

Configurare categorie URL personalizzate in Secure Web Appliance

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Categorie URL personalizzate](#)

[Categorie URL feed attivi](#)

[Passi per la creazione di categorie URL personalizzate](#)

[Definisci Usa espressioni regolari](#)

[Limitazioni e problemi di progettazione](#)

[Usa categorie URL personalizzate nei criteri](#)

[Passaggi Per Configurare I Filtri URL Per I Criteri Di Accesso](#)

[Passaggi Per Configurare I Filtri URL Per I Criteri Di Decrittografia](#)

[Passaggi Per Configurare I Filtri URL Per I Gruppi Di Criteri Di Sicurezza Dati](#)

[Passaggi Per Configurare Il Controllo Delle Richieste Di Caricamento Con Le Categorie URL Personalizzate](#)

[Passaggi per configurare le richieste ControlUpload nei criteri di prevenzione della perdita dei dati esterni](#)

[URL di bypass e pass-through](#)

[Configura Bypass Proxy Web Per Richieste Web](#)

[Report](#)

[Visualizzazione Di Categorie Di URL Personalizzate Nel Log Degli Accessi](#)

[Risoluzione dei problemi](#)

[Categoria non corrispondente](#)

[Riferimento](#)

Introduzione

Questo documento descrive la struttura delle categorie URL (Uniform Resource Locator) personalizzate in Secure Web Appliance (SWA).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Funzionamento del proxy.

- Amministrazione di Secure Web Appliance (SWA).

Cisco raccomanda:

- Installazione di Physical o Virtual Secure Web Appliance (SWA) completata.
- Licenza attivata o installata.
- Installazione guidata completata.

- 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.

Categorie URL personalizzate

Il motore di filtro URL consente di filtrare le transazioni in Criteri di accesso, decrittografia e sicurezza dei dati. Quando si configurano le categorie URL per i gruppi di criteri, è possibile configurare le azioni per le categorie URL personalizzate, se definite, e per le categorie URL predefinite.

È possibile creare categorie di URL di feed attivi personalizzate e esterne che descrivono nomi host specifici e indirizzi IP (Internet Protocol). È inoltre possibile modificare ed eliminare le categorie URL.

Quando si includono queste categorie URL personalizzate nello stesso gruppo di criteri per la sicurezza dei dati di Access, Decrittografia o Cisco e si assegnano azioni diverse a ciascuna categoria, l'azione della categoria URL personalizzata inclusa di livello superiore ha la precedenza.

 **Nota:** se il DNS (Domain Name System) risolve diversi IP in un sito Web e uno di questi IP è un elenco di indirizzi IP bloccati personalizzato, Web Security Appliance blocca il sito Web per tutti gli IP, indipendentemente da quelli non elencati nell'elenco di indirizzi IP bloccati personalizzato.

Categorie URL feed attivi

Le categorie di feed attivi esterni vengono utilizzate per estrarre l'elenco degli URL da un sito specifico, ad esempio per recuperare gli URL di Office 365 da Microsoft.

Se per Tipo di categoria si seleziona Categoria feed esterni quando si creano e si modificano

categorie URL personalizzate ed esterne, è necessario selezionare il formato di feed (formato feed Cisco o formato feed Office 365) e quindi fornire un URL al server di feed appropriato. Di seguito è riportato il formato previsto per ogni file feed:

- Formato feed Cisco: deve essere un file con valori delimitati da virgole (csv), ovvero un file di testo con estensione csv. Ogni voce del file con estensione csv deve trovarsi su una riga distinta, formattata come indirizzo/virgola/tipo di indirizzo (ad esempio: www.cisco.com,site o ad2.*\com,regex). I tipi di indirizzo validi sono site e regex.

Di seguito è riportato un estratto del file con estensione csv Cisco Feed Format:

```
www.cisco.com,site
\.xyz,regex
ad2.*\com,regex
www.cisco.local,site
1:1:1:11:1:1::200,site
```

- Formato feed di Office 365: file XML che si trova in un server Microsoft Office 365 o in un server locale in cui è stato salvato il file. Viene fornito dal servizio di Office 365 e non può essere modificato.

Gli indirizzi di rete nel file sono racchiusi tra tag XML, la seguente struttura: prodotti > prodotto > elenco indirizzi > indirizzo. Nell'implementazione corrente, un "tipo di elenco indirizzi" può essere IPv6, IPv4 o URL [che può includere domini e modelli Regex (Regular Expressions)].

Di seguito è riportato un frammento di un file di feed di Office 365:

```
<products updated="4/15/2016">
<product name="o365">
<addresslist type="IPv6">
<address>fc00:1040:401::d:80</address>
<address>fc00:1040:401::a</address>
<address>fc00:1040:401::9</address>
</addresslist>
<addresslist type="IPv4">
<address>10.71.145.72</address>
<address>10.71.148.74</address>
<address>10.71.145.114</address>
</addresslist>
<addresslist type="URL">
<address>*.cisco.com</address>
<address>*.example.local</address>
</addresslist>
</product>
<product name="LYO">
<addresslist type="URL">
<address>*.subdomain.cisco.com</address>
<address>*.example.local</address>
</addresslist>
```

</product>
</products>

 Nota: non includere http:// o https:// come parte di una voce del sito nel file, altrimenti si verificherà un errore. In altre parole, www.cisco.com viene analizzato correttamente, mentre <http://www.cisco.com> genera un errore

Passi per la creazione di categorie URL personalizzate

Passaggio 1. Scegliere Web Security Manager > Categorie URL personalizzate ed esterne.

Authentication

Identification Profiles

SaaS Policies

Web Policies

Decryption Policies

Routing Policies

Access Policies

Overall Bandwidth Limits

Data Transfer Policies

Cisco Data Security

Outbound Malware Scanning

External Data Loss Prevention

Web Traffic Tap Policies

SOCKS Policies

Custom Policy Elements

Custom and External URL Categories

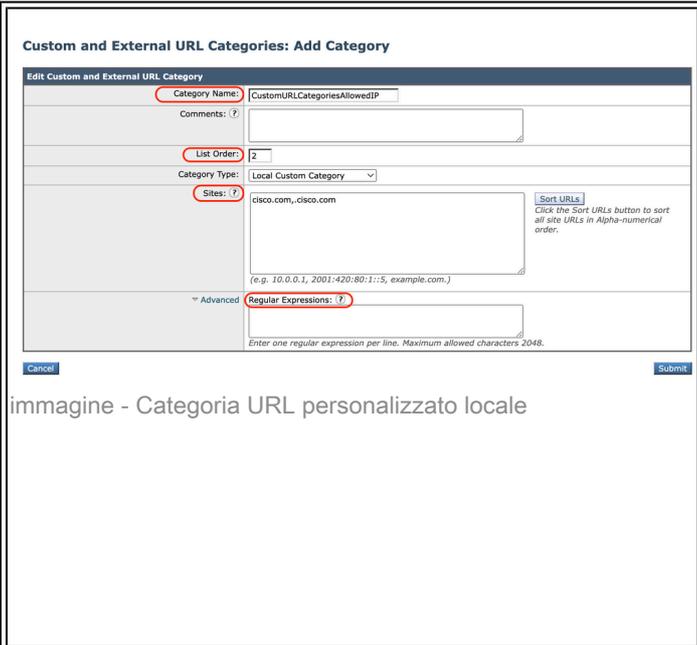
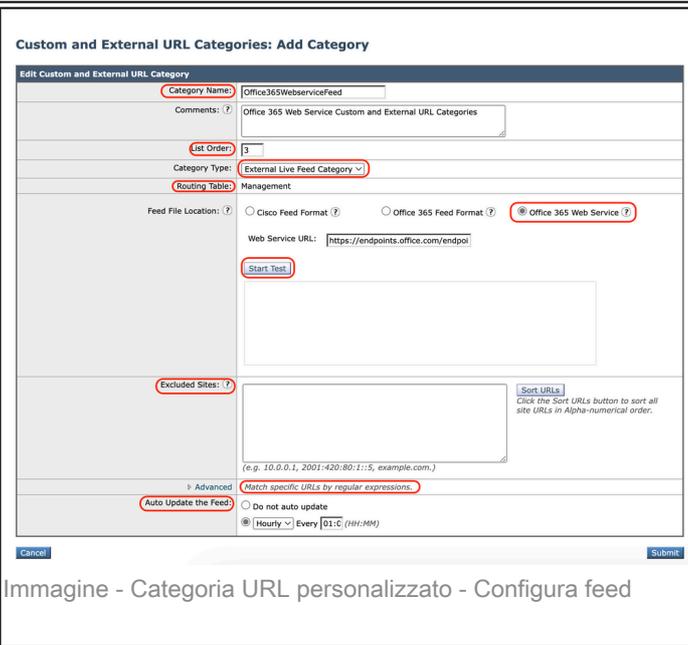
: immettere un identificatore per questa categoria di URL. Questo nome viene visualizzato quando si configura il filtro URL per i gruppi di criteri.

- Ordine elenco: specificare l'ordine di questa categoria nell'elenco delle categorie URL personalizzate. Immettere "1" per la prima categoria di URL nell'elenco.

Il motore di filtro URL valuta una richiesta client in base alle categorie URL personalizzate nell'ordine specificato.

 Nota: quando il motore di filtro URL associa una categoria URL all'URL di una richiesta client, valuta prima l'URL in base alle categorie URL personalizzate incluse nel gruppo di criteri. Se l'URL nella richiesta non corrisponde a una categoria personalizzata inclusa, il motore di filtro URL lo confronta con le categorie URL predefinite. Se l'URL non corrisponde ad alcuna categoria di URL predefinita o personalizzata inclusa, la richiesta non viene classificata.

- Tipo di categoria: scegliere Categoria personalizzata locale o Categoria feed esterno.
- Tabella di routing: scegliere Gestione o Dati. Questa opzione è disponibile solo se è abilitato il "routing suddiviso", ovvero non è disponibile con le categorie personalizzate locali.

| | |
|---|---|
|  <p>immagine - Categoria URL personalizzato locale</p> |  <p>Immagine - Categoria URL personalizzato - Configura feed</p> |
| Categoria personalizzata locale | Categoria feed live esterno |

Definisci Usa espressioni regolari

Secure Web Appliance utilizza una sintassi delle espressioni regolari leggermente diversa da quella utilizzata da altre implementazioni del motore Velocity per la corrispondenza dei pattern.

Inoltre, l'accessorio non supporta la barra rovesciata per l'escape di una barra in avanti. Se è necessario utilizzare una barra in un'espressione regolare, è sufficiente digitare la barra senza una barra rovesciata.

 Nota: da un punto di vista tecnico, AsyncOS for Web utilizza l'analizzatore di espressioni

Per verificare le espressioni regolari è possibile utilizzare questo collegamento: [lint flessibile - Tester/Debugger Regex](#)

 **Attenzione:** le espressioni regolari che restituiscono più di 63 caratteri non hanno esito positivo e generano un errore di immissione non valida. Assicurarsi di creare espressioni regolari che non possano restituire più di 63 caratteri

 **Attenzione:** le espressioni regolari che eseguono un'ampia corrispondenza di caratteri consumano risorse e possono influire sulle prestazioni del sistema. Per questo motivo, le espressioni regolari possono essere applicate con cautela.

È possibile utilizzare le espressioni regolari nelle posizioni seguenti:

- Categorie URL personalizzate per i criteri di accesso. Quando si crea una categoria URL personalizzata da utilizzare con i gruppi di criteri di accesso, è possibile utilizzare le espressioni regolari per specificare più server Web che corrispondono al modello immesso.
- Agenti utente personalizzati da bloccare. Quando si modificano le applicazioni da bloccare per un gruppo di criteri di accesso, è possibile utilizzare le espressioni regolari per immettere agenti utente specifici da bloccare.

 **Suggerimento:** non è possibile impostare il bypass del proxy Web per le espressioni regolari.

di seguito è riportato l'elenco delle classi di caratteri nell'espressione regolare Flex

| Classi di caratteri | |
|--------------------------------|---|
| . | qualsiasi carattere ad eccezione della nuova riga |
| \w \d \s | parola, cifra, spazio |
| \W \D \S | non parola, cifra, spazio |
| [abc] | qualsiasi valore tra a, b o c |
| [^abc] | non a, b o c |
| [a-g] | carattere tra a e g |
| Ancoraggi | |
| ^abc\$ | inizio / fine della stringa |
| \b | limite di parola |
| Caratteri di escape | |
| \. * \\ | caratteri speciali con escape |
| \t \n \r | tabulazione, avanzamento riga, ritorno a capo |
| \u00A9 | escape unicode © |
| Gruppi e soluzioni alternative | |
| abc) | gruppo di acquisizione |

| | |
|------------------------------|-------------------------------|
| \1 | rimando al gruppo n. 1 |
| (?:abc) | gruppo di non acquisizione |
| (?=abc) | uno sguardo positivo |
| (?!abc) | sguardo negativo in avanti |
| Quantificatori e alternative | |
| a* a+ a? | 0 o più, 1 o più, 0 o 1 |
| a{5} a{2,} | esattamente cinque, due o più |
| a{1,3} | tra uno e tre |
| a+? a{2,}? | abbinare il meno possibile |
| ab cd | abbinare ab o cd |

 **Attenzione:** prestare attenzione ai punti non evasi nei modelli lunghi, specialmente nel mezzo dei modelli più lunghi, e diffidare di questo metacarattere (Star *), specialmente in combinazione con il carattere punto. Qualsiasi modello contiene un punto senza escape che restituisce più di 63 caratteri dopo la disattivazione del punto.

Esci sempre *(stella) e . (punto) con \ (barra rovesciata) come \<* e \.

Se si utilizza .cisco.local nell'espressione regolare, anche il dominio Xcisco.local corrisponde.

Il carattere senza escape influisce sulle prestazioni e crea lentezza durante l'esplorazione del Web. Ciò è dovuto al fatto che il motore di ricerca deve passare attraverso migliaia o milioni di possibilità fino a trovare una corrispondenza per la voce corretta anche può avere alcuni problemi di sicurezza per quanto riguarda gli URL simili per i criteri consentiti

È possibile utilizzare l'opzione CLI (Command Line Interface) `advancedproxyconfig > miscellaneous > Do you want to enable URL lower case conversion for velocity regex`, per abilitare o disabilitare la conversione regex predefinita in lettere minuscole per le corrispondenze senza distinzione tra maiuscole e minuscole. Utilizzare in caso di problemi relativi alla distinzione tra maiuscole e minuscole.

Limitazioni e problemi di progettazione

- Non è possibile utilizzare più di 30 file di feed esterni in tempo reale in queste definizioni di categorie di URL e ogni file non deve contenere più di 5000 voci.
- Se il numero di voci di alimentazione esterne aumenta, le prestazioni diminuiscono.
- È possibile utilizzare lo stesso indirizzo in più categorie URL personalizzate, ma l'ordine in cui sono elencate le categorie è rilevante.

Se si includono queste categorie nello stesso criterio e si definiscono azioni diverse per ciascuna di esse, viene applicata l'azione definita per la categoria elencata più in alto nella tabella delle categorie URL personalizzate.

- Quando una richiesta FTP (File Transfer Protocol) nativa viene reindirizzata in modo trasparente al proxy FTP, non contiene informazioni sul nome host per il server FTP, ma solo il relativo indirizzo IP.

Per questo motivo, alcune categorie URL predefinite e filtri Web Reputation che dispongono solo di informazioni sul nome host non corrispondono alle richieste FTP native, anche se le richieste sono destinate a tali server.

Se si desidera bloccare l'accesso a questi siti, è necessario creare categorie URL personalizzate per consentire l'utilizzo dei relativi indirizzi IP.

- Un URL non classificato è un URL che non corrisponde ad alcuna categoria URL predefinita né ad alcuna categoria URL personalizzata inclusa

Usa categorie URL personalizzate nei criteri

Il motore di filtro URL consente di filtrare le transazioni in Criteri di accesso, decrittografia e sicurezza dei dati. Quando si configurano le categorie URL per i gruppi di criteri, è possibile configurare le azioni per le categorie URL personalizzate, se definite, e per le categorie URL predefinite.

Passaggi Per Configurare I Filtri URL Per I Criteri Di Accesso

Passaggio 1. Scegliere Web Security Manager > Criteri di accesso.

Authentication

Identification Profiles

SaaS Policies

Web Policies

Decryption Policies

Routing Policies

Access Policies

Overall Bandwidth Limits

Data Transfer Policies

Cisco Data Security

Outbound Malware Scanning

External Data Loss Prevention

Web Traffic Tap Policies

SOCKS Policies

Custom Policy Elements

Fare clic sul collegamento nella tabella Criteri sotto la colonna Filtro URL per il gruppo di criteri che si desidera modificare.

Access Policies

| Order | Group | Protocols and User Agents | URL Filtering | Applications | Objects | Anti-Malware and Reputation | HTTP ReWrite Profile | Clone Policy | Delete |
|-------|--|---------------------------|-----------------|--------------|------------------|---|----------------------|--------------|--------|
| 1 | Access Policy Identification Profile: Global All identified users | (global policy) | (global policy) | Monitor: 343 | (global policy) | (global policy) | (global policy) | | |
| | Global Policy Identification Profile: All | No blocked items | Monitor: 107 | Monitor: 343 | No blocked items | Web Reputation: Enabled Secure Endpoint: Enabled Anti-Malware Scanning: Enabled | None | | |

Immagine - Aggiungi categoria personalizzata ai criteri di accesso

Passaggio 3. (Facoltativo) Nella sezione Filtro categoria URL personalizzato, è possibile aggiungere categorie URL personalizzate sulle quali eseguire un'azione nel criterio:

a) Fare clic su Seleziona categorie personalizzate.

Access Policies: URL Filtering: Access Policy

Custom and External URL Category Filtering

No Custom Categories are included for this Policy.

Select Custom Categories...

Immagine - Seleziona categoria URL personalizzata

b) Selezionare le categorie URL personalizzate da includere nel criterio e fare clic su Apply (Applica).

Select Custom Categories for this Policy

| Category | Category Type | Setting Selection |
|-------------------------|----------------|---|
| Msoffice365Feed | External Feed | Exclude from policy |
| CustomURLCategoriesA... | Custom (Local) | Include in policy |
| Office365WebserviceF... | External Feed | Use Global Settings (Exclude from policy) |

Cancel Apply

Immagine-Selezione categorie personalizzate da includere nel criterio

Scegliere le categorie URL personalizzate con cui il motore di filtro URL deve confrontare la richiesta client.

Il motore di filtro URL confronta le richieste client con le categorie URL personalizzate incluse e ignora le categorie URL personalizzate escluse.

Il motore di filtro URL confronta l'URL di una richiesta client con le categorie URL personalizzate incluse prima delle categorie URL predefinite.

Le categorie URL personalizzate incluse nel criterio vengono visualizzate nella sezione Filtro categoria URL personalizzato.

Passaggio 4. Nella sezione Filtro categoria URL personalizzato selezionare un'azione per ciascuna categoria URL personalizzata inclusa.

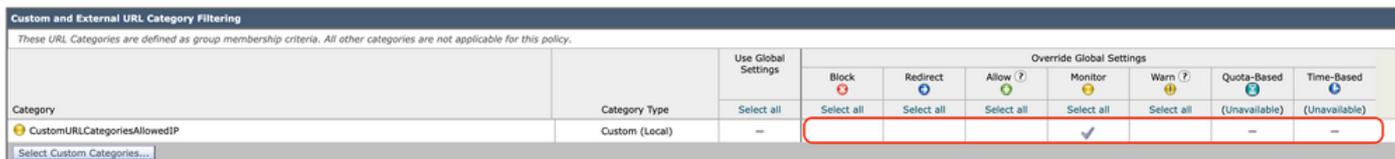


Immagine - Scegli azione per categoria personalizzata

| Azione | Descrizione |
|--------------------------|--|
| Usa impostazioni globali | Utilizza l'azione per questa categoria nel gruppo di criteri globali. Si tratta dell'azione predefinita per i gruppi di criteri definiti dall'utente. Si applica solo ai gruppi di criteri definiti dall'utente. |
| Block (Blocca) | Il proxy Web nega le transazioni che corrispondono a questa impostazione. |
| Reindirizzamento | Reindirizza il traffico originariamente destinato a un URL in questa categoria al percorso specificato. Quando si sceglie questa azione, viene visualizzato il campo Reindirizza a. Immettere un URL a cui reindirizzare tutto il traffico. |
| Allow (Autorizza) | Consente sempre le richieste client per i siti Web in questa categoria. Le richieste consentite ignorano tutti gli ulteriori filtri e le analisi malware. Utilizzare questa impostazione solo per i siti Web attendibili. È possibile utilizzare questa impostazione per i siti interni. |
| Monitor (Monitora) | Il proxy Web non consente né blocca la richiesta. Continua invece a valutare la richiesta client rispetto ad altre impostazioni di controllo del gruppo di criteri, ad esempio il filtro reputazione Web. |

| Azione | Descrizione |
|------------------|---|
| Avvisa | Il proxy Web inizialmente blocca la richiesta e visualizza una pagina di avviso, ma consente all'utente di continuare facendo clic su un collegamento ipertestuale nella pagina di avviso. |
| Basato su quota | Quando un singolo utente si avvicina al volume o alle quote temporali specificate, viene visualizzato un avviso. Quando viene raggiunta una quota, viene visualizzata una pagina di blocco. . |
| Basato sul tempo | Il proxy Web blocca o controlla la richiesta durante gli intervalli di tempo specificati. |

Passaggio 5. Nella sezione Filtro categoria URL predefinito, scegliere una delle seguenti azioni per ciascuna categoria:

- Usa impostazioni globali
- Monitor (Monitora)
- Avvisa
- Block (Blocca)
- Basato sul tempo
- Basato su quota

| Category | Use Global Settings | Override Global Settings | | | | |
|--|---------------------|--------------------------|-------------------------------------|------------|-------------------------------------|-------------------------------------|
| | | Block | Monitor | Warn | Quota-Based | Time-Based |
| Animals and Pets | Select all | Select all | Select all | Select all | | |
| Arts | | | <input checked="" type="checkbox"/> | | | |
| Predefined Quota Profile: 10GBdailyLimit | | | | | <input checked="" type="checkbox"/> | |
| Astrology | | | | | | <input checked="" type="checkbox"/> |
| In time range: MorningShift | | | | | | |
| Action: Warn | | | | | | |
| Otherwise: Block | | | | | | |

Immagine - Selezionare l'azione per la categoria predefinita

Passaggio 6. Nella sezione URL non classificati, scegliere l'azione da eseguire per le richieste dei client ai siti Web che non rientrano in una categoria URL predefinita o personalizzata. Questa impostazione determina anche l'azione predefinita per le categorie nuove e unite risultante dagli aggiornamenti delle serie di categorie URL.

| Uncategorized URLs | |
|---|------------------|
| <i>Specify an action for urls that do not match any category.</i> | |
| Uncategorized URLs: | Monitor |
| Default Action for Update Categories: ? | Most Restrictive |

Immagine: scegliere l'azione da eseguire per gli URL non classificati

Passaggio 7. Invia e conferma modifiche.

Passaggi Per Configurare I Filtri URL Per I Criteri Di Decrittografia

Passaggio 1. Scegliere Web Security Manager > Criteri di decrittografia.

Authentication

Identification Profiles

SaaS Policies

Web Policies

Decryption Policies

Routing Policies

Access Policies

Overall Bandwidth Limits

Data Transfer Policies

Cisco Data Security

Outbound Malware Scanning

External Data Loss Prevention

Web Traffic Tap Policies

SOCKS Policies

Custom Policy Elements

Fare clic sul collegamento nella tabella Criteri sotto la colonna Filtro URL per il gruppo di criteri che si desidera modificare.

Decryption Policies

| Policies | | | | | | |
|---------------|---|---------------------------------------|-----------------|-----------------|--------------|--------|
| Add Policy... | | | | | | |
| Order | Group | URL Filtering | Web Reputation | Default Action | Clone Policy | Delete |
| 1 | DecryptionPolicy Identification Profile: Global All identified users | (global policy) | (global policy) | (global policy) | | |
| | Global Policy Identification Profile: All | Monitor: 1 Decrypt: 106 Drop: 1 | Enabled | Decrypt | | |

Edit Policy Order...

Immagine - Scelta filtro URL

Passaggio 3. (Facoltativo) Nella sezione Filtro categoria URL personalizzato, è possibile aggiungere categorie URL personalizzate sulle quali eseguire un'azione nel criterio:

- a. Fare clic su Seleziona categorie personalizzate.

Decryption Policies: URL Filtering: DecryptionPolicy

Custom and External URL Category Filtering

No Custom Categories are included for this Policy.

Select Custom Categories...

Immagine - Scegli categorie personalizzate

- b. Scegliere le categorie URL personalizzate da includere nel criterio e fare clic su Applica.

Select Custom Categories for this Policy ✕

| Category | Category Type | Setting Selection |
|-------------------------|----------------|--|
| Msoffice365Feed | External Feed | Exclude from policy <input type="button" value="v"/> |
| CustomURLCategoriesA... | Custom (Local) | Include in policy <input type="button" value="v"/> |
| Office365WebserviceF... | External Feed | Use Global Settings (Exclude from policy) <input type="button" value="v"/> |

Immagine-Selezione categorie personalizzate da includere nel criterio

Scegliere le categorie URL personalizzate con cui il motore di filtro URL deve confrontare la richiesta client.

Il motore di filtro URL confronta le richieste client con le categorie URL personalizzate incluse e ignora le categorie URL personalizzate escluse.

Il motore di filtro URL confronta l'URL di una richiesta client con le categorie URL personalizzate incluse prima delle categorie URL predefinite.

Le categorie URL personalizzate incluse nel criterio vengono visualizzate nella sezione Filtro categoria URL personalizzato.

Passaggio 4. Selezionare un'azione per ciascuna categoria di URL predefinita e personalizzata.

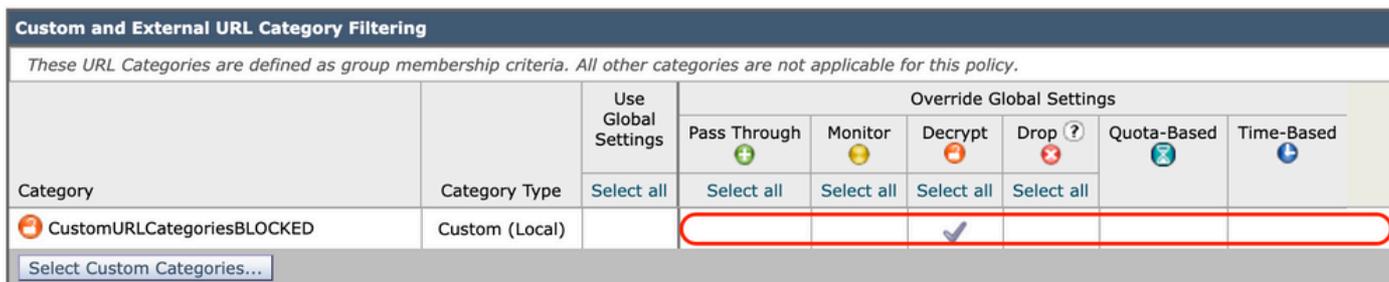


Immagine - Scegliere L'Azione Per I Criteri Di Decrittografia

| Azione | Descrizione |
|--------------------------|--|
| Usa impostazione globale | <p>Utilizza l'azione per questa categoria nel gruppo Criteri di decrittografia globale. Si tratta dell'azione predefinita per i gruppi di criteri definiti dall'utente.</p> <p>Si applica solo ai gruppi di criteri definiti dall'utente.</p> <p>Quando una categoria URL personalizzata viene esclusa dai criteri di decrittografia globali, l'azione predefinita per le categorie URL personalizzate incluse nei criteri di decrittografia definiti dall'utente è Monitoraggio anziché Usa impostazioni globali. Non è possibile scegliere Usa impostazioni globali quando una categoria URL personalizzata è esclusa dai criteri di decrittografia globali.</p> |
| Pass-through | <p>Passa attraverso la connessione tra il client e il server senza esaminare il contenuto del traffico.</p> |
| Monitor (Monitora) | <p>Il proxy Web non consente né blocca la richiesta. Continua invece a valutare la richiesta client rispetto ad altre impostazioni di controllo del gruppo di criteri, ad esempio il filtro reputazione Web.</p> |
| Decrittografa | <p>Consente la connessione, ma controlla il contenuto del traffico. L'accessorio decrittografa il traffico e applica i criteri di accesso al traffico decrittografato come se si trattasse di una connessione HTTP (Hypertext Transfer Protocol) in testo normale. Quando la connessione viene decrittografata e vengono applicati i criteri di accesso, è possibile analizzare il traffico alla ricerca di malware.</p> |

| Azione | Descrizione |
|--------|--|
| Drop | Elimina la connessione e non passa la richiesta di connessione al server. L'accessorio non notifica all'utente l'interruzione della connessione. |

Passaggio 5. Nella sezione URL non classificati, scegliere l'azione da eseguire per le richieste dei client ai siti Web che non rientrano in una categoria URL predefinita o personalizzata.

Questa impostazione determina anche l'azione predefinita per le categorie nuove e unite risultante dagli aggiornamenti delle serie di categorie URL.

Immagine - Criterio di decrittografia non classificato

Passaggio 6. Invia e conferma modifiche.

 **Attenzione:** se si desidera bloccare una determinata categoria di URL per le richieste HTTPS (Hypertext Transfer Protocol Secure), scegliere di decrittografare tale categoria di URL nel gruppo Criterio di decrittografia, quindi scegliere di bloccare la stessa categoria di URL nel gruppo Criteri di accesso.

Passaggi Per Configurare I Filtri URL Per I Gruppi Di Criteri Di Sicurezza Dati

Passaggio 1. Scegliere Web Security Manager > Cisco Data Security.

Authentication

Identification Profiles

SaaS Policies

Web Policies

Decryption Policies

Routing Policies

Access Policies

Overall Bandwidth Limits

Data Transfer Policies

Cisco Data Security

Outbound Malware Scanning

External Data Loss Prevention

Web Traffic Tap Policies

SOCKS Policies

Custom Policy Elements

Custom and External URL Categories

Fare clic sul collegamento nella tabella Criteri sotto la colonna Filtro URL per il gruppo di criteri che si desidera modificare.

Cisco Data Security

| Cisco Data Security Policies | | | | | | |
|------------------------------|--|-----------------|-----------------|---|--------------|--------|
| Add Policy... | | | | | | |
| Order | Cisco Data Security Policy | URL Filtering | Web Reputation | Content | Clone Policy | Delete |
| 1 | CiscoDataSecurityPolicy Identification Profile: Global All identified users | (global policy) | (global policy) | (global policy) | | |
| | Global Policy Identification Profile: All | Monitor: 107 | Enabled | No maximum size for HTTP/HTTPS No maximum size for FTP | | |

Edit Policy Order...

Immagine - Protezione dei dati - Scelta del filtro URL

Passaggio 3. (Facoltativo) Nella sezione Filtro categoria URL personalizzato, è possibile aggiungere categorie URL personalizzate sulle quali eseguire un'azione nel criterio:

- Fare clic su Seleziona categorie personalizzate.

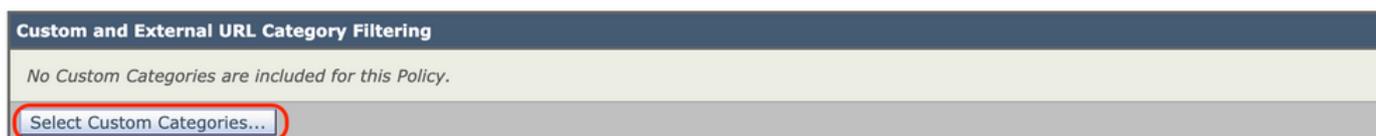


Immagine - Seleziona campo personalizzato

- Scegliere le categorie URL personalizzate da includere nel criterio e fare clic su Applica.

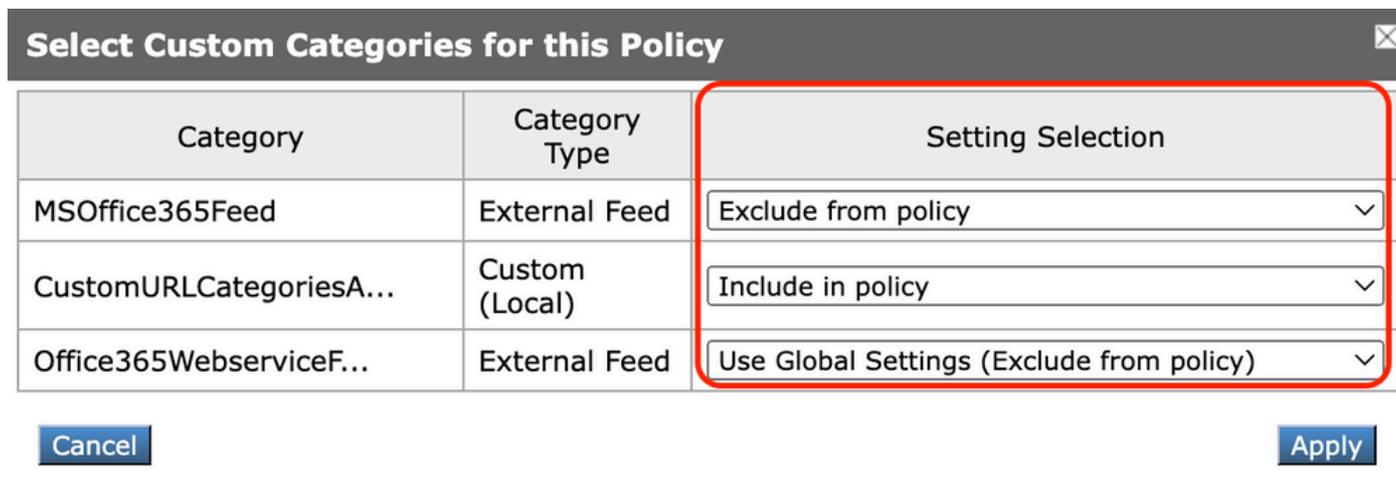


Immagine-Selezione categorie personalizzate da includere nel criterio

Scegliere le categorie URL personalizzate con cui il motore di filtro URL deve confrontare la richiesta client.

Il motore di filtro URL confronta le richieste client con le categorie URL personalizzate incluse e ignora le categorie URL personalizzate escluse.

Il motore di filtro URL confronta l'URL di una richiesta client con le categorie URL personalizzate

incluse prima delle categorie URL predefinite.

Le categorie URL personalizzate incluse nel criterio vengono visualizzate nella sezione Filtro categoria URL personalizzato.

Passaggio 4. Nella sezione Filtro categoria URL personalizzato, scegliere un'azione per ciascuna categoria di URL personalizzati.

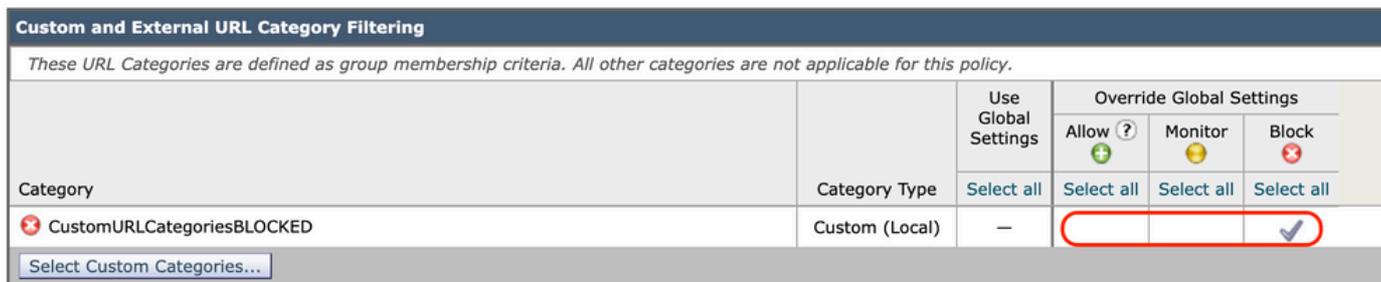


Immagine - Protezione dati - Scegli azione

| Azione | Descrizione |
|--------------------------|--|
| Usa impostazione globale | <p>Utilizza l'azione per questa categoria nel gruppo di criteri globali. Si tratta dell'azione predefinita per i gruppi di criteri definiti dall'utente.</p> <p>Si applica solo ai gruppi di criteri definiti dall'utente.</p> <p>Quando una categoria URL personalizzata viene esclusa dai criteri di sicurezza dei dati Cisco globali, l'azione predefinita per le categorie URL personalizzate incluse nei criteri di sicurezza dei dati Cisco definiti dall'utente è Controlla anziché Usa impostazioni globali. Non è possibile scegliere Usa impostazioni globali quando una categoria URL personalizzata è esclusa dai criteri globali di sicurezza dati Cisco.</p> |
| Allow (Autorizza) | <p>Consente sempre le richieste di caricamento per i siti Web in questa categoria. Si applica solo alle categorie URL personalizzate.</p> <p>Le richieste consentite ignorano tutte le ulteriori analisi di protezione dei dati e vengono valutate in base ai criteri di accesso.</p> <p>Utilizzare questa impostazione solo per i siti Web attendibili. È possibile utilizzare questa impostazione per i siti interni.</p> |
| Monitor (Monitora) | <p>Il proxy Web non consente né blocca la richiesta. Continua invece a valutare la richiesta di caricamento rispetto ad altre impostazioni di controllo del gruppo di criteri, ad esempio il filtro reputazione Web.</p> |

| Azione | Descrizione |
|----------------|---|
| Block (Blocca) | Il proxy Web nega le transazioni che corrispondono a questa impostazione. |

Passaggio 5. Nella sezione Filtro categoria URL predefinito, scegliere una delle seguenti azioni per ciascuna categoria:

- Usa impostazioni globali
- Monitor (Monitora)
- Block (Blocca)

| Predefined URL Category Filtering | | |
|--|---------------------|---|
| <i>These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.</i> | | |
| <i>Apart from the URL categories listed here, all the URL categories from the global access policy will be inherited in this policy.</i> | | |
| Category | Use Global Settings | Override Global Settings |
| | | Monitor  |
| | Select all | Select all |
|  Hunting | | <input checked="" type="checkbox"/> |
|  Illegal Activities | | <input checked="" type="checkbox"/> |

Immagine - Sicurezza dei dati URL predefinito Scegli azione

Passaggio 6. Nella sezione URL non classificati, scegliere l'azione da eseguire per le richieste di caricamento su siti Web che non rientrano in una categoria URL predefinita o personalizzata.

Questa impostazione determina anche l'azione predefinita per le categorie nuove e unite risultante dagli aggiornamenti delle serie di categorie URL.

| Uncategorized URLs | |
|---|--|
| <i>Specify an action for urls that do not match any category.</i> | |
| Uncategorized URLs: | <input type="text" value="Block"/> |
| Default Action for Update Categories:  | <input type="text" value="Least Restrictive"/> |

Immagine - Protezione dati non classificata

Passaggio 7. Invia e conferma modifiche.

 **Attenzione:** se non si disabilita il limite massimo per le dimensioni dei file, Web Security Appliance continua a convalidare le dimensioni massime dei file quando nel filtro URL sono selezionate le opzioni Consenti o Controlla.

Passaggi Per Configurare Il Controllo Delle Richieste Di Caricamento Con Le Categorie URL Personalizzate

Ogni richiesta di caricamento viene assegnata a un gruppo di criteri "Analisi malware in uscita" ed eredita le impostazioni di controllo di tale gruppo.

Dopo aver ricevuto le intestazioni della richiesta di caricamento, il proxy Web dispone delle informazioni necessarie per decidere se è necessario eseguire la scansione del corpo della richiesta.

Il motore DVS analizza la richiesta e restituisce un verdetto al proxy Web. La pagina Blocca viene visualizzata all'utente finale, se applicabile.

| | | |
|--|--|---|
| Passaggio 1 | Scegliere Web Security Manager > Analisi malware in uscita. | |
| Passaggio 2 | Nella colonna Destinazioni fare clic sul collegamento del gruppo di criteri che si desidera configurare. | |
| Passaggio 3 | Nella sezione Modifica impostazioni di destinazione, selezionare "Definisci impostazioni personalizzate di scansione" dal menu a discesa. | |
| Passaggio 4 | Nella sezione Destinazioni da analizzare selezionare una delle opzioni seguenti: | |
| | Opzione | Descrizione |
| | Non analizzare alcun caricamento | Il motore DVS non esegue la scansione delle richieste di caricamento. Tutte le richieste di caricamento vengono valutate in base ai criteri di accesso |
| | Analizza tutti i caricamenti | Il motore DVS analizza tutte le richieste di caricamento. La richiesta di caricamento viene bloccata o valutata in base ai criteri di accesso, a seconda del verdetto di scansione del motore DVS |
| Analizza caricamenti in categorie URL personalizzate specificate | <p>Il motore DVS analizza le richieste di caricamento che appartengono a categorie URL personalizzate specifiche. La richiesta di caricamento viene bloccata o valutata in base ai criteri di accesso, a seconda del verdetto di scansione del motore DVS.</p> <p>Fare clic su Modifica elenco categorie personalizzate per selezionare le categorie URL da analizzare</p> | |

| | |
|-----------------|---|
| Passaggio 5 | Inviare le modifiche. |
| Passaggio 6 | Nella colonna Filtro antimalware fare clic sul collegamento per il gruppo di criteri. |
| Passaggio 7 | Nella sezione Impostazioni antimalware, selezionare Definisci impostazioni personalizzate antimalware. |
| Passaggio 8 | Nella sezione Impostazioni antimalware Cisco DVS selezionare i motori di analisi antimalware da abilitare per questo gruppo di criteri. |
| Passaggio 9 | Nella sezione Categorie di malware, scegliere se monitorare o bloccare le varie categorie di malware. Le categorie elencate in questa sezione dipendono dai motori di digitalizzazione attivati. |
| Passaggio 10 | Invia e conferma modifiche. |

Procedura per configurare le richieste di caricamento del controllo nei criteri di prevenzione della perdita dei dati esterni

Una volta che il proxy Web riceve le intestazioni della richiesta di caricamento, dispone delle informazioni necessarie per decidere se la richiesta può passare al sistema DLP esterno per la scansione.

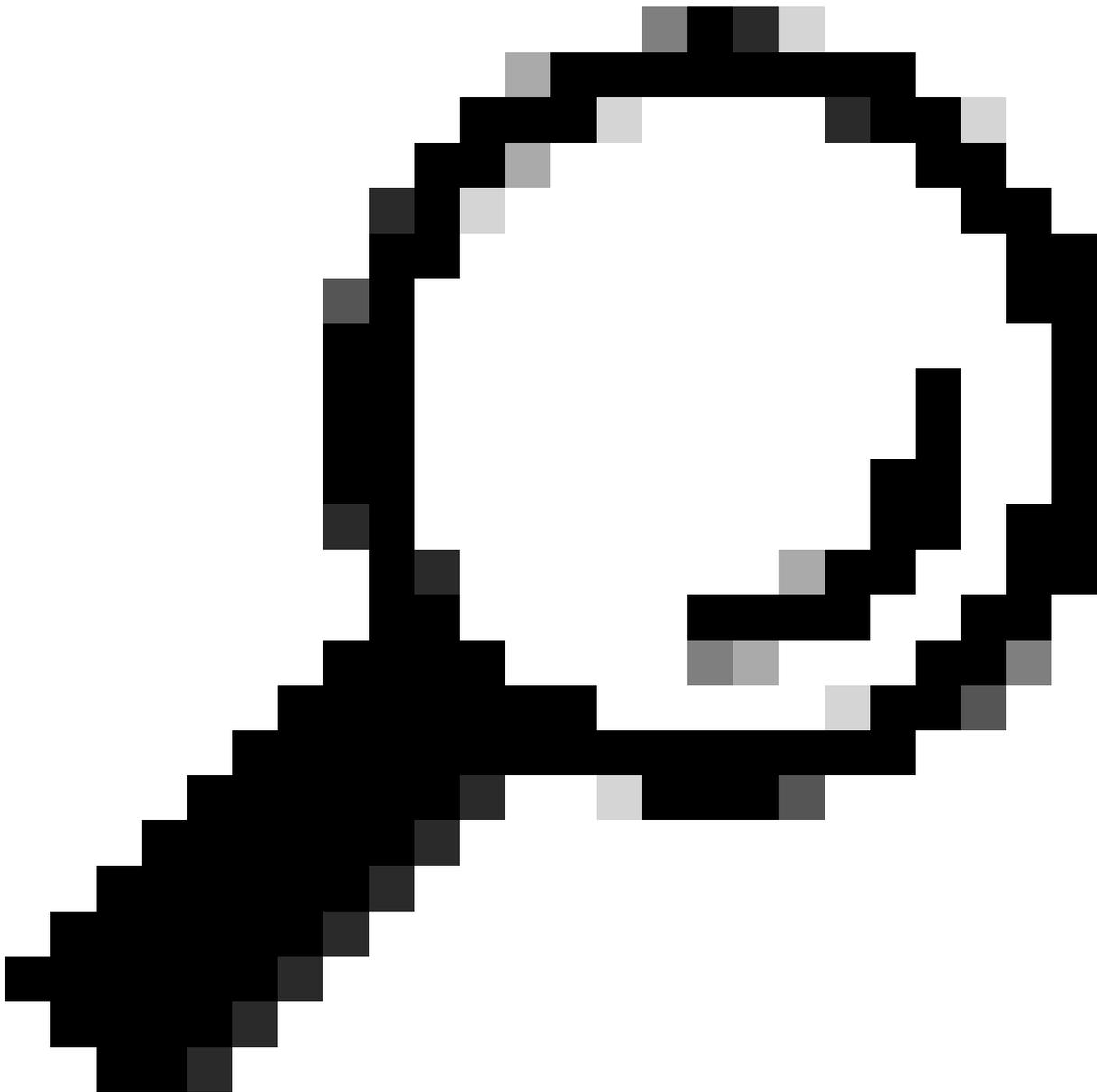
Il sistema DLP analizza la richiesta e restituisce un verdetto al Proxy Web, blocco o monitoraggio (valuta la richiesta rispetto ai Criteri di accesso).

| | |
|----------------|---|
| Passaggio 1 | Scegliere Web Security Manager > Prevenzione perdita dati esterni. |
| Passaggio 2 | Fare clic sul collegamento nella colonna Destinazioni per il gruppo di criteri che si desidera configurare. |
| Passaggio | Nella sezione Modifica impostazioni di destinazione, scegliere "Definisci impostazioni |

| | |
|----------------|--|
| 3 | personalizzate di scansione delle destinazioni." |
| Passaggio 4 | <p>Nella sezione Destinazione da analizzare scegliere una delle opzioni seguenti:</p> <ul style="list-style-type: none"> • Non analizzare i caricamenti. Nessuna richiesta di caricamento viene inviata ai sistemi DLP configurati per la scansione. Tutte le richieste di caricamento vengono valutate in base ai criteri di accesso. • Analizza tutti i caricamenti. Tutte le richieste di caricamento vengono inviate ai sistemi DLP configurati per la scansione. La richiesta di caricamento viene bloccata o valutata in base ai criteri di accesso, a seconda del verdetto della scansione del sistema DLP. • Analizza i caricamenti ad eccezione delle categorie URL personalizzate ed esterne specificate. Le richieste di caricamento che rientrano in categorie URL personalizzate specifiche sono escluse dai criteri di analisi DLP. Fare clic su Modifica elenco categorie personalizzate per selezionare le categorie URL da analizzare. |
| Passaggio 5 | Invia e conferma modifiche. |

URL di bypass e pass-through

È possibile configurare Secure Web Appliance in un'implementazione proxy trasparente per ignorare le richieste HTTP o HTTPS da determinati client o a determinate destinazioni.



Suggerimento: è possibile utilizzare la modalità passthrough per le applicazioni che richiedono traffico per l'accesso all'accessorio, senza necessità di modifiche o controlli dei certificati dei server di destinazione

 **Attenzione:** la funzionalità Mappa dominio funziona in modalità trasparente HTTPS. Questa funzionalità non funziona in modalità esplicita e per il traffico HTTP.

- Per consentire al traffico di utilizzare questa funzionalità, è necessario configurare la categoria personalizzata locale.
- Quando questa funzionalità è attivata, modifica o assegna il nome del server in base al nome del server configurato nella mappa dei domini, anche se sono disponibili informazioni SNI (Server Name Indication).

- Questa funzionalità non blocca il traffico in base al nome di dominio se il traffico corrisponde alla mappa del dominio e alla categoria personalizzata corrispondente, se sono configurati i criteri di decrittografia e l'azione passthrough.
- L'autenticazione non funziona con questa funzionalità pass-through. L'autenticazione richiede la decrittografia, ma in questo caso il traffico non viene decrittografato.
- il traffico non è monitorato. È necessario configurare il traffico UDP in modo che non entri in Web Security Appliance, ma direttamente attraverso il firewall verso Internet per applicazioni quali WhatsApp, Telegram e così via.
- WhatsApp, Telegram e Skype funzionano in modalità trasparente. Tuttavia, alcune app come WhatsApp non funzionano in modalità esplicita a causa delle restrizioni sull'app.

Verificare di disporre di un criterio di identificazione definito per i dispositivi che richiedono traffico pass-through a server specifici. In particolare, è necessario:

- Scegliere Esente da autenticazione/identificazione.
- Specificare gli indirizzi a cui deve essere applicato questo profilo di identificazione. È possibile utilizzare indirizzi IP, blocchi CIDR (Classless Inter-Domain Routing) e subnet.

| | |
|----------------|---|
| Passaggio 1 | Abilita il proxy HTTPS. |
| Passaggio 2 | <p>Scegliere Web Security Manager > Mappa dominio.</p> <ol style="list-style-type: none"> Scegliere Aggiungi dominio. Immettere il nome di dominio o il server di destinazione. Scegliere l'ordine di priorità se sono stati specificati alcuni domini. Immettere gli indirizzi IP. Fare clic su Invia. |
| Passaggio 3 | <p>Scegliere Web Security Manager > Categorie URL personalizzate ed esterne.</p> <ol style="list-style-type: none"> Scegliere Aggiungi categoria. Fornire queste informazioni. |

| Impostazioni | Descrizione |
|-------------------|--|
| Nome categoria | Immettere un identificatore per questa categoria di URL. Questo nome viene visualizzato quando si configura il filtro URL per i gruppi di criteri. |
| Ordine elenco | <p>Specificare l'ordine di questa categoria nell'elenco delle categorie URL personalizzate. Immettere "1" per la prima categoria di URL nell'elenco.</p> <p>Il motore di filtro URL valuta una richiesta client in base alle categorie URL personalizzate nell'ordine specificato.</p> |
| Tipo di categoria | Scegliere Categoria personalizzata locale. |
| Avanzate | <p>È possibile immettere espressioni regolari in questa sezione per specificare ulteriori set di indirizzi.</p> <p>È possibile utilizzare le espressioni regolari per specificare più indirizzi che corrispondono ai criteri immessi.</p> |

c. Inviare e confermare le modifiche.

Passaggio
4

Scegliere Web Security Manager > Criteri di decrittografia.

- a. Crea un nuovo criterio di decrittografia.
- b. Scegliere il profilo di identificazione creato per ignorare il traffico HTTPS per applicazioni specifiche.
- c. Nel pannello Avanzate, fare clic sul collegamento per Categorie URL.
- d. Nella colonna Add (Aggiungi), fare clic su per aggiungere la categoria di URL personalizzati creata nel passaggio 3.
- e. Selezionate Fatto (Done).
- f. Nella pagina Criteri di decrittografia, fare clic sul collegamento per il filtro URL.
- g. Selezionate Pass Through.
- h. Inviare e confermare le modifiche.

| | |
|--|---|
| | (Facoltativo) È possibile utilizzare l'identificatore di formato %(per visualizzare le informazioni del log degli accessi. |
|--|---|

Configura Bypass Proxy Web Per Richieste Web

Dopo aver aggiunto le categorie URL personalizzate all'elenco di esclusione del proxy, tutti gli indirizzi IP e i nomi di dominio delle categorie URL personalizzate vengono ignorati sia per l'origine che per la destinazione.

| | |
|-------------|---|
| Passaggio 1 | Scegliere Web Security Manager > Ignora impostazioni. |
| Passaggio 2 | Fare clic su Modifica impostazioni bypass. |
| Passaggio 3 | Immettere gli indirizzi per i quali si desidera ignorare il proxy Web.  Nota: quando si configura /0 come subnet mask per qualsiasi indirizzo IP presente nell'elenco di esclusione, l'accessorio ignora tutto il traffico Web. In questo caso, la configurazione viene interpretata come 0.0.0.0/0. |
| Passaggio 4 | Scegliere le categorie URL personalizzate da aggiungere all'elenco di esclusione proxy. |
| Passaggio 5 | Inviare e confermare le modifiche. |

 Attenzione: non è possibile impostare il bypass del proxy Web per le espressioni regolari.

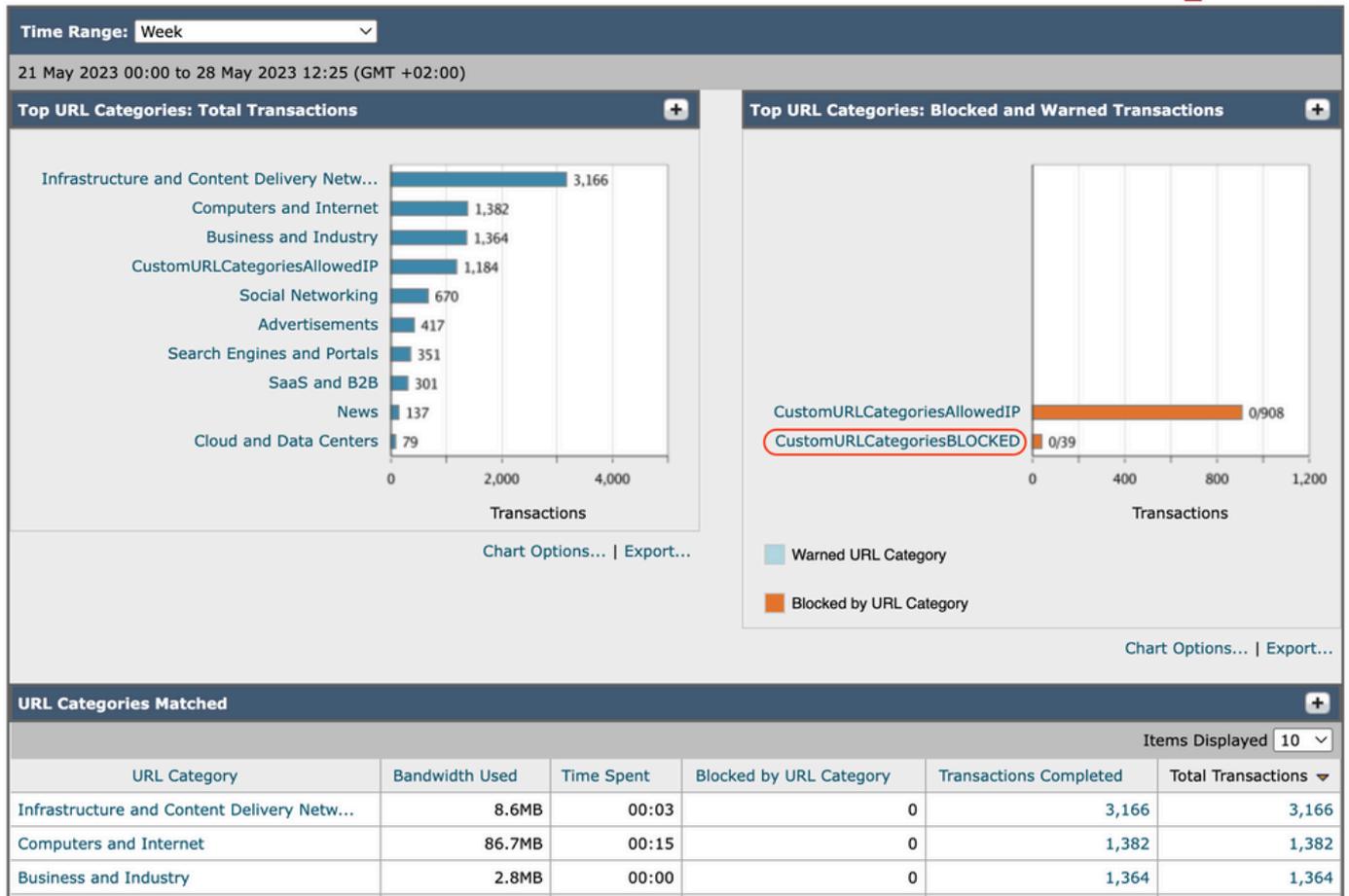
Report

Nella pagina "Reporting" >> Categorie URL viene fornita una visualizzazione collettiva delle statistiche URL che include informazioni sulle categorie URL principali corrispondenti e sulle categorie URL principali bloccate.

In questa pagina vengono visualizzati i dati specifici della categoria per i risparmi sulla larghezza di banda e le transazioni Web.

| Sezione | Descrizione |
|--|---|
| Intervallo di tempo (elenco a discesa) | Scegliere l'intervallo di tempo per il rapporto. |
| Principali categorie URL per transazioni totali | In questa sezione sono elencate in formato grafico le principali categorie URL visitate nel sito. |
| Principali categorie URL per transazioni bloccate e con avvisi | Elenca l'URL superiore che ha attivato un'azione di blocco o di avviso per ogni transazione in formato grafico. |
| Categorie URL corrispondenti | <p>Mostra la disposizione delle transazioni per categoria URL durante l'intervallo di tempo specificato, oltre alla larghezza di banda utilizzata e al tempo trascorso in ciascuna categoria.</p> <p>Se la percentuale di URL non classificati è superiore al 15-20%, prendere in considerazione le seguenti opzioni:</p> <ul style="list-style-type: none"> • Per URL localizzati specifici, è possibile creare categorie URL personalizzate e applicarle a utenti o criteri di gruppo specifici. • È possibile segnalare gli URL non classificati o classificati in modo errone e gli URL a Cisco per la valutazione e l'aggiornamento del database. • Verificare che il filtro reputazione Web e il filtro antimalware siano abilitati. |

URL-Categories



Report categoria URL immagine

È possibile fare clic sul nome di una categoria per visualizzare ulteriori dettagli relativi a tale categoria, ad esempio Domini corrispondenti o elenco utenti.

URL Categories > CustomURLCategoriesBLOCKED

Printable PDF 

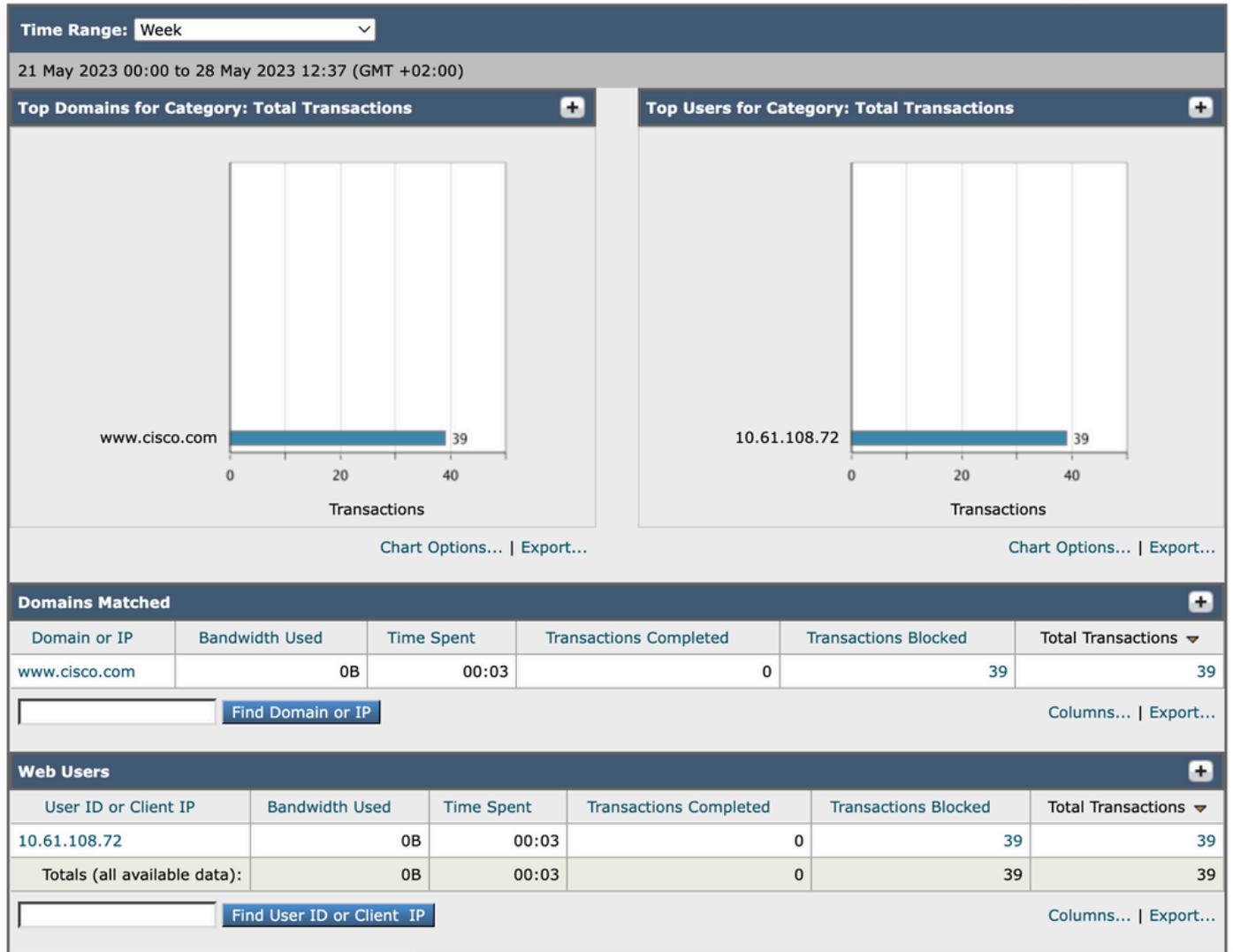


Immagine - Pagina report dettagliato

L'insieme di categorie URL predefinite può essere aggiornato periodicamente e automaticamente su Web Security Appliance.

Quando si verificano questi aggiornamenti, i vecchi nomi di categoria continuano a essere visualizzati nei report fino a quando i dati associati alle categorie precedenti non sono troppo vecchi per essere inclusi nei report.

I dati del report generati dopo l'aggiornamento di una serie di categorie URL utilizzano le nuove categorie, pertanto è possibile visualizzare nello stesso report sia le categorie precedenti che quelle nuove.

Nelle statistiche degli URL della pagina Categorie di URL dei report, è importante comprendere come interpretare questi dati:

| Tipo di dati | Descrizione |
|---------------------|---|
| Filtro URL ignorato | Rappresenta l'agente utente di criteri, porte e amministratori bloccato che si verifica prima del |

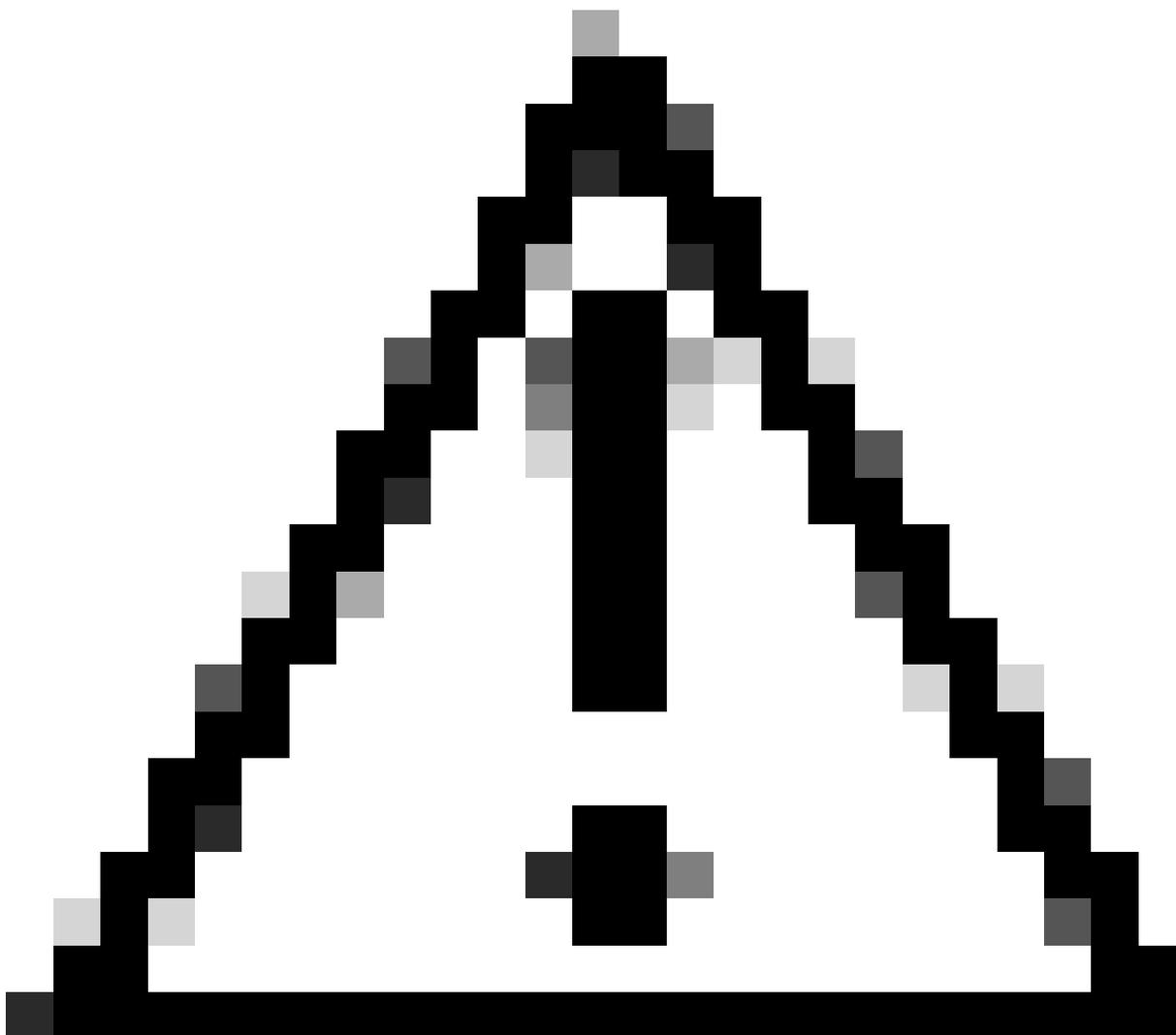
| | |
|----------------------|---|
| | filtro URL. |
| URL non classificato | Rappresenta tutte le transazioni per le quali viene eseguita una query sul motore di filtro URL, ma per le quali non viene trovata una corrispondenza per alcuna categoria. |

Visualizzazione Di Categorie Di URL Personalizzate Nel Log Degli Accessi

Secure Web Appliance utilizza i primi quattro caratteri dei nomi delle categorie di URL personalizzati preceduti da "c_" nei log degli accessi.

In questo esempio il nome della categoria è CustomURLCategoriesBLOCKED e nei log degli accessi è possibile visualizzare C_Cust:

```
1685269516.853 86 10.61.108.72 TCP_DENIED_SSL/403 0 GET https://www.cisco.com:443/ - NONE/- - DROP_CUST
```



Attenzione: considerare il nome della categoria dell'URL personalizzato se si utilizza Sawmill per analizzare i log degli accessi. Se i primi quattro caratteri della categoria dell'URL personalizzato includono uno spazio, Sawmill non è in grado di analizzare correttamente la voce del log degli accessi. Utilizzare invece solo i caratteri supportati nei primi quattro caratteri.

 Suggerimento: per includere il nome completo di una categoria URL personalizzata nei log degli accessi, aggiungere l'identificatore di formato %XF ai log degli accessi.

Quando un gruppo di criteri di accesso al Web ha una categoria URL personalizzata impostata su Monitoraggio e un altro componente, ad esempio i filtri della reputazione Web o il motore DVS (Different Verdicts Scanning), prende la decisione finale di consentire o bloccare una richiesta di URL nella categoria URL personalizzata, la voce del log degli accessi relativa alla richiesta mostra la categoria URL predefinita anziché la categoria URL personalizzata.

Per ulteriori informazioni su come configurare i campi personalizzati nei log di accesso, visitare:

Risoluzione dei problemi

Categoria non corrispondente

Dai log degli accessi è possibile visualizzare l'appartenenza della richiesta a quale categoria di URL personalizzato, se la selezione non è quella prevista:

- Se la richiesta è classificata in altre categorie di URL personalizzati, verificare la presenza di URL duplicati o di un'espressione regolare corrispondente in altre categorie oppure spostare la categoria di URL personalizzati all'inizio e provare nuovamente. È consigliabile esaminare attentamente la categoria di URL personalizzati compilata.

- Se la richiesta è classificata in categorie predefinite, verificare le condizioni nella categoria di URL personalizzati esistente, se tutte corrispondono, provare ad aggiungere l'indirizzo IP e verificare o accertarsi che sia stato digitato il testo e che sia stata utilizzata l'eventuale espressione regolare corretta.

Le Categorie Predefinite Non Sono Aggiornate

Se le categorie predefinite non sono aggiornate o nei log degli accessi viene visualizzato "err" nella sezione della categoria URL, verificare che TLSv1.2 sia abilitato per l'aggiornamento.

Per modificare la configurazione SSL dell'Updater, attenersi alla seguente procedura dalla GUI:

Passaggio 1. Da Amministrazione sistema, scegliere Configurazione SSL

System Administration

Policy Trace

Alerts

Log Subscriptions

Return Addresses

SSL Configuration

Users

Network Access

Immagine - configurazione SSL

Passaggio 2. Scegliere Modifica impostazioni.

Passaggio 3. Nella sezione Aggiorna servizio scegliere TLSv1.2

SSL Configuration

| SSL Configuration | |
|---|--|
| <p>Disabling SSLv3 for all services is recommended for best security. Depending on your network requirements, you may also choose to disable some versions of TLS for specific services.</p> <p>Note that the SSL/TLS service on remote servers may require that the selected TLS versions be sequential. So to avoid communications errors, always select a contiguous set of versions for each service. For example, do not enable TLS 1.0 and 1.2, while leaving TLS 1.1 disabled.</p> | |
| Appliance Management Web User Interface: | <p>Changing this option will disconnect all active Web User Interface connections on Commit. You will need to log in again.</p> <p>Enable protocol versions: <input checked="" type="checkbox"/> TLS v1.2 <input type="checkbox"/> TLS v1.1 <input type="checkbox"/> TLS v1.0</p> |
| Proxy Services: | <p>Proxy services include HTTPS Proxy and credential encryption for secure client.</p> <p>Enable protocol versions: <input checked="" type="checkbox"/> TLS v1.3 <input checked="" type="checkbox"/> TLS v1.2 <input type="checkbox"/> TLS v1.1 <input type="checkbox"/> TLS v1.0</p> <p><input checked="" type="checkbox"/> Disable TLS Compression (Recommended) TLS compression should be disabled for best security.</p> <p>Cipher(s) to Use: EECDH:DSS:RSA:NULL:NULL:NULL:EXPORT:3DES:SEED:CAMELLIA</p> |
| Secure LDAP Services: | <p>Secure LDAP services include Authentication, External Authentication, SaaS SSO, and Secure Mobility.</p> <p>Enable protocol versions: <input type="checkbox"/> TLS v1.2 <input checked="" type="checkbox"/> TLS v1.1 <input type="checkbox"/> TLS v1.0</p> |
| RADSEC Services: | <p>Enable protocol versions: <input checked="" type="checkbox"/> TLS v1.2 <input checked="" type="checkbox"/> TLS v1.1</p> |
| Secure ICAP Services (External DLP): | <p>Enable protocol versions: <input checked="" type="checkbox"/> TLS v1.2 <input checked="" type="checkbox"/> TLS v1.1 <input type="checkbox"/> TLS v1.0</p> |
| Update Service: | <p>Enable protocol versions: <input type="checkbox"/> TLS v1.2 <input checked="" type="checkbox"/> TLS v1.1 <input type="checkbox"/> TLS v1.0</p> |

Cancel Submit

Immagine - Aggiornamento servizio TLSv1.2

Passaggio 4. Invia e conferma modifiche

Per modificare la configurazione SSL dell'Updater, attenersi alla seguente procedura dalla CLI:

Passaggio 1. Dalla CLI, eseguire sslconfig

Passaggio 2. Digitare version e premere Invio

Passaggio 3. Scegli programma di aggiornamento

Passaggio 4. Scegliere TLSv1.2

Passaggio 5. Premere Invio per uscire dalla procedura guidata

Passaggio 6. eseguire il commit delle modifiche.

```
SWA_CLI> sslconfig
```

```
Disabling SSLv3 is recommended for best security.
```

Note that the SSL/TLS service on remote servers may require that the selected TLS versions be sequential 1.2, while leaving TLS 1.1 disabled.

Choose the operation you want to perform:

- VERSIONS - Enable or disable SSL/TLS versions
- COMPRESS - Enable or disable TLS compression for Proxy Service
- CIPHERS - Set ciphers for services in Secure Web Appliance
- FALLBACK - Enable or disable SSL/TLS fallback option
- ECDHE - Enable or disable ECDHE Authentication.

[> versions

SSL/TLS versions may be enabled or disabled for the following services:

- LDAPS - Secure LDAP Services (including Authentication, External Authentication, SaaS SSO, Secure Updater - Update Service
- WebUI - Appliance Management Web User Interface
- RADSEC - Secure RADSEC Services (including Authentication, External Authentication)
- SICAP - Secure ICAP Service
- Proxy - Proxy Services (including HTTPS Proxy, Credential Encryption for Secure Client)

Currently enabled SSL/TLS versions by service: (Y : Enabled, N : Disabled)

| | LDAPS | Updater | WebUI | RADSEC | SICAP | Proxy |
|---------|-------|---------|-------|--------|-------|-------|
| TLSv1.0 | N | N | N | N/A | N | N |
| TLSv1.1 | Y | Y | N | Y | Y | N |
| TLSv1.2 | N | N | Y | Y | Y | Y |
| TLSv1.3 | N/A | N/A | N/A | N/A | N/A | Y |

Select the service for which to enable/disable SSL/TLS versions:

1. LDAPS
2. Updater
3. Proxy
4. RADSEC
5. SICAP
6. WebUI
7. All Services

[> 2

Currently enabled protocol(s) for Updater are TLSv1.1.

To change the setting for a specific protocol, select an option below:

1. TLSv1.0
2. TLSv1.1
3. TLSv1.2

[> 3

TLSv1.2 support for Update Service is currently disabled. Do you want to enable it? [N]> Y

Currently enabled protocol(s) for Updater are TLSv1.1, TLSv1.2.

Riferimento

[Linee guida sulle best practice di Cisco Web Security Appliance - Cisco](#)

[BRKSEC-3303 \(Colive\)](#)

[Guida per l'utente di AsyncOS 14.5 for Cisco Secure Web Appliance - GD \(General Deployment\) - Connessione, installazione e configurazione \[Cisco Secure Web Appliance\] - 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).