Ignorare il traffico in Secure Web Appliance

Sommario

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).

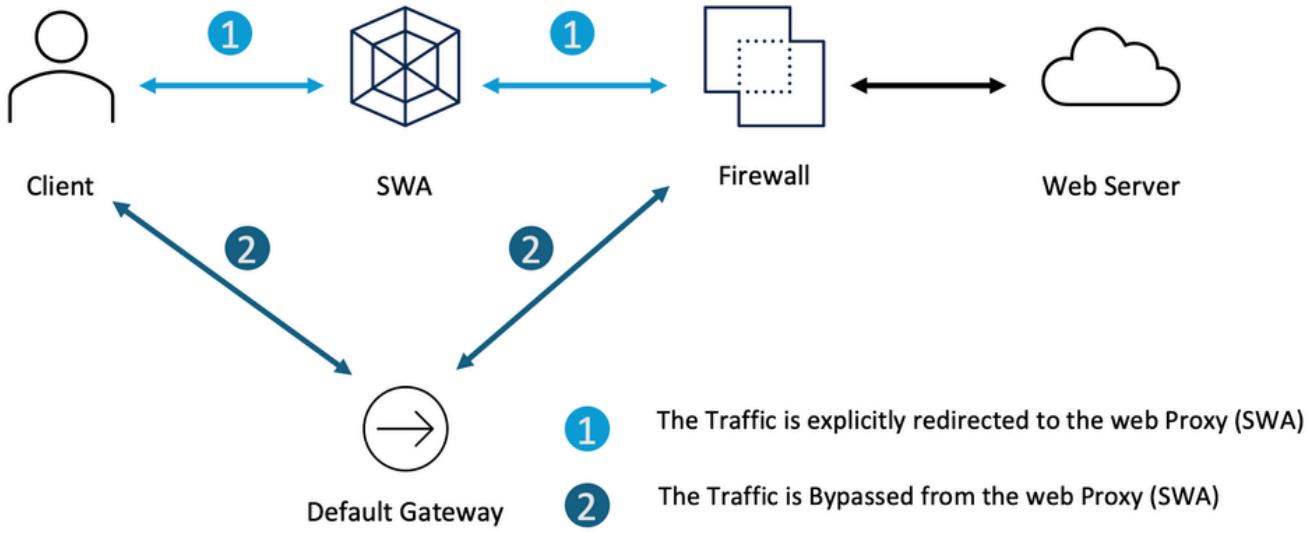


Immagine - Ignorare il traffico nella distribuzione esplicita

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	A seconda di come è stato configurato il file PAC, è possibile definire l'elenco di eccezioni e impostare l'azione su DIRECT.
	
	Di seguito sono riportati alcuni esempi per evitare che l'indirizzo IP privato raggiunga lo SWA
	
	`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";`
	
	Questo è un esempio di come evitare il traffico diretto a www.cisco.com per il reindirizzamento del SWA
	
	`if (localHostOrDomainIs(host, "www.cisco.com")) return "DIRECT";`
	
	In questo esempio vengono ignorati tutti i sottodomini di cisco.com dal

	reindirizzamento del file SWA `if (dnsDomainIs(host, ".cisco.com")) return "DIRECT";` 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.
Configurazione browser (Microsoft Edge, Internet Explorer, Google Chrome)	Passaggio 1. Nel menu Start, digitare "Opzioni Internet" e premere Invio Passaggio 2. Passare alla scheda Connessioni e fare clic su Impostazioni LAN Passaggio 3. Fare clic su Advanced Passaggio 4. Definire gli URL desiderati nella sezione Eccezioni.

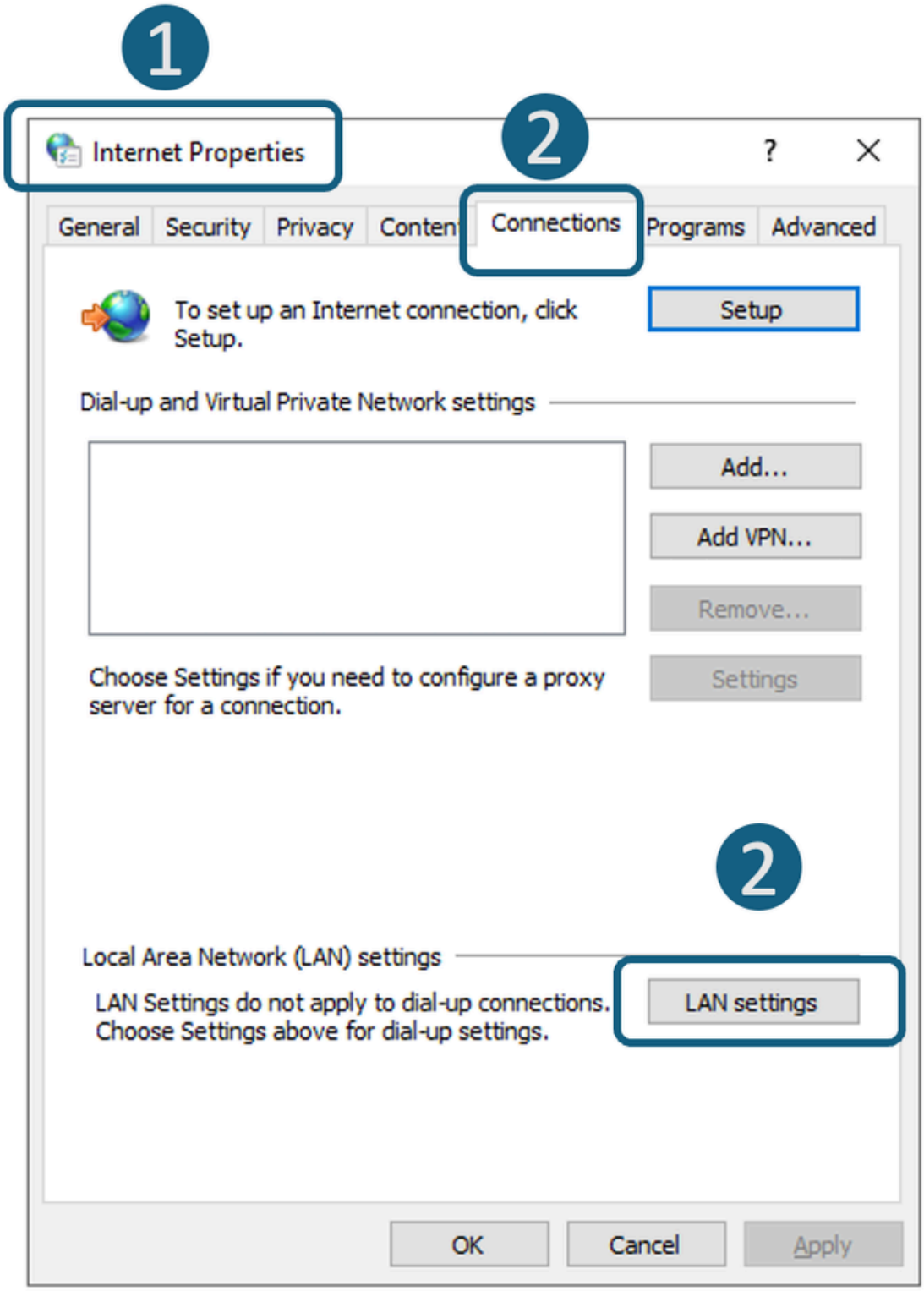


Immagine - Passa alle impostazioni LAN

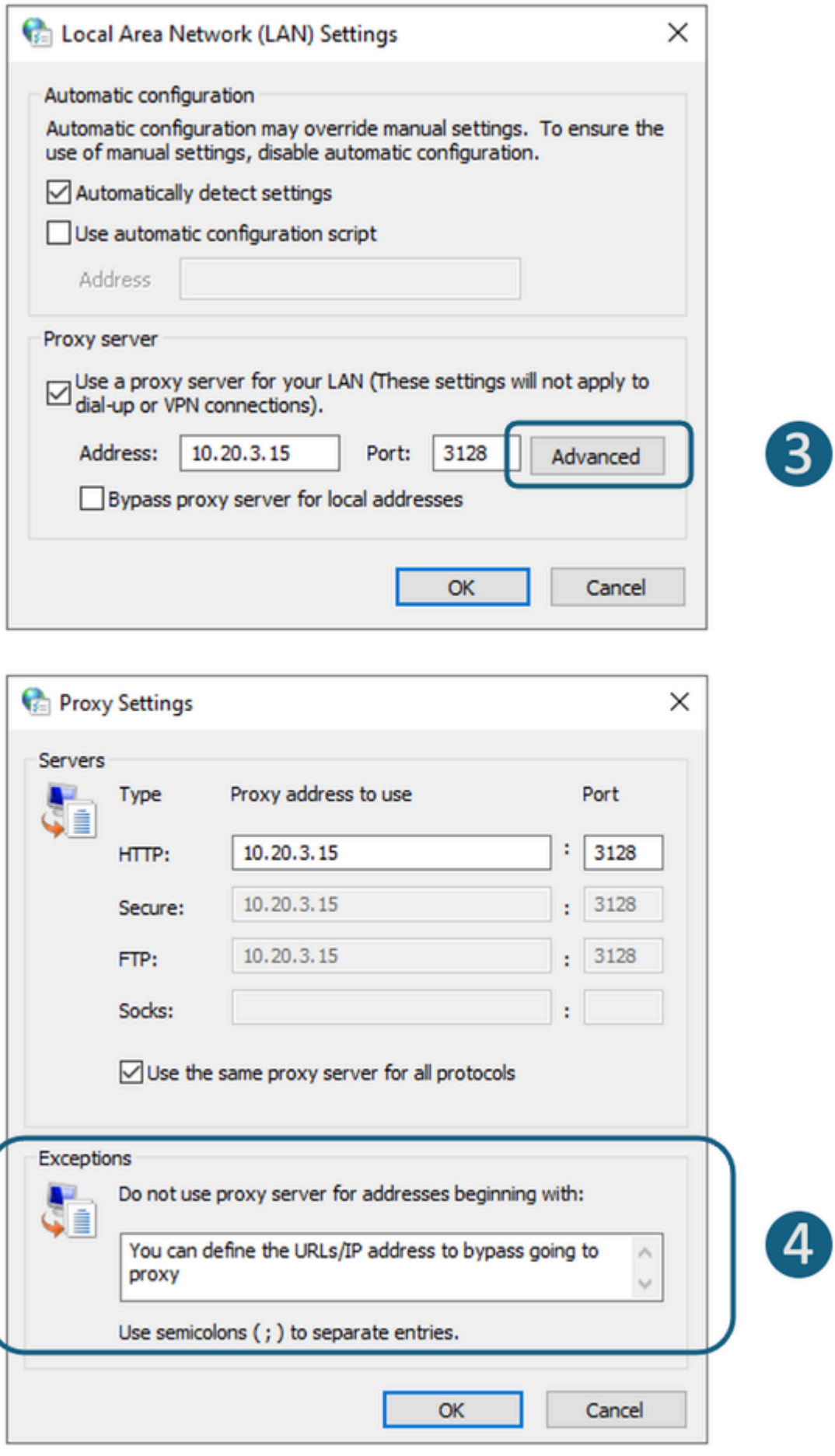
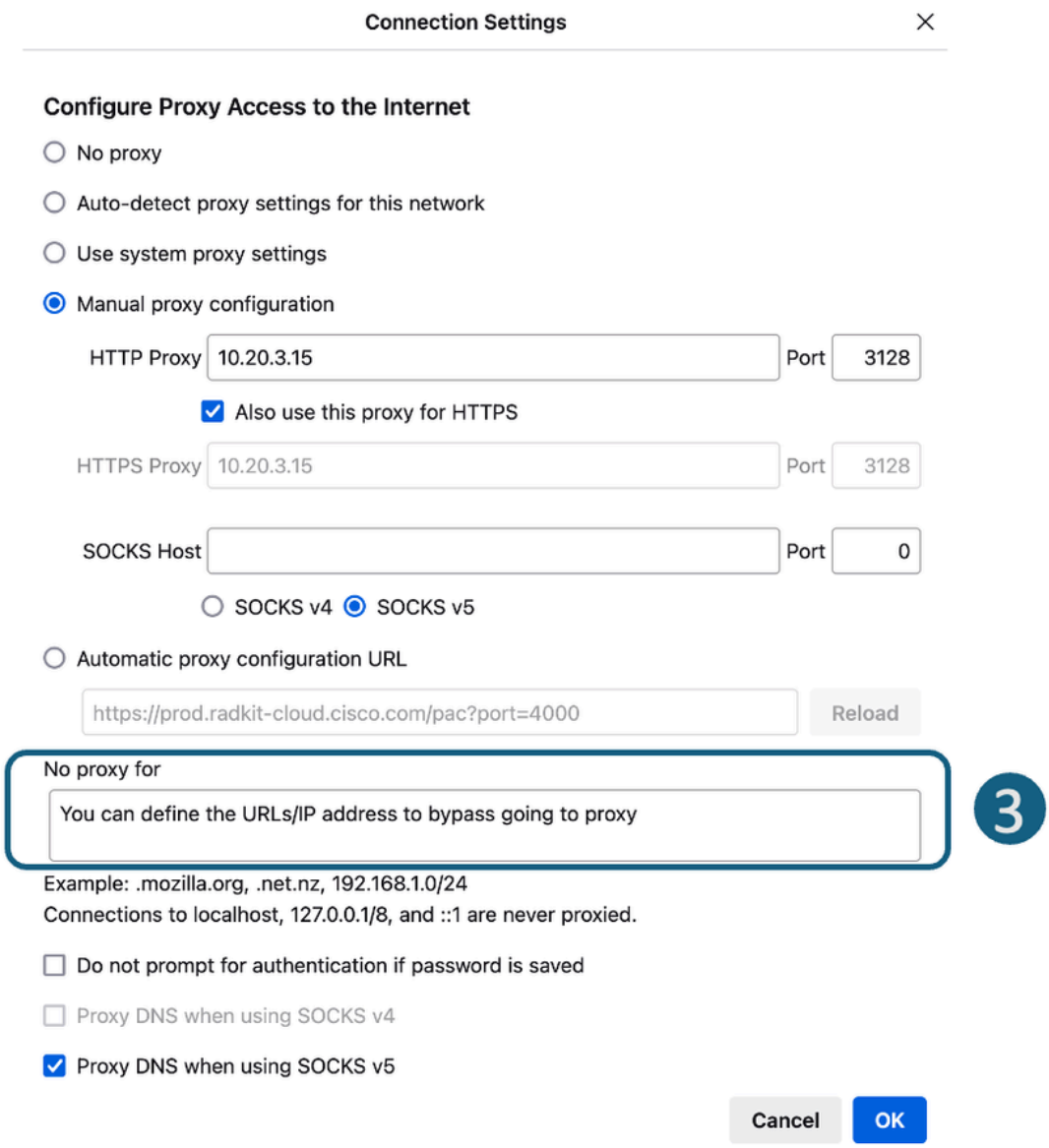
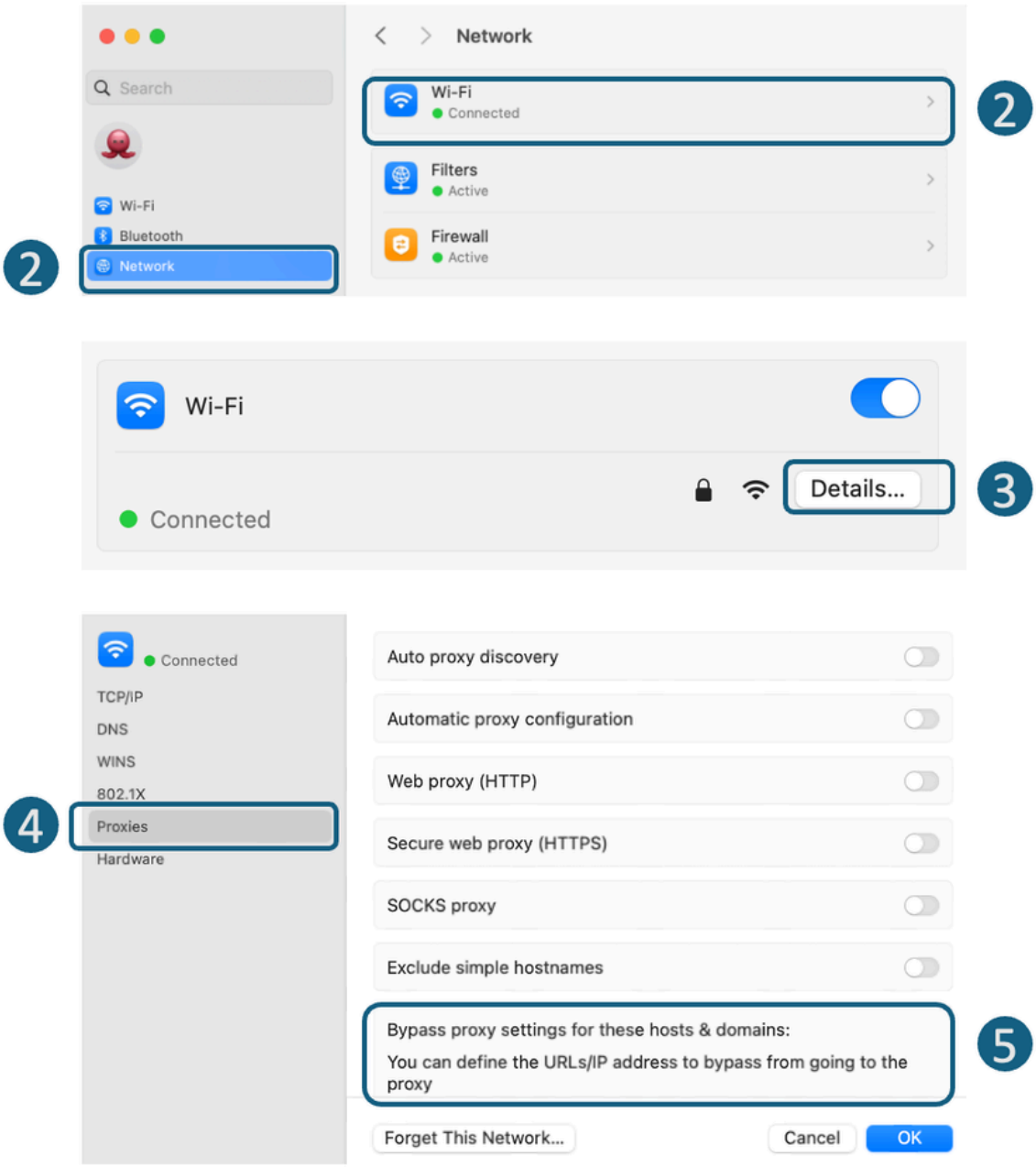


Immagine - Definizione delle eccezioni

Configurazione browser (Mozila 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.  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.

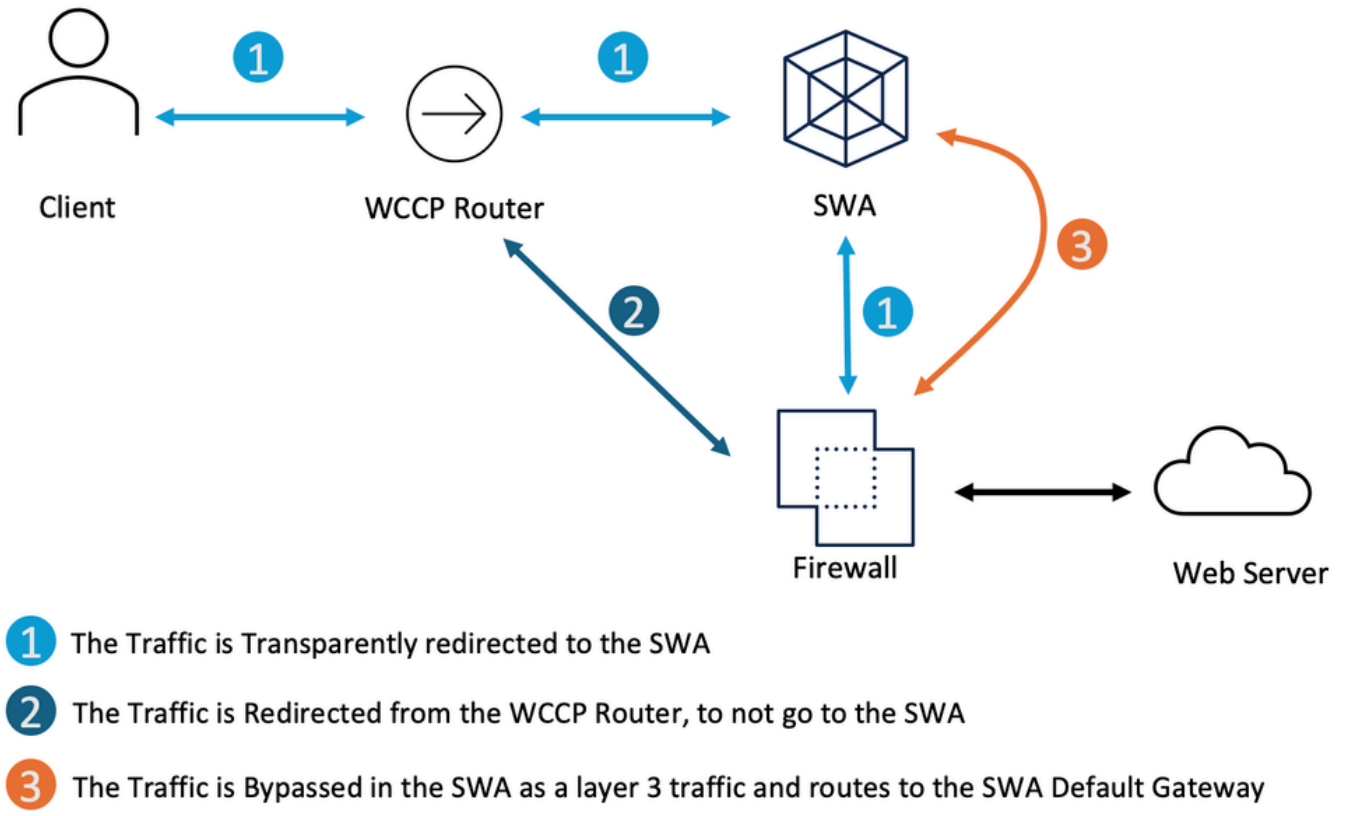
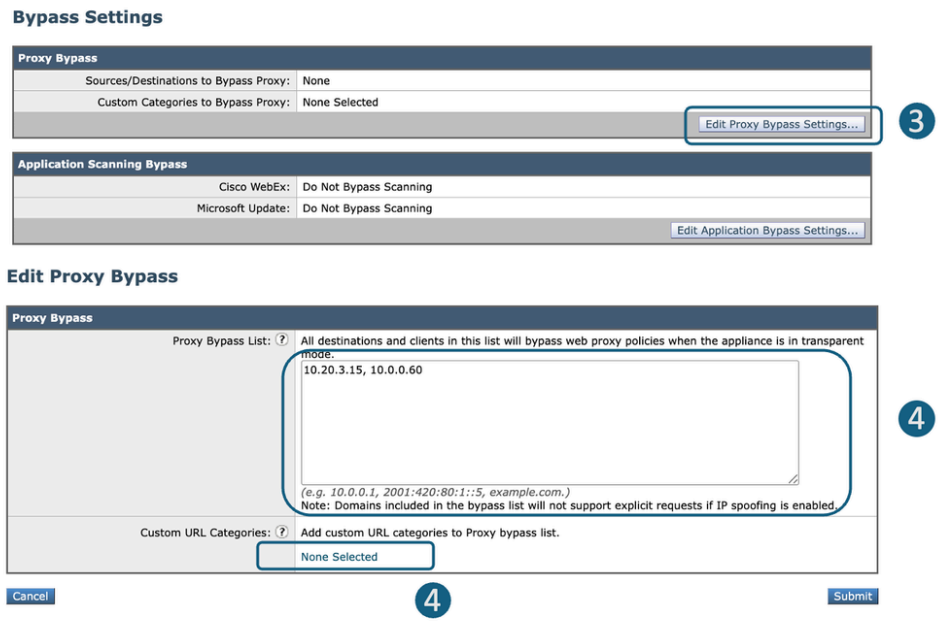


Immagine - Ignorare il traffico nella distribuzione trasparente

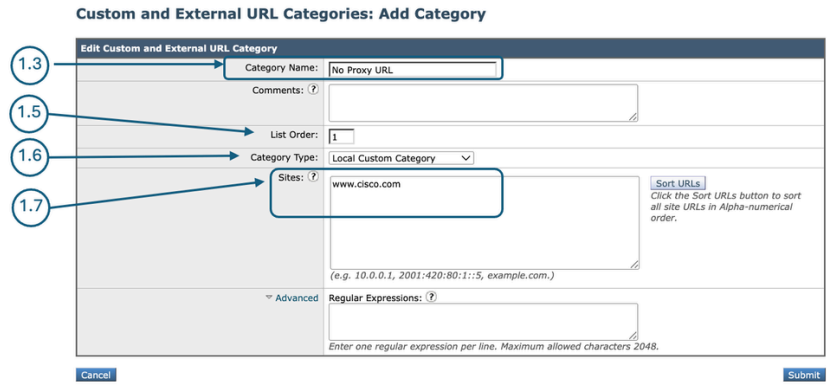
Distribuzione del proxy trasparente di traffico ignorata	Istruzioni per evitare il traffico proveniente dal raggiungimento dell'SWA
Impostazione bypass SWA	Passaggio 1. Dalla GUI, Scegliere Web Security Manager. Passaggio 2. Selezionare Bypass Settings. Passaggio 3. Fare clic su Edit Proxy Bypass Settings.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

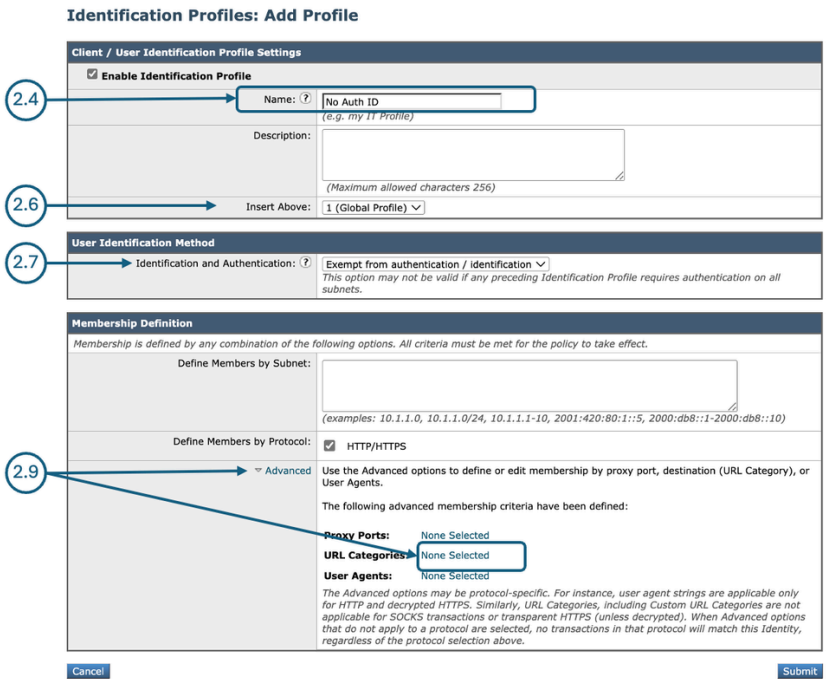
	 Immagine - Configurazione impostazioni bypass Suggerimento: Il traffico ignorato con queste impostazioni non viene registrato nei log degli accessi e può essere visualizzato nei log Bypass.
Reindirizzamento del traffico dal router WCCP/PBR	È possibile configurare l'indirizzo IP di origine o di destinazione 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.  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.  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.

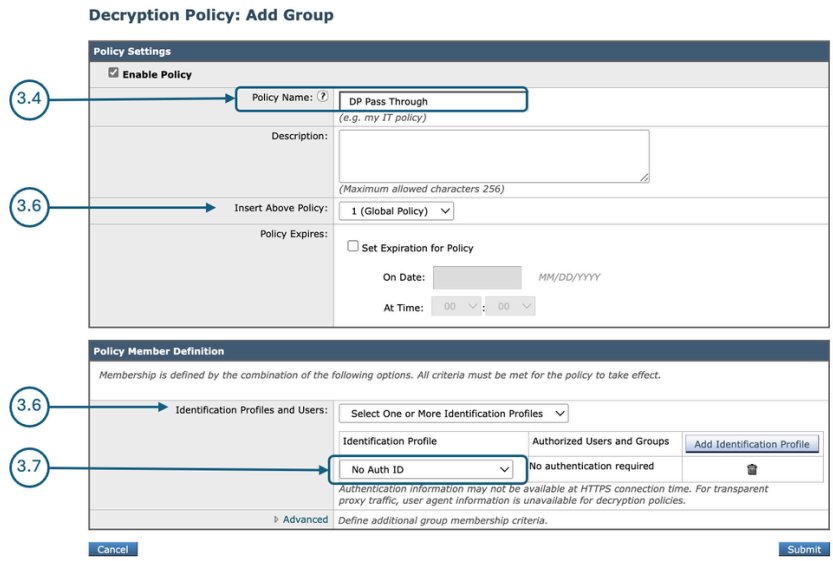


Immagine - Creazione di un criterio di decrittografia

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

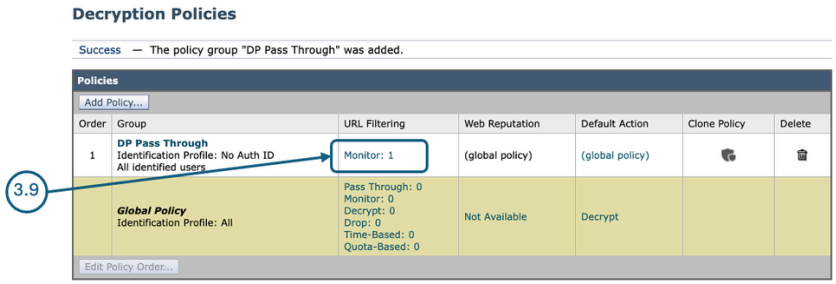


Immagine - Selezione del filtro URL

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

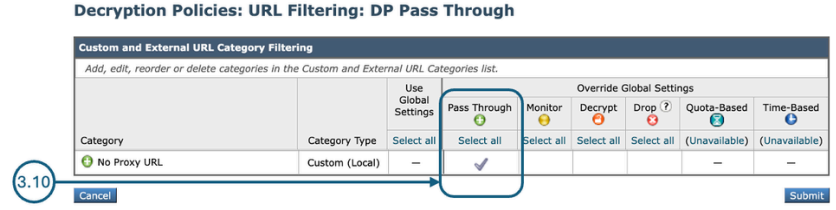
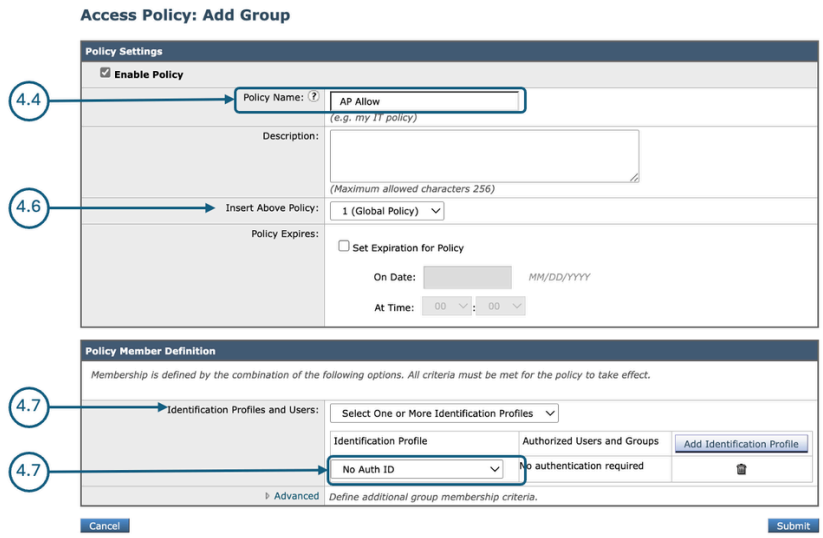
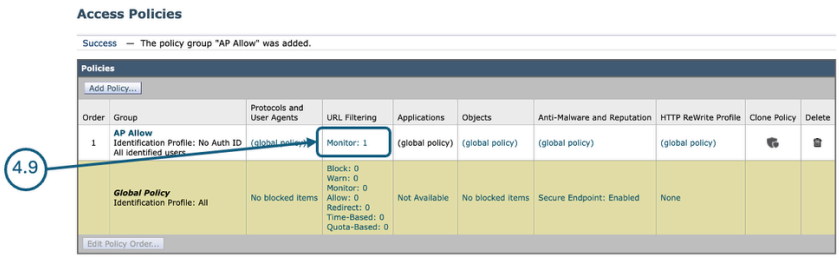
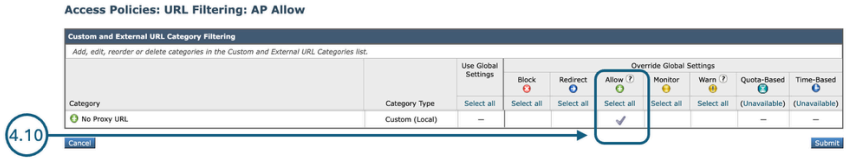


Immagine - Imposta l'azione per il passaggio

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.  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.  Immagine - Selezione del filtro URL Passaggio 4.10.Selezionare Allowerazione per la categoria

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