# Konfiguration einer SSL-Überprüfungsrichtlinie für das Cisco FireSIGHT-System

# Inhalt

Einführung Voraussetzungen Verwendete Komponenten **Konfigurationen** 1. Entschlüsseln und Rückzeichnen Option 1: Verwenden des FireSIGHT Center als Stammzertifizierungsstelle (Certificate Authority, CA) Option 2: Signieren Sie Ihr Zertifikat mit einer internen Zertifizierungsstelle. Option 3: Importieren eines Zertifizierungsstellenzertifikats und -schlüssels 2. Entschlüsseln mit einem bekannten Schlüssel Importieren eines bekannten Zertifikats (Alternative zum Entschlüsseln und Zurücksetzen) Zusätzliche Konfigurationen Überprüfung Entschlüsseln - Zurücksetzen Entschlüsseln - Bekanntes Zertifikat Fehlerbehebung Ausgabe 1: Einige Websites werden möglicherweise nicht im Chrome-Browser geladen Ausgabe 2: Abrufen einer nicht vertrauenswürdigen Warnung/eines nicht vertrauenswürdigen Fehlers in einigen Browsern Referenzen Ähnliche Diskussionen in der Cisco Support Community

# Einführung

Mit der SSL-Überprüfungsfunktion können Sie verschlüsselten Datenverkehr blockieren, ohne ihn zu überprüfen, oder verschlüsselten oder entschlüsselten Datenverkehr mit Zugriffskontrolle überprüfen. In diesem Dokument werden die Konfigurationsschritte zum Einrichten einer SSL-Überprüfungsrichtlinie für das Cisco FireSIGHT-System beschrieben.

# Voraussetzungen

### Verwendete Komponenten

- Cisco FireSIGHT Management Center
- Cisco FirePOWER-Appliances der Serien 7000 oder 8000
- Softwareversion 5.4.1 oder höher

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

**Warnung:** Wenn Sie eine SSL-Überprüfungsrichtlinie auf Ihrem verwalteten Gerät anwenden, kann dies die Netzwerkleistung beeinträchtigen.

## Konfigurationen

Sie können eine SSL-Überprüfungsrichtlinie folgendermaßen konfigurieren, um Datenverkehr zu entschlüsseln:

- 1. Entschlüsseln und Rückzeichnen:
  - Option 1: Verwenden Sie das FireSIGHT Center als Stammzertifizierungsstelle (Certificate Authority, CA), oder
  - Option 2: eine interne Zertifizierungsstelle haben, die Ihr Zertifikat signiert, oder
  - Option 3: Importieren eines Zertifizierungsstellenzertifikats und -schlüssels
- 2. Entschlüsseln mit einem bekannten Zertifikat:
  - Melden Sie sich beim FireSIGHT Management Center an, und navigieren Sie dann zu **Objects**.
  - Erweitern Sie auf der Seite Objekte die PKI, und wählen Sie Interne CAs aus.
- 1. Entschlüsseln und Rückzeichnen

Option 1: Verwenden des FireSIGHT Center als Stammzertifizierungsstelle (Certificate Authority, CA)

i. Klicken Sie auf CA generieren.



ii) Geben Sie die relevanten Informationen ein.

enerate Internal Certificate	Authority	r
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	
C	Consists will size of Ch.	Cancel

iii) Klicken Sie auf Eigensignierte CA generieren.

Option 2: Signieren Sie Ihr Zertifikat mit einer internen Zertifizierungsstelle.

i. Klicken Sie auf CA generieren.

🕕 Health System Help 🔻	admin 🔻
Generate CA O Import CA Silter	

ii) Geben Sie die relevanten Informationen ein.

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	

**Hinweis:**Wenden Sie sich an den Administrator der Zertifizierungsstelle, um festzustellen, ob eine Vorlage für die Signierungsanfrage vorhanden ist.

iii) Kopieren Sie das gesamte Zertifikat einschließlich der - BEGIN CERTIFICATE REQUEST - und —END CERTIFICATE REQUEST - und speichern Sie es dann in einer Textdatei mit der Erweiterung .req.

Generate Internal Certificate Authority	? ×
<ul> <li>Subject:</li> <li>Common Name: InternalCA</li> <li>Organization: Sourcefire</li> <li>Organization Unit: TAC</li> </ul>	
CSR: BEGIN CERTIFICATE REQUEST MIIB42CCAUwCAQAwZTELMAkGA1UEBhMCVVMxCzAJBgNVBAgMAk1EMREwDwYDVQQH DAhDb2x1bWJpYTETMBEGA1UECgwKU291cmNlZmlyZTEMMAoGA1UECwwDVEFDMRMw EQYDVQQDDApJbnRlcm5hbENBMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC5 XTQjxBMnyPNmGTvAXrqG7LhXPXxZ7lgF6MfKxwLh8rVwoejHhwbAUro8ju/R3Ig7 Ty1cwNpr4Bnbk9kDS9jDYqftFJzOu8UJ6wKcmxg2IUx80r9y1SKzSiRprJdSBaRc LSHey3dI0K5SXNKtTb8vBV97RYAfX4VDR7iVDKwxzQIDAQABoD4wPAYJKoZIhvcN AQkOMS8wLTAdBgNVHQ4EFgQUih/JeYfJm2itIE3spLdPqzpTXGkwDAYDVR0TBAUw AwEB/zANRokobkiG9w0BAOUEAAORoORIbazWEeXilos25vxfvLlo/W92uI4DeVLm9	•
OK Cance	

Hinweis: Ihr CA-Administrator bittet um eine weitere Dateierweiterung neben .req.

Option 3: Importieren eines Zertifizierungsstellenzertifikats und -schlüssels



- i. Klicken Sie auf CA importieren.
- ii) Suchen Sie das Zertifikat, oder fügen Sie es ein.
- iii) Navigieren Sie zum privaten Schlüssel, oder fügen Sie ihn ein.
- iv) Aktivieren Sie das verschlüsselte Feld, und geben Sie ein Kennwort ein.

Import Internal Certificate Authority	? ×
Name: Win2008R2	
Certificate Data or, choose a file: Browse	
IBEGIN CERTIFICATE MIDYTCCAkmgAwIBAgIQCT2sLHNRsZxB6e0Z2AMMojANBgkghkiG9w0BAQUFADBD MRMwEQYKCZImiZPyLGQBGRYDY29tMRQwEgYKCZImiZPyLGQBGRYEemVyZzEWMBQG ALUEAxMNemVyZy1XSU4wOC1DQTAeFw0xNTA1MzEwNzA2MtNaFw0yMDA1MzEwNzE2 MtNaMEMxEzARBgoJkialk/IsZAEZEgNb20xFDA5BgoJkialk/IsZAEZEgR6ZXJn MRYwFAYEVQODEw16ZXJnLVdJTjA4LUNBMIIBIDANBgkghkiG9w0BAQEFAAOCAQ8A MIBCgKCAQEAzwGkBhtUBogN+wNU1K6BgbDyCYNmEKinVUPTQJHwEL3MKbz+ox x9UEgQ3crg2ykhmP4DgDuzUSamSsWt+he9Whxx5NQ2vNx5s3faAOSPngGAvfMXV nh8YEx1r0suAhVw+ZFPjE1a386iGtN6ILM+SB3cGgoomNiFW+fmJe4zclEyUpcYF	- -
Key or, choose a file: Browse	
BEGIN PRIVATE KEY MIEvoIBADANBokohkiG9w0BAQEFAASCBKowooSkAgEAAoIBAQDONAaQGG1QGmA3 7A1SWMroGBs08Jo2YQqOdVQ9M4kfAQvcwpvP6iHH1Q5A7dyun/KSGY/qOAO7NQU o2Kxa36F71aHHHk1Bm83Hmzd9oA5I+eAYC98xdWeHxqXHWvSy4CFXD5kU+MTVonz oIa03qUsz5HdwaqiY2IVb5+YI7INvUTJSbgUvQxzfGFi8tczDkEky+8yGSluY AqbJEK6n9SR7pBTIHwzPLZJJcvAqMy/LEe9o9GovRkqwKQfHnRObvJm2ia0NtgPo NAUy9PUpfHpCtvcS5MVrvZJ+08U12BLaWnG0WsShI7RIV02WedOE8Ft47TSiWtoG JmD/1+AvAqMBAAECogEAZZWQzRUT8y9INVqNG+CCphfihC7Zvg1mMKe74++FfPT4 rV39T+Iv2UI3U5vQE9w6Rciux8LxI3D2K06Z3HZ1VvQe8skTUICMvrCvfx6/dmE	-
Encrypted, and the password is:	
Save	Cancel

Hinweis: Wenn kein Kennwort vorhanden ist, aktivieren Sie das verschlüsselte Feld, und lassen Sie es leer.

#### 2. Entschlüsseln mit einem bekannten Schlüssel

#### Importieren eines bekannten Zertifikats (Alternative zum Entschlüsseln und Zurücksetzen)

i. Erweitern Sie auf der Seite Objekte auf der linken Seite PKI, und wählen Sie Interne Zertifikate aus.

ii) Klicken Sie auf Internes Zertifikat hinzufügen.

- iii) Suchen Sie das Zertifikat, oder fügen Sie es ein.
- iv) Navigieren Sie zum privaten Schlüssel, oder fügen Sie ihn ein.

v. Aktivieren Sie das Feld Verschlüsselt, und geben Sie ein Kennwort ein.

dd Kn	own Internal Certificat	e	? >
Name:	KnownCert		
Certifica	ate Data or, choose a file:	Browse	
MIIDOD UZELMA Y2VmaX MDZaFw MASGA1 A1RBQZ AQEAxA	IN CERTIFICATE CCAIACCODssfBhdDsHTDANBgk kGAIUECAwCTUQxETAPBgNVE UIMQwwCgYDVQQLDANUQUMx IOXODA2MDQxN2A4MDZaMF4xC IUEBwwIQ29sdW1iaWExE2ARB EMMAoGA1UEAwwDVEFDMIIBI kHMrRPPyysIwkgwAH0ELtIHmY	aghkiG9w0BAQUFADBeMQswCQYDVQQGEwJV AcMCENvbHVtYmlhMRMwEQYDVQQKDApTb3Vy DDAKBgNVBAMMA1RBQzAeFw0xNTA2MDgxNzA4 zAJBgNVBAYTAIVTMQswCQYDVQQIDAJNRDER gNVBAoMCINvdXJjZWZpcmUxDDAKBgNVBAsM JANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC 'Q3/i+MgMzmQiuAhrE3AZmh7t6BZQrwFgK	Î
Key or,	choose a file: Browse		
BEG MIIEpAI h7t6B20 wG5wc0 JFX8WV FrtH/eN YonbuE Sm6R00	IN RSA PRIVATE KEY BAAKCAQEAxAkHMrRPPyysIwk QwFgKeMX1KV7LuxXnsuJfpNk IMVe/baDT2B/XQt3BLUgLsL+T Jt3SqYtjzw41vU9gai2OuVaANr 9+/p66tUSILV23rUKUKM0gkht UCpEtJDWctl/P2rriWECMsumJI ZCOZTUaTeNFud1SO1IfrFR13IS	wAH0ELtlHmYQ3/i+MgMzmQiuAhrE3AZm 3Dp8fm33TMJQiuA2W6zpusgQOKS3yU94E PipUgazzrP3rOECvroPxDRCQ/fz8A2XJV IB5iz+9NnwNTpVGvrwHx+IOI/e2ZARI1 8IPs2mu17Upgqv3uYW2OWvnQsz41CGzht v7hNfKQIDAQA8AoIBAC;SNHSDhYkDNWkq wqsM58ArfWuj3rF6P4khWHBh+LDxc1UvP	Î
Encry	ypted, and the password is:		
		Save	Cancel

Hinweis: Wenn kein Kennwort vorhanden ist, lassen Sie das Feld Verschlüsselt leer.

4. Navigieren Sie zu Richtlinien > SSL, und klicken Sie dann auf Neue Richtlinie.

Overview Analysis Policies Devices Objects AMP	🐠 Health System Help 🕶 admin 🕶
Access Control Intrusion • Files Network Discovery SSL Application Detectors Users Correlation	Actions •
	Compare Policies O New Policy
SSL Policy	Last Hodified
SSL Policy	2015-06-02 03:43:44
New COL Deliver	
New SSL Policy	7.4
Name:	
Description:	
Default Action:	
Save	Cancel

5. Geben Sie einen Namen ein, und wählen Sie eine **Standardaktion aus**. Die Seite mit dem SSL Policy Editor wird angezeigt. Die Seite des SSL Policy Editor entspricht der Seite des Access Control Policy-Editors.

Hinweis: Wenn Sie sich über die Standardaktion nicht sicher sind, entschlüsseln Sie nicht den empfohlenen Ausgangspunkt.

6. Klicken Sie auf der Seite des SSL-Policy-Editors auf **Regel hinzufügen**. Geben Sie im Fenster Regel hinzufügen einen Namen für die Regel ein, und füllen Sie alle anderen relevanten Informationen aus.

Add Ru	le						? ×	
Name	Resign	]	🕑 Enal	oled	Insert below rule	ow rule 💙 1		
Zon	Decrypt - Known Key	Users Applications	Ports Category	Certificate DN	Cert Status Cipher S	Suite Version	Logging	
Sea Sea 701 701 10 70 70 70 70 70 70 70 70 70 7	bo not decrypt     Block     Monitor External HomeSet Internal	Ad So Ad Dest	d to urce d to nation			any		
							Add Cancel	

Im folgenden Abschnitt werden verschiedene Optionen im Fenster Regel hinzufügen beschrieben:

Aktion

#### Entschlüsseln - Zurücksetzen

• Der Sensor agiert als Man in the Middle (MitM) und akzeptiert die Verbindung mit dem Benutzer, stellt dann eine neue Verbindung zum Server her. Beispiele: Benutzertypen in https://www.facebook.com in einem Browser. Der Datenverkehr

erreicht den Sensor, der Sensor verhandelt dann mit dem Benutzer über das ausgewählte CA-Zertifikat und der SSL-Tunnel A wird erstellt. Gleichzeitig stellt der Sensor eine Verbindung zu https://www.facebook.com her und erstellt SSL-Tunnel B. • Endergebnis: Benutzer sehen das Zertifikat in der Regel, nicht in Facebook's.

• Für diese Aktion ist eine interne CA erforderlich. Wählen Sie Schlüssel ersetzen, wenn der Schlüssel ersetzt werden soll. Der Benutzer erhält das ausgewählte Zertifikat.

Hinweis: Dies kann nicht im passiven Modus verwendet werden.

#### Entschlüsseln - Bekannter Schlüssel

- Der Sensor verfügt über den Schlüssel, der zum Entschlüsseln des Datenverkehrs verwendet wird. Beispiele: Benutzertypen in https://www.facebook.com in einem Browser. Der Datenverkehr erreicht den Sensor, der Sensor entschlüsselt den Datenverkehr und überprüft anschließend den Datenverkehr.
- Endergebnis: Benutzer sieht das Facebook-Zertifikat
- Für diese Aktion ist ein internes Zertifikat erforderlich. Dies wird unter Objekte > PKI > Interne Zertifikate hinzugefügt.

**Hinweis:** Ihre Organisation muss der Eigentümer der Domäne und des Zertifikats sein. Zum Beispiel von facebook.com wäre die einzige Möglichkeit, den Endbenutzer zu sehen, Facebook's Zertifikat wäre, wenn Sie tatsächlich Eigentümer der Domain facebook.com (d.h. Ihr Unternehmen ist Facebook, Inc) und haben Eigentümer des facebook.com Zertifikat signiert von einer öffentlichen CA. Sie können nur mit bekannten Schlüsseln für Sites entschlüsseln, die im Besitz Ihres Unternehmens sind.

Der Hauptzweck der Entschlüsselung eines bekannten Schlüssels besteht in der Entschlüsselung des Datenverkehrs zu Ihrem HTTPS-Server, um Ihre Server vor externen Angriffen zu schützen. Für die Überprüfung des clientseitigen Datenverkehrs zu externen HTTPS-Sites verwenden Sie die Rückmeldung entschlüsseln, da Sie nicht Eigentümer des Servers sind. Sie sind daran interessiert, den Client-Datenverkehr in Ihrem Netzwerk zu überprüfen, der mit externen verschlüsselten Sites verbunden ist.

Hinweis: Damit DHE und ECDHE entschlüsseln können, müssen wir in-line sein.

#### Nicht entschlüsseln

Der Datenverkehr umgeht die SSL-Richtlinie und setzt die Zugriffskontrollrichtlinie fort.

Zertifikat

Regel gleicht SSL-Datenverkehr mit diesem speziellen Zertifikat ab.

Zones	Networks	VLAN Tags	Users	Applications	Ports	Category	Certificate	DN	Cert Status	Cipher Suite	Version	Logging
Available 0	ertificates (	\$				0		Sele	ted Certificate	; (0)		
Search	by name or v	alue						any				
							Add to Rule					

#### DN

Regel gleicht SSL-Datenverkehr mithilfe bestimmter Domänennamen in den Zertifikaten ab.

Zones	Networks	VLAN Tags	Users	Applications	Ports	Category	Certificate	DN	Cert Status	Ciphe	r Suite	Version	Logging
Available D	vailable DNs 🖒 🔘			0		Subject D	Vs (0)						
🔍 Search	by name or va	lue				any					any		
Source	fire Undecrypt	able Sites											
🚍 CN=*.4	citrixonline.com	n											
🚍 CN=*.4	fata.toolbar.ya	hoo.com											
🚍 CN=*.!	edoraproject.o	rg											
🚍 CN=*.)	tunes.apple.co	m		4	dd to								
🚍 CN=*J	ogmein.com												
🚍 CN=*./	nozilla.org												
🚍 CN=*./	hn.redhat.com	1											
🚍 CN=*.4	ls.microsoft.c	om											
🚍 CN=*u	pdate.microsol	ft.com											
CN=ac	count.live.com												
🚍 Google													
						Enter DN (	or CN				Enter 0	N or CN	Add

#### Zertifizierungsstatus

Regel gleicht SSL-Datenverkehr mit diesen Zertifikatsstatus ab.

Zones	Networks	VLAN Tags	Users	Applications	Ports	Category	Certificate	DN	Cert Status	Cipher Suite	Version		
Revoked:			Yes	No Do Not N	1atch								
Self-signed:				Yes No Do Not Match									
Valid:				Yes No Do Not Match									
Invalid sigr	nature:		Yes	Yes No Do Not Match									
Invalid issu	ler:		Yes	No Do Not N	1atch								
Expired:			Yes	No Do Not N	1atch								
Not yet valid:			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**

Regel gleicht SSL-Datenverkehr mit diesen Cipher-Suites ab.



#### Version

Regeln gelten nur für SSL-Datenverkehr mit den ausgewählten SSL-Versionen.

Zones	Networks	VLAN Tags	Users	Applications	Ports	Category	Certificate	DN	Cert Status	Cipher Suite	Version
SSL v3.0											
TLS v1.0											
TLS v1.1											
TLS v1.2											

#### Protokollieren

Aktivieren Sie die Protokollierung, um Verbindungsereignisse für den SSL-Datenverkehr anzuzeigen.

7. Klicken Sie auf Vertrauenswürdiges CA-Zertifikat. Hier wird die vertrauenswürdige CA der Richtlinie hinzugefügt.

Rules	Trusted CA Certificates	Undecryptable Actions			
Availal	ole Trusted CAs 🛭 🖒		٥	Selected Trusted CAs	
🔍 Sei	arch			🖶 Sourcefire Trusted Authorities	6
📥 So	urcefire Trusted Authorities		<b>A</b>		
<i>≫</i> A-'	Trust-nQual-01				
<i>₽</i> -1	Trust-nQual-03				

8. Klicken Sie auf **Unentschlüsselbare Aktionen**. Hier sind die Aktionen, für die der Sensor den Datenverkehr nicht entschlüsseln kann. Die Definitionen finden Sie in der Online-Hilfe (**Hilfe > Online**) des FireSIGHT Management Center.

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	nake Errors	Inherit Default Action	¥
Decryp	otion Errors	Block	~

- Komprimierte Sitzung: Die SSL-Sitzung wendet eine Datenkomprimierungsmethode an.
- SSLv2-Sitzung: Die Sitzung wird mit SSL Version 2 verschlüsselt. Beachten Sie, dass Datenverkehr entschlüsselt werden kann, wenn die Client-Hello-Nachricht SSL 2.0 und der

Rest des übertragenen Datenverkehrs SSL 3.0 ist.

- Unbekannte Cipher Suite: Das System erkennt die Verschlüsselungssuite nicht.
- Nicht unterstützte Cipher Suite: Das System unterstützt die Entschlüsselung auf der Grundlage der erkannten Verschlüsselungssuite nicht.
- Sitzung nicht zwischengespeichert: Bei der SSL-Sitzung ist die Sitzungswiederverwendung aktiviert, der Client und der Server haben die Sitzung mit der Sitzungskennung wiederhergestellt, und das System hat die Sitzungskennung nicht zwischengespeichert.
- Handshake-Fehler: Bei der SSL-Handshake-Aushandlung ist ein Fehler aufgetreten.
- Entschlüsselungsfehler: Bei der Entschlüsselung des Datenverkehrs ist ein Fehler aufgetreten.

**Hinweis:** Standardmäßig erben diese die Standardaktion. Wenn die Standardaktion "Blockieren" lautet, treten möglicherweise unerwartete Probleme auf.

9. Speichern Sie die Richtlinie.

10. Navigieren Sie zu **Richtlinien > Zugriffskontrolle**. Bearbeiten Sie Ihre Richtlinie, oder erstellen Sie eine neue Zugriffskontrollrichtlinie.

11. Klicken Sie auf Erweitert, und bearbeiten Sie die allgemeinen Einstellungen.

Overview Analysis Policies Devices	Objects AMP						
Access Control Intrusion - Files N	letwork Discovery	SSL Ap	plication D	etectors	Users	Correlation	Actions 🔻
TAC Access Control							
Enter a description							
Rules Targets (1) Security Intelligence	HTTP Responses	dvanced					
General Settings			Ø	Trans	port/Net	twork Layer	Preprocessor Se
Maximum URL characters to store in connection	n events		1024	Ignor	e the VLAN	N header when	tracking connection
Allow an Interactive Block to bypass blocking f	or (seconds)		600	Detec	tion Enh	ancement S	ettings
SSL Policy to use for inspecting encrypted com	nections		None	Adapt	ive Profile	5	
Inspect traffic during policy apply Yes Performan				mance s	Settings		
Network Analysis and Intrusion Policie	General Settings						? × t
Intrusion Policy used before Access Control r determined	Maximum URL charact	ers to store in	n	1024			
Intrusion Policy Variable Set	Allow an Interactive Bl	ock to bypass	s blocking	600			
Default Network Analysis Policy	for (seconds)			000			
Files and Malware Settings	SSL Policy to use for in connections	nspecting end	crypted	SSL Policy			× .
Limit the number of bytes inspected when do	Inspect traffic during	policy apply	6				
Allow file if cloud lookup for Block Malware to	Revert to Defaults					ок	Cancel

12. Wählen Sie aus dem Dropdown-Menü Ihre SSL-Richtlinie aus.

13. Klicken Sie zum Speichern auf OK.

#### Zusätzliche Konfigurationen

Folgende Änderungen sollten an den Intrusion-Policies vorgenommen werden, damit eine

i. Ihre \$HTTP\_PORTS-Variable sollte Port 443 und alle anderen Ports mit HTTPS-Datenverkehr enthalten, die von Ihrer Richtlinie entschlüsselt werden (**Objekte > Objektverwaltung > Variablensatz > Variablensatz bearbeiten**).



ii) Die Network Analysis-Richtlinie, die den verschlüsselten Datenverkehr prüft, muss Port 443 (und alle anderen Ports mit HTTPS-Datenverkehr, die von Ihrer Richtlinie entschlüsselt werden) im Port-Feld der HTTP-Präprozessoreinstellungen enthalten. Andernfalls werden keine der HTTP-Regeln mit HTTP-Inhaltsmodifizierern (z. B. http\_uri, http\_header usw.) ausgelöst, da dies von den HTTP-Ports abhängt. und die HTTP-Puffer in snort werden nicht für Datenverkehr gefüllt, der nicht über die angegebenen Ports läuft.

iii) (Optional, aber für eine bessere Überprüfung empfohlen) Fügen Sie Ihre https-Ports den Einstellungen für die **TCP-Stream-Konfiguration** im Feld **Perform Stream Reassembly** (Reassemblierung des Perform-Streams auf beiden Ports) hinzu.

iv) Überarbeitete Zugriffskontrollrichtlinie während eines geplanten Wartungsfensters erneut anwenden.

**Warnung:** Diese geänderte Richtlinie kann erhebliche Leistungsprobleme verursachen. Dies sollte außerhalb der Produktionszeiten getestet werden, um das Risiko von Netzwerkausfällen oder -leistung zu reduzieren.

# Überprüfung

Entschlüsseln - Zurücksetzen

1. Öffnen Sie einen Webbrowser.

**Hinweis:** Im Beispiel unten wird der Firefox-Browser verwendet. Dieses Beispiel funktioniert möglicherweise nicht in Chrome. Weitere Informationen finden Sie im Abschnitt Fehlerbehebung.

2. Navigieren Sie zu einer SSL-Website. Im Beispiel unten wird https://www.google.com verwendet, die Websites der Finanzinstitute wird auch funktionieren. Sie sehen eine der folgenden Seiten:



**Hinweis:**Die obige Seite wird angezeigt, wenn das Zertifikat selbst nicht vertrauenswürdig ist und das signierende Zertifizierungsstellenzertifikat von Ihrem Browser nicht als vertrauenswürdig eingestuft wird. Wie der Browser vertrauenswürdige Zertifizierungsstellenzertifikate auswählt, erfahren Sie im Abschnitt Vertrauenswürdige Zertifizierungsstellen weiter unten. E

☆ 自 ♣

Gmail Images

Google						
Google Search	I'm Feeling Lucky					
Page Info - https://www.google.com/?gws_rd=ssl						
General       Image: Constraint of the second						
Verified by: Sourcefire	snip information.	View Certificate				
Privacy & History	N 977 //					
Have I visited this website prior to today? 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						

**Hinweis:** Wenn diese Seite angezeigt wird, haben Sie den Datenverkehr erfolgreich neu signiert. Beachten Sie den Abschnitt **Verified by: Sourcefire**.

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

Issued To
-----------

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

Hinweis: Dies ist ein genauerer Blick auf dasselbe Zertifikat.

3. Gehen Sie im Management Center zu Analysis > Connections > Events.

4. Abhängig von Ihrem Workflow wird möglicherweise die Option SSL-Entschlüsselung angezeigt. Klicken Sie auf **Tabellenansicht von Verbindungsereignissen**.

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

No Search Constraints (Edit Search)

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

5. Navigieren Sie nach rechts, und suchen Sie nach dem SSL-Status. Folgende Optionen sind

#### ähnlich:

<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

Entschlüsseln - Bekanntes Zertifikat

1. Navigieren Sie im FireSIGHT Management Center zu Analysis > Connections > Events.

2. Je nach Workflow wird die Option SSL-Entschlüsselung möglicherweise nicht angezeigt. Klicken Sie auf **Tabellenansicht von Verbindungsereignissen**.

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

#### No Search Constraints (Edit Search)

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

3. Navigieren Sie nach rechts, und suchen Sie nach dem SSL-Status. Folgende Optionen sind ähnlich:

<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

## Fehlerbehebung

Ausgabe 1: Einige Websites werden möglicherweise nicht im Chrome-Browser geladen

#### **Beispiel**

www.google.com lädt möglicherweise nicht mit einer Entschlüsselung - Resign using Chrome.

#### Grund

Der Google Chrome-Browser ist in der Lage, betrügerische Zertifikate für Google-Eigenschaften zu erkennen, um Man-in-the-Middle-Angriffe zu verhindern. Wenn der Chrome-Browser (Client) versucht, eine Verbindung zu einer google.com-Domäne (Server) und ein Zertifikat zurückgegeben wird, das kein gültiges Google-Zertifikat ist, verweigert der Browser die Verbindung.

#### Lösung

Wenn dies auftritt, fügen Sie eine **Do Not Decrypt-**Regel für DN=\*.google.com, \*.gmail.com, \*.youtube.com hinzu. Löschen Sie anschließend den Browser-Cache und den Browserverlauf.

# Ausgabe 2: Abrufen einer nicht vertrauenswürdigen Warnung/eines nicht vertrauenswürdigen Fehlers in einigen Browsern

#### Beispiel

Wenn Sie mit Internet Explorer und Chrome eine Verbindung zu einer Website herstellen, erhalten Sie keine Sicherheitswarnung. Wenn Sie jedoch den Firefox-Browser verwenden, müssen Sie der Verbindung bei jedem Schließen und erneuten Öffnen des Browsers vertrauen.

#### Grund

Die Liste der vertrauenswürdigen CAs hängt vom Browser ab. Wenn Sie einem Zertifikat vertrauen, wird es nicht über alle Browser verteilt, und der vertrauenswürdige Eintrag wird in der Regel nur bei geöffnetem Browser beibehalten. Wenn der Browser geschlossen ist, werden alle vertrauenswürdigen Zertifikate gelöscht, und beim nächsten Öffnen des Browsers und beim nächsten Besuch der Site müssen Sie das Zertifikat erneut zur Liste der vertrauenswürdigen Zertifikate hinzufügen.

#### Lösung

In diesem Szenario verwenden sowohl IE als auch Chrome die Liste der vertrauenswürdigen CAs im Betriebssystem, Firefox pflegt jedoch eine eigene Liste. Das CA-Zertifikat wurde also in den OS-Store importiert, aber nicht in den Firefox-Browser importiert. Um die Sicherheitswarnung in Firefox zu vermeiden, müssen Sie das CA-Zertifikat als vertrauenswürdige CA in den Browser importieren.

#### Vertrauenswürdige Zertifizierungsstellen

Wenn eine SSL-Verbindung hergestellt wird, prüft der Browser zuerst, ob dieses Zertifikat vertrauenswürdig ist (d.h. Sie waren vor dieser Site und haben dem Browser manuell mitgeteilt, dass er diesem Zertifikat vertrauen soll). Wenn das Zertifikat nicht vertrauenswürdig ist, überprüft der Browser das Zertifikat der Zertifizierungsstelle (Certificate Authority, CA), das das Zertifikat für diese Site verifiziert hat. Wenn das Zertifizierungsstellenzertifikat vom Browser als vertrauenswürdig eingestuft wird, wird es als vertrauenswürdiges Zertifikat betrachtet und die Verbindung zugelassen. Wenn das Zertifizierungsstellenzertifikat nicht vertrauenswürdig ist, zeigt der Browser eine Sicherheitswarnung an und zwingt Sie, das Zertifikat manuell als vertrauenswürdiges Zertifikat hinzuzufügen.

Die Liste der vertrauenswürdigen CAs in einem Browser ist vollständig von der Implementierung des Browsers abhängig, und jeder Browser kann seine vertrauenswürdige Liste anders als andere Browser ausfüllen. Im Allgemeinen gibt es zwei Möglichkeiten, wie aktuelle Browser eine Liste vertrauenswürdiger CAs ausfüllen:

- 1. Sie verwenden die Liste der vertrauenswürdigen CAs, denen das Betriebssystem vertraut.
- 2. Sie liefern eine Liste der vertrauenswürdigen CAs zusammen mit der Software und ist in den Browser integriert.

Für die gängigsten Browser werden die vertrauenswürdigen CAs wie folgt aufgefüllt:

- Google Chrome: Vertrauenswürdige CA-Liste des Betriebssystems
- Firefox: Behält seine eigene vertrauenswürdige CA-Liste bei
- Internet Explorer: Vertrauenswürdige CA-Liste des Betriebssystems
- Safari: Vertrauenswürdige CA-Liste des Betriebssystems

Es ist wichtig, den Unterschied zu kennen, da das Verhalten, das auf dem Client gesehen wird, je nach dem variieren wird. Um beispielsweise eine vertrauenswürdige CA für Chrome und IE hinzuzufügen, müssen Sie das CA-Zertifikat in den vertrauenswürdigen CA-Speicher des Betriebssystems importieren. Wenn Sie das Zertifizierungsstellenzertifikat in den vertrauenswürdigen Zertifizierungsstellenspeicher des Betriebssystems importieren, wird keine Warnung mehr angezeigt, wenn Sie eine Verbindung zu Standorten herstellen, für die ein von dieser Zertifizierungsstelle signiertes Zertifikat vorliegt. Im Firefox-Browser müssen Sie das CA-Zertifikat manuell in den vertrauenswürdigen CA-Speicher im Browser selbst importieren. Danach erhalten Sie keine Sicherheitswarnung mehr, wenn Sie eine Verbindung zu Sites herstellen, die von dieser CA überprüft wurden.

## Referenzen

Erste Schritte mit SSL-Regeln