

Configuratie van YouTube Traffic Optimization met Akamai Connect

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Akamai Connect en WAAS](#)

[Configureren](#)

[Stap 1. U hebt een SSL-certificaat nodig dat is ondertekend door uw interne/openbare CA.](#)

[Stap 2. U moet uw intermediair en/of de basiscertificeringsinstantie \(CA\) in uw hele organisatie vertrouwen.](#)

[Stap 3. Maak een SSL-versnelde Service op WAAS-apparaat met WAAS Central Manager GUI.](#)

[Stap 4. Configuratie van de SSL Versnelde Service.](#)

[Stap 5. Uploadcertificaat en particuliere sleutel.](#)

[Stap 6. Controleer de geüploade certificaatinformatie.](#)

[Stap 7. Klik op de knop INVOEREN en dit is het eindresultaat.](#)

[Stap 8. Schakel Akamai Connect in.](#)

[Stap 9. Schakel de SSL-interposer in de aftakking WAAS in \(alleen vereist voor Single Side Setup\).](#)

[Verifiëren](#)

[Stap 1. U moet Akamai Connect op branche WAAS hebben ingeschakeld.](#)

[Stap 2. Controleer de versnelling van YouTube op de client.](#)

[Stap 3. Controleer WAAS.](#)

[Problemen oplossen](#)

[Probleem: Het verkeer wordt niet versneld door SSL AO.](#)

[Probleem: De browser kan geen verbinding maken met YouTube en er is geen certificaat aangezet.](#)

[Probleem: Het verkeer slaat Akamai Connect Engine in, maar er is geen cache hit.](#)

[Probleem: Akamai Cache breekt een HTTPS-verbinding wanneer u een proxy met verificatie maakt.](#)

Inleiding

Dit document beschrijft de gewenste stappen voor het configureren van YouTube-versnelling op Cisco Wide Area Application Services (WAAS) met behulp van Akamai Connect-functie.

Opmerking: In dit artikel wordt de term WAAS-apparaat gebruikt om gezamenlijk te verwijzen naar WAAS Central Managers en WAE's in uw netwerk. Het begrip WAE (Wide Area Application Engineer) verwijst naar WAE- en WAVE-apparaten, SM-SRE-modules met WAAS en vWAAS-instanties.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco WAAS
- Publieke sleutelinfrastructuur
- Secure Socrates Layer (SSL)-certificaat

Gebruikte componenten

De informatie in dit document is gebaseerd op deze softwareversies:

- Cisco WAAS versie 5.5.1
- Cisco WAAS versie 6.2.1

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Achtergrondinformatie

Akamai Connect en WAAS

De Akamai Connect-functie is een HTTP/S object cache-component toegevoegd aan Cisco WAAS. Het is geïntegreerd in de bestaande WAAS-softwarestapel en wordt via de HTTP-optimalisator gebruikt. Akamai Connect helpt de latentie voor HTTP/S-verkeer voor zakelijke en webtoepassingen te verminderen en kan de prestaties voor veel toepassingen verbeteren, waaronder POS (Point of Sale), HD-video, digitale signalering en verwerking van bestellingen in-Store. Het biedt significante en meetbare WAN-gegevensoffload en is compatibel met bestaande WAAS-functies zoals DRE (deduplicatie), LZ (compressie), TFO (Transport Flow Optimization) en SSL-versnelling (beveiligd/versleuteld) voor de eerste en de tweede pass versnelling.

Deze termen worden gebruikt met Akamai Connect en WAAS:

- Akamai Connect - Akamai Connect is een HTTP/S-doelcache-component toegevoegd aan Cisco WAAS, geïntegreerd in de bestaande WAAS-softwarestack en gebruikt via de HTTP-Application Optimizer. WAAS met Akamai Connect helpt de latentie voor HTTP/S-verkeer voor zakelijke en webtoepassingen te verminderen.
- Akamai Connected Cache - Akamai Connected Cache is een onderdeel van Akamai Connect, waardoor de cache engine (CE) content kan cache plaatsen die wordt geleverd door een Edge-server op het Akamai Intelligent Platform.

Configureren

Stap 1. U hebt een SSL-certificaat nodig dat is ondertekend door uw interne/openbare CA.

Het certificaat moet de volgende OnderwerpAltName bevatten:

*.youtube.com

*.googlevideo.com

*.ytimg.com

*.gpht.com

youtube.com

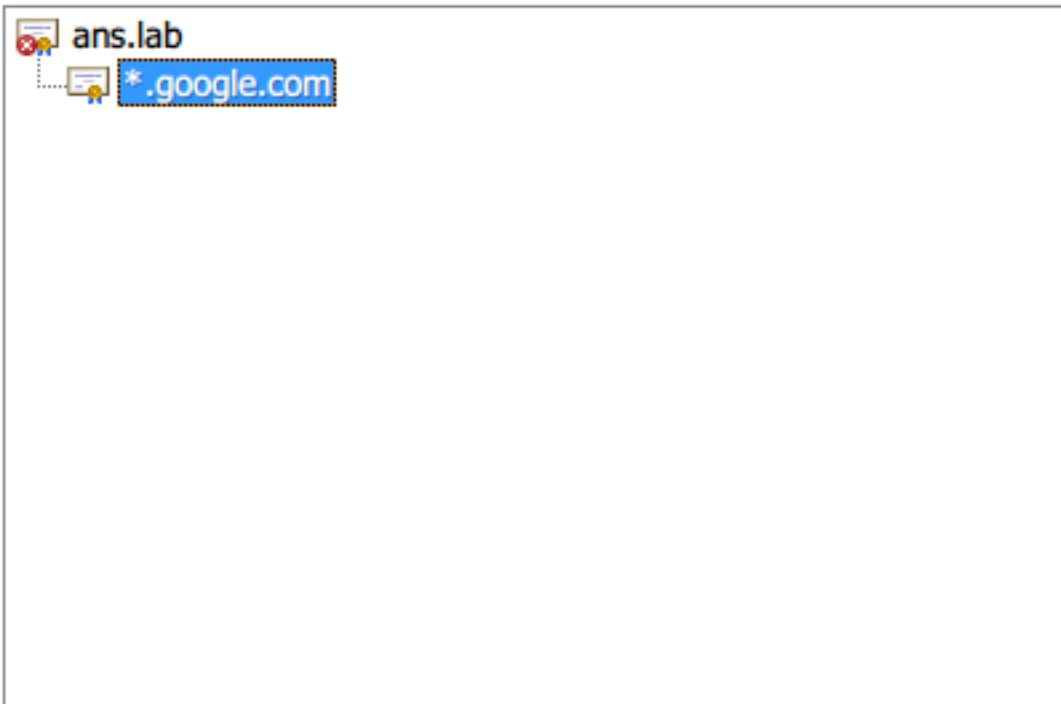
Dit is een voorbeeldcertificaat:

Certificate



General Details Certification Path

Certification path



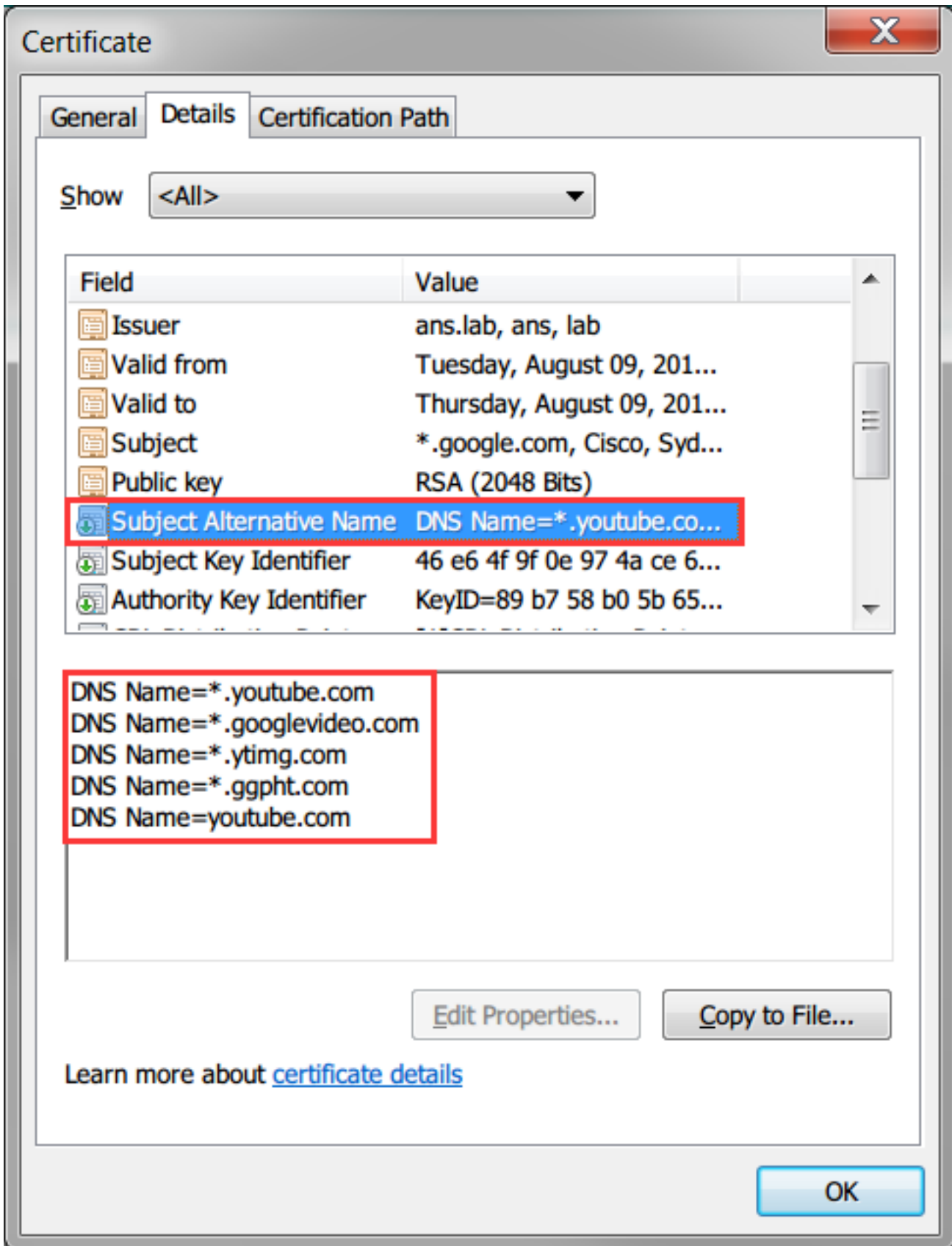
View Certificate

Certificate status:

This certificate is OK.

Learn more about [certification paths](#)

OK



Stap 2. U moet uw intermediair en/of de basiscertificeringsinstantie (CA) in uw hele organisatie vertrouwen.

Dit kan worden bereikt door het groepsbeleid te gebruiken in het domein van de actieve map.

Als u deze instelling in een laboratorium test, kunt u de intermediaire en/of de wortel CA in het clientapparaat als Trusted CA installeren.

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

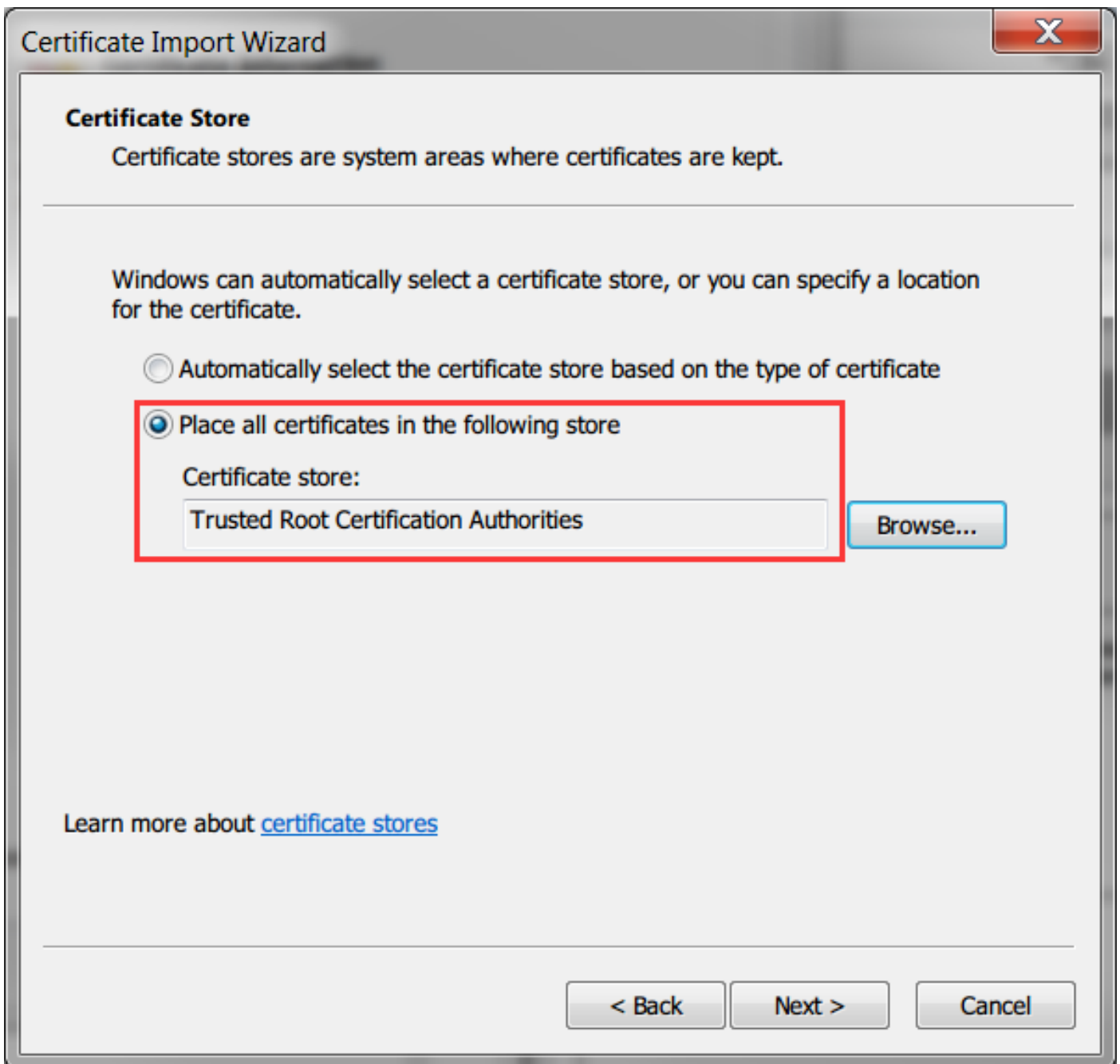
Valid from 8/ 8/ 2016 **to** 8/ 8/ 2021

Install Certificate...

Issuer Statement

Learn more about [certificates](#)

OK



Stap 3. Maak een SSL-versnelde Service op WAAS-apparaat met WAAS Central Manager GUI.

Op Akamai met twee zijden (pre WAAS 6.2.3) moet u de SSL-versnelde service op de kerncentrale WAAS configureren. Voor Akamai met één kant (WAAS 6.2.3 of hoger) moet u de SSL-versnelde server op de tak WAAS configureren en de SSL-interposer inschakelen. Dit is het enige verschil tussen dubbele installatie aan de zijkant en één instelling aan de zijkant.

Opmerking: WAAS dat softwarerelease vóór 6.2.3 draait, heeft een dubbele Akamai-instelling nodig om YouTube-verkeer te versnellen. De kern WAAS ontleent de SSL-verbinding naar YouTube. WAAS met softwarerelease 6.2.3 of hoger ondersteunt SSL AO v2 (SAKE). Dit staat de tak WAAS toe om de SSL verbinding te volmaken wanneer de tak direct verkeer naar het internet verstuurt zonder door de datacenterinfrastructuur te worden geleid.

Navigeren naar **Apparaten > Configureren > Acceleration > SSL Accelerated Service**, zoals in de

afbeelding weergegeven:

The screenshot shows the Fortinet configuration interface. At the top, there are tabs for 'Devices', 'AppNav Clusters', and 'Locations'. Below these are dropdown menus for 'Configure', 'Monitor', and 'Admin'. The main content area is divided into three columns of configuration options:

- 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

Stap 4. Configuratie van de SSL Versnelde Service.

Als u een expliciete proxy gebruikt, moet Protocol Chaining worden ingeschakeld. HTTP moet worden toegepast op de TCP-poort die wordt gebruikt voor het opnieuw genereren van het verkeer (bijvoorbeeld 80 of 8080).

Aanwijzing van overeenkomende servernaam moet worden gecontroleerd. In deze instelling, wanneer de kern WAAS SSL-verkeer ontvangt, vergelijkt het SNI-veld in de client Hallo met de subjectAltName in het geüploade certificaat. Als het SNI-veld overeenkomt met onderwerpregelAltName de kern van WAAS dit SSL-verkeer verlengt.

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 Any Server Port: 443 Add

Type	Address	Port

Wanneer het veld **Naam** van de **overeenkomende server** is ingeschakeld, gebruikt u **Any** voor IPA-adres en **443** voor serverpoort. Klik op **Add** om deze ingang toe te voegen.

▾ 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**

Naam van server (SNI)

Stap 5. Uploadcertificaat en particuliere sleutel.

U moet een certificaat en een privésleutel opgeven. Het voorbeeld in de afbeelding gebruikt PEM-indeling:

[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](#)

Stap 6. Controleer de geüploade certificaatinformatie.

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	

Stap 7. Klik op de knop INVOEREN en dit is het eindresultaat.

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			

Stap 8. Schakel Akamai Connect in.

Navigeer naar **Apparaten > Configureren > Caching > Akamai Connect**.

Cache Settings
Cache Prepositioning

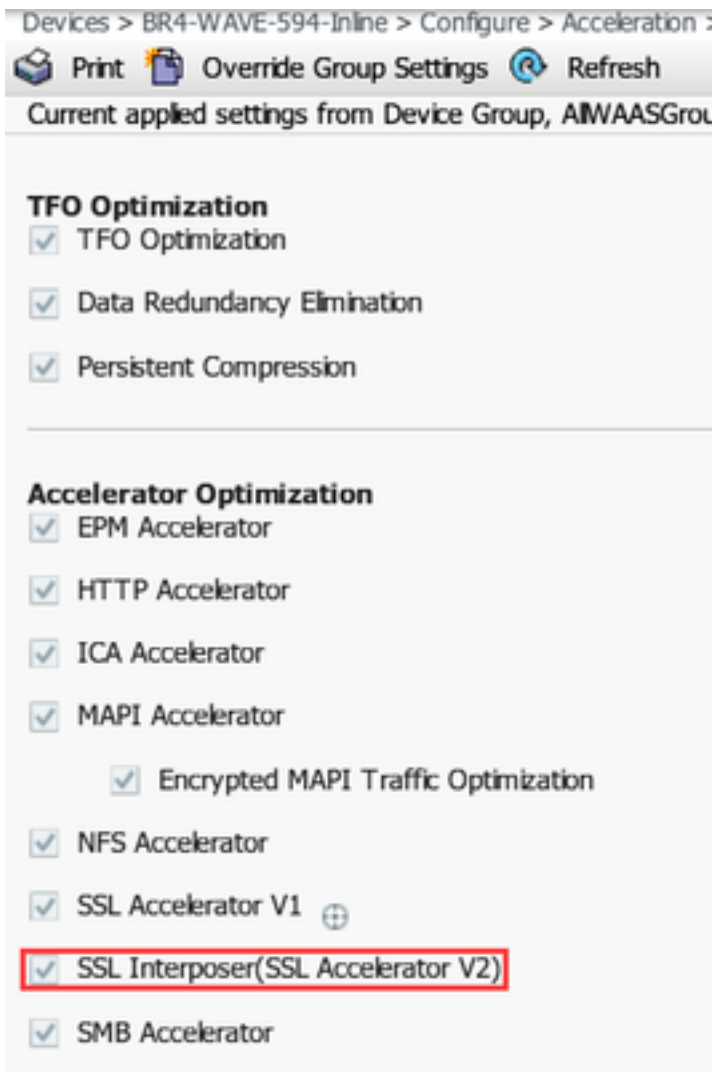
Enable Akamai Connect

▼ **Edit Settings**

 Akamai Connected Cache

Over the top Cache

Stap 9. Schakel de SSL-interposer in de aftakking WAAS in (alleen vereist voor Single Side Setup).



Verifiëren

Stap 1. U moet Akamai Connect op branche WAAS hebben ingeschakeld.

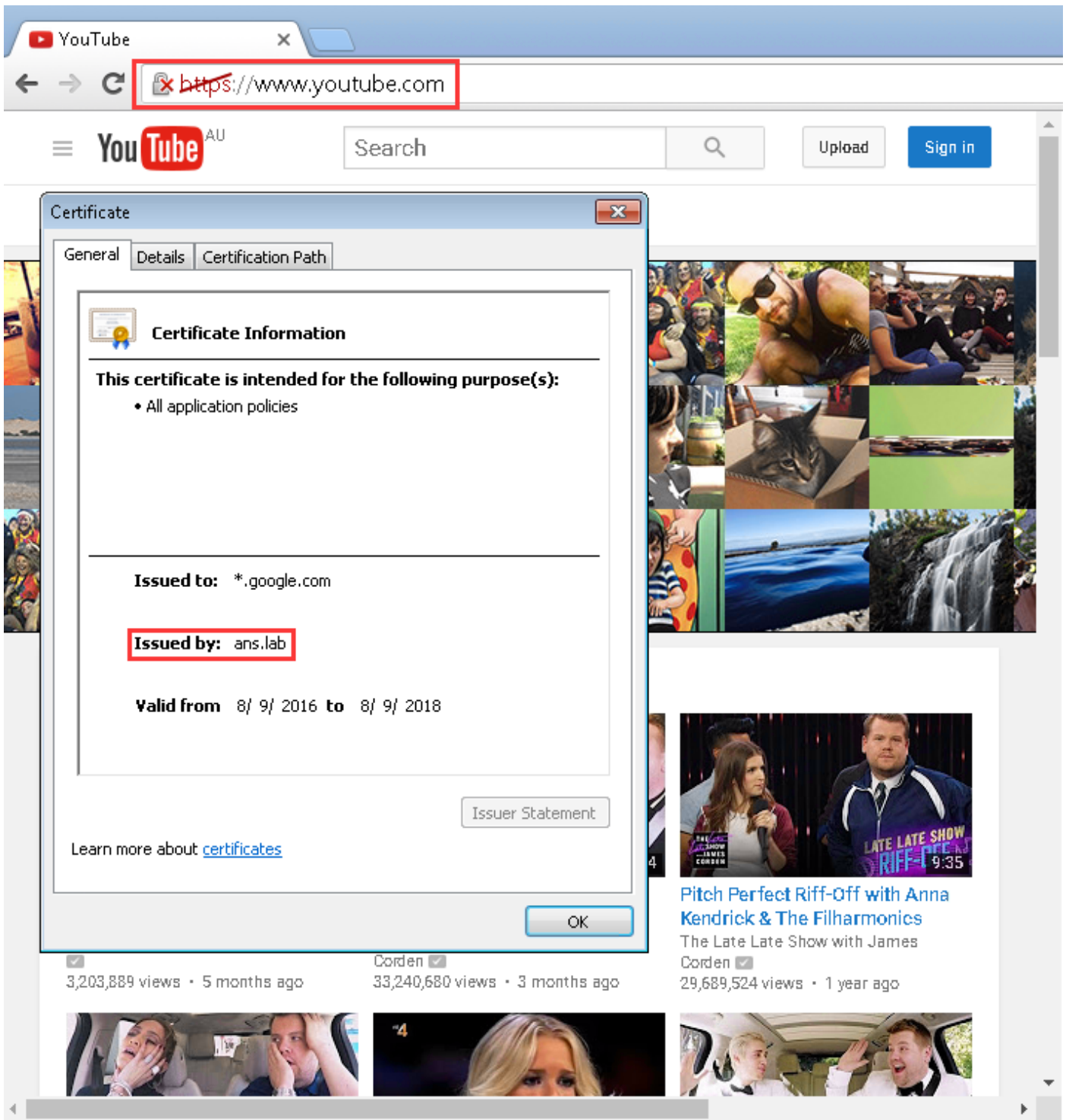
WAAS-BRANCH#-show accelerator http object-cache

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

Zorg ervoor dat de operationele status **actief** is en dat de verbindingstaat **aangesloten** is.

Stap 2. Controleer de versnelling van YouTube op de client.

Wanneer u toegang hebt tot YouTube, dient u het certificaat te zien dat door uw eigen CA is ondertekend:



Stap 3. Controleer WAAS.

Controleer of SSL AO correct op het verkeer wordt toegepast:

Voorbeelden van uitvoer van de CLI bij het gebruik van WAAS-software vóór 6.2.3 (SSL AO v1 en Dual Site Setup)

WAAS-BRANCH# toont statistische verbinding

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%
```

Voorbeelden van uitvoer van de CLI bij het gebruik van WAAS-software 6.2.3 of hoger (SSL AO v2 en Single Site Setup)

WAAS-BRANCH# toont statistische verbinding

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%

Controleer het ce-access-errorlog op de aftakking WAAS. Logingangen voor geoptimaliseerd verkeer hebben een code van 10000 die met hen is geassocieerd (aangegeven als OTT-Youtube) en h - - 200 geeft aan dat het object cache wordt geraakt en het verkeer lokaal wordt verzorgd. De meest acceleratie wordt verwacht op googlevideo. U kunt meerdere browsers op de testmachine openen en tegelijkertijd dezelfde video afspelen om de instellingen te testen:

Uitvoer uit 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&lmt=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&lmt=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 - -
```

De output van **show static Acceleration http object-cache** moet ook tonen dat het aantal YouTube-hits toeneemt:

```
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  
.....
```

Problemen oplossen

Probleem: Het verkeer wordt niet versneld door SSL AO.

Oplossing:

Controleer of SSL AO met deze debug opdracht overeenkomt met de SNI in de kern WAAS:

Dit is een voorbeeld van een succesvol resultaat van 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]
```

Dit is een voorbeeld van een onsuccesvolle uitvoer van 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]
```

Probleem: De browser kan geen verbinding maken met YouTube en er is geen certificaat aangezet.

Oplossing:

Dit kan worden veroorzaakt door de kern van WAAS die het certificaat dat door YouTube is gestuurd niet vertrouwd.

Schakel deze optie uit op SSL-versnelde service.

SSL Accelerated Service

Basic **Advanced**

SSL Settings

SSL version:

CipherList:

CipherList Configured

CipherList Name:

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

Authentication

Verify client certificate
 Disable revocation check of client certificates

Verify server certificate
 Disable revocation check of server certificates

Probleem: Het verkeer slaat Akamai Connect Engine in, maar er is geen cache hit.

Oplossing:

Dit kan worden veroorzaakt door het opleggen van de IF-Modified-sinds (IMF) check van de tak WAAS. De optie IMS kan de gedwongen houtkap van gebruikersactiviteit aan een volmachtserver of een gebruiksanalyseapparaat controleren. Als IMS-controle is ingeschakeld, vraagt Youtube in de huidige OTT-versie altijd van de client om de laatste kopie van de oorspronkelijke server op te halen.

Dit kan worden waargenomen in ce-access-errorlog:

```
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%2CinIcwndbps%2Cip%2Cipbits%2C
itag%2Ckeepalive%2Clmt%2Cmime%2Cmm%2Cmn%2Cms%2Cmv%2Cpl%2Crequiresl%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&inIcwndbps=9551250&ipbits=0&mime=video%2Fmp4&upn=B-
BbHfjKlaI&source=yo
utube&dur=308.475&id=o-ABCCH12_QzDMemZ8Eh7hbsSbhXZQ7yt325a-
xfqNRok1&lmt=1389684805775554&itag=138&requiresl=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 - -

Schakel deze uit op de WAAS-aftakking om IMS-controle uit te schakelen:

Navigeren in **het configureren > Caching > 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 ?

Deze kwestie zal naar verwachting in WAAS 6.3 en daarna worden geregeld.

Probleem: Akamai Cache breekt een HTTPS-verbinding wanneer u een proxy met verificatie maakt.

Oplossing:

Als je door een proxy moet gaan voordat je naar het internet gaat en de proxy moet zijn beveiligd, kan WAAS de HTTPS-verbinding verbreken. Packet shot genomen op tak WAAS toont de

respons van HTTP 407 van de serversite. De opname stopt echter na het eerste pakket. De volgende pakketten worden niet verzonden en de respons is onvolledig.

Dit wordt gevolgd door defect [CSCva26420](#) en zal waarschijnlijk in de WAAS 6.3-vrijgave worden bevestigd.