

Konfigurieren der Optimierung des Datenverkehrs von YouTube mit Akamai Connect

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Akamai Connect und WAAS](#)

[Konfigurieren](#)

[Schritt 1: Sie benötigen ein SSL-Zertifikat, das von Ihrer internen/öffentlichen CA signiert wird.](#)

[Schritt 2: Sie müssen Ihrem Vermittler und/oder Ihrer Stammzertifizierungsstelle \(Certificate Authority, CA\) im gesamten Unternehmen vertrauen.](#)

[Schritt 3: Erstellen Sie mithilfe der Benutzeroberfläche von WAAS Central Manager einen SSL-beschleunigten Service auf dem WAAS-Gerät.](#)

[Schritt 4: Konfigurieren Sie den SSL Accelerated Service.](#)

[Schritt 5: Zertifikat und privaten Schlüssel hochladen.](#)

[Schritt 6: Überprüfen Sie die hochgeladenen Zertifikatsinformationen.](#)

[Schritt 7: Klicken Sie auf die Schaltfläche SENDEN. Dies ist das Endergebnis.](#)

[Schritt 8: Aktivieren Sie Akamai Connect.](#)

[Schritt 9: Aktivieren Sie den SSL Interposer in der WAAS-Außenstelle \(nur für Single-Side-Setup erforderlich\).](#)

[Überprüfen](#)

[Schritt 1: Sie müssen Akamai Connect auf WAAS der Außenstelle aktivieren.](#)

[Schritt 2: Überprüfen Sie Youtube Acceleration auf Client.](#)

[Schritt 3: Überprüfen Sie das WAAS.](#)

[Fehlerbehebung](#)

[Problem: Der Datenverkehr wird nicht durch SSL AO beschleunigt.](#)

[Problem: Der Browser kann keine Verbindung zu Youtube herstellen, und es wird kein Zertifikat übertragen.](#)

[Problem: Der Datenverkehr trifft die Akamai Connect Engine, aber es gibt keinen Cache-Treffer.](#)

[Problem: Akamai Cache bricht die HTTPS-Verbindung, wenn ein Proxy mit Authentifizierung durchläuft.](#)

Einführung

Dieses Dokument beschreibt die erforderlichen Schritte zur Konfiguration von Youtube Acceleration auf Cisco Wide Area Application Services (WAAS) mithilfe der Akamai Connect-Funktion.

Hinweis: In diesem Artikel wird der Begriff "WAAS-Gerät" verwendet, um gemeinsam auf die WAAS Central Manager und WAEs in Ihrem Netzwerk zu verweisen. Der Begriff WAE (Wide Area Application Engineer) bezieht sich auf WAE- und WAVE-Appliances, SM-SRE-Module mit WAAS- und vWAAS-Instanzen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Cisco WAAS
- Public Key-Infrastruktur
- SSL-Zertifikat (Secure Sockets Layer)

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Softwareversionen:

- Cisco WAAS Version 5.5.1
- Cisco WAAS Version 6.2.1

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Akamai Connect und WAAS

Die Akamai Connect-Funktion ist eine HTTP/S-Objektcache-Komponente, die Cisco WAAS hinzugefügt wurde. Sie ist in den vorhandenen WAAS-Software-Stack integriert und wird über den HTTP Application Optimizer genutzt. Akamai Connect trägt zur Reduzierung der Latenz für HTTP/S-Datenverkehr für Geschäfts- und Webanwendungen bei und kann die Leistung für viele Anwendungen verbessern, darunter POS (Point of Sale), HD-Video, digitale Beschilderung und Bestellabwicklung im Geschäft. Sie bietet eine erhebliche und messbare WAN-Datenauslagerung und ist mit bestehenden WAAS-Funktionen wie DRE (Deduplizierung), LZ (Komprimierung), TFO (Transport Flow Optimization) und SSL-Beschleunigung (sicher/verschlüsselt) für die Beschleunigung der ersten und zweiten Durchlaufphase kompatibel.

Diese Begriffe werden zusammen mit Akamai Connect und WAAS verwendet:

- Akamai Connect - Akamai Connect ist eine der Cisco WAAS hinzugefügte HTTP/S-Objektcache-Komponente, die in den vorhandenen WAAS-Software-Stack integriert und über den HTTP Application Optimizer genutzt wird. WAAS mit Akamai Connect trägt zur

Reduzierung der Latenz für HTTP/S-Datenverkehr für Geschäfts- und Webanwendungen bei.

- Akamai Connected Cache - Akamai Connected Cache ist eine Komponente von Akamai Connect, mit der die Cache-Engine (CE) Inhalte zwischenspeichern kann, die von einem Edge-Server auf der Akamai Intelligent Platform bereitgestellt werden.

Konfigurieren

Schritt 1: Sie benötigen ein SSL-Zertifikat, das von Ihrer internen/öffentlichen CA signiert wird.

Das Zertifikat muss folgenden SubjectAltName enthalten:

*.youtube.com

*.googlevideo.com

*.ytimg.com

*.ggpht.com

youtube.com

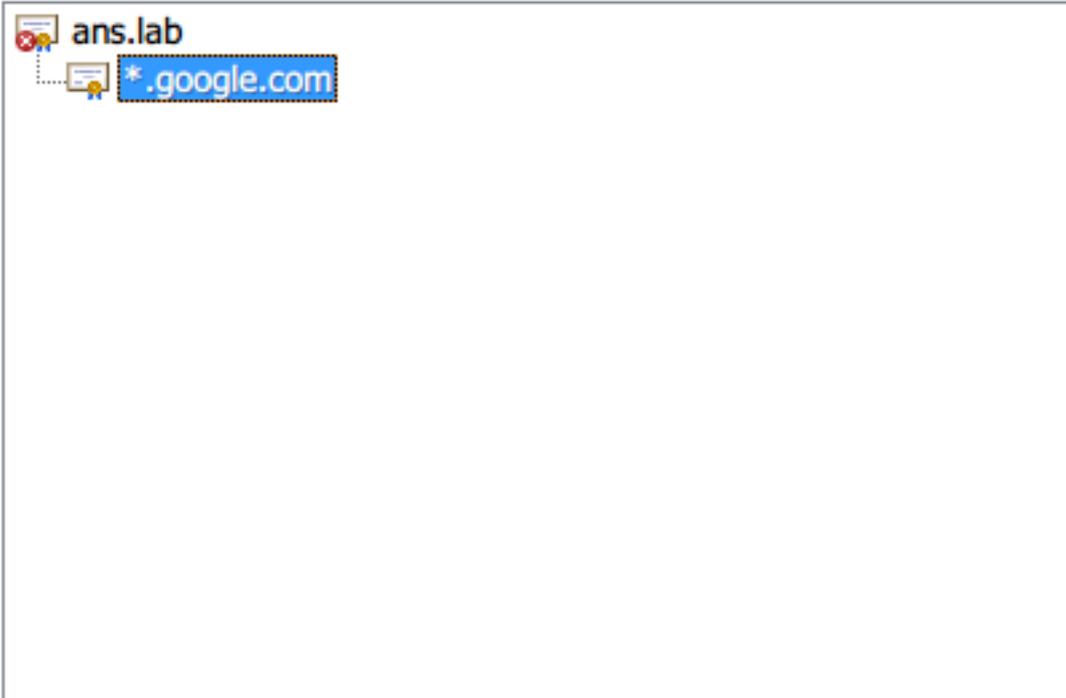
Dies ist ein Beispielzertifikat:

Certificate



General Details Certification Path

Certification path



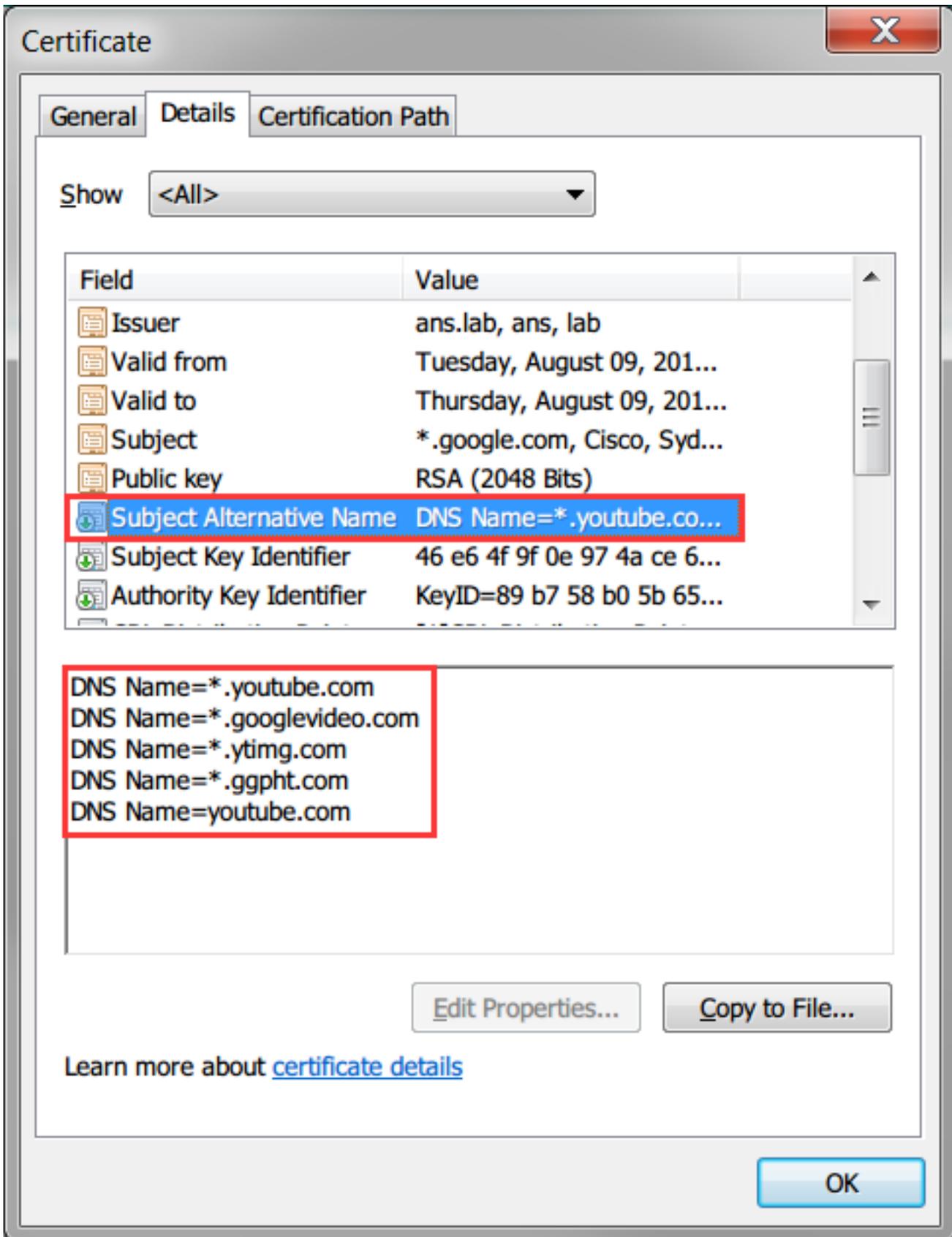
View Certificate

Certificate status:

This certificate is OK.

Learn more about [certification paths](#)

OK

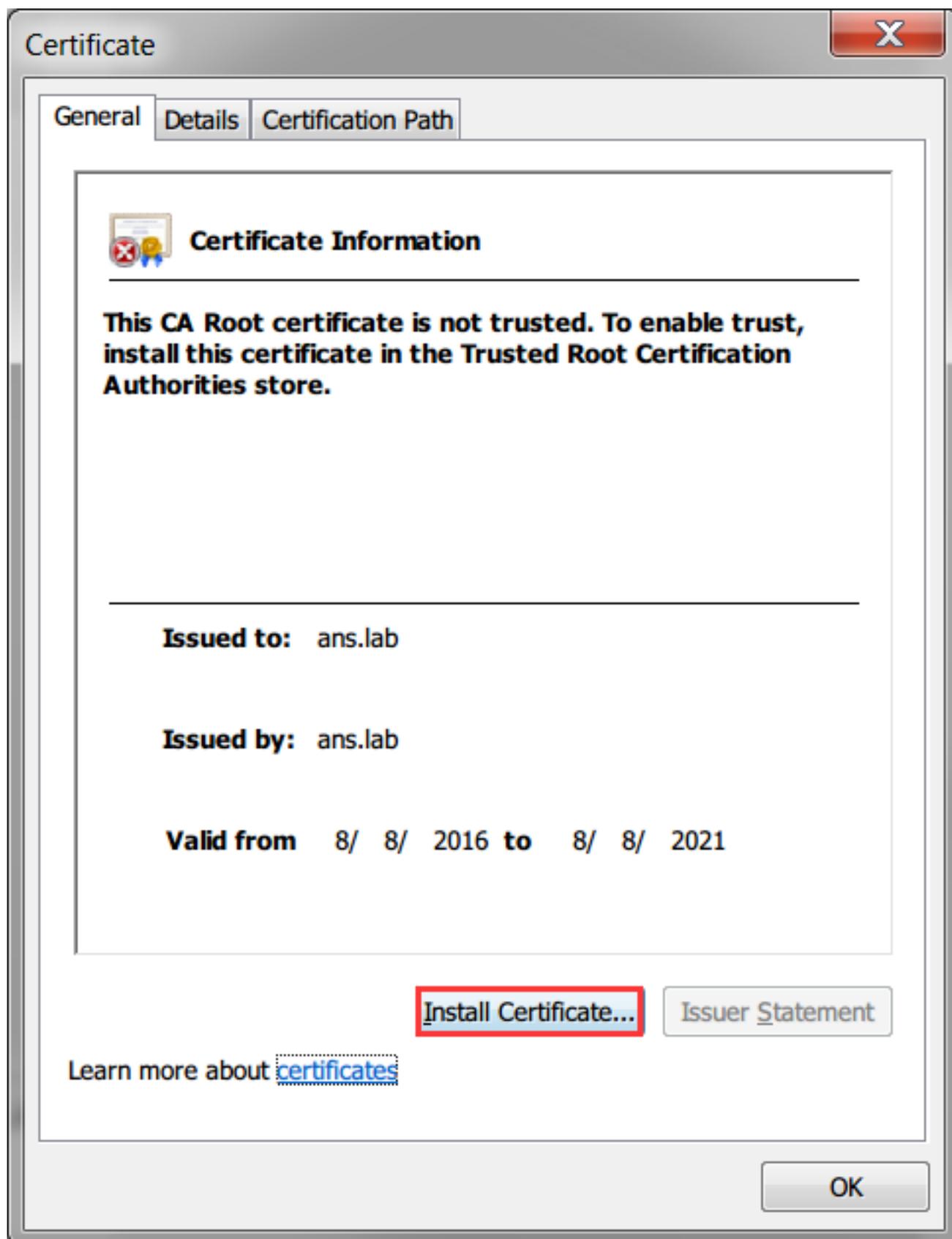


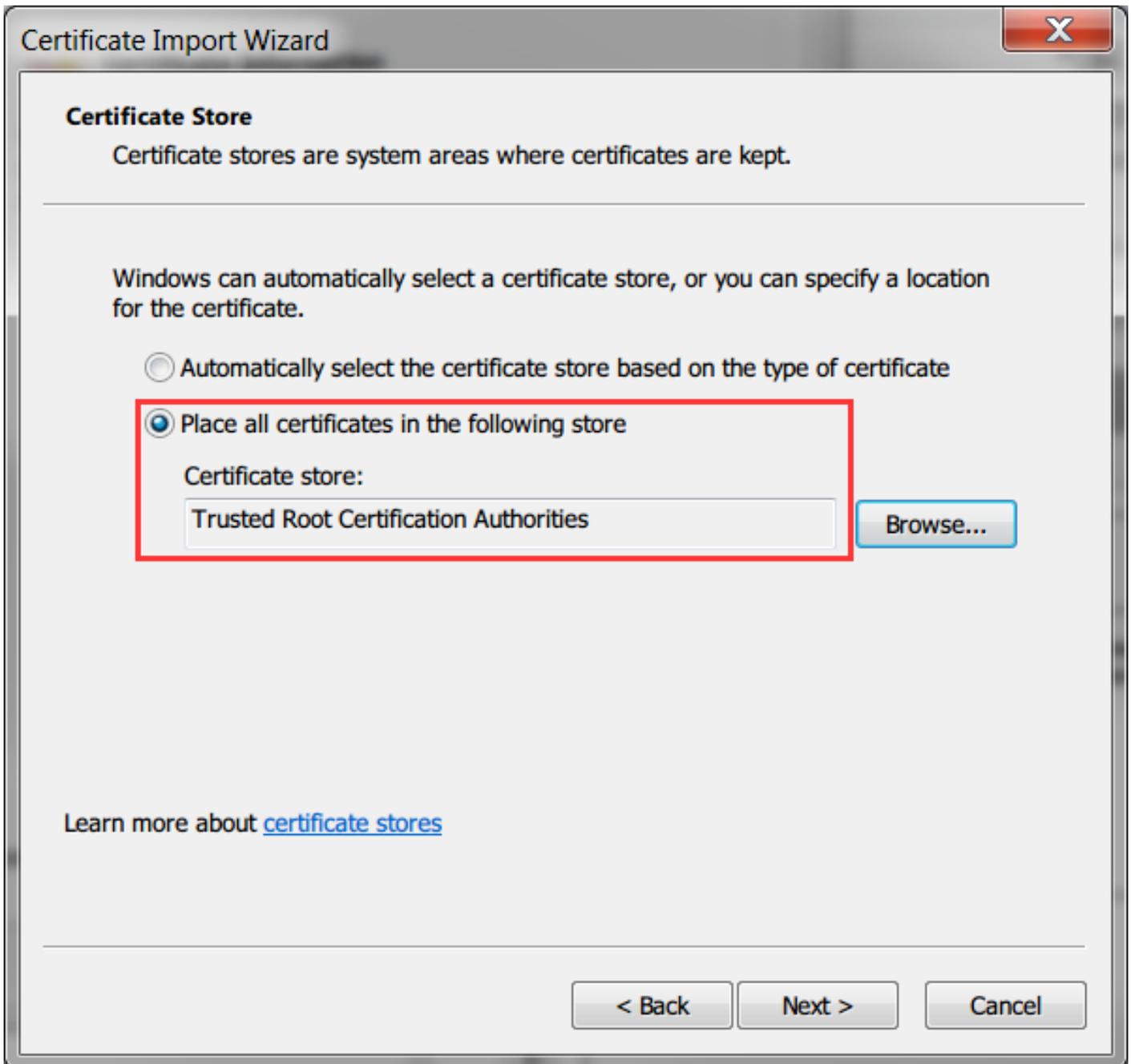
Schritt 2: Sie müssen Ihrem Vermittler und/oder Ihrer Stammzertifizierungsstelle (Certificate Authority, CA) im gesamten Unternehmen vertrauen.

Dies kann durch die Verwendung von Gruppenrichtlinien in der gesamten Active Directory-Domäne erreicht werden.

Wenn Sie diese Konfiguration in einer Übung testen, können Sie die Zwischen- und/oder Root-CA

auf dem Client-Gerät als vertrauenswürdige CA installieren.





Schritt 3: Erstellen Sie mithilfe der Benutzeroberfläche von WAAS Central Manager einen SSL-beschleunigten Service auf dem WAAS-Gerät.

Auf Dual-Sided Akamai (vor WAAS 6.2.3) konfigurieren Sie den SSL-beschleunigten Service auf der Core-WAAS. Für einseitige Akamai (WAAS 6.2.3 oder höher) konfigurieren Sie den SSL-beschleunigten Server in der WAAS-Außenstelle und aktivieren den SSL-Interposer. Dies ist der einzige Unterschied zwischen der Dual-Side-Konfiguration und der Single-Side-Konfiguration.

Hinweis: Für WAAS, die eine Softwareversion vor 6.2.3 ausführen, ist eine Dual-Sided-Akamai-Konfiguration erforderlich, um den YouTube-Datenverkehr zu beschleunigen. Die Core-WAAS proxyn die SSL-Verbindung, die zu Youtube führt. WAAS mit Softwareversion 6.2.3 oder höher unterstützt SSL AO v2 (SAKE). Dadurch kann die Zweigstellen-WAAS die SSL-Verbindung proxylieren, wenn die Zweigstelle Datenverkehr direkt an das Internet sendet, ohne dass diese über die Infrastruktur des Rechenzentrums geleitet wird.

Navigieren Sie zu **Geräte > Konfigurieren > Beschleunigung > SSL Accelerated Service**, wie im

Bild gezeigt:

The screenshot shows the configuration interface for AppNav Clusters. The top navigation bar includes 'Devices', 'AppNav Clusters', and 'Locations'. Below this, there are 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

Schritt 4: Konfigurieren Sie den SSL Accelerated Service.

Wenn Sie einen expliziten Proxy verwenden, muss die Protokoll-Verkettung aktiviert werden. HTTP AO muss auf den TCP-Port angewendet werden, der zum Proxying des Datenverkehrs verwendet wird (z. B. 80 oder 8080).

Die Angabe des Servernamens muss überprüft werden. Wenn die Core-WAAS in dieser Konfiguration SSL-Datenverkehr empfängt, vergleicht sie das SNI-Feld im Client Hello mit dem SubjectAltName im hochgeladenen Zertifikat. Wenn das SNI-Feld mit dem SubjectAltName übereinstimmt, leitet die Core-WAAS diesen SSL-Datenverkehr weiter.

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

Wenn das Feld "Match Server Name Indication" (Servernamenangabe zuordnen) aktiviert ist, verwenden Sie **Any** für IPA-Adresse und **443** für Server-Port. Klicken Sie auf **Hinzufügen**, um diesen Eintrag hinzuzufügen.

TLV1 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**

Servernamenanzeige (SNI)

Schritt 5: Zertifikat und privaten Schlüssel hochladen.

Sie müssen ein Zertifikat und einen privaten Schlüssel angeben. Im Beispiel im Bild wird das PEM-Format verwendet:

[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](#)

Schritt 6: Überprüfen Sie die hochgeladenen Zertifikatsinformationen.

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	

Schritt 7: Klicken Sie auf die Schaltfläche SENDEN. Dies ist das Endergebnis.

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			

Schritt 8: Aktivieren Sie Akamai Connect.

Navigieren Sie zu **Devices > Configure > Caching > Akamai Connect**.

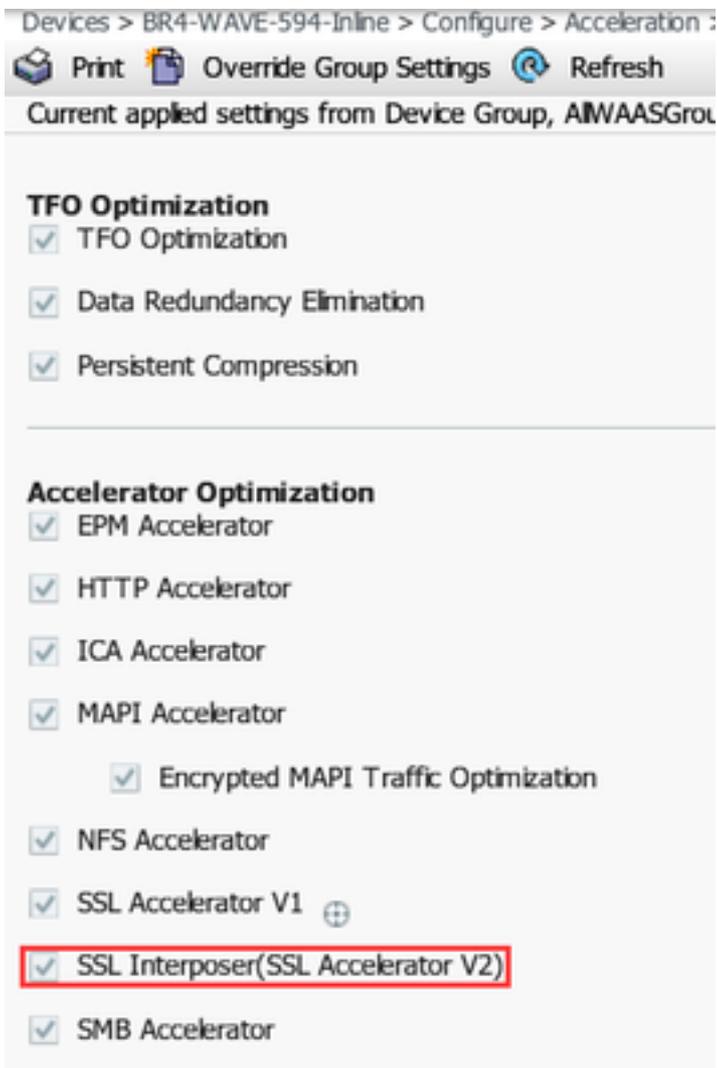
Cache Settings
Cache Prepositioning

Enable Akamai Connect

▼ **Edit Settings**

 Akamai Connected Cache
 Over the top Cache

Schritt 9: Aktivieren Sie den SSL Interposer in der WAAS-Außenstelle (nur für Single-Side-Setup erforderlich).



Überprüfen

Schritt 1: Sie müssen Akamai Connect auf WAAS der Außenstelle aktivieren.

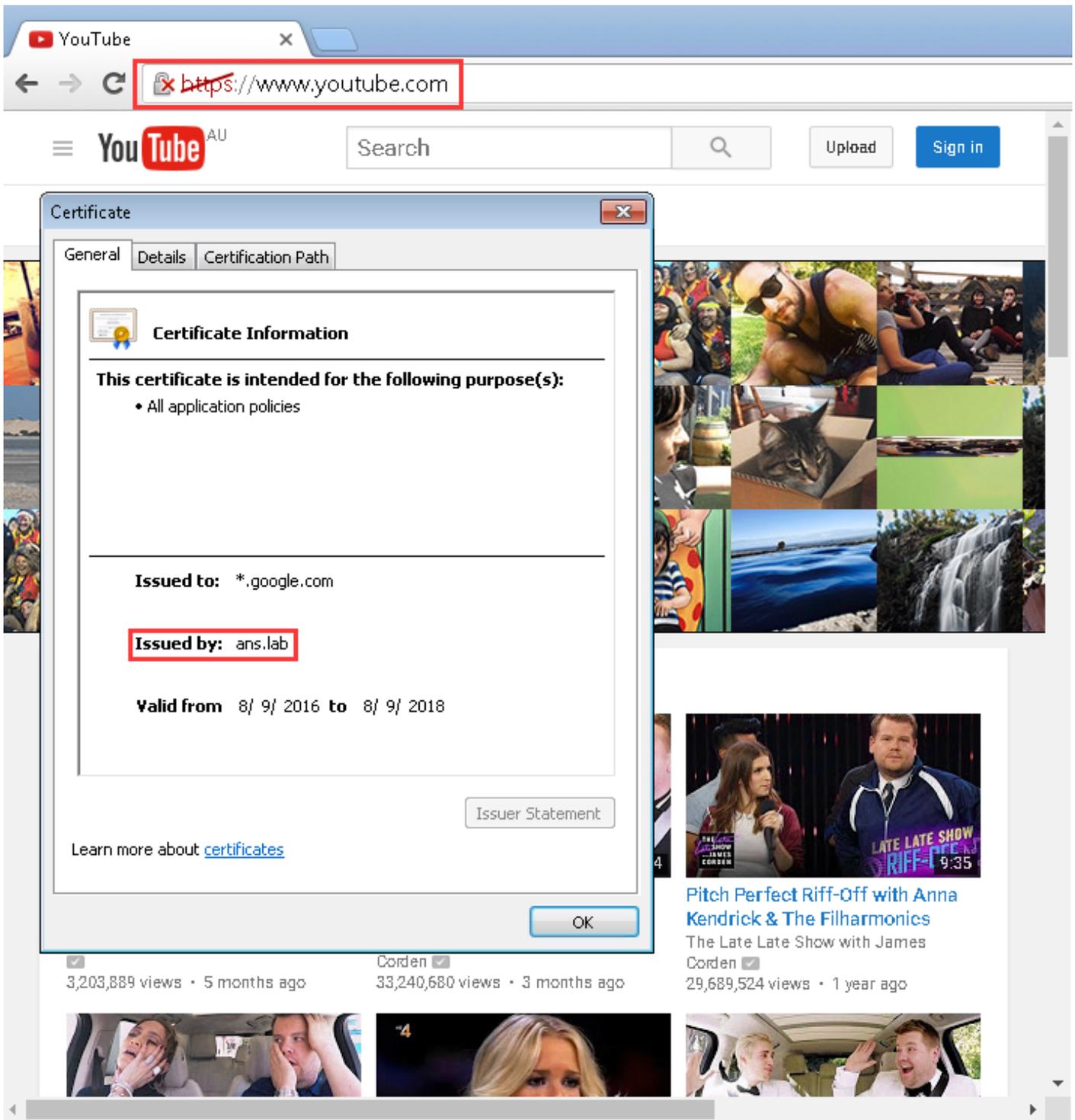
WAAS-BRANCH# show Accelerator http object-cache

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

Stellen Sie sicher, dass der Betriebsstatus **ausgeführt** und der Verbindungsstatus **verbunden** ist.

Schritt 2: Überprüfen Sie Youtube Acceleration auf Client.

Wenn Sie auf Youtube zugreifen, müssen Sie das Zertifikat sehen, das von Ihrer Zertifizierungsstelle signiert wurde:



Schritt 3: Überprüfen Sie das WAAS.

Überprüfen Sie, ob SSL AO korrekt auf den Datenverkehr angewendet wurde:

Beispielausgabe aus der CLI bei Ausführung der WAAS-Software vor 6.2.3 (SSL AO v1 und Dual Site Setup)

WAAS-ZWEIGSTELLE# Statistische Verbindung anzeigen

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%
```

Beispielausgabe aus der CLI bei Ausführung der WAAS-Software 6.2.3 oder höher (SSL AO v2 und Single Site Setup)

WAAS-ZWEIGSTELLE# Statistische Verbindung anzeigen

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%

Überprüfen Sie das ce-access-errorlog auf der WAAS-Außenstelle. Protokolleinträge für optimierten Datenverkehr haben einen Code von 10000 (als OTT-Youtube klassifiziert), und h - - - 200 gibt an, dass der Objekt-Cache erreicht wird und der Datenverkehr lokal verarbeitet wird. Die meisten Beschleunigung ist für Google Video erwartet. Sie können mehrere Browser auf dem Testcomputer öffnen und gleichzeitig dasselbe Video abspielen, um die Einrichtung zu testen:

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

Die Ausgabe von **show statistic accelerc http object-cache** muss auch zeigen, ott-youtube Treffer zunehmen:

```
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
.....
```

Fehlerbehebung

Problem: Der Datenverkehr wird nicht durch SSL AO beschleunigt.

Lösung:

Überprüfen Sie, ob SSL AO mit dem folgenden Debug-Befehl mit der SNI auf der WAAS-Core-Lösung übereinstimmt:

Dies ist ein Beispiel für eine erfolgreiche Ausgabe von 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]
```

Dies ist ein Beispiel für eine fehlgeschlagene Ausgabe von 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]
```

Problem: Der Browser kann keine Verbindung zu Youtube herstellen, und es wird kein Zertifikat übertragen.

Lösung:

Dies kann durch die Core-WAAS verursacht werden, die nicht dem von Youtube gesendeten Zertifikat vertrauen.

Deaktivieren Sie diese Option auf SSL-beschleunigtem Dienst.

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

Authentication

Verify client certificate

Disable revocation check of client certificates

Verify server certificate

Disable revocation check of server certificates

Problem: Der Datenverkehr trifft die Akamai Connect Engine, aber es gibt keinen Cache-Treffer.

Lösung:

Dies kann durch die Erzwingung des If-Modified-seit (IWF)-Schecks in der WAAS-Außenstelle verursacht werden. Die IMS-Option kann die erzwungene Protokollierung der Benutzeraktivitäten auf einem Proxyserver oder einem Gerät zur Nutzungsanalyse überprüfen. Wenn IMS Check aktiviert ist, fordert Youtube in der aktuellen OTT-Version immer den Client auf, die neueste Kopie vom Ursprungsserver abzurufen.

Dies ist im ce-access-errorlog zu beobachten:

```
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.58BA962C80C0E7DFA9A6664ECDCC6404A3E2C65&clen=601694377&pl=24&mv=m&mt=146897480
l&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%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&initcwndbps=9551250&ipbits=0&mime=video%2Fmp4&upn=B-
BbHfjKlaI&source=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 - -

Deaktivieren Sie diese in der WAAS-Außenstelle, um die IMS-Prüfung zu deaktivieren:

Navigieren Sie zu **Configure > 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 ?

Dieses Problem soll in WAAS 6.3 und höher behoben werden.

Problem: Akamai Cache bricht die HTTPS-Verbindung, wenn ein Proxy mit Authentifizierung durchläuft.

Lösung:

Wenn Sie einen Proxy durchlaufen müssen, bevor Sie zum Internet gehen, und der Proxy eine Authentifizierung erfordert, kann WAAS die HTTPS-Verbindung unterbrechen. Die Paketerfassung in der Zweigstellen-WAAS zeigt die Antwort von HTTP 407 vom Server-Standort. Die Erfassung wird jedoch nach dem ersten Paket beendet. Nachfolgende Pakete werden nicht gesendet, und die Antwort ist unvollständig.

Dies wird im Fehler [CSCva26420](#) nachverfolgt und wird wahrscheinlich in der Version WAAS 6.3 behoben sein.