# Cisco FireSIGHT システムの SSL 検査ポリシーの設定

# 内容

#### <u>概要</u>

前提条件 使用する<u>コンポーネント</u> 設定 1.復号化と再署名 <u>オプション1:FireSIGHT Center をルート認証局(CA)として使用する</u> オプション2:内部 CA に証明書に署名してもらう オプション 3: CA 証明書とキーをインポートする 2.既知のキーで復号化 既知の証明書のインポート(復号化と再署名の代替手段) その他の設定 確認 **Decrypt - Resign Decrypt - Known Certificate** トラブルシューティング 問題1:一部の Web サイトを Chrome ブラウザでロードできない 問題2:一部のブラウザでサイトの信頼性に関する警告/エラーが表示される 参考資料 関連するシスコ サポート コミュニティ ディスカッション

## 概要

この SSL 検査機能により、暗号化トラフィックを検査せずにブロックするか、暗号化/復号済み トラフィックをアクセス制御で検査するかを選択できるようになります。このドキュメントでは 、Cisco FireSIGHT システムに SSL 検査ポリシーをセットアップするための設定手順を説明しま す。

# 前提条件

### 使用するコンポーネント

- Cisco FireSIGHT Management Center
- Cisco FirePOWER 7000 または 8000 アプライアンス
- ・ソフトウェア バージョン 5.4.1 以降

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。 警告:管理対象デバイスで SSL 検査ポリシーを適用すると、ネットワークのパフォーマンスに影響を及ぼす可能性があります。

# 設定

以下の方法で、トラフィックを復号化するための SSL 検査ポリシーを設定することができます。 1.復号化と再署名:

•オプション1: FireSIGHT Center をルート認証局(CA)として使用する

•オプション2:内部 CA に証明書に署名してもらう

•オプション 3: CA 証明書とキーをインポートする 2.既知の証明書で復号化:

• FireSIGHT Management Center にログインし、[Objects] に移動します。

• [Objects] ページで [PKI] を展開し、[Internal CAs] を選択します。

#### 1.復号化と再署名

オプション1: FireSIGHT Center をルート認証局(CA)として使用する

i. [Generate CA] をクリックします。

	🕕 Health	System	Help 🔻	admin 🔻
Generate CA	Import	CA 🔍 F	ilter	

ii.関連情報を入力します

Name:	InternalCA	
Country Name (two-letter code):	US	
State or Province:	MD	
Locality or City:	Columbia	
Organization:	Sourcefire	
Organizational Unit (Department):	TAC	
Common Name:	InternalCA	

iii.[Generate self-signed CA]をクリックします。

オプション 2:内部 CA に証明書に署名してもらう

i.[Generate CA] をクリックします。

🕕 Health System Help 🔻	admin 🔻
🕒 Generate CA 💽 Import CA 🤍 Filter	

ii.関連情報を入力します。

Name:	InternalCA	
Country Name (two-letter code):	US	
State or Province:	MD	
Locality or City:	Columbia	
Organization:	Sourcefire	
Organizational Unit (Department):	TAC	
Common Name:	InternalCA	

**注**:CA 管理者に問い合わせて、署名要求のテンプレートがあるかどうか確認する必要があ る場合もあります。

iii.—BEGIN CERTIFICATE REQUESTと – END CERTIFICATE REQUESTを含む証明書全体をコ ピーして、.req拡張子を持つテキストファイルに保存します。

enerate Internal Certificate Authority	? ×
▲ Subject:	
Common Name: InternalCA	
Organization: Sourcefire	
Organization Unit: TAC	
CSR:	
BEGIN CERTIFICATE REQUEST	
MIIB4zCCAUwCAQAwZTELMAkGA1UEBhMCVVMxCzAJBgNVBAgMAk1EMREwDwYDVQQH	
EQYDVQQDDApJbnRicm5hbENBMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC5	w
XTQjxBMnyPNmGTvAXrqG7LhXPXxZ7igF6MfKxwLh8rVwoejHhwbAUro8ju/R3Ig7	
LSHey3dI0K5SXNKtTb8vBV97RYAfX4VDR7iVDKwxzQIDAQABoD4wPAYJKoZIhvcN	
AQkOMS8wLTAdBgNVHQ4EFgQUih/JeYfJm2itIE3spLdPqzpTXGkwDAYDVR0TBAUw	-
MARE DO AND DATING THE REPORT OF A DATA STRUCTURE AND THE AND THE	

**注:** CA 管理者が .req とは別のファイル拡張子を要求する場合があります。

#### オプション3: CA 証明書とキーをインポートする

	🕕 Health	System	Help 🔻	admin 🔻
💿 Generate CA	💿 Import	CA 🔍 F	ilter	

i.[Import CA] をクリックします。

ii.証明書を参照または貼り付けます。

iii.秘密キーを参照または貼り付けます。

iv.[Encrypted] チェックボックスをオンにして、パスワードを入力します。

Import	Internal Certificate Au	thority		? ×
Name:	Win2008R2			
Certifica	te Data or, choose a file:	Browse		
HIDYT MRMWE ALUEAX MINAME MRXWE MRXWE MIBCO X9UEQC ob8YEX	IN CERTIFICATE CCAkmoAwIBAgIOCT2sLHNRsZ QYKCZImiZPyLGOBGRYDY29tM MNemVyZy1XSU4wOC1DDTAe MxEzARBgoJkiaJk/IsZAEZFoNt NYDVQQDEw16ZXJnLVdJTJA4LJ (CAQEAzreGkBhtUBogN+wNU) J3crg7ykhmP4DgDuzUJSamSsy 1r0suAhVw+ZFPjE1aJ86iGtN6	k86e0.22.4MMoiANBokahkiG9w0BAQUFAD RQwEgYKCZImiZPyLGOBGRYEemVy2zEW Fw0xNTA1MzEwNzA2MINaFw0yMDA1MzE 20xFDA5BgoJkiaJk/IsZAEZFgR6ZXJn INBMIIBIJANBgkohkiG9w0BAQEFAAOCAQ K6BgbDyCYNmEKinVUPTOJHwEL3MKbz+ VI+he9Whxx5NQZyNx5s3faAOSPngGAvfI JM+SB3cGgoomNiFW+fmJe4zclEyUpcYF	BD MBOG wNzE2 8A ox MXV	•
Key or,	choose a file: Browse			
BEG MIIEval ZA1SW aZKxa3 aIa03al AgbJEK NaUy91 JmD/1+ tV391+	IN PRIVATE KEY BADANBokohkiG9w0BAQEFAAS MroGBs0BJo2YQQOdVQ9M4kfA 6F71aHHHk1Bm83Hmzd9oA5I Isz5IHdwaqiiY2IVb5+Yl7INvUT 6n9SR7pBTIHwzPLZJJcvAgMy/ UpfHgCtycS5MViyZ1+0BU12B AvAgMBAAECogEAZZW0ZRUTS IY2U3U5yQE9w6Bciux8LxI3D	CBKgwggSkAgEAAoIBAQDOt4aQGG1OGr QxcwpyP6JHH1OSAZdyuryKSGY/gOAOZN +eAYC98xdWeHxgXHWySy4CEXD5kU+M JSlxgUvOwzfGFr8tczDkEky+8yGSluY LEe9o9GpyRkgwKQfHnRObyJm2Ja0NtgPv LaWnGOWSShIZRIVO2WedOE8R4ZTSWt y9JNVgNG+CCphflhCZZyg1mMKeZ4++E 2K06Z3HZ1VvOe8skTUICMuYCyfk6/dmE	nA3 QU TVonz QG fPT4	•
Encr	ypted, and the password is:	•••••		
			Save Cance	•

**注**: パスワードがない場合は、[Encrypted] チェックボックスをオンにしてパスワード フィールドを空白のままにします。

2.既知のキーで復号化

#### 既知の証明書のインポート(復号化と再署名の代替手段)

i.左側の [Objects] ページで [PKI] を展開し、[Internal Certs] を選択します。

ii.[Add Internal Cert]をクリックします。

iii.証明書を参照または貼り付けます。

iv.秘密キーを参照または貼り付けます。

v. [Encrypted]ボックスに**チェック**を入れ、パスワードを入力します。

id Kno	own Internal Certificate	? ×
lame:	KnownCert	
Certifica	te Data or, choose a file: Browse	
BEG MIIDOD JZELMA (2VmaX MDZaFw MASGA1 A1RBQ2 AQEAxA	IN CERTIFICATE CCAIACCQDssfBhdDsHTDANBgkghkiG9w0BAQUFADBeMQswCQYDVQQGEwJV kGA1UECAwCTUQxETAPBgNVBAcMCENvbHVtYmlhMRMwEQYDVQQKDApTb3Vy JIMQwwCgYDVQQLDANUQUMxDDAKBgNVBAMMA1RBQzAeFw0xNTA2MDgxNzA4 0xODazMDQxNzA4MDZaMF4xCzAJBgNVBAYTAIVTMQswCQYDVQQIDAJNRDER UEBwwIQ29sdW1iaWExEzARBgNVBAoMCINvdXJj2WZpcmUxDDAKBgNVBAsM EMMAoGA1UEAwwDVEFDMIJBIJANBgkghkiG9w0BAQEFAAOCAQ8AMIJBCgKC kHMrRPPyysIwkgwAH0ELtIHmYQ3/i+MgMzmQiuAhrE3AZmh7t6BZQrwFgK	Î
ey or,	choose a file: Browse	
BEG MIEpAI 776820 vG5wco FX8WV AtH/eN fonbuE	IN RSA PRIVATE KEY BAAKCAQEAxAkHMrRPPyysIwkgwAH0ELtHmYQ3/i+MgMzmQiuAhrE3AZm pwFgKeMX1KV7LuxXnsuJfpNk3Dp8fm33TMJQiuAZW6zpusjgOKS3yUs4E MVe/baDT2B/XQt3BLUgLsL+TPipUgazzrPt3rOECvroPxDRCQ/fz8AzXJV Jt3SqYttpw41vU9gai2OuVaANrIB5iz+9NnwNTpVGvrwHx+iOI/e2ZARI1 9+/p66tUSILV23rUKUKM0gkh8IPs2mu17Upgqv3uYW2OWvnQsz41CGzht UCpEtDWctl/P2rriWECMsumJN7hNfKQIDAQABAoIBACJSNH5DhYkDNWkq	Â
Enco	and and the parsword in	¥
- Entry		
	Save	Cancel

注:パスワードがない場合は、[Encrypted] ボックスを空白のままにします。

4.「ポリシー」>「SSL」に移動し、「新規ポリシー」をクリックします。

Overview Analysis Policies Devices Objects AM		🕔 Health System He	sp <b>v admin v</b> ql
Access Control Intrusion • Files Network Discovery	SL Application Detectors Users Correlation	Actions •	
		Compare Policies	O New Policy
SSL Policy		Last Modified	
SSL Policy		2015-06-02 03:43:44	B 2 8
New SSL Policy		? ×	
Name:			
Description:			
Default Action:	Block O Block Block with reset		
	Save	Cancel	

5.名前を指定し、「デフォルト・アクション」**を選択します**。SSL ポリシー エディタ ページが表 示されます。SSL ポリシー エディタ ページは、アクセス コントロール ポリシー エディタ ペー ジと同じように機能します。

**注**: [Default Action] に何を選択してよいかわからない場合、出発点として [Do not decrypt] をアクションとして選択することを推奨します。

6. SSLポリシーエディタページで、[ルールの追加]をクリ**ックします**。[Add Rule] ウィンドウで、 ルールに名前を付けて、その他すべての該当する情報を入力します。

Add Rule						? ×
Name Resign		🕑 Ena	bled	Insert below rule	▼ 1	
Action Do not decrypt	<b>*</b>					
Zone 🔂 Decrypt - Resign	Users Applications	Ports Category	Certificate DN	Cert Status Cipher S	uite Version	Logging
Available into the Do not decrypt		Source Zo	nes (0)	De	estination Zones (0)	
Sear 🗙 Block		any		a	ny	
🐴 701( 💢 Block with reset						
為 701( 👃 Monitor						
🔔 📐 External						
A HomeSet		Add to				
station and the second		Source				
		Add to				
					A	dd Cancel

次のセクションで、[Add Rule] ウィンドウで提供されるさまざまなオプションについて説明します。:

アクション

#### Decrypt - Resign

• 中間者(MitM)として機能するセンサーが、ユーザとの接続を受け入れてから、サーバへの新しい接続を確立します。以下 に、いくつかの例を示します。ユーザがブラウザに https://www.facebook.com と入力します。このトラフィックがセンサー に到達すると、センサーは選択された CA 証明書を使用してユーザとネゴシエートし、SSL トンネル A を確立します。それ と同時にセンサーは https://www.facebook.com に接続し、SSL トンネル B を確立します。

- 最終結果:ユーザには Facebook の証明書ではなく、ルールに含まれる証明書が表示されます。
- このアクションには内部CAが必要です。キーを置き換える場合は、「キーの置き換え」を選 択します。ここで選択した証明書がユーザに送信されます。

**注**: このオプションはパッシブ モードでは使用できません。

#### **Decrypt - Known Key**

- トラフィックの復号化に使用するためのキーは、センサーが保持します。以下に、いくつかの例を示します。ユーザがブラ ウザに https://www.facebook.com と入力します。このトラフィックがセンサーに到達すると、センサーはトラフィックを復 号化してから、トラフィックを検査します。
- 最終結果:ユーザには Facebook の証明書が表示されます
- このアクションには内部証明書が必要です。内部証明書を追加するには、[Objects] > [PKI] > [Internal Certs] の順に選択します。

注: ドメインおよび証明書の所有者は、所属組織でなければなりません。facebook.com を 例として取り上げると、エンドユーザに Facebook の証明書が表示されるのは、組織が実際 にドメイン facebook.com の所有者であり(つまり、所属企業が Facebook, Inc であること )、パブリック CA によって署名された facebook.com 証明書の所有権を持っている場合の みです。復号化できるのは、所属組織が所有するサイトの既存のキーを使用する場合のみで す。

既知のキーを使用して復号化する主な目的は、HTTPS サーバへのトラフィックを復号化して、社 内サーバを外部の攻撃から保護することです。外部 HTTPS サイトへのクライアント側トラフィ ックを検査する場合は、外部サーバに対する所有権はなく、ネットワーク内で外部の暗号化サイ トに接続するクライアント トラフィックを検査することが目的であるため、復号化および再署名 を使用します。

**注**: DHE と ECDHE で復号化するには、双方の協力が必要です。

#### Do Not Decrypt

SSL ポリシーはバイパスしてアクセス コントロール ポリシーをトラフィックに適用します。

証明書

特定の証明書を使用して、SSLトラフィックにルールが適用されます。

Zones Network	s VLAN Tags	Users	Applications	Ports	Category	Certificate	DN	Cert Status	Cipher Suite	Version	Logging
Available Certificates	c				0		Selec	cted Certificates	: (0)		
Search by name o	r value						any				
						Add to Rule					

DN

証明書内の特定のドメイン名を使用して、SSL トラフィックにルールが適用されます。

Zones	Networks	VLAN Tags	Users	Applications	Ports	Category	Certificate	DN	Cert Status	Ciphe	r Suite	Version	Logging
Available D	kvailable DNs 🖒 🔘		Subject DI	Subject DNs (0)			Issuer DNs (0)						
🔍 Search	by name or va	slue				any					any		
Source	fire Undecrypt	able Sites											
🚍 CN=*.4	citrixonline.com	n											
🚍 CN=*.4	fata.toolbar.ya	hoo.com											
🚍 CN=*.!	edoraproject.o	×g											
🚍 (N=*.)	tunes.apple.co	om			dd to								
🚍 CN=*J	logmein.com												
🚍 CN=*./	mozilla.org												
🚍 CN="./	rhn.redhat.com	n											
🚍 CN=".4	sls.microsoft.c	om											
🚍 CN=*u	pdate.microsol	ft.com											
CN=ac	count.live.com												
🚍 Google													
						Enter DN o	er CN				Enter D	N or CN	Add

#### Cert Status

#### 以下の証明書ステータスに基づいて、SSL トラフィックにルールが適用されます。

Zones	Networks	VLAN Tags	Users	Applications	Ports	Category	Certificate	DN	Cert Status	Cipher Suite	Version
Revoked:			Yes	No Do Not N	latch						
Self-signed	l:		Yes	No Do Not N	1atch						
Valid:			Yes	No Do Not N	1atch						
Invalid sigr	nature:		Yes	No Do Not N	1atch						
Invalid issu	ler:		Yes	No Do Not N	1atch						
Expired:			Yes	No Do Not N	1atch						
Not yet val	id:		Yes	No Do Not N	1atch						
Invalid Cer	tificate:		Yes	No Do Not N	1atch						
Invalid CRI	L:		Yes	No Do Not N	latch						

#### Cipher Suite

#### 以下の暗号スイートを使用して、SSL トラフィックにルールが適用されます。

Zones	Networks	VLAN Tags	Users	Applications	Ports	Category	Certificate	DN	Cert Status	Cipher Suite	Version	Logging
Available	Available Cipher Suites C 🔘					Sel	ected Cipher S	uites (0)				
Search	by name or vi	alue						an	Y			
SSL_RSA_FIPS_WITH_JDES_EDE_CBC_SHA     SSL_RSA_FIPS_WITH_DES_CBC_SHA     TLS_DHE_RSA_WITH_JDES_EDE_CBC_SHA     TLS_DHE_RSA_WITH_AES_128_CBC_SHA												
@ TLS_0 @ TLS_0 @ TLS_0	HE_RSA_WITH HE_RSA_WITH HE_RSA_WITH	(_AES_128_CBC (_AES_128_GC) (_AES_256_CBC	_SHA256 (_SHA256 _SHA				Add to Rule					

#### バージョン

選択したバージョンの SSL を使用した SSL トラフィックだけにルールが適用されます。

Zones	Networks	VLAN Tags	Users	Applications	Ports	Category	Certificate	DN	Cert Status	Cipher Suite	Version
SSL v3.0											
TLS v1.0											
TLS v1.1		<b>√</b>									
TLS v1.2											
		_									

#### Logging

#### SSL トラフィックの接続イベントを確認するには、ロギングを有効にします。

7.[Trusted CA Certificate] をクリックします。ここで、信頼された CA をポリシーに追加します。

Rules Trusted CA Certificates Undecryptable Actions			
Available Trusted CAs 👌	0	Selected Trusted CAs	
🔍 Search		🔁 Sourcefire Trusted Authorities	8
🖶 Sourcefire Trusted Authorities	<b>A</b>		
➢ A-Trust-nQual-01			
➢ A-Trust-nQual-03			

8.[Undecryptable Actions] をクリックします。これらのアクションは、センサーがトラフィック を復号化できない場合に適用されます。定義については、FireSIGHT Management Center のオン ライン ヘルプ([Help] > [Onlinie])を参照してください。

Rules	Trusted CA Certificates	Undecryptable Actions	
Compr	essed Session	Inherit Default Action	~
SSLv2	Session	Inherit Default Action	~
Unkno	wn Cipher Suite	Inherit Default Action	~
Unsup	ported Cipher Suite	Inherit Default Action	•
Sessio	n not cached	Inherit Default Action	•
Handsl	hake Errors	Inherit Default Action	•
Decryp	otion Errors	Block	•

- Compressed Session: SSL セッションでデータ圧縮方式が適用されます。
- SSLv2 Session: セッションはSSLバージョン2で暗号化されます。クライアントのhelloメッ セージがSSL 2.0の場合はトラフィックが復号化され、送信されたトラフィックの残りがSSL 3.0であることに注意してください。
- Unknown Cipher Suite:システムが暗号スイートを認識しません。

- Unsupported Cipher Suite:システムが、検出された暗号スイートに基づく復号化をサポート しません。
- Session not cached: SSL セッションにおいてセッションの再利用が可能になっていて、クライアントとサーバがセッション ID でセッションを再確立したときに、システムがそのセッション ID をキャッシュに入れなかったことを意味します。
- Handshake Errors: SSL ハンドシェーク ネゴシエーション中にエラーが発生しました。
- Decryption Errors: トラフィックの復号化中にエラーが発生しました。

**注**: デフォルトでは、デフォルト アクションが継承されます。デフォルト アクションが [Block] である場合、予期しない問題が発生する可能性があります。

9.ポリシーを保存します。

10.[Policies] > [Access Control] に移動します。ポリシーを編集するか、新しいアクセス コントロール ポリシーを作成します。

11. [Advanced]をクリックし、一般的な設定を編集します。

Overview Analysis Policies Devices	s Objects AM	IP							
Access Control Intrusion ▼ Files M	Network Discovery	SSL	Application [	Dete	ctors	Users	Correlation	Actions 🔻	
TAC Access Control									
Enter a description			-						
Rules Targets (1) Security Intelligence	HTTP Responses	Advance	ed						
General Settings			Ø	_	Trans	port/Net	work Layer	Preprocess	or Se
Maximum URL characters to store in connection events 102				ŧ.	Ignore the VLAN header when tracking connection				
Allow an Interactive Block to bypass blocking for (seconds)					Detection Enhancement Settings				
SSL Policy to use for inspecting encrypted connections Non					Adaptive Profiles				
Inspect traffic during policy apply			Yes		Perfo	mance S	Settings		
Network Analysis and Intrusion Policie	General Setting	s						?	×t
Intrusion Policy used before Access Control r	Maximum UDL share								
aeterninea	connection events	acters to st	ore in	102	24				
Intrusion Policy Variable Set	Allow an Interactive	Block to by	pass blocking	600					
Default Network Analysis Policy	for (seconds)								
Files and Malware Settings	connections	r inspectin <u>i</u>	j encrypteu	SSL	Policy			¥	
Limit the number of bytes inspected when do	Inspect traffic durin	ng policy ap	ply						
Allow file if cloud lookup for Block Malware ta	Revert to Defaults	;					ок	Cancel	

12.ドロップダウンメニューからSSLポリシーを選択します。

13. 「OK」をクリックして保存してください。

#### その他の設定

適切に識別するためには、侵入ポリシーに以下の変更を加える必要ががあります。

i.\$HTTP\_PORTS 変数に、ポート 443 と、ポリシーで復号化する HTTPS トラフィックを受け入 れるその他すべてのポートを含める必要があります([Objects] > [Object Management] > [Variable Set] > [Edit] の順に移動して変数セットを編集します)。

Vetwork	Name		t	escription			
Object Groups	Default Set		,	his Variable Set is provided by Sourcefire.		0	
ty Intelligence	Home Variables					05	l
idual Objects		Edit Veriable HTTP POPTS			2 4		
ct Groups		Edit Variable HTTP_PORTS			2 ×		
idual Obiects		Name: HTTP PORTS					
ct Groups		Type: Port					
ndividual Objects		Available Ports C O	Included Ports (110)	Excluded Ports (0)			
bject Groups		Search by name or value	2 36 A 00	none none			
ation Filters		RADIUS	- 80 				
le Set		JP RIP	2 01 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	8			
rity Zones		n SIP	₩ 83	6			
er Suite List		JP SMTP	se = 1 2 <sup>™</sup> 84	8			
inguished Name			Include 🔗 85	-			
Individual Objects		de SNMP	2 86	8			
Object Groups		🤌 SSH	Exclude 87				
I		Je SYSLOG	88				
location		TCP high ports	89				
		J TELNET	📌 311				
		J TFTP	283				
		Jahoo Messenger Messages	555	<b></b>			
		Yahoo Messenger Voice Chat (TCP)	- dit cont				

ii.暗号化トラフィックを検査するネットワーク分析ポリシーで、HTTP プリプロセッサ設定のポ ート フィールドにポート 443(およびポリシーで復号化する HTTPS トラフィックを受け入れる その他すべてのポート)が設定されている必要があります。そうでないと、HTTP コンテンツ修 飾子(例として、http\_uri、http\_header)付きの HTTP ルールがトリガーされません。なぜなら 、ネットワーク分析ポリシーは定義済み HTTP ポートに依存することから、指定されたポートで 送受信されないトラフィックについては Snort の HTTP バッファに入れられないためです。

iii.(オプションですが、より良い検査のために推奨)両方のポートでストリームの再構成を実行 するフィールドのTCPストリームの構成**設定にhttpsポートを追加**します。

iv.スケジュールされたメンテナンス時間帯に、変更されたアクセスコントロールポリシーを再適 用します。

**警告:この変更**されたポリシーは、パフォーマンスの重大な問題を引き起こす可能性があり ます。実稼働時間外にポリシーをテストして、ネットワークの停止やパフォーマンスのリス クを減らしてください。

#### 確認

Decrypt - Resign

1. Webブラウザを開きます。

**注:次**の例では、Firefoxブラウザを使用しています。 この例は、Chrome では機能しない 可能性があります。詳細については、「トラブルシューティング」のセクションを参照して ください。

2. SSL Webサイトに移動します。以下の例では、https://www.google.com を使用していますが、 金融機関の Web サイトを使用することもできます。次のようなページが表示されます。

💮 htt	ps://v	vww.goog	le.com/	?gws_rd=ssl
-------	--------	----------	---------	-------------

2	This Connection is Untrusted You have asked Firefox to connect securely to <b>www.google.com</b> , but we can't confirm that you connection is secure.
	Add Security Exception
	You are about to override how Firefox identifies this site. Legitimate banks, stores, and other public sites will not ask you to do this. Server Location: https://www.google.com/?gws rd=ssl Get Certificate
	Certificate Status This site attempts to identify itself with invalid information. <u>V</u> iew
	Unknown Identity The certificate is not trusted because it hasn't been verified as issued by a trusted authority using a secure signature.

**注**:証明書自体が信頼されていない場合、署名付き CA 証明書がブラウザで信頼されていな ければ、上記のページが表示されます。特定のブラウザが、信頼された CA 証明書を判断す る方法については、以下の「信頼された認証局」セクションを参照してください。

t

```
☆ 自 🖡
```

Gmail Images

Google						
Google Search	I'm Feeling Lucky					
Page Info - https://www.google.com/?gws_rd=ssl						
General Media Permissions Security						
Website Identity         Website:       www.google.com         Owner:       This website does not supply ownership information.         Verified by:       Sourcefire						
		View Certificate				
Privacy & History						
Have I visited this website prior to today?	Yes, 277 times					
is this website storing information (cookies) on my computer?	Yes	View Coo <u>k</u> ies				
Have I saved any passwords for this website?	No	Vie <u>w</u> Saved Passwords				
Technical Details						

**注:** このページが表示された場合、トラフィックへの再署名が成功したことを意味します。[Verified by:] セクションに**Sourcefire** と示されていることに注目してください。

#### Could not verify this certificate because the issuer is unknown.

	-
Issued	10
1330.00	

Common Name (CN)	www.google.com
Organization (O)	Google Inc
Organizational Unit (OU)	<not certificate="" of="" part=""></not>
Serial Number	13:E3:D5:7D:4E:5F:8F:E7

#### Issued By

Common Name (CN)	Sourcefire TAC
Organization (O)	Sourcefire
Organizational Unit (OU)	Tac

#### Period of Validity

Begins On	5/6/2015
Expires On	8/3/2015

#### Fingerprints

SHA-256 Fingerprint	20:00:CB:25:13:8B:1F:89:4D:4A:CF:C5:E2:21:38:92: 06:66:00:2E:B7:83:27:72:98:EA:B1:6A:10:B3:67:A1
SHA1 Fingerprint	1B:C2:30:D9:66:84:DB:97:CF:A9:5E:5F:29:DA:4C:3F:13:E9:DE:5D

**注**:上記は、同じ証明書をクローズアップして表示したものです。

3. Management Centerで、[Analysis] > [Connections] > [Events]に移動します。

4.ワークフローによっては、SSL復号化オプションが表示される場合と表示されない場合があり ます。[Table View of Connection Events] をクリックします。

#### Connections with Application Details > Table View of Connection Events

No Search Constraints (Edit Search)

Jump to.	🔻			
	▼ <u>First Packet</u>	Last Packet	<u>Action</u>	<u>Reason</u>

5.右にスクロールし、[SSL Status]を探します。次のようなオプションが表示されます。

<u>443 (https) / tcp</u>	Decrypt (Resign)	HTTPS	Secure Web browser	Skype Tunneling
<u>443 (https) / tcp</u>	Decrypt (Resign)	HTTPS	Secure Web browser	Google

#### Decrypt - Known Certificate

1. FireSIGHT Management Centerで、[Analysis] > [Connections] > [Events]に移動します。

2.ワークフローによっては、SSL復号化オプションが表示される場合と表示されない場合があり ます。[Table View of Connection Events] をクリックします。

#### Connections with Application Details > Table View of Connection Events

#### No Search Constraints (Edit Search)

Jump to.	🔻				
	▼ <u>Fin</u>	st Packet	Last Packet	<u>Action</u>	<u>Reason</u>

#### 3.右にスクロールし、[SSL Status]を探します。次のようなオプションが表示されます。

<u>443 (https) / tcp</u>	🔒 Decrypt (Resign)	HTTPS	Secure Web browser	Skype Tunneling
<u>443 (https) / tcp</u>	Decrypt (Resign)	HTTPS	Secure Web browser	Google

# トラブルシューティング

## 問題1:一部の Web サイトを Chrome ブラウザでロードできない

#### 例

[Decrypt - Resign] が設定されている状態では、Chrome で www.google.com をロードできない場 合があります。

#### 原因

中間者攻撃を防ぐために、Google Chrome ブラウザには、Google の資産に対する不正な証明書 を検出する機能が備わっています。Chrome ブラウザ(クライアント)が google.com ドメイン (サーバ)に接続しようとして、有効な Google 証明書ではない証明書が返された場合、ブラウ ザは接続を拒否します。

#### 解決方法

この問題が発生した場合は、DN=\*.google.com、\*.gmail.com、\*.youtube.comのDo Not Decryptル ールを追加してください。その後、ブラウザのキャッシュと履歴を消去します。

#### 問題 2: 一部のブラウザでサイトの信頼性に関する警告/エラーが表示される

#### 例

Internet Explorer や Chrome を使用してサイトに接続するときはセキュリティ警告が表示されな いのに、Firefox ブラウザを使用すると、ブラウザを閉じて開くたびに接続を信頼することを確認 しなければなりません。

#### 原因

信頼済み CA のリストは、ブラウザに依存します。証明書を信頼しても、その設定はすべてのブ ラウザに伝搬されません。通常、信頼済みエントリは、ブラウザが開いている間だけ存続するた め、ブラウザを閉じると、信頼されたすべての証明書がプルーニングされます。それで、次回ブ ラウザを開いてサイトにアクセスするときには、信頼済み証明書のリストに再度追加する必要が あります。

#### 解決方法

このシナリオでは、IE と Chrome はどちらもオペレーティング システムの信頼済み CA のリスト を使用しますが、Firefox は独自のリストを維持します。そのため、CA 証明書は OS のストアに インポートされても、Firefox ブラウザにはインポートされません。Firefox でセキュリティ警告 が表示されないようにするには、CA 証明書を信頼済み CA としてブラウザにインポートする必 要があります。

#### 信頼された認証局

SSL 接続を確立する際に、ブラウザはまず、サイトの証明書が信頼されているかどうか(つまり 、このサイトに以前アクセスして、ブラウザがこの証明書を信頼するよう手動で設定したかどう か)を検査します。 証明書が信頼されていなければ、ブラウザはこのサイトの証明書を検証した 認証局(CA)証明書を検査します。CA 証明書がブラウザで信頼されている場合、ブラウザはサ イトの証明書を信頼できるものとみなし、接続を許可します。CA 証明書が信頼されていない場 合、ブラウザはセキュリティ警告を表示して、証明書を信頼済み証明書として手動で追加するよ う強制します。

ブラウザ内の信頼済み CA のリストは、そのブラウザの実装に完全に依存し、各ブラウザが取り 込む信頼済み CA のリストは他のブラウザとは異なる場合があります。一般に、信頼済み CA の リストに最近のブラウザがエントリを追加する方法には、次の 2 つがあります。

- 1. オペレーティング システムの信頼済み CA のリストを使用する方法
- 2. 信頼済み CA のリストをソフトウェアで配布し、ブラウザに組み込む方法
- 一般によく使用されるブラウザでは、信頼済み CA には次のようにエントリが追加されます。
  - Google Chrome:オペレーティング システムの信頼済み CA のリスト
  - Firefox: 独自の信頼済み CA のリストを維持
  - Internet Explorer:オペレーティング システムの信頼済み CA のリスト
  - Safari:オペレーティングシステムの信頼済み CA のリスト

クライアント上で見られる動作の違いはこうしたことが要因となるため、この違いを把握するこ とが重要です。たとえば、Chrome および IE に信頼済み CA を追加するには、その CA 証明書を OS の信頼済み CA ストアにインポートする必要があります。CA 証明書を OS の信頼済み CA ス トアにインポートすると、その CA によって署名された証明書を使用するサイトに接続する際に 警告が表示されることはなくなります。Firefox ブラウザでは、ブラウザ自体の信頼済み CA スト アに CA 証明書を手動でインポートする必要があります。インポートした後は、その CA によっ て署名された証明書を使用するサイトに接続する際に警告が表示されることはなくなります。

# 参考資料

• <u>SSL ルールの概要</u>