policy group "DP Pass Through" was added.

Order	Group	URL Filtering	Web Reputation	Default Action	Clone Policy	Delete
1	DP Pass Through Identification Profiles: No Auth ID All identified users	Monitor: 1	(global policy)	(global policy)	<input type="button" value="Clone"/>	<input type="button" value="Delete"/>
	Global Policy Identification Profile: All	Pass Through: 0 Monitor: 0 Decrypt: 0 Drop: 0 Time-Based: 0 Quota-Based: 0	Not Available	Decrypt		

Immagine - Selezione del filtro URL

Passaggio 3.10. Select Pass Through come azione per la categoria dell'URL creata nel passaggio 1.

Decryption Policies: URL Filtering: DP Pass Through

Custom and External URL Category Filtering

Add, edit, reorder or delete categories in the Custom and External URL Categories list.

Category	Category Type	Use Global Settings	Override Global Settings					
			Pass Through	Monitor	Decrypt	Drop ?	Quota-Based	Time-Based
<input checked="" type="checkbox"/> No Proxy URL	Custom (Local)	Select all	<input checked="" type="checkbox"/>	Select all	Select all	Select all	(Unavailable)	(Unavailable)

Immagine - Imposta l'azione per il passaggio

Passaggio 3.11. Inoltra.

Passaggio 4. Creare un criterio di accesso per consentire il traffico degli aggiornamenti Microsoft.

Passaggio 4.1. Dalla GUI, selezionare Web Security Manager, quindi fare clic su Access Policy.

Passaggio 4.2. Fare clic su Aggiungi criterio per aggiungere un criterio di accesso.

Passaggio 4.3. Utilizzare la casella di controllo Abilita criterio per abilitare questo criterio.

Passaggio 4.4. Assegnare un PolicyName univoco.

Passaggio 4.5. (Facoltativo) Aggiungere Una Descrizione.

Passaggio 4.6. Dall'elenco a discesa Inserisci sopra criterio, scegliere il primo criterio.

Passaggio 4.7. Da Profili di identificazione e utenti, scegliere il Profilo di identificazione creato nel Passaggio 2.

Passaggio 4.8. Inviare.

4.4 → Policy Name: ? AP Allow
(e.g. my 11 policy)

4.6 → Insert Above Policy: 1 (Global Policy)

4.7 → Identification Profiles and Users: Select One or More Identification Profiles

4.7 → Identification Profile: No Auth ID

Immagine - Crea criteri di accesso

Passaggio 4.9. Nella pagina Criteri di accesso, in Filtro URL, fare clic sul collegamento associato a questi nuovi criteri di accesso.

Success - The policy group "AP Allow" was added.

Order	Group	Protocols and User Agents	URL Filtering	Applications	Objects	Anti-Malware and Reputation	HTTP Rewrite Profile	Clone Policy	Delete
1	AP Allow Identification Profile: No Auth ID All identified users	(global policy)	Monitor: 1	(global policy)	(global policy)	(global policy)	(global policy)		
	Global Policy Identification Profile: All	No blocked items	Block: 0 Warn: 0 Monitor: 0 Allow: 0 Redirect: 0 Time-Based: 0 Quota-Based: 0	Not Available	No blocked items	Secure Endpoint: Enabled	None		

Immagine - Selezione del filtro URL

Passaggio 4.10. Selezionare Allow per la categoria

URL personalizzato creata per la categoria URL creata nel passaggio 1.

Access Policies: URL Filtering: AP Allow

Custom and External URL Category Filtering		Use Global Settings			Override Global Settings				
Category	Category Type	Block	Redirect	Allow	Monitor	Warn	Quota-Based	Time-Based	
		Select all	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)	
No Proxy URL	Custom (Local)	--		<input checked="" type="checkbox"/>					

4.10

Immagine - Imposta l'azione su Consenti

Passaggio 4.11. Sottomettere.

Passaggio 4.12. Eseguire il commit delle modifiche.

Informazioni correlate

- [Ignora traffico aggiornamenti Microsoft in Secure Web Appliance](#)
- [Bypass Authentication in Secure Web Appliance - Cisco](#)
- [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](#)
- [Blocca il traffico in Secure Web Appliance](#)
- [Blocca il traffico di caricamento in Secure Web Appliance](#)
- [Blocca download file eseguibile in SWA](#)

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).