Blocca download file eseguibile in SWA

Sommario

Introduzione

In questo documento viene descritto il processo di configurazione di Secure Web Appliance (SWA) per bloccare il download di file eseguibili.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Accesso all'interfaccia grafica dell'SWA
- Accesso amministrativo all'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.

Operazioni preliminari

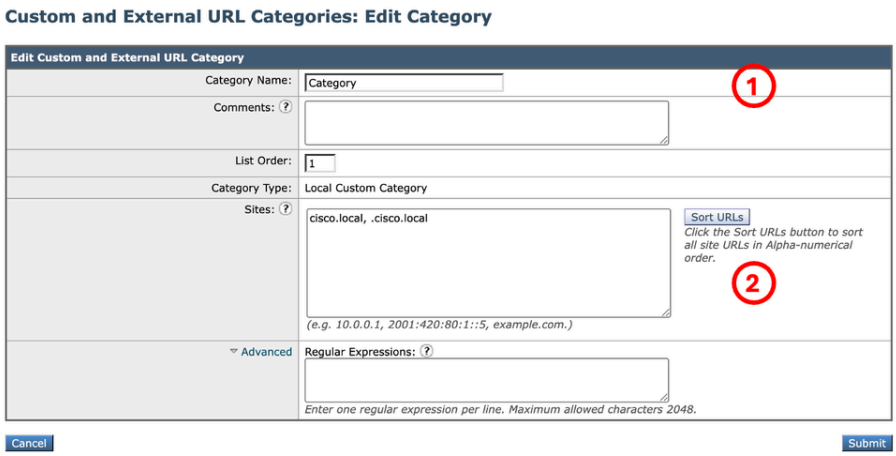
Cisco SWA può bloccare in modo efficace il download di file eseguibili ispezionando il tipo MIME (Multipurpose Internet Mail Extensions) di contenuto Web. Identificando tipi di file quali application/x-msdownload, application/x-msi e altri tipi MIME correlati, SWA applica criteri che impediscono il recapito degli eseguibili agli utenti. Oltre al rilevamento del tipo MIME, SWA può utilizzare il filtro delle estensioni dei file, l'analisi basata sulla reputazione e le regole

personalizzate per rafforzare ulteriormente la protezione da download indesiderati o rischiosi. Queste funzionalità aiutano le organizzazioni a mantenere un ambiente di navigazione sicuro e a ridurre il rischio di infezioni da malware.

Suggerimento: SWA non è in grado di identificare il tipo MIME del file, a meno che il traffico non venga decrittografato.

application/octet-stream è un tipo MIME generico utilizzato per indicare che un file contiene dati binari. Non specifica la natura del file, quindi può essere utilizzato per qualsiasi file che non si adatta a un tipo MIME più specifico. Questo tipo viene in genere assegnato ai file eseguibili, ai programmi di installazione e ad altri file non di testo quando il server Web non è in grado di determinare un tipo più preciso.

Procedura di configurazione

Passaggio 1. Creare una categoria URL personalizzata per il sito Web.	Passaggio 1.1.Dalla GUI, passare a Web Security Manager e scegliereCategorie URL personalizzate ed esterne. Passaggio 1.2.Fare clic su Aggiungi categoria per creare una nuova categoria di URL personalizzati. Passaggio 1.3.Inserire il nome della nuova categoria. Passaggio 1.4.Definire il dominio e/o i sottodomini del sito Web che si sta tentando di bloccare il traffico di caricamento (in questo esempio è cisco.local e tutti i relativi sottodomini). Passaggio 1.5.Inviare le modifiche.  Immagine - Crea categoria URL personalizzata Suggerimento: Per ulteriori informazioni su come configurare le categorie URL personalizzate, visitare:

	https://www.cisco.com/c/en/us/support/docs/security/secure-web-appliance-virtual/220557-configure-cu...
Passaggio 2. Decrittografare il traffico per l'URL	Attenzione: La decrittografia di un numero elevato di URL può causare una riduzione delle prestazioni. Passaggio 2.1. Dalla GUI, passare a Web Security Manager e scegliere Decryption Policies (Criteri di decrittografia) Passaggio 2.2. Fare clic su Aggiungi criterio. Passaggio 2.3.EnterName per il nuovo criterio. Passaggio 2.4.(Facoltativo) Selezionare il profilo di identificazione a cui applicare il criterio. Suggerimento: (Facoltativo) Se si desidera applicare il criterio a tutti gli utenti, anche se non sono autenticati, scegliere Tutti gli utenti (autenticati e non autenticati). Passaggio 2.5.Dalla sezione Definizione del membro dei criteri, fare clic su URL Categorieslinks (Categorie URL) per aggiungere la categoria URL personalizzata. Passaggio 2.6.Selezionare la categoria dell'URL creata nel Passaggio 1. Passaggio 2.7.Fare clic su Sottometti.

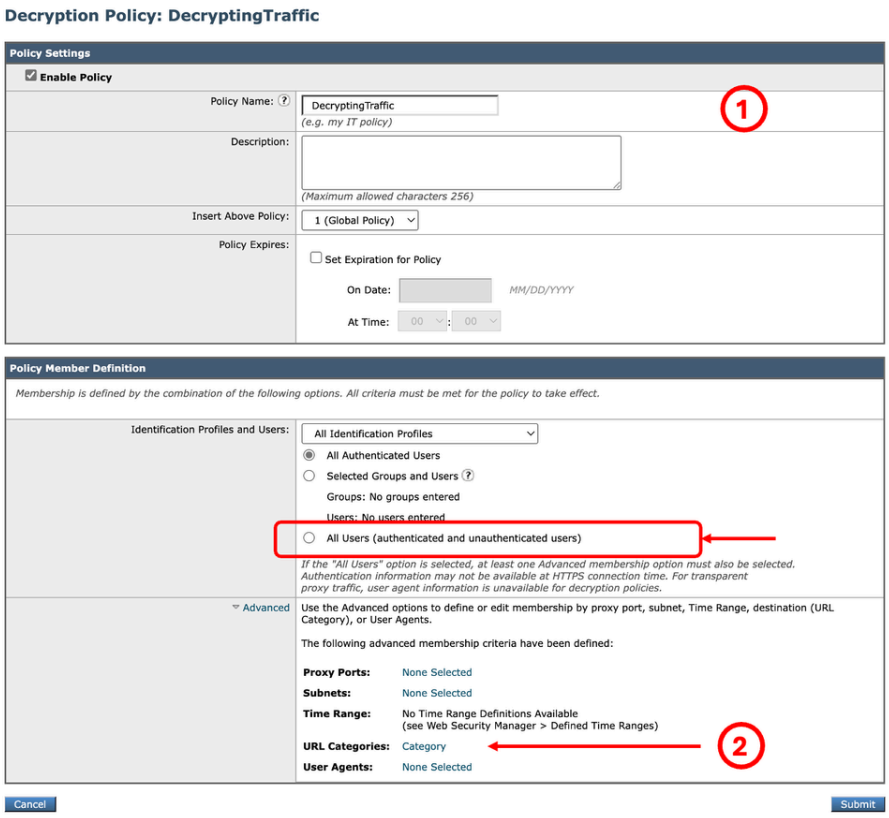


Immagine - Crea criterio di decrittografia

Passaggio 2.8.Nella pagina Criteri di decrittografia, fare clic sul collegamento da Filtro URL per il nuovo criterio.

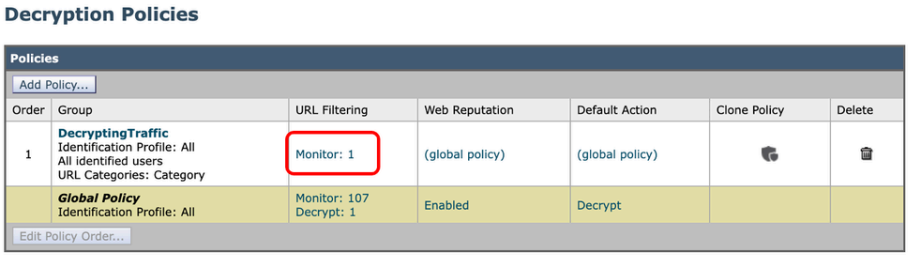


Immagine - Selezionare il filtro URL

Passaggio 2.9.ChooseDecrypt come azione per la categoria URL personalizzato.

Passaggio 2.10.Fare clic su Sottometti.

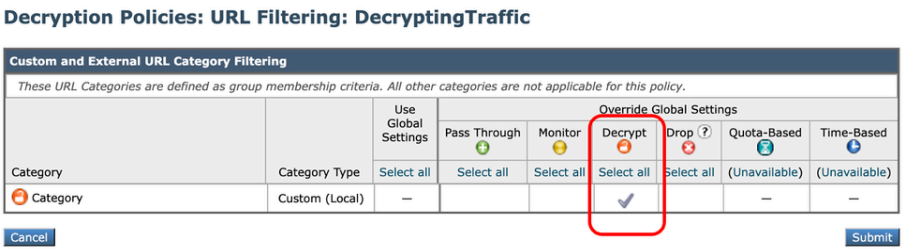


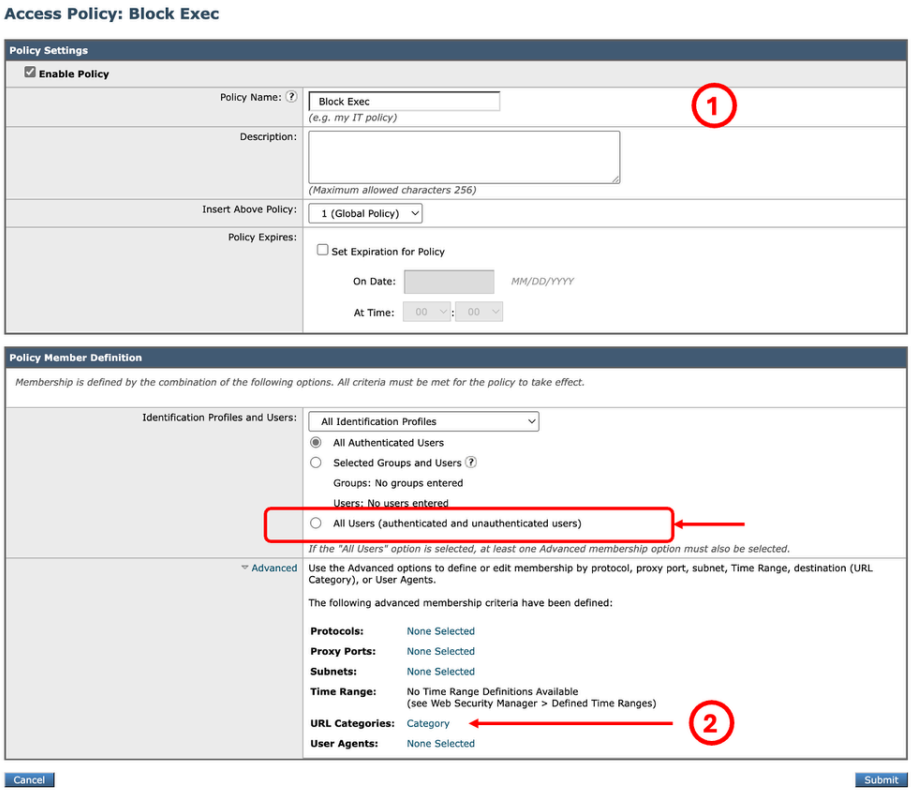
	Immagine - Imposta decrittografia come azione
Passaggio 3.Bloccare i file eseguibili	Passaggio 3.1.Dalla GUI, passare a Web Security Manager e selezionare Access Policies (Policy di accesso). Passaggio 3.2.Fare clic su Aggiungi criterio. Passaggio 3.3.EnterName per il nuovo criterio. Passaggio 3.4.(Facoltativo) Selezionare il profilo di identificazione a cui applicare il criterio. Suggerimento: (Facoltativo) Se si desidera applicare il criterio a tutti gli utenti, anche se non sono autenticati, scegliere Tutti gli utenti (autenticati e non autenticati). Passaggio 3.5.Dalla sezione Definizione membri dei criteri, fare clic sui collegamenti Categorie URL per aggiungere la categoria URL personalizzata. Passaggio 3.6.Selezionare la categoria dell'URL creata nel Passaggio 1. Passaggio 3.7.Fare clic su Sottometti. 

Immagine - Criteri di accesso

Suggerimento: Ai fini della creazione di report, è consigliabile scegliere un nome diverso da qualsiasi altro criterio di accesso/decrittografia.

Passaggio 3.8.Nella pagina Criteri di accesso, verificare che l'azione Filtro URL sia impostata su Monitoraggio.

Passaggio 3.9. Nella pagina Criteri di accesso, fare clic sul collegamento da Oggetti per il nuovo criterio.

Immagine - Seleziona oggetti

Immagine - Selezionare il filtro URL

Passaggio 3.10. Dal menu a discesa scegliere Definisci impostazioni blocco oggetti personalizzati.

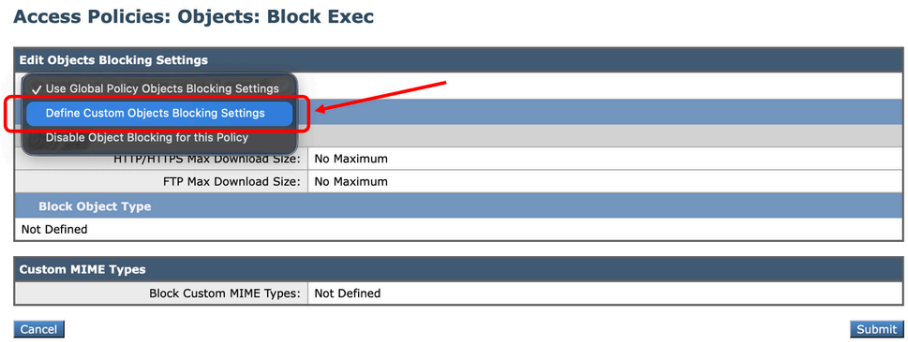


Immagine - Definizione oggetti personalizzati

Passaggio 3.11.Fare clic su Codice eseguibile per selezionare i tipi di oggetti da bloccare.

Passaggio 3.12.Fare clic su Installatori per selezionare i tipi di oggetti da bloccare.

Passaggio 3.13. È inoltre possibile immettere i tipi MIME dei file

che si desidera bloccare nella sezione Tipi MIME personalizzati.

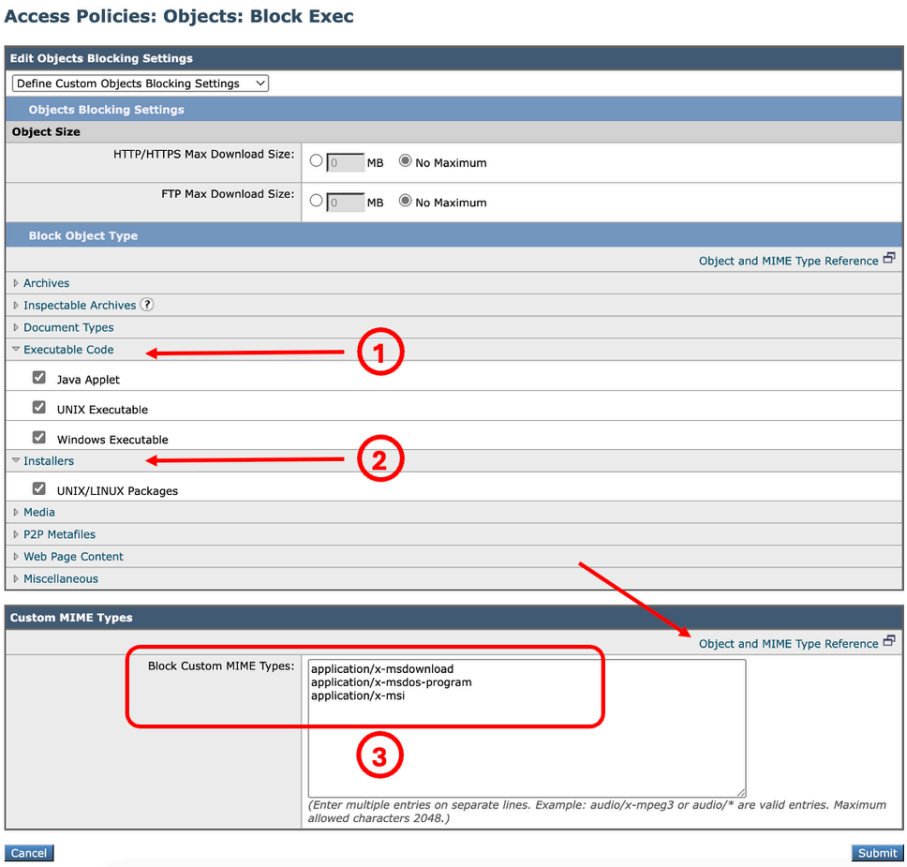


Immagine - Configurazione degli oggetti da bloccare

Suggerimento: Per visualizzare l'elenco dei tipi MIME, fare clic su Riferimento a oggetti e tipi MIME.

Passaggio 3.14.Inoltrare.

Passaggio 3.15.Eseguire il commit delle modifiche.

Convalida del blocco delle estensioni dei file

In questo esempio, quando un utente tenta di scaricare un file eseguibile, viene visualizzata la seguente pagina di avviso:

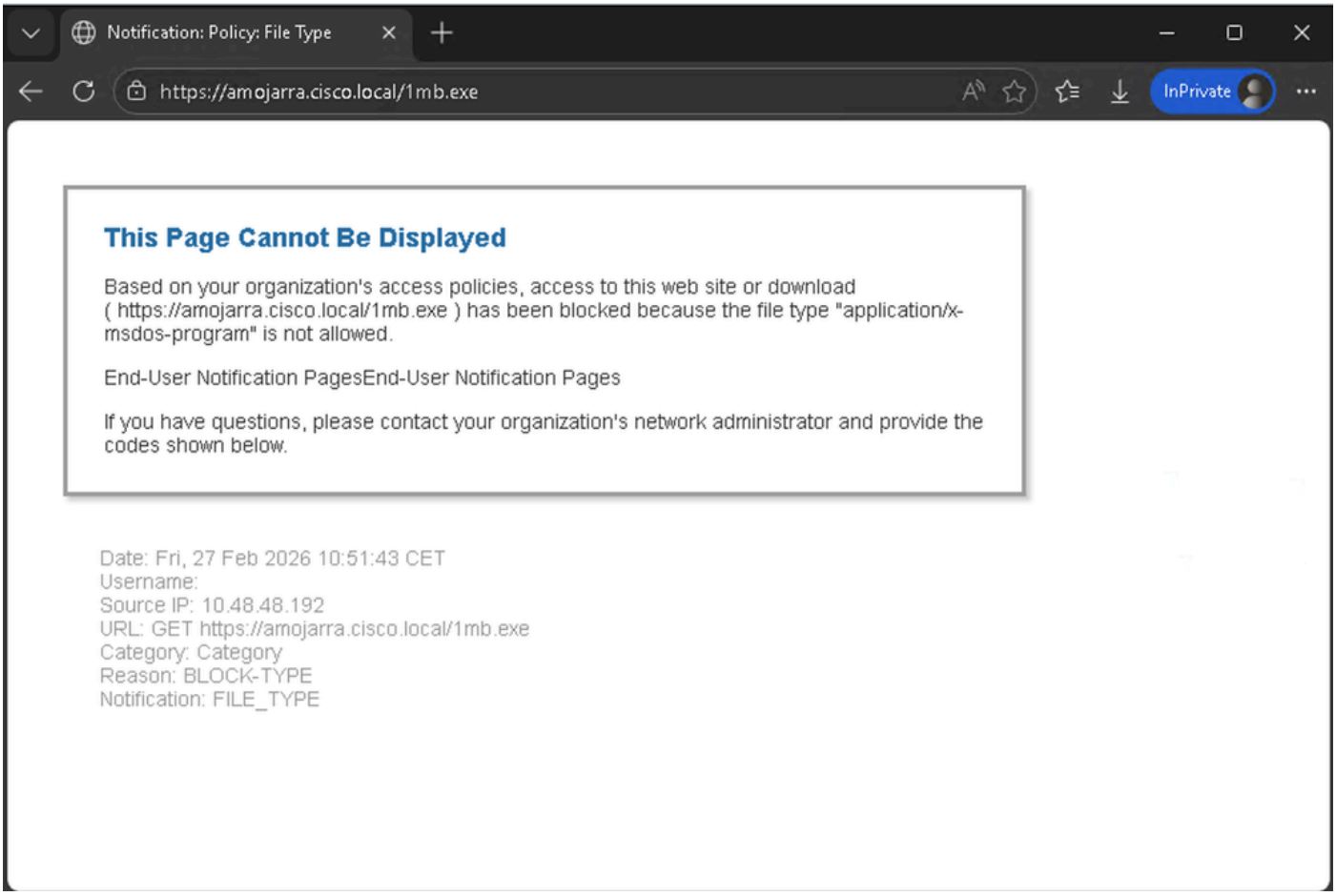


Immagine - Pagina Notifica di blocco

Suggerimento: Per configurare la pagina Notifica utente finale (EUN), dalla GUI passare a Servizi di sicurezza e fare clic su Notifica utente finale e modificare la sezione Pagine di notifica utente finale.

Dai log degli accessi è possibile visualizzare due righe di log correlate al traffico.

La prima riga di registro è correlata al criterio di decrittografia (nome: DecryptingTraffic) che sta decrittografando il traffico. L'azione è DECRYPT_CUSTOMCAT

La seconda riga del log degli accessi è correlata ai criteri di accesso (Nome: Block_Exec) che è stato creato nel passo 1.3. L'azione è BLOCK_ADMIN_FILE_TYPE

Policy	Log degli accessi
Criterio di decrittografia	1772186569.823 182 10.48.48.192 TCP_MISS_SSL/200 39 CONNECT tunnel://amojarra.cisco.local:443/ - DIRECT/amojarra.cisco.local - DECRYPT_CUSTOMCAT_7-DecryptingTraffic-DefaultGroup-NONE-NONE-LAB_Access-NONE <"C_Cate",-,-,"-",-,-,-,-,"-",-,-,-,"-",-,-,-,"-","-",-,-,-,"-",-,"-","-","-","-",-","-","-","-",-",1.71,0,-,"-","-",-,"-",-,-,"-","-",-,-,-,"-",-,-> -

Criteri di accesso	1772186576.735 2242 10.48.192 TCP_DENIED_SSL/403 0 GET https://amojarra.cisco.local:443/1mb.exe - DIRECT/amojarra.cisco.local application/x-msdos-program BLOCK_ADMIN_FILE_TYPE_12-Block_Exec-DefaultGroup-NONE-NONE-NONE-LAB_Access-NONE <"C_Cate",ns,0,"-",0,0,0,-,"-",-,-,-,"-",-,"-","-",-,-,"nc",-,"-","-","-","Sconosciuto","-","-",-",-",0.00,0,-,"Sconosciuto","-,-,"-,-,"-",-",-,-,"-,-",-,-,-> -

Informazioni correlate

- Guida per l'utente di AsyncOS 15.2 per Cisco Secure Web Appliance
- Guida all'installazione di Cisco Secure Email e Web Virtual Appliance
- Configurazione di categorie URL personalizzate in Secure Web Appliance - Cisco
- Utilizzare le procedure ottimali per Secure Web Appliance
- Configurare il firewall per Secure Web Appliance
- Configura certificato di decrittografia in Appliance Web sicura
- Configurazione e risoluzione dei problemi di SNMP in SWA
- Configurazione dei log di push SCP in Secure Web Appliance con Microsoft Server
- Abilita canale/video YouTube specifico e blocca resto di YouTube in SWA
- Informazioni sul formato HTTPS Accesslog in Secure Web Appliance
- Accesso ai registri protetti di Web Appliance
- Ignora autenticazione in Secure Web Appliance
- Blocca il traffico in Secure Web Appliance
- Ignora traffico aggiornamenti Microsoft in Secure Web Appliance

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).