

Configura richiesta intervallo per il traffico di Microsoft Update in SWA

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Richiesta intervallo](#)

[Richiesta intervallo nell'ambiente proxy](#)

[Abilitazione della richiesta di intervallo per gli aggiornamenti Microsoft](#)

[Passaggi per abilitare la richiesta di intervallo solo per gli aggiornamenti Microsoft](#)

[Passaggio 1. Abilitare la richiesta di intervallo](#)

[Passaggio 2. Creare una categoria URL personalizzata per gli URL di Microsoft Update](#)

[Passaggio 3. \(Facoltativo\) Creare un profilo di identificazione per escludere il traffico degli aggiornamenti Microsoft dall'autenticazione](#)

[Passaggio 4. \(Facoltativo\) Creare un criterio di decrittografia per il passaggio attraverso il traffico degli aggiornamenti Microsoft](#)

[Passaggio 5. Creare un criterio di accesso per consentire la richiesta di intervalli per il traffico di aggiornamenti Microsoft](#)

[Modifica dei log degli accessi](#)

[Verifica](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come consentire a Microsoft Updates Traffic di utilizzare Range Request in Secure Web Appliance (SWA).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Amministrazione della SWA.

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.

Richiesta intervallo

Una richiesta di intervallo è una funzionalità del protocollo HTTP che consente a un client, ad esempio un browser Web o un gestore di download, di richiedere solo una parte specifica di un file da un server, anziché scaricare l'intero file contemporaneamente. Ciò è particolarmente utile per riprendere download interrotti, eseguire lo streaming dei file multimediali o accedere in modo efficiente a file di grandi dimensioni. Il client specifica l'intervallo di byte desiderato nell'intestazione Range della richiesta HTTP e il server risponde con un codice di stato 206 Partial Content se supporta le richieste Range, consegnando solo il segmento richiesto del file.

Questo meccanismo migliora le prestazioni e l'esperienza dell'utente in diversi scenari. Ad esempio, nello streaming video, le richieste di intervallo consentono ai giocatori di recuperare solo i segmenti necessari per la riproduzione, riducendo l'utilizzo della larghezza di banda e migliorando i tempi di risposta. Analogamente, i gestori di download utilizzano le richieste di intervallo per suddividere un file in blocchi e scaricarli in parallelo, velocizzando il processo. Le richieste Range svolgono un ruolo chiave anche nella cache e nei sistemi proxy, consentendo aggiornamenti parziali e riducendo i trasferimenti di dati ridondanti.

Richiesta intervallo nell'ambiente proxy

In un ambiente proxy, le richieste dell'intervallo svolgono un ruolo cruciale nell'ottimizzazione dell'utilizzo della larghezza di banda e nel miglioramento dell'efficienza nella distribuzione dei contenuti. Quando le richieste di intervallo sono abilitate, il server proxy può recuperare solo i segmenti di byte richiesti dal server di origine e memorizzarli nella cache locale. Questo consente ai client di richiedere contenuti parziali, come segmenti specifici di un video o un file di grandi dimensioni, e di riceverli rapidamente dalla cache proxy, se disponibile. Consente inoltre di eseguire download paralleli e funzionalità di ripristino, che risultano particolarmente utili in ambienti con larghezza di banda limitata o alta latenza.

Tuttavia, quando le richieste di intervallo sono disabilitate, il proxy deve recuperare l'intero file dal server di origine anche se il client richiede solo una piccola parte. Questo comporta un trasferimento di dati non necessario, un aumento del carico sui server proxy e di origine e tempi di risposta più lenti per i client. Impedisce inoltre l'adozione di strategie efficienti di memorizzazione nella cache, poiché il proxy non è in grado di archiviare o gestire parte del contenuto. Negli scenari di streaming, ciò può causare ritardi nel buffer o degradazione dell'esperienza utente. La disattivazione delle richieste di intervallo può avvenire per motivi di sicurezza o di policy, ma spesso avviene a costo di prestazioni e flessibilità.

Si consideri ad esempio uno scenario in cui 10 utenti stanno tentando di scaricare 1 MB ciascuno da un file di 100 MB tramite un server proxy.

Richieste intervallo disabilitate:

Quando le richieste di intervallo sono disabilitate, il proxy non può recuperare solo il segmento da 1 MB di cui ogni utente ha bisogno. Deve invece scaricare l'intero file da 100 MB dal server di origine per ogni richiesta. Il risultato è:

Totale traffico dall'origine al proxy: $10 \times 100 \text{ MB} = 1000 \text{ MB}$ (1 GB)

Solo 10 MB di tali dati vengono effettivamente utilizzati dai client.

I restanti 990 MB vengono sprecati, determinando un utilizzo inefficiente della larghezza di banda e un aumento del carico sui server proxy e di origine.

Richieste intervallo abilitate:

Con le richieste di intervallo abilitate, il proxy recupera solo i 1 MB richiesti per utente:

Totale traffico dall'origine al proxy: $10 \times 1 \text{ MB} = 10 \text{ MB}$

Il proxy può memorizzare nella cache questi segmenti e servirli ad altri utenti, se necessario.

Ciò consente di ridurre di 90 volte il traffico, di accelerare i tempi di risposta e di ottimizzare l'utilizzo delle risorse.

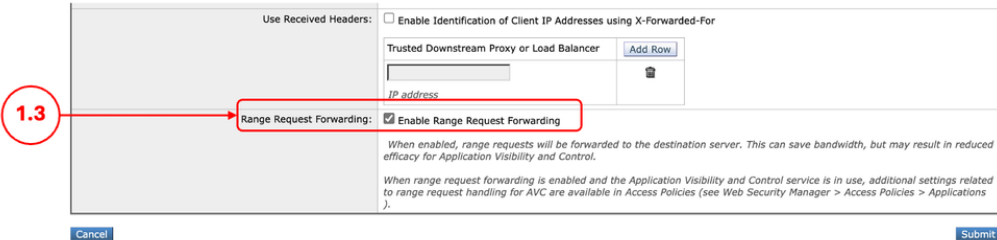
Abilitazione della richiesta di intervallo per gli aggiornamenti Microsoft

Sebbene le richieste di intervalli migliorino le prestazioni, ostacolano la scansione e l'applicazione delle policy di sicurezza negli ambienti SWA, poiché questi sistemi non possono ispezionare completamente i contenuti parziali. In questo articolo l'utilizzo delle richieste di intervallo è limitato esclusivamente al traffico di Microsoft Update.

 Attenzione: l'abilitazione dell'inoltro delle richieste di intervallo può interferire con l'efficienza AVC (Application Visibility and Control) basata su policy e compromettere la sicurezza.

Passaggi per abilitare la richiesta di intervallo solo per gli aggiornamenti Microsoft

Passaggio 1. Abilitare la richiesta	Passaggio 1.1. Dalla GUI, fare clic su Security Services e selezionare Web Proxy.
--	---

di intervallo	Passaggio 1.2. Fare clic su Modifica impostazioni. Passaggio 1.3. Selezionare la casella di controllo Abilita inoltra richiesta intervallo. Passaggio 1.4. Fare clic su Sottometti.  Immagine - Abilita inoltra richieste intervallo
Passaggio 2. Creare una categoria URL personalizzata per gli URL di Microsoft Update	Passaggio 2.1. Dalla GUI, selezionare Web Security Manager, quindi fare clic su Categorie URL personalizzate ed esterne. Passaggio 2.2. Fare clic su Aggiungi categoria per aggiungere una categoria URL personalizzata. Passaggio 2.3. Assegnare un CategoryName univoco. Passaggio 2.4. (Facoltativo) Aggiungere Una Descrizione. Passaggio 2.5. Da Ordine elenco, scegliere la prima categoria da posizionare in alto. Passaggio 2.6. Dall'elenco a discesa Category Typedrop, scegliere Local Custom Category (Categoria personalizzata locale). Passaggio 2.7. Aggiungere gli URL di Microsoft Update nella sezione Siti.  Suggerimento: È possibile controllare l'elenco degli aggiornamenti Microsoft dal seguente collegamento: Passaggio 2 - Configurazione di WSUS Microsoft Learn  Attenzione: Non copiare/incollare gli URL come nei documenti Microsoft; formattarli correttamente come formato SWA. Per ulteriori informazioni, visitare: Configure Custom URL Categories in Secure Web Appliance - Cisco Di seguito è riportato un esempio:

http://windowsupdate.microsoft.com ==> windowsupdate.microsoft.com
http://*.windowsupdate.microsoft.com ==> .windowsupdate.microsoft.com

Passaggio 2.8. Fare clic su Invia.

Custom and External URL Categories: Add Category

Edit Custom and External URL Category

2.3 Category Name:

Comments: ?

2.5 List Order:

2.6 Category Type:

2.7 Sites: ?

[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

Enter one regular expression per line. Maximum allowed characters 2048.

Immagine - Creazione di una categoria URL personalizzata

Passaggio 3.
(Facoltativo) Creare un profilo di identificazione per escludere il traffico degli aggiornamenti Microsoft dall'autenticazione

 Nota: Questa azione consente di ridurre il carico di autenticazione sull'SWA per il traffico verso gli aggiornamenti Microsoft.

Passaggio 3.1. Dalla GUI, Scegliere Web Security Manager e fare clic su Profili di identificazione.

Passaggio 3.2. Fare clic su Aggiungi profilo per aggiungere un profilo.

Passaggio 3.3. Assicurarsi che la casella di controllo Abilita profilo di identificazione sia selezionata.

Passaggio 3.4. Assegnare un profileName univoco.

Passaggio 3.5. (Facoltativo) Aggiungere Una Descrizione.

Passaggio 3.6. Dall'elenco a discesa Inserisci sopra, scegliere la posizione in cui visualizzare il profilo nella tabella.

Passaggio 3.7. Nella sezione Metodo di identificazione utente, scegliere Esenzione da autenticazione/identificazione.

Passaggio 3.8. Nella finestra Definisci membri per subnet, se si desidera che il traffico Microsoft venga inoltrato per alcuni utenti specifici, immettere gli indirizzi IP o le subnet applicabili oppure lasciare vuoto questo campo per includere tutti gli indirizzi IP.

Passaggio 3.9. Dalla sezione Avanzate, scegliere Categorie URL personalizzate.

Passaggio 3.10. Aggiungere la categoria URL personalizzato creata per gli aggiornamenti Microsoft.

Passaggio 3.11. Fare clic su Fine.

Passaggio 3.12. Fare clic su Sottometti.

Identification Profiles: Add Profile

Client / User Identification Profile Settings

☒ **Enable Identification Profile**

3.4 Name:
(e.g. my IT Profile)

Description:
(Maximum allowed characters 256)

3.6 Insert Above:

User Identification Method

3.7 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

3.9 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:

3.10 **Proxy Ports:**

URL Categories:

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 - Crea profilo di identificazione

Passaggio 4.
(Facoltativo) Creare un criterio di decrittografia per il passaggio attraverso il traffico degli aggiornamenti Microsoft

 Nota: In Microsoft Update viene utilizzato il protocollo HTTP e il traffico HTTPS viene utilizzato per il push dei collegamenti degli aggiornamenti. Questa azione consente di ridurre il carico di

Passaggio 4.1.Dalla GUI, selezionare Web Security Manager, quindi fare clic su Criterio di decrittografia.

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

Passaggio 4.3.Assegnare un PolicyName univoco.

Passaggio 4.4. (Facoltativo) Aggiungere Una Descrizione.

Passaggio 4.5.Dall'elenco a discesa Inserisci sopra criterio, scegliere il primo criterio.

Passaggio 4.6.Da Profili di identificazione e utenti, scegliere Seleziona uno o più profili di identificazione.

Passaggio 4.7. Selezionare il profilo di identificazione creato al passaggio 3 e andare al passaggio 4.11.

Passaggio 4.8. Se non è stato creato alcun profilo ID per gli aggiornamenti di Windows, dalla sezione Avanzate scegliere Categorie URL personalizzate.

Passaggio 4.9. Aggiungere la categoria URL personalizzato creata per gli aggiornamenti Microsoft nel Passaggio 2.

Passaggio 4.10. Fare clic su Fine.

Passaggio 4.11. Fare clic su Sottometti.

Decryption Policy: Add Group

Policy Settings

☒ **Enable Policy**

Policy Name: (e.g. my policy)

Description:

Insert Above Policy:

Policy Expires: ☐ Set Expiration for Policy

On Date:

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:

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

The following advanced membership criteria have been defined:

Proxy Ports: None Selected

Subnets: None Selected

Time Range: No Time Range Definitions Available (see Web Security Manager > Defined Time Ranges)

URL Categories: URL Categories Windows Update URLs in Identification Profile MS Update No Auth

User Agents: None Selected

Immagine - Crea criterio di decrittografia

Passaggio 4.12. Nella pagina Criteri di decrittografia, in Filtro URL, fare clic sul collegamento associato a questo nuovo criterio di decrittografia.

Passaggio 4.13. Select Pass Through come categoria di azioni per gli URL degli aggiornamenti Microsoft.

Decryption Policies

Policies

Order	Group	URL Filtering	Web Reputation	Default Action	Clone Policy	Delete
1	Bypass MS Update DP Identification Profile: MS Update No Auth All identified users	Monitor: 1	(global policy)	(global policy)		
	Global Policy Identification Profile: All	Monitor: 81 Decrypt: 4	Enabled	Decrypt		

Decryption Policies: URL Filtering: Bypass MS Update DP

Custom and External URL Category Filtering

These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.

Category	Category Type	Select all	Pass Through	Monitor	Decrypt	Drop	Quota-Based	Time-Based
Windows Update URLs	Custom (Local)	☒	☒	☐	☐	☐	☐	☐

Immagine - Impostazione del pass-through dell'azione per la categoria URL

Passaggio 4.12. Fare clic su Sottometti.

Passaggio 5.
Creare un criterio di
accesso per
consentire la
richiesta di intervalli
per il traffico di
aggiornamenti
Microsoft

Passaggio 5.1.Dalla GUI, fare clic su Web Security Manager e
selezionare Access Policy.

Passaggio 5.2. Fare clic su Aggiungi criterio per aggiungere un criterio di
accesso.

Passaggio 5.3.Assegnare un PolicyName univoco.

Passaggio 5.4. (Facoltativo) Aggiungere Una Descrizione.

Passaggio 5.5.Dall'elenco a discesa Inserisci sopra criterio, scegliere il
primo criterio.

Passaggio 5.6.Da Profili di identificazione e utenti, scegliere Seleziona
uno o più profili di identificazione.

Passaggio 5.7. Selezionare il profilo di identificazione creato al passaggio
3, quindi andare al passaggio 5.11.

Passaggio 5.8. Se non è stato creato alcun profilo ID per gli
aggiornamenti di Windows, dalla sezione Avanzate scegliere Categorie
URL personalizzate.

Passaggio 5.9. Aggiungere la categoria URL personalizzato creata per gli
aggiornamenti Microsoft nel Passaggio 2.

Passaggio 5.10. Fare clic su Fine.

Passaggio 5.11. Sottomettere.

Access Policy: AP Windows Update

Policy Settings

☒ Enable Policy

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

Description:
(Maximum allowed characters: 256)

Insert Above Policy:

Policy Expires: ☐ Set Expiration for Policy

On Date:

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:

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

The following advanced membership criteria have been defined:

Protocols: HTTP/HTTPS/FTP over HTTP in Identification Profile MS Update No Auth

Proxy Ports: None Selected

Subnets: None Selected

Time Range: No Time Range Definitions Available
(see Web Security Manager > Defined Time Ranges)

URL Categories: URL Categories Windows Update URLs in Identification Profile MS Update No Auth

User Agents: None Selected

Immagine - Creazione del criterio di accesso

Passaggio 5.12. Nella pagina Criteri di accesso, in Filtro URL, fare clic sul collegamento associato a questo nuovo criterio di accesso

Passaggio 5.13. Selezionare Consenti come azione per la categoria URL personalizzato creato per gli aggiornamenti Microsoft.

Passaggio 5.14. Fare clic su Submit (Invia).

Access Policies

Policies

Order	Group	Protocols and User Agents	URL Filtering	Applications	Objects	Anti-Malware and Reputation	HTTP ReWrite Profile	Clone Policy	Delete
1	AP Windows Update Identification Profile: MS Update No Auth All identified users	(global policy)	Monitor: 1	Block: 6 Monitor: 318	(global policy)	(global policy)	(global policy)		
	Global Policy Identification Profile: All	No blocked items	Monitor: 85	Block: 6 Monitor: 318	No blocked items	Web Reputation: Enabled Secure Endpoint: Enabled Anti-Malware Scanning: Enabled	None		

Access Policies: URL Filtering: AP Windows Update

Custom and External URL Category Filtering

These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.

Category	Category Type	Use Global Settings	Block	Redirect	Allow	Monitor	Warn	Quota-Based	Time-Based
Windows Update URLs	Custom (Local)	—	Select all	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)

Cancel Submit

Immagine - Impostazione dell'azione Consenti per la categoria URL

Passaggio 5.15. Nella pagina Criteri di accesso, in Applicazioni fare clic sul collegamento associato a questo nuovo criterio di accesso

Access Policies

Policies

Order	Group	Protocols and User Agents	URL Filtering	Applications	Objects	Anti-Malware and Reputation	HTTP ReWrite Profile	Clone Policy	Delete
1	AP Windows Update Identification Profile: MS Update No Auth All identified users	(global policy)	Allow: 1	Monitor: 324	(global policy)	(global policy)	(global policy)		
	Global Policy Identification Profile: All	No blocked items	Monitor: 85	Monitor: 324	No blocked items	Web Reputation: Enabled Secure Endpoint: Enabled Anti-Malware Scanning: Enabled	None		

Immagine - Modifica visibilità e controllo applicazione

Passo 5.16. In Modifica impostazioni applicazioni, sezione, selezionare Definisci impostazioni personalizzate applicazioni.

Passaggio 5.17. Dalla sezione Impostazioni applicazioni, fare clic su Modifica tutto per l'applicazione Giochi, quindi impostare l'azione su Blocca.

Passaggio 5.18. Fare clic su Apply (Applica).

Access Policies: Applications Visibility and Control: AP Windows Update

Edit Applications Settings

5.16 → Define Applications Custom Settings

Applications Settings

Browse Application Types

To identify some applications, inspection of HTTPS content may be required. For best efficacy, enable the HTTPS Proxy, then select the option that enables decryption for application visibility and control (see Security Services > HTTPS Proxy).

Applications	Settings
Blogging	22 Monitor Edit all...
Collaboration	8 Monitor Edit all...
Enterprise Applications	6 Monitor Edit all...
Facebook	Bandwidth Limit: No Bandwidth Limit 10 Monitor Edit all...
File Sharing	39 Monitor Edit all...
Games	Set action for 6 applications of type: Games ☐ Leave current settings ☐ Use Global Settings (6 Monitor) ☒ Block ☐ Monitor 5.17 → Block 5.18 → Apply Cancel Apply

Immagine - Impostare un'azione dell'applicazione su Blocca

Passaggio 5.19. Scorrere verso il basso fino alla sezione Impostazioni richiesta intervallo per criterio, accertarsi che Inoltra richieste intervallo sia selezionato,

Total: 324 Applications (6 Blocked, 318 Monitored)

Range Request Settings for Policy

5.19 → Range Request Bypass: Forward range requests

For optimum application detection, range requests should be ignored (not forwarded to the web server) when using AVC. However, this will result in higher bandwidth usage. Exceptions to this setting may be specified below.

Exception list: ?

Enter a newline delimited list of clients or destinations. Regular expressions are accepted.

Cancel Submit

Immagine - Impostazioni richiesta intervallo per criterio

Passaggio 5.20. Inviare.

Passaggio 5.21. Nella pagina Criteri di accesso, in Applicazioni fare clic sul collegamento associato al criterio globale.

Access Policies

Order	Group	Protocols and User Agents	URL Filtering	Applications	Objects	Anti-Malware and Reputation	HTTP ReWrite Profile	Clone Policy	Delete
1	AP Windows Update Identification Profile: MS Update No Auth All identified users	(global policy)	Allow: 1	Block: 6 Monitor: 318	(global policy)	(global policy)	(global policy)		
	Global Policy Identification Profile: All	No blocked items	Monitor: 85	Monitor: 324	No blocked items	Web Reputation: Enabled Secure Endpoint: Enabled Anti-Malware Scanning: Enabled	None		

5.21 → Monitor: 324

Immagine - Impostazioni predefinite applicazione criteri di accesso

	Passaggio 5.2. Scorrere verso il basso fino alla sezione Impostazioni richiesta intervallo per criterio, accertarsi che Non inoltrare richieste intervallo sia selezionato, Passaggio 5.23. Esecuzione del commit delle modifiche.
--	--

Modifica dei log degli accessi

Per ottenere una maggiore visibilità sulle richieste Range dai log degli accessi, è possibile aggiungere i campi personalizzati seguenti:

[Intervallo client = %<Intervallo:]	Mostra l'intervallo richiesto dal client (byte)
[content= %>Content-Length:]	Mostra le dimensioni del contenuto scaricato (byte)

Per ulteriori informazioni sull'aggiunta di un campo personalizzato ai log degli accessi SWA, visitare il collegamento [Configura parametro prestazioni nei log degli accessi](#)

Verifica

Utilizzare questo comando CURL per inviare una richiesta Range all'SWA:

```
curl -vvvk -H "Pragma: no-cache" -x 10.48.48.181:3128 -H 'Range: bytes=0-100' 'http://catalog.sf.dl.delivery.mp.microsoft.com/filestreamingservice/files/f263aa64-f367-42f0-9cad-1b1a1e1f1e1f'
```

Dall'output del comando CURL, è possibile vedere che la risposta HTTP è HTTP/1.1 206:

```
> GET http://catalog.sf.dl.delivery.mp.microsoft.com/filestreamingservice/files/f263aa64-f367-42f0-9cad-1b1a1e1f1e1f
> Host: catalog.sf.dl.delivery.mp.microsoft.com
> User-Agent: curl/8.7.1
> Accept: */*
> Proxy-Connection: Keep-Alive
> Pragma: no-cache
> Range: bytes=0-100
>
* Request completely sent off
< HTTP/1.1 206 Partial Content
```

Dai log degli accessi è possibile vedere che l'azione è TCP_CLIENT_REFRESH_MISS/206:

Informazioni correlate

- [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](#)
- [Configura parametro prestazioni nei log degli accessi](#)
- [Uso delle best practice di Secure Web Appliance - Cisco](#)
- [Bypass Authentication in 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).