

Configurazione dell'ottimizzazione del traffico Youtube con Akamai Connect

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Akamai Connect e WAAS](#)

[Configurazione](#)

[Passaggio 1. È necessario un certificato SSL firmato dalla CA pubblica/interna.](#)

[Passaggio 2. È necessario considerare attendibile l'intermediario e/o l'autorità di certificazione \(CA\) principale dell'organizzazione.](#)

[Passaggio 3. Creare un servizio accelerato SSL sul dispositivo WAAS utilizzando l'interfaccia utente di WAAS Central Manager.](#)

[Passaggio 4. Configurare il servizio accelerato SSL.](#)

[Passaggio 5. Caricare il certificato e la chiave privata.](#)

[Passaggio 6. Verificare le informazioni del certificato caricate.](#)

[Passaggio 7. Fare clic sul pulsante SUBMIT \(INVIA\) per visualizzare il risultato finale.](#)

[Passaggio 8. Abilitare Akamai Connect.](#)

[Passaggio 9. Abilitare SSL Interposer nel branch WAAS \(obbligatorio solo per l'installazione lato singolo\).](#)

[Verifica](#)

[Passaggio 1. È necessario che Akamai Connect sia abilitato sul branch WAAS.](#)

[Passaggio 2. Verificare l'accelerazione di YouTube sul client.](#)

[Passaggio 3. Verificare in WAAS.](#)

[Risoluzione dei problemi](#)

[Problema: Il traffico non è accelerato da SSL AO.](#)

[Problema: Impossibile connettersi a YouTube. Nessun certificato sottoposto a push.](#)

[Problema: Il traffico raggiunge Akamai Connect Engine ma non è presente alcun accesso alla cache.](#)

[Problema: La cache Akamai interrompe la connessione HTTPS quando si passa attraverso un proxy con autenticazione.](#)

Introduzione

In questo documento viene descritto come configurare YouTube Acceleration su Cisco Wide Area Application Services (WAAS) con la funzione Akamai Connect.

Nota: In questo articolo, il termine dispositivo WAAS viene utilizzato per riferirsi collettivamente ai WAAS Central Manager e ai WAEs della rete. Il termine WAE (Wide Area Application Engineer) si riferisce agli accessori WAE e WAVE, ai moduli SM-SRE che

eseguono istanze WAAS e vWAAS.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco WAAS
- Infrastruttura a chiave pubblica
- Certificato SSL (Secure Sockets Layer)

Componenti usati

Le informazioni di questo documento si basano sulle seguenti versioni software:

- Cisco WAAS versione 5.5.1
- Cisco WAAS versione 6.2.1

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.

Premesse

Akamai Connect e WAAS

La funzione Akamai Connect è un componente della cache degli oggetti HTTP/S aggiunto a Cisco WAAS. È integrato nello stack di software WAAS esistente e viene utilizzato tramite HTTP Application Optimizer. Akamai Connect consente di ridurre la latenza per il traffico HTTP/S per le applicazioni aziendali e Web e può migliorare le prestazioni di molte applicazioni, tra cui POS (Point of Sale), video HD, digital signage ed elaborazione degli ordini nel punto vendita. Fornisce un offload significativo e misurabile dei dati WAN ed è compatibile con le funzioni WAAS esistenti quali DRE (deduplicazione), LZ (compressione), TFO (Transport Flow Optimization) e l'accelerazione SSL (protetta/crittografata) per il primo e il secondo passaggio.

Questi termini vengono utilizzati con Akamai Connect e WAAS:

- Akamai Connect - Akamai Connect è un componente della cache degli oggetti HTTP/S aggiunto a Cisco WAAS, integrato nello stack software WAAS esistente e sfruttato tramite HTTP Application Optimizer. WAAS con Akamai Connect consente di ridurre la latenza per il traffico HTTP/S per le applicazioni aziendali e Web.
- Cache connessa Akamai - La cache connessa Akamai è un componente di Akamai Connect, che consente al motore di cache (CE) di memorizzare nella cache il contenuto fornito da un

server perimetrale sulla piattaforma intelligente Akamai.

Configurazione

Passaggio 1. È necessario un certificato SSL firmato dalla CA pubblica/interna.

Il certificato deve includere il seguente SubjectAltName:

*.youtube.com

*.googlevideo.com

*.ytimg.com

*.ggpht.com

youtube.com

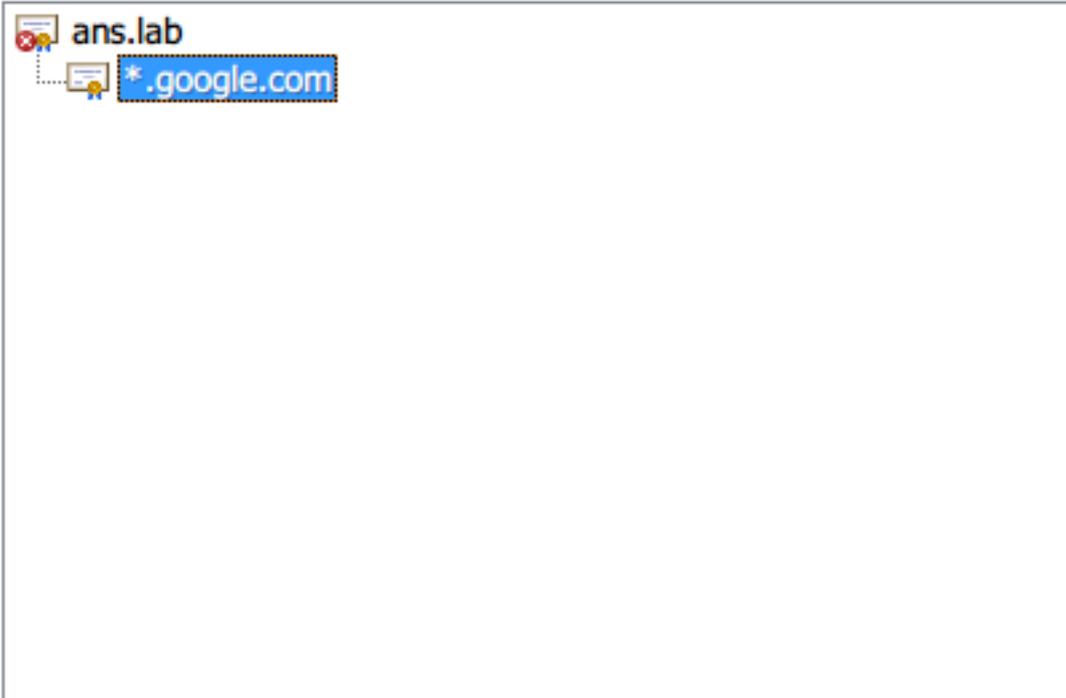
Questo è un esempio di certificato:

Certificate



General Details Certification Path

Certification path



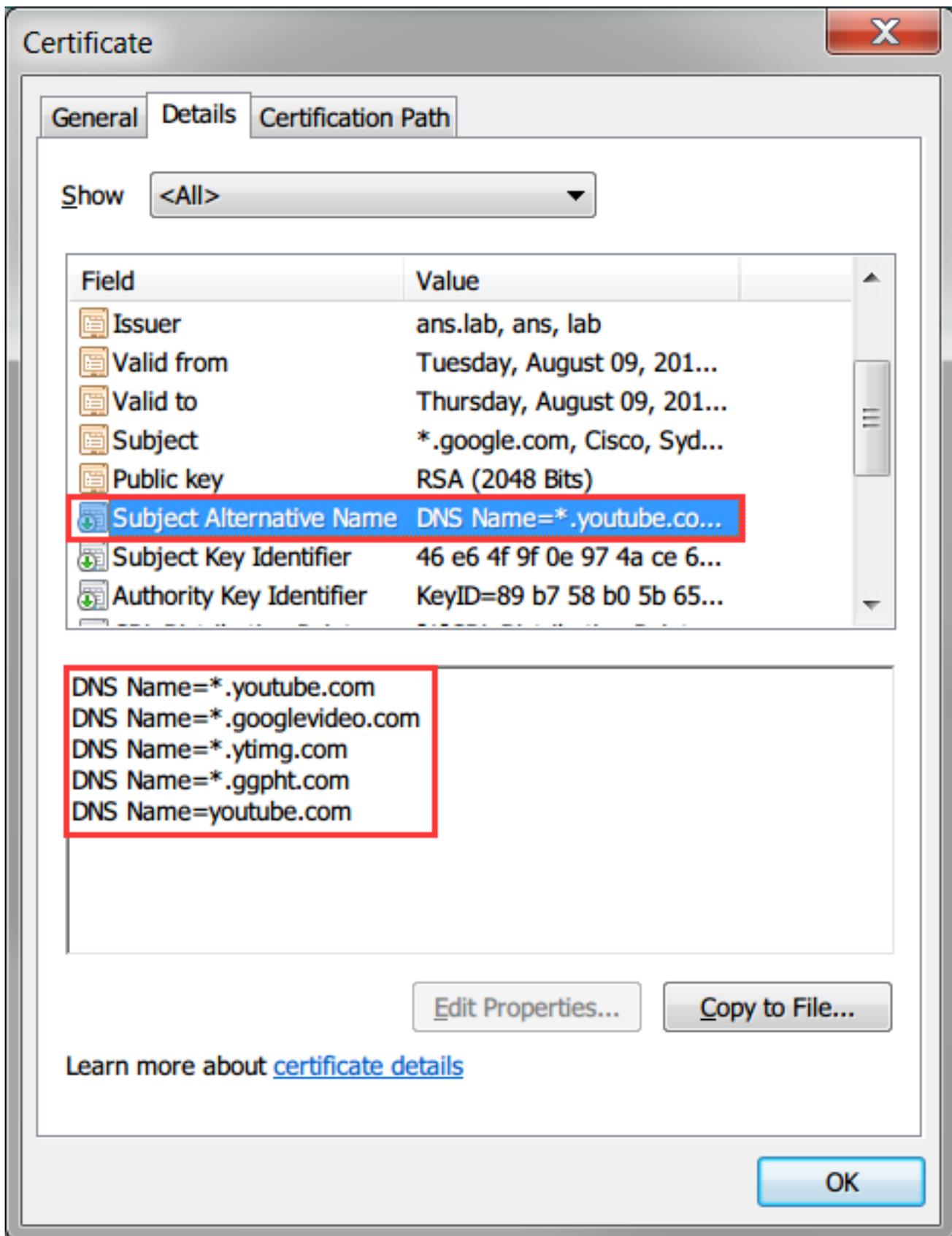
View Certificate

Certificate status:

This certificate is OK.

Learn more about [certification paths](#)

OK



Passaggio 2. È necessario considerare attendibile l'intermediario e/o l'autorità di certificazione (CA) principale dell'organizzazione.

A tale scopo, è possibile utilizzare Criteri di gruppo nel dominio Active Directory.

Se si sta testando l'installazione in un laboratorio, è possibile installare la CA intermedia e/o la CA radice nel dispositivo client come CA attendibile.

Certificate



General Details Certification Path



Certificate Information

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: ans.lab

Issued by: ans.lab

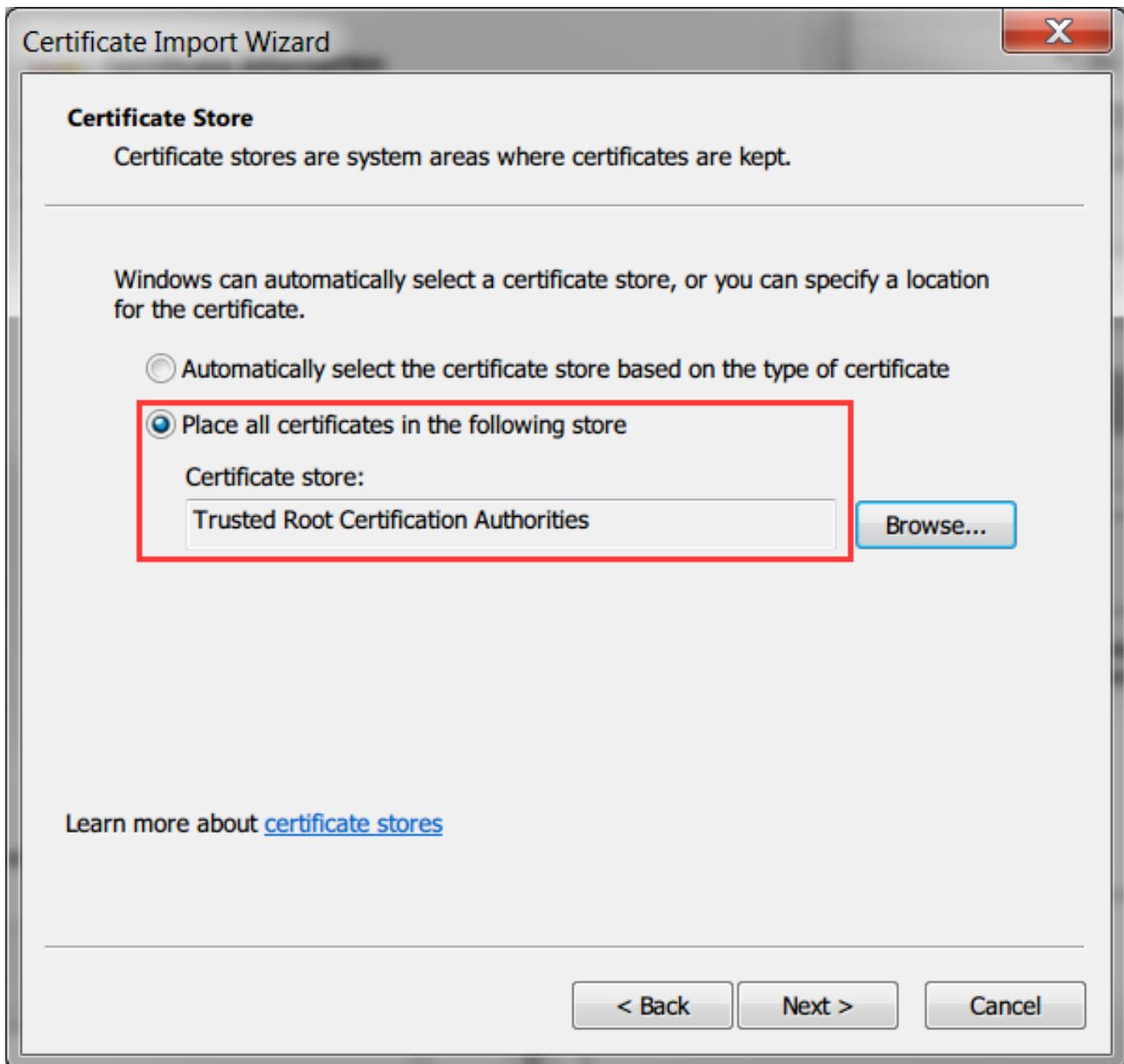
Valid from 8/ 8/ 2016 **to** 8/ 8/ 2021

Install Certificate...

Issuer Statement

Learn more about [certificates](#)

OK



Passaggio 3. Creare un servizio accelerato SSL sul dispositivo WAAS utilizzando l'interfaccia utente di WAAS Central Manager.

Su Akamai a due lati (precedente a WAAS 6.2.3) configurare il servizio accelerato SSL sul server WAAS di base. Per Akamai a lato singolo (WAAS 6.2.3 o versioni successive), configurare il server con accelerazione SSL sul server WAAS del ramo e abilitare l'interposer SSL. Questa è l'unica differenza tra la configurazione a doppio lato e la configurazione a lato singolo.

Nota: WAAS che esegue una versione del software precedente alla 6.2.3 richiede un'installazione Akamai a due lati per accelerare il traffico su Youtube. Il core WAAS proxy la connessione SSL verso Youtube. Il software WAAS versione 6.2.3 o successive supporta SSL AO v2 (SAKE). In questo modo, la filiale WAAS può fungere da proxy per la connessione SSL quando invia il traffico direttamente a Internet senza essere diretta attraverso l'infrastruttura del centro dati.

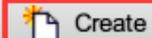
Selezionare **Dispositivi > Configura > Accelerazione > SSL Accelerated Service**, come mostrato

nell'immagine:

The screenshot shows the configuration interface for a device. At the top, there are tabs for 'Devices', 'AppNav Clusters', and 'Locations'. Below these are sub-tabs for 'Configure', 'Monitor', and 'Admin'. The main content area is divided into three columns of settings:

- AppNav Cluster**
 - AppNav Cluster
- Interception**
 - Interception Configuration
 - Interception Access List
- Acceleration**
 - Enabled Features
 - Accelerator Threshold
 - TCP Settings
 - TCP Adaptive Buffering Settings
 - DRE Settings
 - HTTP/HTTPS Settings
 - SMB Settings
 - SMB Preposition Settings
 - MAPI Settings
 - ICA Settings
 - Optimization Class-Map
 - Optimization Policies
 - SSL Accelerated Services** (highlighted with a red box)
- File Services**
 - SMB Dynamic Shares
- Caching**
 - Akamai Connect
 - Device Profile
- Storage**
 - Disk Encryption
- Security**
 - Secure Store
 - Windows Domain
 - SSL
 - Peering Service
 - Management Service
 - AAA
- Peers**
 - Peer Settings
- Network**
 - Network Interfaces
 - Default Gateway
 - Management Interface Settings
 - Jumbo MTU
 - Port Channel
 - TCP/IP Settings
 - CDP
 - DNS
 - Network Services
 - Console Access
- Monitoring**
 - Alarm Overload Detection
 - Flow Monitor
 - SNMP
 - Log Settings
- Date/Time**
 - NTP
 - Time Zone

Devices > DC-WAVE-7571 > Configure > Acceleration > **SSL Accelerated Services**

SSL Accelerated Services for WAE, DC-WAVE-7571  Create  Refresh  Print

Current applied settings from WAE, *DC-WAVE-7571*

SSL Accelerated Services

Passaggio 4. Configurare il servizio accelerato SSL.

Se si utilizza un proxy esplicito, è necessario attivare Concatenamento protocollo. È necessario applicare l'operatore ADO HTTP alla porta TCP utilizzata per l'inoltro del traffico (ad esempio, 80 o 8080).

È necessario controllare l'**indicazione del nome del server corrispondente**. In questa configurazione, quando il server WAAS principale riceve traffico SSL, confronta il campo SNI in Client Hello con SubjectAltName nel certificato caricato. Se il campo SNI corrisponde a SubjectAltName, il server WAAS principale invia questo traffico SSL.

Basic Advanced

This service is bound to 'SSL' application policy. The optimization actions accelerating traffic matching this service are DRE, LZ and TFO.

Service Name: * Youtube-OTT

In service:

Client version rollback check:

Enable protocol chaining:

Match Server Name Indication: If enabled, the SSL setup message is parsed for destination hostname (in "Server Name Indication"), which is matched against SANs in the SSL certificate. Recommended for optimizing SaaS apps which typically have dynamic server domains.

Description:

Server addresses

Please specify the IP Address, Hostname or Domain of an accelerated server. Use 'Any' keyword to match any server IP Address. Note that hostname and domain server address types are only supported on devices using WAAS versions 4.2.X or later.

It is recommended to have maximum 32 server entries and up to 64 characters per entry. The combined length of all the server address:port entries should not exceed 2048 characters.

Server: IPAddress Server Port:

Type	Address	Port
<input type="checkbox"/>		

Quando il campo **Corrispondenza nome server** è selezionato, utilizzare **Any** per IP Address e **443** per Server Port. Fare clic su **Add** per aggiungere questa voce.

▾ TLSv1 Record Layer: Handshake Protocol: **Client Hello**

Content Type: Handshake (22)

Version: TLS 1.0 (0x0301)

Length: 198

▾ Handshake Protocol: Client Hello

Handshake Type: Client Hello (1)

Length: 194

Version: TLS 1.2 (0x0303)

▷ Random

Session ID Length: 0

Cipher Suites Length: 28

▷ Cipher Suites (14 suites)

Compression Methods Length: 1

▷ Compression Methods (1 method)

Extensions Length: 125

▷ Extension: renegotiation_info

▾ Extension: server_name

Type: server_name (0x0000)

Length: 20

▾ Server Name Indication extension

Server Name list length: 18

Server Name Type: host_name (0)

Server Name length: 15

Server Name: **www.youtube.com**

SNI (Server Name Indication)

Passaggio 5. Caricare il certificato e la chiave privata.

È necessario specificare un certificato e una chiave privata. L'esempio riportato nell'immagine utilizza il formato PEM:

[Generate self-signed certificate and private key](#)

[Import existing certificate and optionally private key](#)

i It is recommended to use certificates of 1024 bit key size and avoid using certificate chains if you plan to configure more than 128 accelerated services(up to 512).

Mark private key as exportable

Upload file in PKCS#12 format

Upload file in PEM format

Paste certificate and key in PEM-format

Passphrase to decrypt private key:

Upload key: Google.com.key

Upload certificate: Google.com.cer

[Export certificate and key](#)

[Generate certificate signing request](#)

Optional Client Certificate and private key

[Import existing client certificate and optionally private key](#)

Passaggio 6. Verificare le informazioni del certificato caricate.

Certificate Info Certificate in PEM encoded form

Issued To	Issued By
Common Name: *.google.com	Common Name: ans.lab
Email:	Email:
Organization:	Organization:
Organization Unit: Cisco	Organization Unit:
Locality: Sydney	Locality:
State: NSW	State:
Country: AU	Country:
Serial Number: 199666714554801961566220	

Validity

Issued On: Mon Aug 08 14:58:06 GMT 2016

Expires On: Wed Aug 08 15:08:06 GMT 2018

Fingerprint

SHA1: 0A:A3:69:A2:5D:91:5F:66:1E:F2:59:76:A0:A8:DB:21:E3:AE:68:84

Base64: CqNpol2RX2Ye8ll2oKjbIeOuaIQ=

Key

Type: SHA1WITHRSA

Size (Bits): 2048

Passaggio 7. Fare clic sul pulsante SUBMIT (INVIA) per visualizzare il risultato finale.

SSL Accelerated Services for WAE, DC-WAVE-7571							Create	Refresh	Print
Current applied settings from WAE, DC-WAVE-7571				- Go to the SSL Global Settings page to modify selection.					
SSL Accelerated Services			Items 1-1 of 1		Rows per page: 25	Go			
<input type="checkbox"/>	Name ▲	Service Address/Port	Issued To	Issuer	Expiry Date	Service Status			
<input type="checkbox"/>	 Youtube-OTT	Any:443		ans.lab	Aug 08 2018	Enabled			

Passaggio 8. Abilitare Akamai Connect.

Selezionare Dispositivi > Configura > Memorizzazione nella cache > Akamai Connect.

Cache Settings
Cache Prepositioning

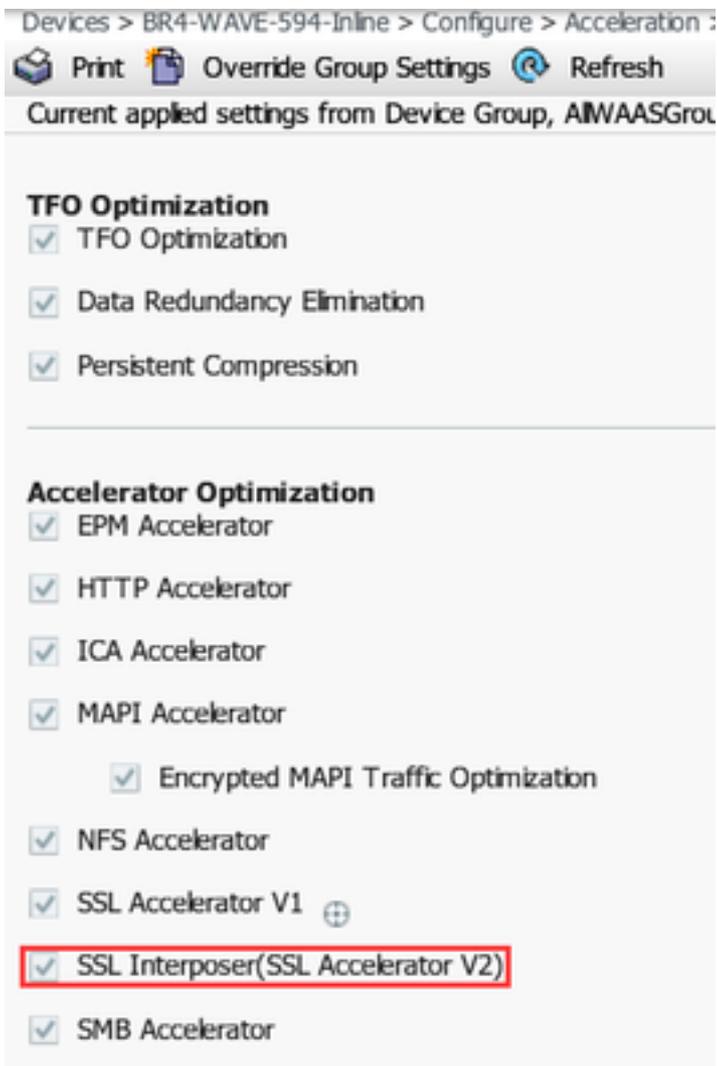
Enable Akamai Connect

▼ **Edit Settings**

Akamai Connected Cache

Over the top Cache

Passaggio 9. Abilitare SSL Interposer nel branch WAAS (obbligatorio solo per l'installazione lato singolo).



Verifica

Passaggio 1. È necessario che Akamai Connect sia abilitato sul branch WAAS.

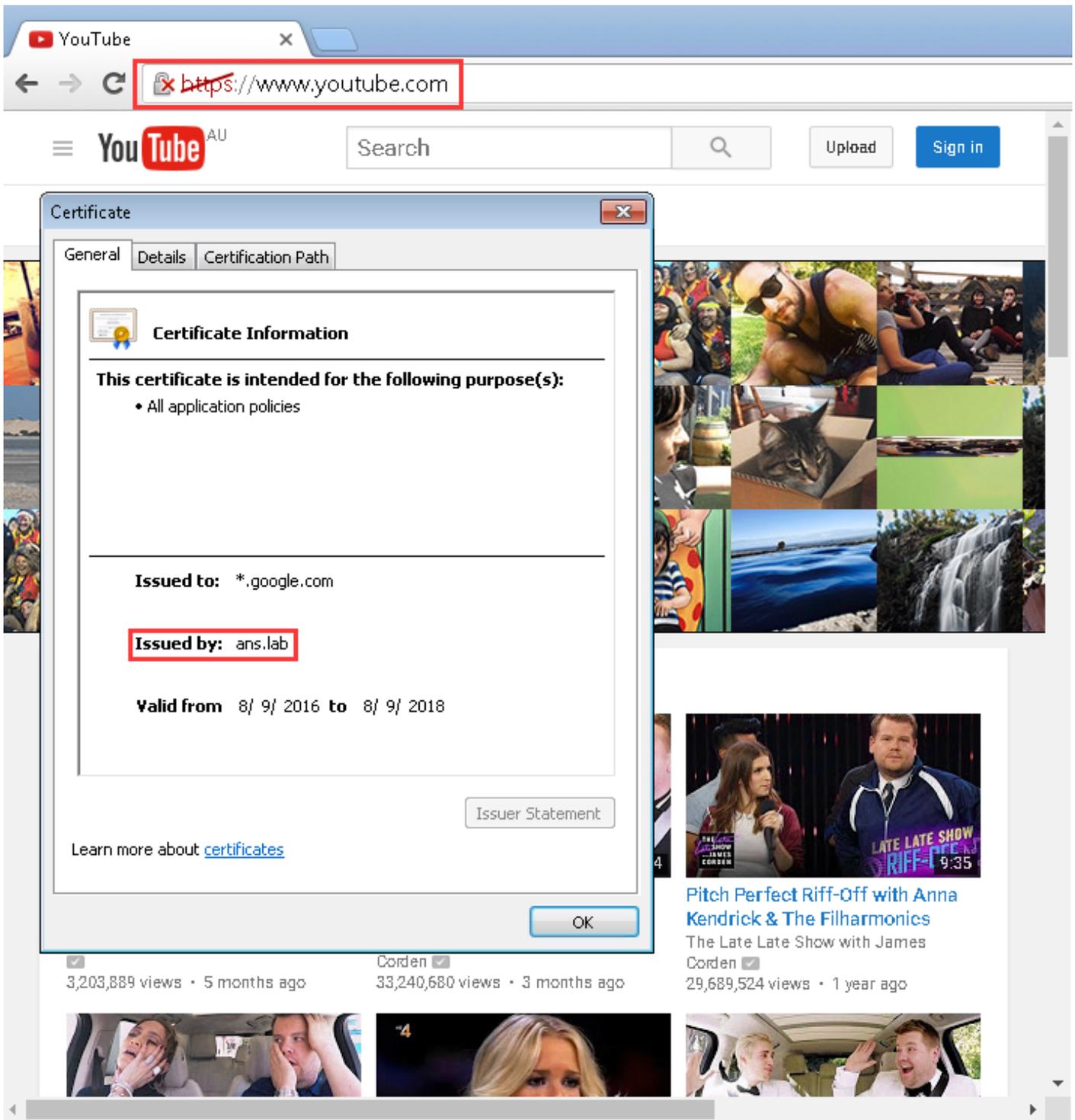
WAAS-BRANCH# show accelerator http object-cache

```
HTTP Object-cache
.....
Status
-----
                Operational State
                -----
                Running
                Akamai Connected Cache State
                -----
                Connected
```

Verificare che lo stato operativo sia in esecuzione e che lo stato di connessione sia **Connesso**.

Passaggio 2. Verificare l'accelerazione di YouTube sul client.

Quando si accede a YouTube, è necessario che il certificato sia firmato dalla propria CA:



Passaggio 3. Verifica tramite WAAS.

Verificare che SSL AO sia applicato correttamente al traffico:

Output di esempio dalla CLI quando si esegue il software WAAS prima della versione 6.2.3 (SSL AO v1 e Dual Site Setup)

WAAS-BRANCH# mostra connessione statistiche

ConnID	Source IP:Port	Dest IP:Port	PeerID	Accel	RR
6859	10.66.86.90:13110	10.66.85.121:80	00:06:f6:e6:58:56	THSDL	51.9%
6839	10.66.86.90:13105	10.66.85.121:80	00:06:f6:e6:58:56	THSDL	16.6%
6834	10.66.86.90:13102	10.66.85.121:80	00:06:f6:e6:58:56	THSDL	93.5%

```
6733 10.66.86.90:13022 10.66.85.121:80 00:06:f6:e6:58:56 THSDL 72.7%
6727 10.66.86.90:13016 10.66.85.121:80 00:06:f6:e6:58:56 THSDL 03.9%
```

Output di esempio dalla CLI quando si esegue il software WAAS 6.2.3 o versioni successive (SSL AO v2 e Single Site Setup)

WAAS-BRANCH# mostra connessione statistiche

ConnID	Source IP:Port	Dest IP:Port	PeerID	Accel	RR
3771	10.66.86.66:60730	58.162.61.183:443	N/A	THs	50.9%
3770	10.66.86.66:60729	58.162.61.183:443	N/A	THs	52.1%
3769	10.66.86.66:60728	58.162.61.183:443	N/A	THs	03.0%
3752	10.66.86.66:60720	208.117.242.80:443	N/A	THs	54.8%
3731	10.66.86.66:60705	203.37.15.29:443	N/A	THs	13.8%
3713	10.66.86.66:60689	58.162.61.142:443	N/A	THs	40.4%
3692	10.66.86.66:60669	144.131.80.15:443	N/A	THs	10.4%

Controllare il registro degli errori di accesso alla porta sul server WAAS del branch. Alle voci di log per il traffico ottimizzato è associato un codice di 10000 (indicare classificato come OTT-Youtube) e h - - - 200 indica che la cache degli oggetti viene trovata e il traffico viene gestito localmente. La maggiore accelerazione è prevista su googlevideo. È possibile aprire più browser sul computer di prova e riprodurre lo stesso video contemporaneamente per verificare l'impostazione:

Output di esempio di ce-errorlog:

```
08/09/2016 01:49:26.612 (fl=5948) 10000 0.002 0.033 1356 - - 148814 10.66.86.90 10.66.85.121
2905 h - - - 200 GET
https://r5---sn-uxanug5-
ntqk.googlevideo.com/videoplayback?dur=703.721&ei=ozapV8jrGdWc4AKytYaYBQ&fexp=3300116%2C3
300131%2C3300161%2C3312739%2C3313265%2C9422596%2C9428398%2C9431012%2C9433096%2C9433223%2C9433946
%2C9435526%2C9437
066%2C9437552%2C9438327%2C9438662%2C9438804%2C9439580%2C9442424%2C9442920&requiresssl=yes&initcwn
dbps=6383750&gir=
yes&sparams=clen%2Cdur%2Cei%2Cgir%2Cid%2Cinitcwndbps%2Cip%2Cipbits%2Citag%2Ckeepalive%2Clmt%2Cmi
me%2Cmm%2Cmn%2Cms
%2Cmv%2Cpl%2Crequiresssl%2Csource%2Cupn%2Cexpire&signature=34635AFA02C12695F90E50E067E6BD4B7E5821
32.DEB68217D77D25
F02925B272C6B3F032D3764535&ipbits=0&ms=au&mt=1470706873&pl=22&mv=m&mm=31&mn=sn-uxanug5-
ntqk&keepalive=yes&key=yt6
&ip=64.104.248.209&clen=10444732&sver=3&source=youtube&itag=251&lt=1466669747365466&upn=1700mSa
Uqq4&expire=14707
28963&id=o-ABXm_M_rqaPqauN_rtx9jNvU4NPYMD-wx-oJw0mAUclg&mime=audio%2Fwebm&cpn=YsB-Jmb04EU-
BeHl&alr=yes&ratebypass
=yes&c=WEB&cver=1.20160804&range=136064-284239&rn=4&rbuf=8659 - -
```

```
08/09/2016 01:49:26.899 (fl=5887) 10000 0.003 0.029 1357 - - 191323 10.66.86.90 10.66.85.121
2905 h - - - 200 GET
https://r5---sn-uxanug5-
ntqk.googlevideo.com/videoplayback?dur=703.721&ei=ozapV8jrGdWc4AKytYaYBQ&fexp=3300116%2C3
300131%2C3300161%2C3312739%2C3313265%2C9422596%2C9428398%2C9431012%2C9433096%2C9433223%2C9433946
%2C9435526%2C9437
066%2C9437552%2C9438327%2C9438662%2C9438804%2C9439580%2C9442424%2C9442920&requiresssl=yes&initcwn
dbps=6383750&gir=
yes&sparams=clen%2Cdur%2Cei%2Cgir%2Cid%2Cinitcwndbps%2Cip%2Cipbits%2Citag%2Ckeepalive%2Clmt%2Cmi
me%2Cmm%2Cmn%2Cms
%2Cmv%2Cpl%2Crequiresssl%2Csource%2Cupn%2Cexpire&signature=34635AFA02C12695F90E50E067E6BD4B7E5821
32.DEB68217D77D25
F02925B272C6B3F032D3764535&ipbits=0&ms=au&mt=1470706873&pl=22&mv=m&mm=31&mn=sn-uxanug5-
ntqk&keepalive=yes&key=yt6
&ip=64.104.248.209&clen=10444732&sver=3&source=youtube&itag=251&lt=1466669747365466&upn=1700mSa
```

```
Uqq4&expire=14707 28963&id=o-ABXm_M_rqaPqauN_rtx9jNvU4NPYMD-wx-  
oJw0mAUclg&mime=audio%2Fwebm&cpn=YsB-Jmb04EU-BeHl&alr=yes&ratebypass  
=yes&c=WEB&cver=1.20160804&range=284240-474924&rn=6&rbuf=17442 - -
```

Anche l'output del comando **show statistic acceleration http object-cache** deve mostrare un aumento dei risultati ottenuti:

```
WAAS-BRANCH# show statistics accelerator http object-cache  
..... Object Cache Caching Type: ott-youtube Object cache transactions served from cache:  
52  
Object cache request bytes for cache-hit transactions: 68079  
Object cache response bytes for cache-hit transactions: 14650548  
.....
```

Risoluzione dei problemi

Problema: Il traffico non è accelerato da SSL AO.

Soluzione:

Verificare se l'oggetto attivazione SSL corrisponde all'interfaccia SNI sul server WAAS principale con il seguente comando debug:

Questo è un esempio di un output riuscito del comando `ssl-errorlog`:

```
WAAS# debug accelerator ssl sni  
08/09/2016 01:33:23.721sslao(20473 4.0) TRCE (721383) SNI(youtube.com) matched with certificate  
SNA youtube.com [c2s.c:657] 08/09/2016 01:33:23.962sslao(20473 6.0) TRCE (962966)  
SNI(youtube.com) matched with certificate SNA youtube.com [c2s.c:657]
```

Questo è un esempio di output non riuscito per `ssl-errorlog`:

```
WAAS# debug accelerator ssl sni  
08/09/2016 01:19:35.929sslao(20473 5.0) NTCE (929983) Unknown SNI: youtube.com [sm.c:4312]  
08/09/2016 01:20:58.913sslao(20473 3.0) TRCE (913804) Pipethrough connection unknown  
SNI:youtube.com IP:10.66.85.121 ID:655078 [c2s.c:663]
```

Problema: Impossibile connettersi a YouTube. Nessun certificato sottoposto a push.

Soluzione:

Ciò può essere causato dal fatto che il componente principale WAAS non considera attendibile il certificato inviato da YouTube.

Deselezionare per il servizio accelerato SSL.

SSL Accelerated Service

Basic **Advanced**

SSL Settings

SSL version: Inherited ▼

CipherList: Inherited ▼ Create New

CipherList Configured

CipherList Name: Inherited

	Cipher list Configured	Priority
<input type="checkbox"/>		
<input type="checkbox"/>		1

Authentication

Verify client certificate

Disable revocation check of client certificates

Verify server certificate

Disable revocation check of server certificates

Problema: Il traffico raggiunge Akamai Connect Engine ma non è presente alcun accesso alla cache.

Soluzione:

Ciò può essere causato dall'applicazione del controllo If-Modified-Since (FMI) sul branch WAAS. L'opzione IMS può verificare la registrazione imposta dell'attività degli utenti su un server proxy o un dispositivo di analisi dell'utilizzo. Quando il controllo IMS è abilitato, nella versione OTT corrente, Youtube richiede sempre al client di recuperare l'ultima copia dal server di origine.

Ciò può essere osservato nel log degli errori di accesso:

```
07/20/2016 00:41:49.420 (fl=36862) 10000 2.511 0.000 1312 1383 4194962 4194941 10.37.125.203
10.6.76.220 2f25 l-s
s-ims-fv - - 200 GET https://r3---sn-jpuxj-
coxe.googlevideo.com/videoplayback?signature=AACC537F02B652FEA0600C90
0B069CA3063C15CD.58BA962C80C0E7DFA9A6664ECDCE6404A3E2C65&clen=601694377&pl=24&mv=m&mt=146897480
1&ms=au&ei=a8iOV-
HZG4u24gL-hpu4BQ&mn=sn-jpuxj-
coxe&mm=31&key=yt6&sparams=clen%2Cdur%2Cei%2Cgir%2Cid%2Cinetcwndbps%2Cip%2Cipbits%2C
itag%2Ckeepalive%2Clmt%2Cmime%2Cmm%2Cmn%2Cms%2Cmv%2Cpl%2Crequiressl%2Csource%2Cupn%2Cexpire&sver
=3&gir=yes&fexp=9
416891%2C9422596%2C9428398%2C9431012%2C9433096%2C9433221%2C9433946%2C9435526%2C9435876%2C9437066
%2C9437553%2C9437
742%2C9438662%2C9439652&expire=1468996811&inetcwndbps=9551250&ipbits=0&mime=video%2Fmp4&upn=B-
BbHfjKlaI&source=yo
utube&dur=308.475&id=o-ABCCH12_QzDMemZ8Eh7hbsSbhXZQ7yt325a-
xfqNROk1&lmt=1389684805775554&itag=138&requiressl=yes&
ip=203.104.11.77&keepalive=yes&cpn=4cIAF7ZEwNbfV7Cr&alr=yes&ratebypass=yes&c=WEB&cver=1.20160718
```

Deselezionare questi elementi nel branch WAAS per disabilitare il controllo IMS:

Selezionare **Configura > Memorizzazione nella cache > Akamai Connect**.

Cache Settings Cache Prepositioning

Enable Akamai Connect

▶ **Edit Settings**

▼ **Advanced Cache Settings**

Default Transparent Caching Policy: *

Site Specific Transparent Caching Policy

 Add Site Specific Transparent Caching Policy  Edit  Delete

	<input type="checkbox"/>	Hostname/IP	Transparent Caching Policy
1	<input type="checkbox"/>	broomenorthp...	Bypass

Force IMS DIA ?

Force IMS Always ?

Use HTTP Proxy for connections to Akamai network ?

Questo problema dovrebbe essere risolto in WAAS 6.3 e versioni successive.

Problema: La cache Akamai interrompe la connessione HTTPS quando si passa attraverso un proxy con autenticazione.

Soluzione:

Quando è necessario passare attraverso un proxy prima di accedere a Internet e il proxy richiede l'autenticazione, WAAS potrebbe interrompere la connessione HTTPS. L'acquisizione di pacchetti

eseguita sul branch WAAS mostra la risposta di HTTP 407 dal sito del server. Tuttavia, l'acquisizione viene interrotta dopo il primo pacchetto. I pacchetti successivi non vengono inviati e la risposta è incompleta.

Questo problema è stato rilevato con il difetto [CSCva26420](#) ed è probabile che venga risolto in WAAS 6.3.