

使用Akamai Connect配置Youtube流量最佳化

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[Akamai Connect和WAAS](#)

[設定](#)

[步驟1. 您需要由您的內部/公共CA簽署的SSL憑證。](#)

[步驟2. 您需要信任整個組織中的中介和/或根證書頒發機構\(CA\)。](#)

[步驟3. 使用WAAS中央管理器GUI在WAAS裝置上建立SSL加速服務。](#)

[步驟4. 配置SSL加速服務。](#)

[步驟5. 上傳證書和私鑰。](#)

[步驟6. 驗證上傳的憑證資訊。](#)

[步驟7. 按一下SUBMIT按鈕，這是最終結果。](#)

[步驟8. 啟用Akamai Connect。](#)

[步驟9. 在分支WAAS上啟用SSL轉接程式 \(僅單端設定需要該程式 \) 。](#)

[驗證](#)

[步驟1. 需要在分支WAAS上啟用Akamai Connect。](#)

[步驟2. 驗證客戶端上的Youtube加速。](#)

[步驟3. 在WAAS上驗證。](#)

[疑難排解](#)

[問題：SSL AO不會加速流量。](#)

[問題：瀏覽器無法連線到Youtube，並且未推送證書。](#)

[問題：流量命中Akamai Connect Engine，但沒有快取命中。](#)

[問題：Akamai快取在使用身份驗證通過代理時斷開HTTPS連線。](#)

簡介

本文檔介紹使用Akamai Connect功能在思科廣域應用服務(WAAS)上配置Youtube加速所需的步驟。

附註：在本文中，術語WAAS裝置統稱為網路中的WAAS中央管理器和WAE。術語WAE (廣域應用工程師) 指的是WAE和WAVE裝置、運行WAAS的SM-SRE模組和vWAAS例項。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco WAAS
- 公開金鑰基礎架構
- 安全套接字層(SSL)證書

採用元件

本檔案中的資訊是根據以下軟體版本：

- Cisco WAAS版本5.5.1
- Cisco WAAS版本6.2.1

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

背景資訊

Akamai Connect和WAAS

Akamai Connect功能是新增加到Cisco WAAS的HTTP/S對象快取元件。它整合到現有的WAAS軟體堆疊中，並通過HTTP應用最佳化程式加以利用。Akamai Connect有助於降低業務和Web應用的HTTP/S流量的延遲，並可提高許多應用的效能，包括POS（銷售點）、高畫質影片、數位標牌和店內訂單處理。它提供顯著且可衡量的廣域網資料解除安裝，並與現有WAAS功能相容，例如DRE（重複資料消除）、LZ（壓縮）、TFO（傳輸流最佳化）以及用於第一和第二通道加速的SSL加速（安全/加密）。

以下術語用於Akamai Connect和WAAS:

- Akamai Connect - Akamai Connect是新增加到Cisco WAAS的HTTP/S對象快取元件，整合到現有WAAS軟體堆疊中，並通過HTTP應用最佳化程式加以利用。帶Akamai Connect的WAAS有助於減少業務和網路應用的HTTP/S流量延遲。
- Akamai Connected Cache - Akamai Connected Cache是Akamai Connect的一個元件，它允許快取引擎(CE)快取由Akamai智慧平台上的邊緣伺服器提供的內容。

設定

步驟1。您需要由您的內部/公共CA簽署的SSL憑證。

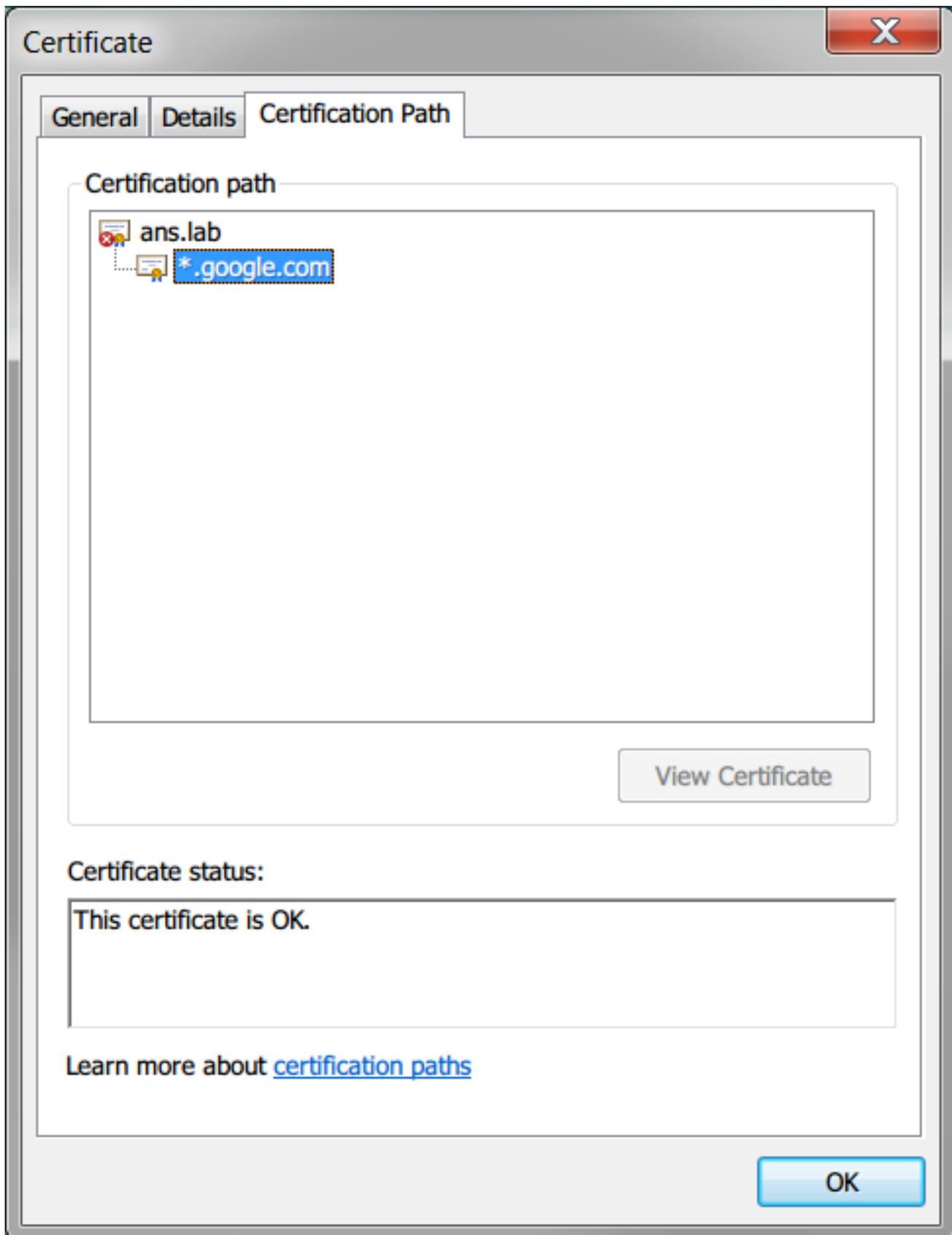
證書需要包含以下SubjectAltName:

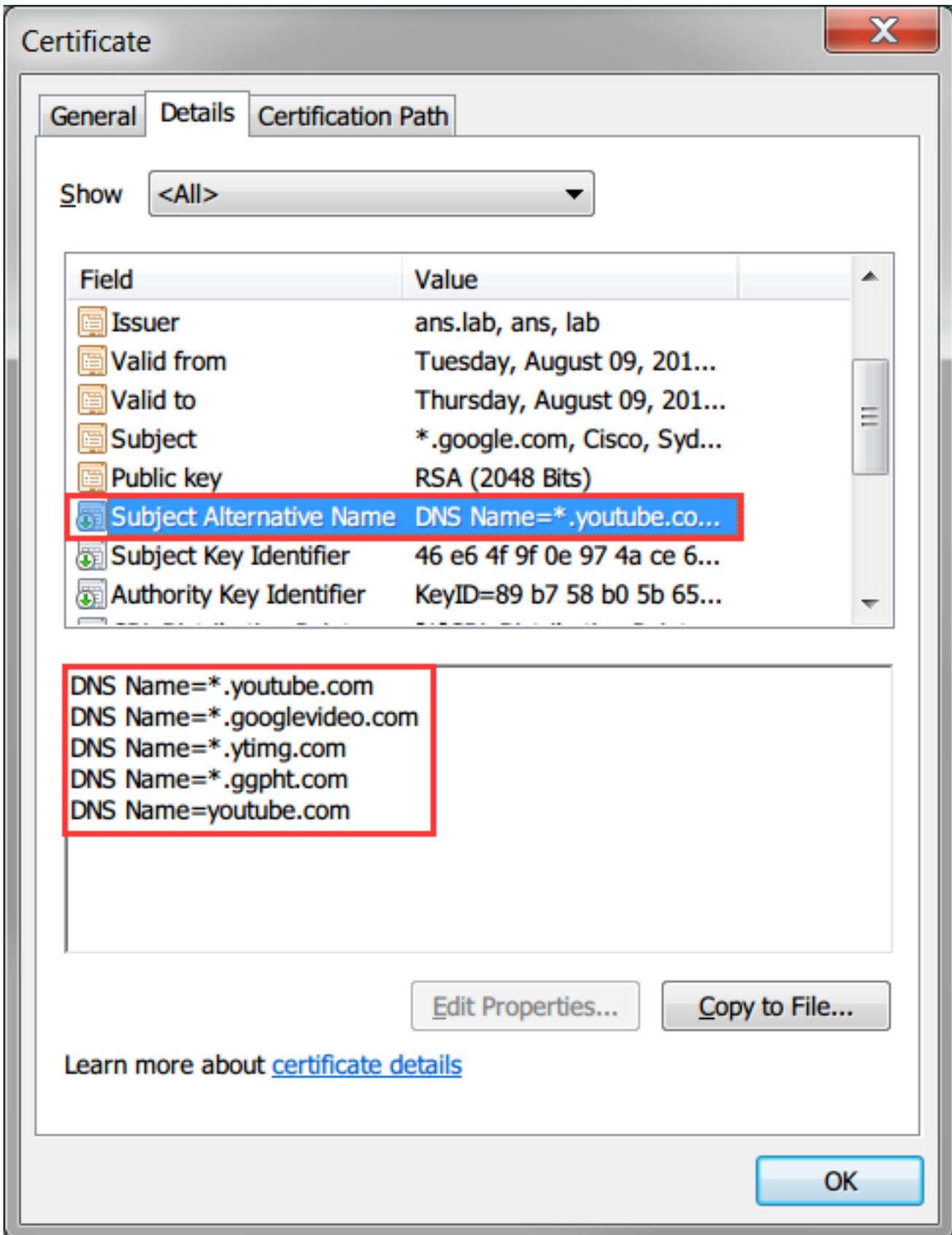
- *.youtube.com
- *.googlevideo.com
- *.yimg.com

*.ggpht.com

youtube.com

以下是憑證範例：





步驟2.您需要信任整個組織中的中介和/或根證書頒發機構(CA)。

這可以通過在Active Directory域中使用組策略來實現。

如果在實驗室中測試此安裝程式，則可以將中間和/或根CA作為受信任CA安裝在客戶端裝置中。

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

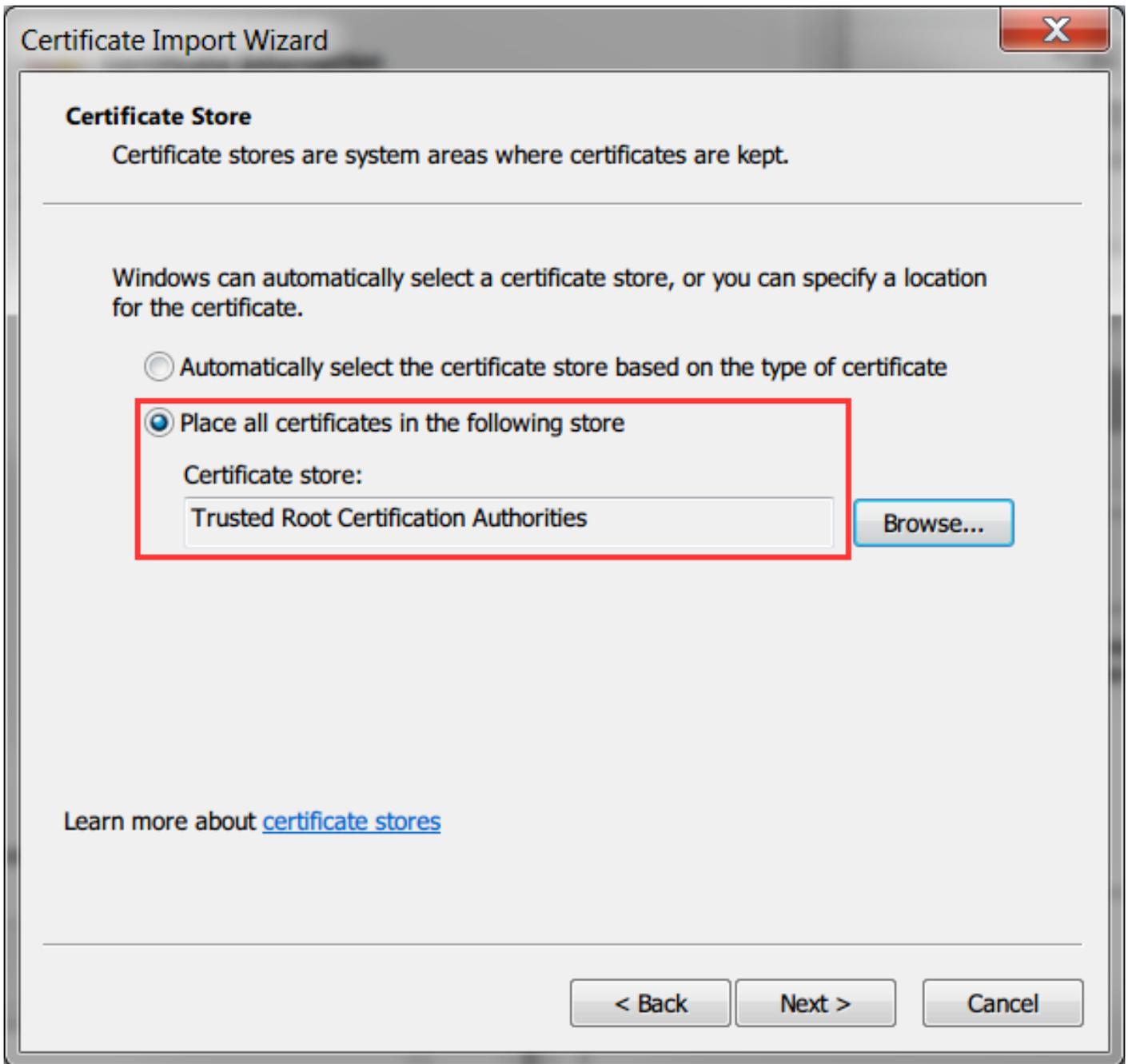
Valid from 8/ 8/ 2016 **to** 8/ 8/ 2021

Install Certificate...

Issuer Statement

Learn more about [certificates](#)

OK



步驟3.使用WAAS中央管理器GUI在WAAS裝置上建立SSL加速服務。

在雙面Akamai (WAAS 6.2.3之前的版本) 上，在核心WAAS上配置SSL加速服務。對於單面Akamai (WAAS 6.2.3或更高版本)，在分支WAAS上配置SSL加速伺服器並啟用SSL內插器。這是雙面設定與單面設定之間的唯一差異。

附註：運行低於6.2.3的WAAS軟體需要雙面Akamai設定來加速Youtube流量核心WAAS代理指向Youtube的SSL連線。運行軟體版本6.2.3或更高版本的WAAS支援SSL AO v2(SAKE)。這樣，當分支機構直接將流量傳送到網際網路而不通過資料中心基礎設施時，分支機構WAAS便可以代理SSL連線。

導覽至Devices > Configure > Acceleration > SSL Accelerated Service，如下圖所示：

- 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**
- 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

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

Current applied settings from WAE, DC-WAVE-7571

SSL Accelerated Services

步驟4.配置SSL加速服務。

如果使用顯式代理，則需要啟用協定鍵。HTTP AO必須應用於用於代理流量的TCP埠（例如80或8080）。

需要檢查匹配伺服器名稱指示。在此設定中，當核心WAAS收到SSL流量時，它將將Client Hello中的SNI欄位與上傳證書中的SubjectAltName進行比較。如果SNI欄位與SubjectAltName匹配，則核心WAAS會代理此SSL流量。

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: *

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: Server Port: Add

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

選中Match Server Name Indication欄位後，請對IPAddress使用Any，對伺服器埠使用443。按一下Add以新增此條目。

- ▾ 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

伺服器名稱指示(SNI)

步驟5.上傳證書和私鑰。

您需要提供證書和私鑰。圖中所示的範例使用PEM格式：

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](#)

步驟6.驗證上傳的憑證資訊。

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: CqNpol2RX2Ye8llZoKjbIeOuaIQ=

Key

Type: SHA1WITHRSA
 Size (Bits): 2048

步驟7.按一下SUBMIT按鈕，這是最終結果。

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

步驟8.啟用Akamai Connect。

導航到Devices > Configure > Caching > Akamai Connect。

Cache Settings Cache Prepositioning

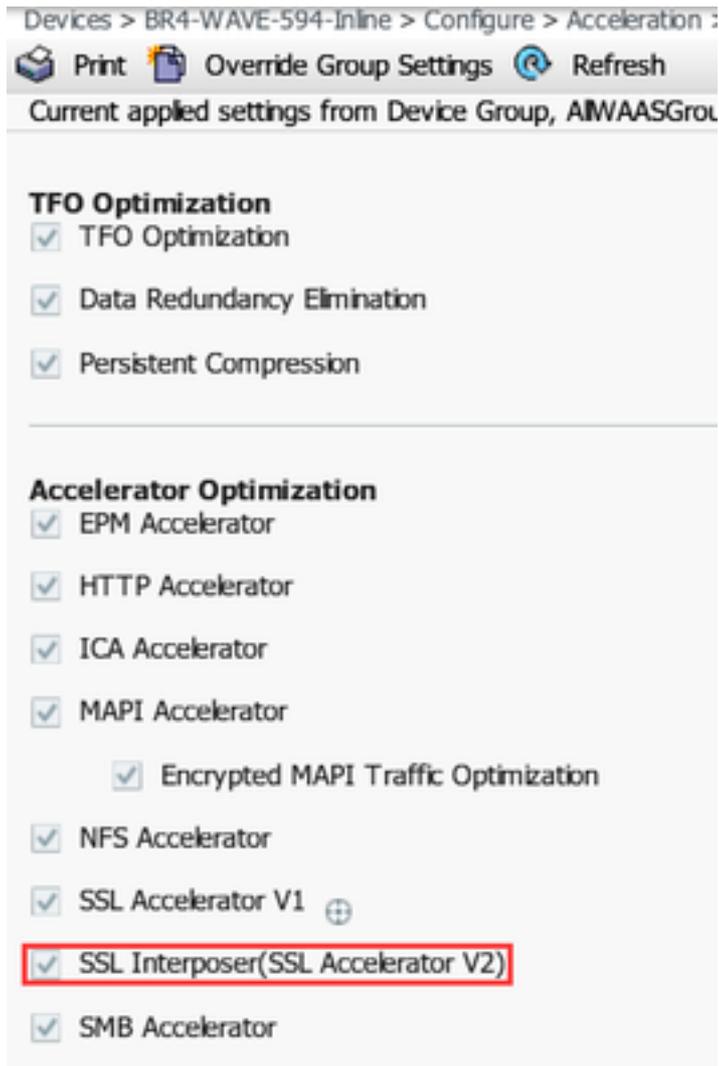
Enable Akamai Connect

▼ **Edit Settings**

Akamai Connected Cache

Over the top Cache

步驟9.在分支WAAS上啟用SSL轉接程式 (僅單端設定需要該程式)。



驗證

步驟1.需要在分支WAAS上啟用Akamai Connect。

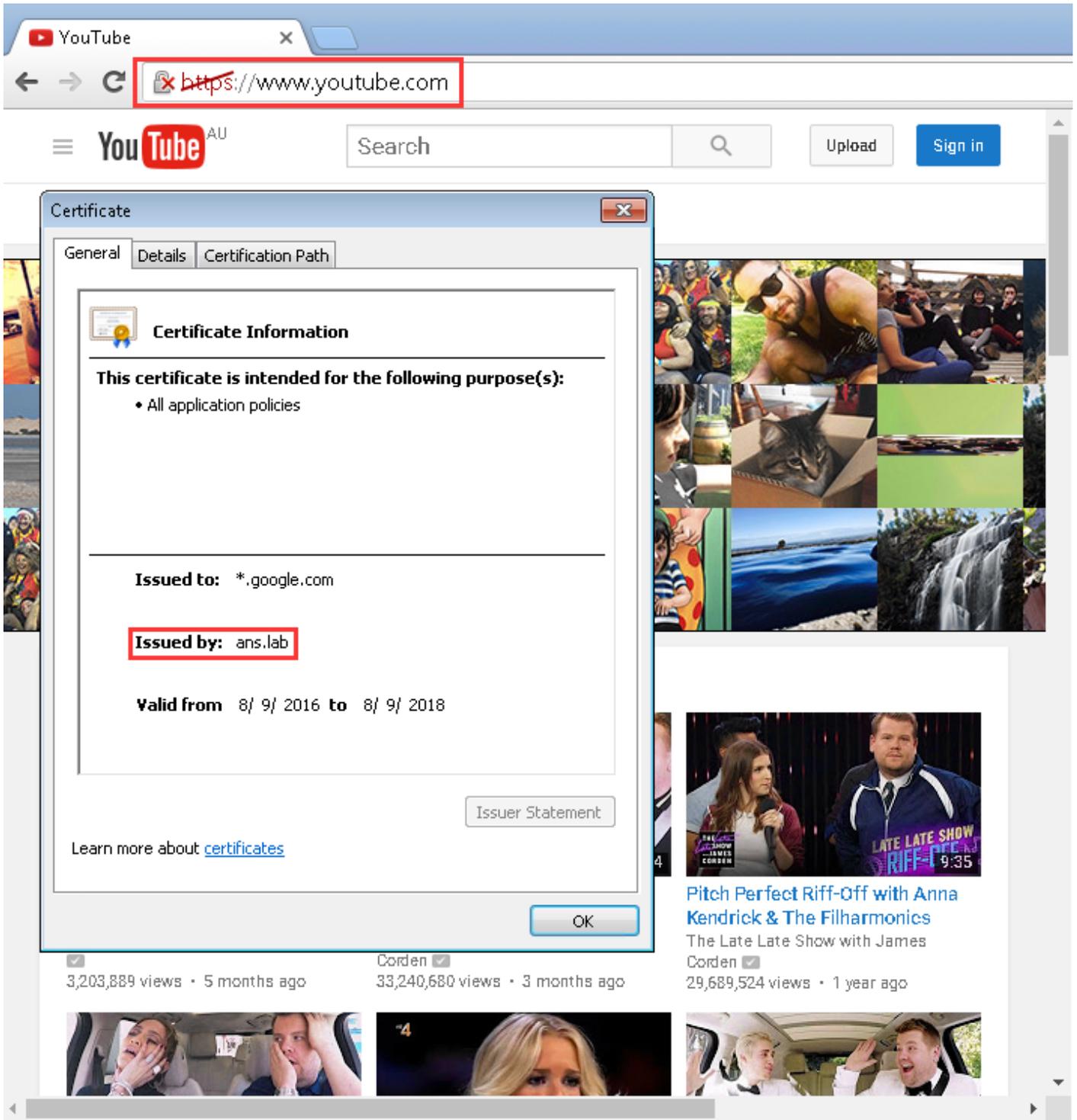
WAAS-BRANCH# show accelerator http object-cache

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

確保運行狀態為Running，連線狀態為Connected。

步驟2.驗證客戶端上的Youtube加速。

當您訪問Youtube時，您必須看到由您自己的CA簽名的證書：



步驟3.驗證WAAS。

驗證SSL AO是否已正確應用於流量：

運行6.2.3之前的WAAS軟體（SSL AO v1和雙站點設定）時CLI的輸出示例

WAAS-BRANCH# **show statistics connection**

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%

```

運行WAAS軟體6.2.3或更高版本 (SSL AO v2和單站點設定) 時CLI的輸出示例

WAAS-BRANCH# show statistics connection

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%

檢查分支WAAS上的ce-access-errorlog。最佳化流量的日誌條目具有與之關聯的代碼10000 (指示分類為OTT-Youtube) , h — - 200指示對象快取被命中且流量在本地得到服務。Google影片的加速預期最高。您可以在測試電腦上開啟多個瀏覽器 , 同時播放相同的影片來測試設定 :

ce-errorlog的輸出示例 :

```

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-JmbO4EU-
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-JmbO4EU-BeHl&alr=yes&ratebypass
=yes&c=WEB&cver=1.20160804&range=284240-474924&rn=6&rbuf=17442 - -

```

show statistic acceleration http object-cache的輸出也必須顯示ott-youtube命中數增加：

```
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
.....
```

疑難排解

問題：SSL AO不會加速流量。

解決方案:

使用以下調試命令檢查SSL AO是否與核心WAAS上的SNI匹配：

以下是ssl-errorlog成功輸出的範例：

```
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]
```

以下是ssl-errorlog輸出不成功的範例：

```
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]
```

問題：瀏覽器無法連線到Youtube，並且未推送證書。

解決方案：

這可能是因為核心WAAS不信任Youtube推送的證書。

取消選中SSL加速服務上的此項。

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

問題：流量命中Akamai Connect Engine，但沒有快取命中。

解決方案：

這可能是由對分支WAAS強制執行If-Modified-since(IMF)檢查引起的。IMS選項可以檢查將使用者活動強制記錄到代理伺服器或使用分析裝置。啟用IMS檢查後，在當前OTT版本中，Youtube總是請求客戶端從源伺服器獲取最新副本。

可從ce-access-errorlog中觀察到這種情況：

```
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 1-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%2Cinitcwndbps%2Cip%2Cipbits%2C
itag%2Ckeepalive%2Clmt%2Cmime%2Cmm%2Cmn%2Cms%2Cmv%2Cpl%2Crequiresssl%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&initcwndbps=9551250&ipbits=0&mime=video%2Fmp4&upn=B-
BbHfjKlaI&ssource=yo
utube&dur=308.475&id=o-ABCCH12_QzDMemZ8Eh7hbsSbhXZQ7yt325a-
xfqNRok1&lmt=1389684805775554&itag=138&requiresssl=yes&
ip=203.104.11.77&keepalive=yes&cpn=4cIAF7ZEwNbfV7Cr&alr=yes&ratebypass=yes&c=WEB&cver=1.20160718
&range=193174249-
197368552&rn=68&rbuf=23912 - -
```

在分支WAAS上取消選中以下選項以禁用IMS檢查：

導航至配置>快取> 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 ?

預計此問題將在WAAS 6.3及更高版本中修復。

問題： Akamai快取在使用身份驗證通過代理時斷開HTTPS連線。

解決方案：

如果您在訪問Internet之前需要通過Proxy，並且代理要求身份驗證，WAAS可能會中斷HTTPS連線。分支WAAS上的資料包捕獲顯示來自伺服器站點的HTTP 407響應。但是，擷取會在第一個封包之後停止。後續資料包不傳送，並且響應不完整。

此問題在缺陷[CSCva26420](#)中跟蹤，並可能在WAAS 6.3版本中修復。