

Akamai ConnectによるYoutubeトラフィック最適化の設定

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[Akamai ConnectおよびWAAS](#)

[設定](#)

[ステップ1：内部/パブリックCAによって署名されたSSL証明書が必要です。](#)

[ステップ2：組織の中間またはルート認証局\(CA\)を信頼する必要があります。](#)

[ステップ3:WAAS Central Manager GUIを使用して、WAASデバイスでSSLアクセラレーションサービスを作成します。](#)

[ステップ4:SSL Accelerated Serviceを設定します。](#)

[ステップ5：証明書と秘密キーをアップロードします。](#)

[ステップ6：アップロードした証明書情報を確認します。](#)

[ステップ7:\[SUBMIT \(送信\)\]ボタンをクリックします。これが最終結果です。](#)

[ステップ8:Akamai Connectを有効にします。](#)

[ステップ9：ブランチWAASでSSLインターポーザを有効にします \(シングルサイド設定でのみ必要\)。](#)

[確認](#)

[ステップ1：ブランチWAASでAkamai Connectを有効にする必要があります。](#)

[ステップ2：クライアントでYoutubeアクセラレーションを確認します。](#)

[ステップ3:WAASで確認します。](#)

[トラブルシュート](#)

[問題：トラフィックはSSL AOによって加速されません。](#)

[問題：ブラウザがYoutubeに接続できず、プッシュされた証明書がありません。](#)

[問題：トラフィックはAkamai Connect Engineにヒットしますが、キャッシュヒットはありません。](#)

[問題：Akamai Cacheは、認証でプロキシを通過するときにHTTPS接続を切断します。](#)

概要

このドキュメントでは、Akamai Connect機能を使用してCisco Wide Area Application Services(WAAS)でYoutube Accelerationを設定するために必要な手順について説明します。

注：この記事では、WAASデバイスという用語を使用して、ネットワーク内のWAAS Central ManagerとWAEを総称しています。WAE (ワイドエリアアプリケーションエンジニア) とは、WAEおよびWAVEアプライアンス、WAASを実行するSM-SREモジュール、およびvWAASインスタンスを指します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco WAAS
- 公開キーインフラストラクチャ
- セキュアソケットレイヤ(SSL)証明書

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

- Cisco WAAS/バージョン5.5.1
- Cisco WAAS/バージョン6.2.1

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

背景説明

Akamai ConnectおよびWAAS

Akamai Connect機能は、Cisco WAASに追加されるHTTP/Sオブジェクトキャッシュコンポーネントです。既存のWAASソフトウェアスタックに統合され、HTTPアプリケーション最適化を介して活用されます。Akamai Connectは、ビジネスおよびWebアプリケーションのHTTP/Sトラフィックの遅延を削減し、POS(Point of Sale)、HDビデオ、デジタルサイネージ、店舗内注文処理などの多くのアプリケーションのパフォーマンスを向上させます。WANデータの大幅なオフロードを実現し、DRE（重複排除）、LZ（圧縮）、TFO（トランスポートフロー最適化）、SSLアクセラレーション（セキュア/暗号化）などの既存のWAAS機能と互換性があります。

これらの用語は、Akamai ConnectおよびWAASで使用されます。

- Akamai Connect: Akamai Connectは、Cisco WAASに追加され、既存のWAASソフトウェアスタックに統合され、HTTP Application Optimizerを介して活用されるHTTP/Sオブジェクトキャッシュコンポーネントです。Akamai Connectを搭載したWAASは、ビジネスおよびWebアプリケーションのHTTP/Sトラフィックの遅延を低減するのに役立ちます。
- Akamai Connected Cache - Akamai Connected CacheはAkamai Connectのコンポーネントで、キャッシュエンジン(CE)がAkamai Intelligent Platform上のエッジサーバによって配信されるコンテンツをキャッシュできるようにします。

設定

ステップ1：内部/パブリックCAによって署名されたSSL証明書が必要です。

証明書には、次のSubjectAltNameを含める必要があります。

*.youtube.com

*.googlevideo.com

*.ytimg.com

*.ggpht.com

youtube.com

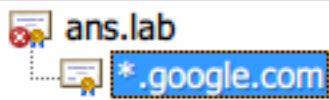
次に証明書の例を示します。

Certificate



General Details Certification Path

Certification path



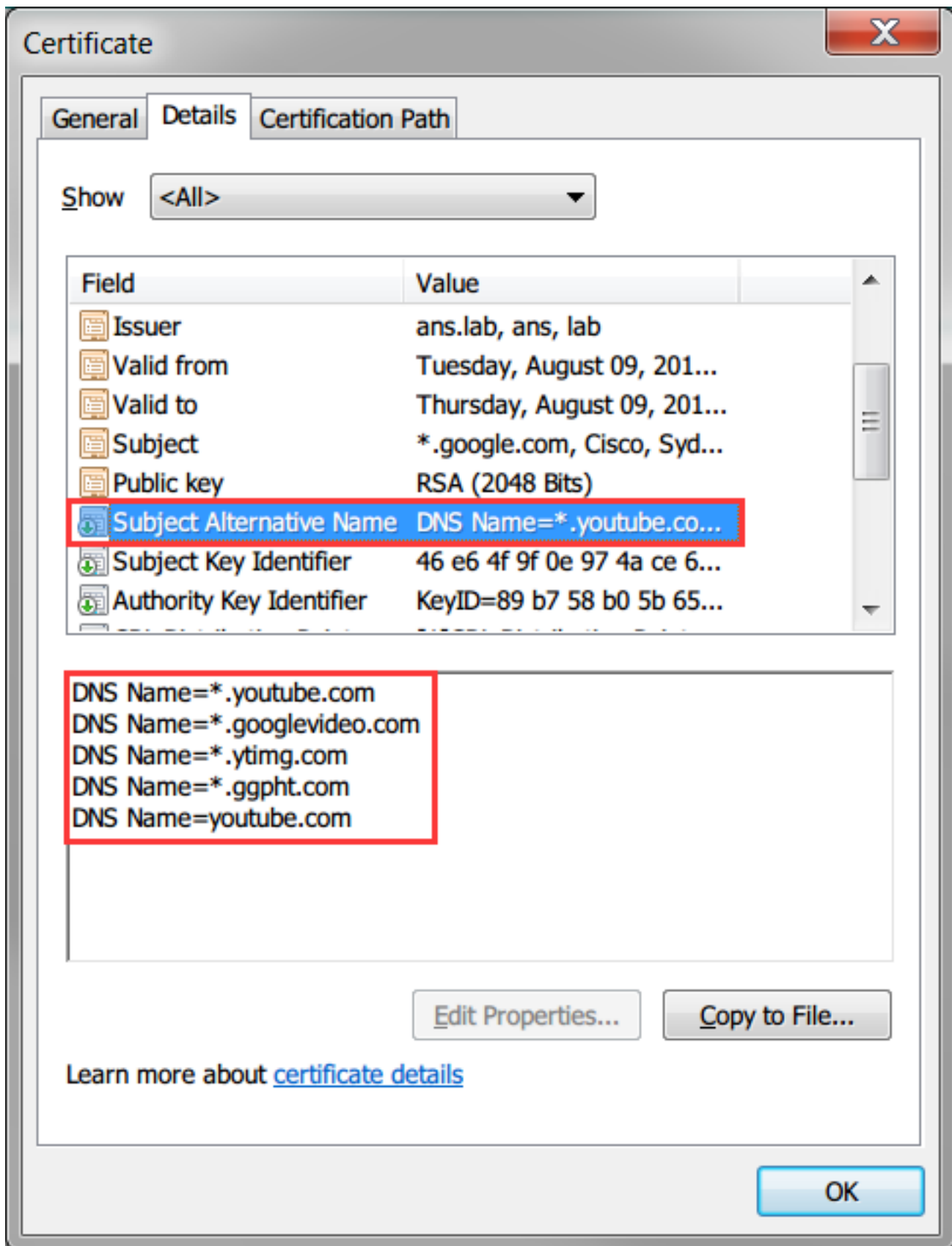
View Certificate

Certificate status:

This certificate is OK.

Learn more about [certification paths](#)

OK



ステップ2：組織の中間またはルート認証局(CA)を信頼する必要があります。

これは、Active Directoryドメイン全体でグループポリシーを使用することで実現できます。

ラボでこの設定をテストする場合は、中間CAまたはルートCAを信頼できるCAとしてクライアントデバイスにインストールできます。

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

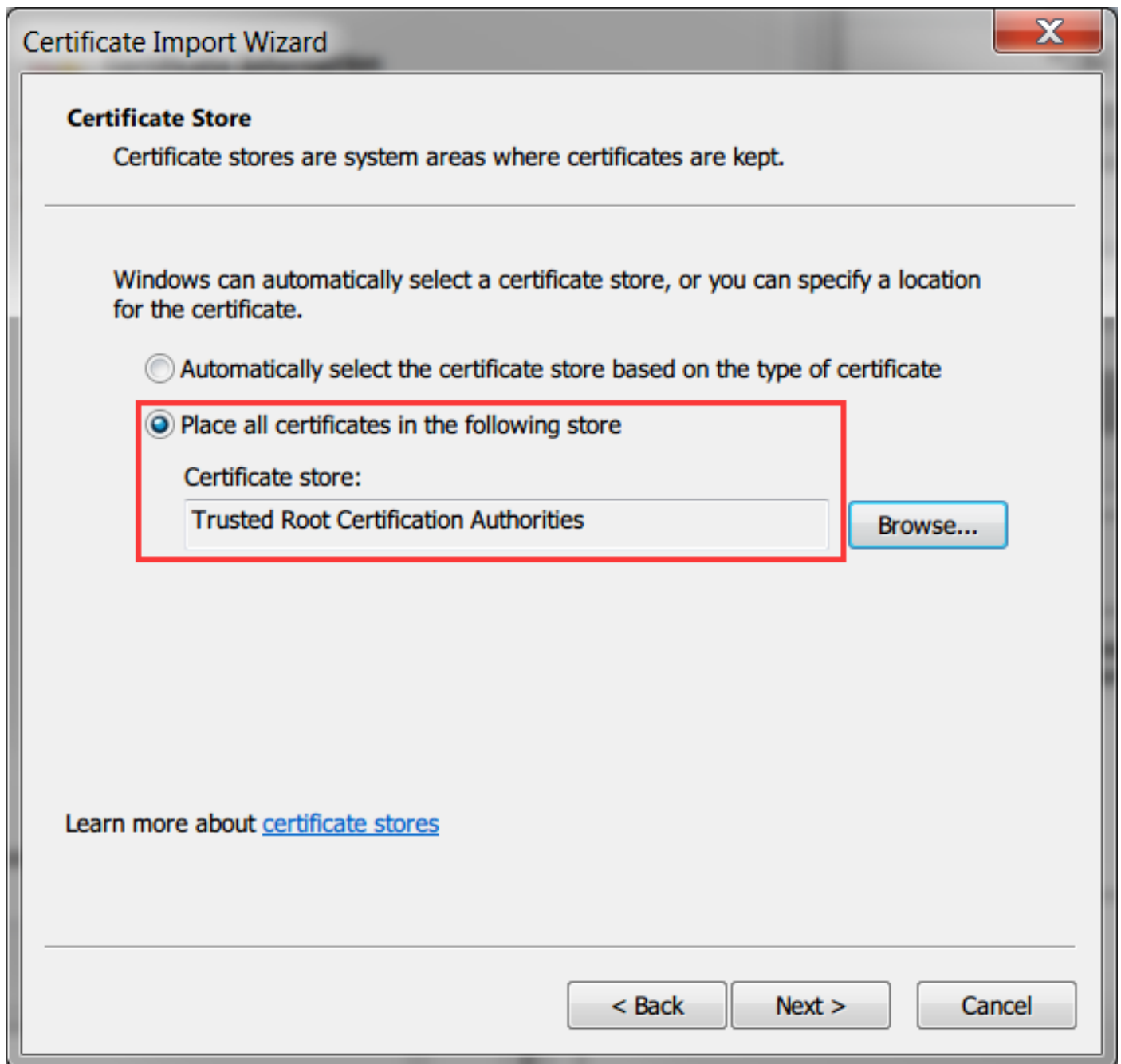
Valid from 8/ 8/ 2016 **to** 8/ 8/ 2021

[Install Certificate...](#)

[Issuer Statement](#)

Learn more about [certificates](#)

OK



ステップ3:WAAS Central Manager GUIを使用して、WAASデバイスでSSLアクセラレーションサービスを作成します。

デュアルサイドAkamai(WAAS 6.2.3より前)で、コアWAASにSSLアクセラレーションサービスを設定します。シングルサイドAkamai(WAAS 6.2.3以降)の場合、ブランチWAASでSSLアクセラレーションサーバを設定し、SSLインターポーザを有効にします。これは、デュアルサイド設定とシングルサイド設定の唯一の違いです。

注：6.2.3より前のソフトウェアリリースを実行しているWAASでは、Youtubeトラフィックを高速化するためにAkamaiのデュアルサイドセットアップが必要です。コアWAASは、YoutubeへのSSL接続をプロキシします。ソフトウェアリリース6.2.3以降を実行しているWAASは、SSL AO v2(SAKE)をサポートしています。これにより、ブランチWAASは、データセンターのインフラストラクチャを経由せずにトラフィックをインターネットに直接送信するときに、SSL接続をプロキシできます。

図に示すように、[Devices] > [Configure] > [Acceleration] > [SSL Accelerated Service]に移動しま

す。

Devices | AppNav Clusters | Locations

Configure | Monitor | Admin

- 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

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

ステップ4:SSL Accelerated Serviceを設定します。

明示的なプロキシを使用する場合は、プロトコルチェーンを有効にする必要があります。HTTP AOは、トラフィックのプロキシに使用されるTCPポート（80や8080など）に適用する必要があります。

Match Server Name Indicationをチェックする必要があります。この設定では、コアWAASがSSLトラフィックを受信すると、Client HelloのSNIフィールドと、アップロードされた証明書のSubjectAltNameを比較します。SNIフィールドがSubjectAltNameと一致する場合、コアWAASはこのSSLトラフィックをプロキシします。

Basic Advanced

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

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:

Server Address/Ports		
☐	Type	Address
☐		

[サーバ名の指示の一致]フィールドがオンの場合は、IPAddressにはAny、Server Portには443を使用します。このエントリを追加するには、[追加]をクリックします。

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

サーバ名表示(SNI)

ステップ5：証明書と秘密キーをアップロードします。

証明書と秘密キーを指定する必要があります。図に示す例では、PEM形式を使用しています。

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

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

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](#)

ステップ6 : アップロードした証明書情報を確認します。

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		

ステップ7:[SUBMIT (送信)]ボタンをクリックします。これが最終結果です。

SSL Accelerated Services for WAE, DC-WAVE-7571

CreateRefreshPrint

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: 25Go

	Name	Service Address/Port	Issued To	Issuer	Expiry Date	Service Status
	Youtube-OTT	Any:443		ans.lab	Aug 08 2018	Enabled

ステップ8: Akamai Connectを有効にします。

[Devices] > [Configure] > [Caching] > [Akamai Connect]に移動します。

Cache Settings
Cache Prepositioning

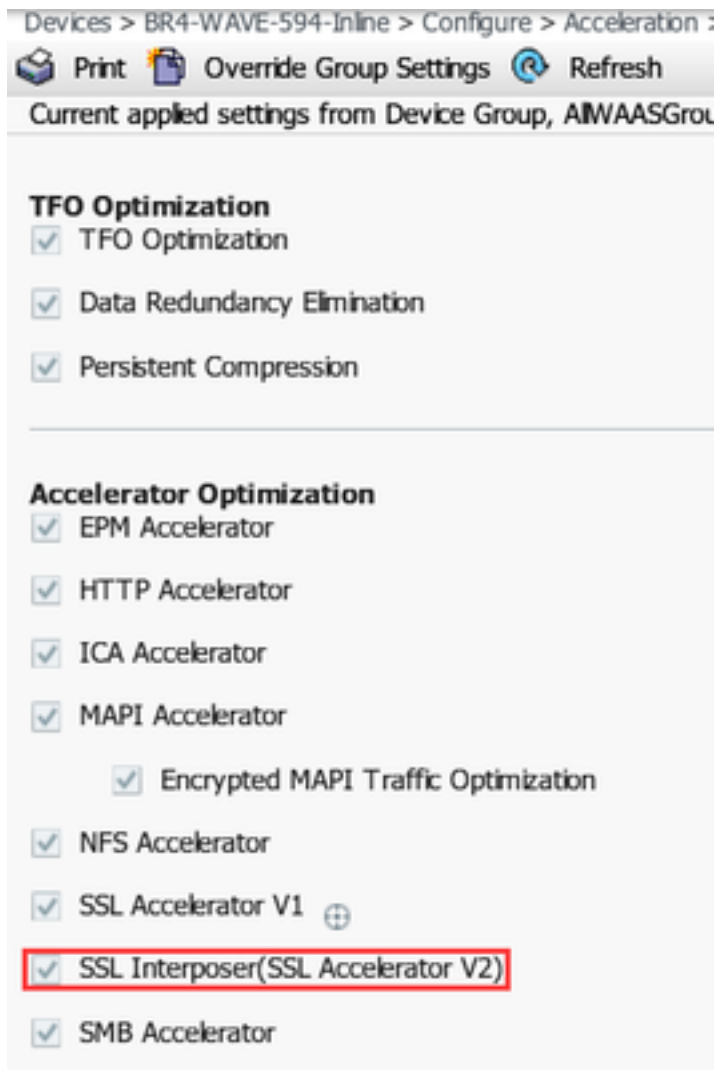
☒ Enable Akamai Connect

▼ Edit Settings

☒ Akamai Connected Cache

☒ Over the top Cache

ステップ9 : ブランチWAASでSSLインターポーザを有効にします (シングルサイド設定でのみ必要) 。



確認

ステップ1：ブランチWAASでAkamai Connectを有効にする必要があります。

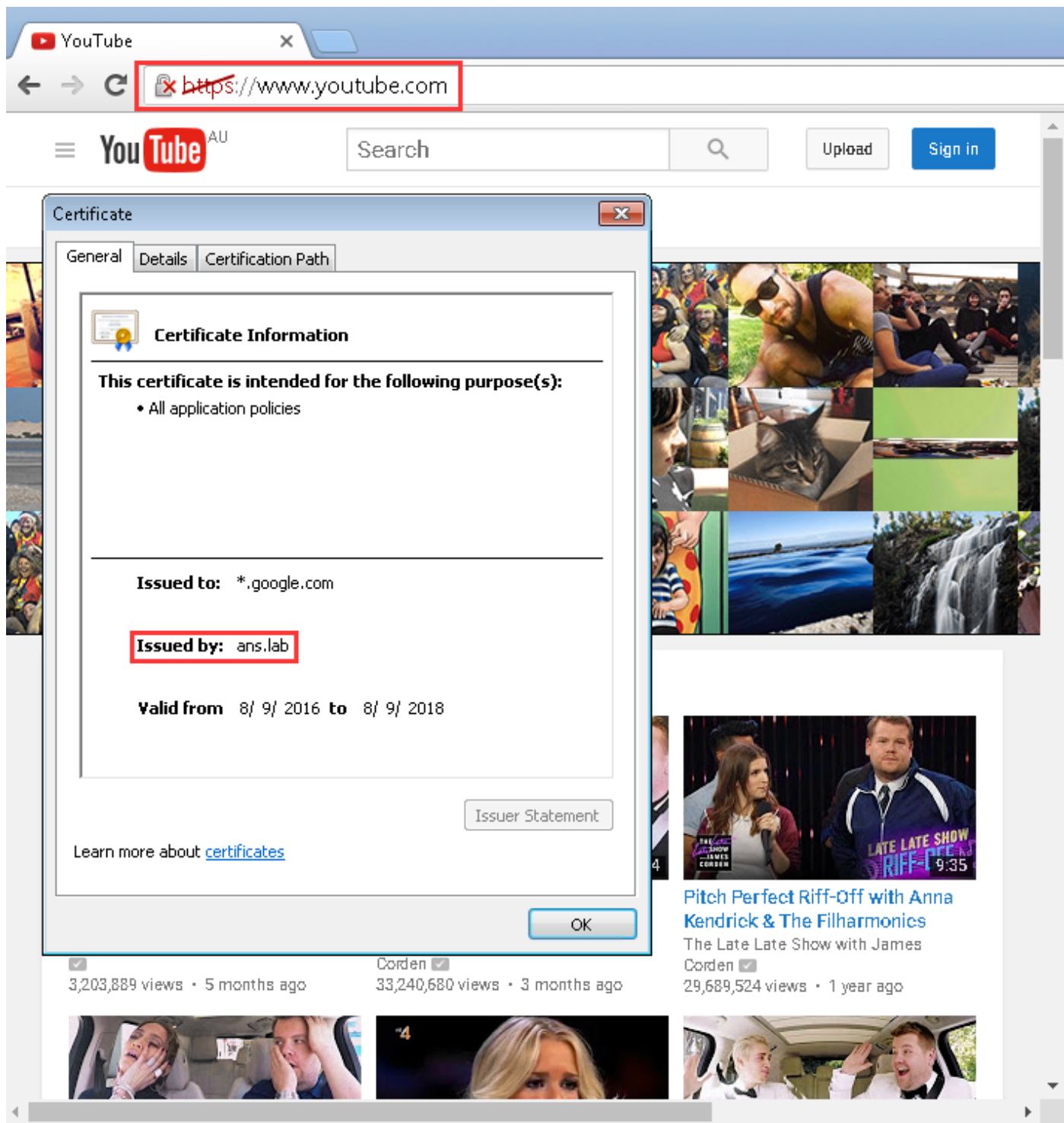
WAAS-BRANCH# show accelerator http object-cache

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

[Operational State]が[Running]、[Connect State]が[Connected]であることを確認します。

ステップ2：クライアントのYoutubeアクセラレーションを確認します。

Youtubeにアクセスすると、自分のCAによって署名された証明書が表示されます。



ステップ3:WAASで確認します。

SSL AOがトラフィックに正しく適用されているかどうかを確認します。

6.2.3 (SSL AO v1およびデュアルサイト設定) より前のWAASソフトウェアを実行したときのCLIからの出力例

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%

WAASソフトウェア6.2.3以降 (SSL AO v2およびシングルサイト設定) を実行している場合のCLIからの出力例

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%

ブランチWAASのce-access-errorlogを確認します。最適化されたトラフィックのログエントリには、10000というコードが関連付けられています (OTT-Youtubeに分類されます)。h - - 200は、オブジェクトキャッシュがヒットし、トラフィックがローカルで処理されることを示します。Google Videoでは最も高速化が期待されます。テストマシンで複数のブラウザを開き、同じビデオを同時に再生してセットアップをテストできます。

ce-errorlogの出力例 :

```
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&requiressl=yes&initcwn
dbps=6383750&gir=
yes&sparams=crlen%2Cdur%2Ceir%2Cgir%2Cid%2Cinitcwndbps%2Cip%2Cipbits%2Citag%2Ckeepalive%2Clt%2Cmi
me%2Cmm%2Cmn%2Cms
%2Cmv%2Cpl%2Crequiressl%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&crlen=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&requiressl=yes&initcwn
dbps=6383750&gir=
yes&sparams=crlen%2Cdur%2Ceir%2Cgir%2Cid%2Cinitcwndbps%2Cip%2Cipbits%2Citag%2Ckeepalive%2Clt%2Cmi
me%2Cmm%2Cmn%2Cms
%2Cmv%2Cpl%2Crequiressl%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&crlen=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 - -
```

show statistic acceleration http object-cacheの出力にも、show ott-youtube hits increasing:

```
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  
.....
```

トラブルシューティング

問題：トラフィックはSSL AOによって加速されません。

解決方法:

次のdebugコマンドを使用して、SSL AOがコアWAASのSNIと一致するかどうかを確認します。

ssl-errorlogからの正常な出力の例を次に示します。

```
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]
```

ssl-errorlogからの出力が失敗した例を次に示します。

```
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：ブラウザがYoutubeに接続できず、プッシュされた証明書がありません。

ソリューション：

これは、コアWAASがYoutubeによってプッシュされた証明書を信頼していないことが原因である可能性があります。

SSL accelerated serviceの場合は、このチェックボックスをオフにします。

SSL Accelerated Service

Basic **Advanced**

SSL Settings

SSL version: Inherited

CipherList: Inherited Create New

CipherList Configured

CipherList Name: Inherited

Cipher list Configured

	Priority
☐	
☐	1
☐	1
☐	1
☐	1
☐	1
☐	1
☐	1

Authentication

☐ Verify client certificate

☐ Disable revocation check of client certificates

☐ Verify server certificate

☐ Disable revocation check of server certificates

問題：トラフィックはAkamai Connect Engineにヒットしますが、キャッシュヒットはありません。

ソリューション：

これは、ブランチWAASでIf-Modified-since(IMF)チェックを実行することによって発生する可能性があります。IMSオプションは、ユーザのアクティビティのプロキシサーバまたは使用状況分析デバイスへの強制ログインをチェックできます。IMSチェックが有効な場合、現在のOTTバージョンでは、Youtubeは常にクライアントにオリジンサーバから最新のコピーを取得するように要求します。

これは、ce-access-errorlogで確認できます。

```
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
1&ms=au&ei=a8i0V-
HZG4u24gL-hpu4BQ&mn=sn-jpuxj-
coxe&mm=31&key=yt6&sparams=clen%2Cdur%2Ce%2Cgir%2Cid%2Cinitcwndbps%2Cip%2Cipbits%2C
itag%2Ckeepalive%2Clmt%2Cmime%2Cmm%2Cmn%2Cms%2Cmv%2Cpl%2Crequires%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=youtu
tube&dur=308.475&id=o-ABCCHl2_QzDMemZ8Eh7hbsSbhXZQ7yt325a-
```


xfqNR0k1&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 - -

IMSチェックを無効にするには、ブランチWAASで次のチェックボックスをオフにします。

[Configure] > [Caching] > [Akamai Connect]に移動します。

Cache Settings

Cache Prepositioning

☒ Enable Akamai Connect

[▶ Edit Settings](#)

▼ Advanced Cache Settings

Default Transparent Caching Policy: *

Standard ▼

Site Specific Transparent Caching Policy

 Add Site Specific Transparent Caching Policy

 Edit

 Delete

	☐ Hostname/IP	Transparent Caching Policy	
1	☐ broomenorthp...	Bypass	

☐ Force IMS DIA ?

☐ Force IMS Always ?

☐ Use HTTP Proxy for connections to Akamai network ?

この問題は、WAAS 6.3以降で修正される予定です。

問題： Akamai Cacheは、認証でプロキシを通過するときにHTTPS接続を切断します。

ソリューション：

インターネットにアクセスする前にプロキシを通過する必要があり、プロキシで認証が必要な場合、WAASによってHTTPS接続が切断される可能性があります。ブランチWAASで取得されたパケットキャプチャは、サーバサイトからのHTTP 407の応答を示します。ただし、最初のパケットの後にキャプチャが停止します。後続のパケットは送信されず、応答は不完全です。

これは[CSCva26420](#)不具合で追跡され、WAAS 6.3リリースで修正される可能性があります。