Configuración de una Política de Inspección SSL en Cisco FireSIGHT System

Contenido

Introducción **Prerequisites Componentes Utilizados Configuraciones** 1. Descifrar y renunciar Opción 1: Utilice FireSIGHT Center como autoridad de certificados raíz (CA) Opción 2: Tenga una CA interna que firme su certificado Opción 3: Importar un certificado de CA y una clave 2. Descifrar con clave conocida Importación de certificado conocido (alternativa a descifrar y renunciar) **Configuraciones adicionales** Verificación Descifrar - Renuncia Descifrar - Certificado conocido Resolución de problemas Problema 1: Es posible que algunos sitios web no se carguen en el navegador Chrome Problema 2: Obtención de una advertencia/error no fiable en algunos navegadores Referencias Conversaciones relacionadas de la comunidad de soporte de Cisco

Introducción

La función de inspección SSL permite bloquear el tráfico cifrado sin inspeccionarlo, o bien inspeccionar el tráfico cifrado o descifrado con control de acceso. Este documento describe los pasos de configuración para configurar una política de inspección SSL en Cisco FireSIGHT System.

Prerequisites

Componentes Utilizados

- Cisco FireSIGHT Management Center
- Dispositivos Cisco Firepower 7000 u 8000
- Versión de software 5.4.1 o posterior

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Advertencia: Si aplica una política de inspección SSL en su dispositivo administrado, puede afectar al rendimiento de la red.

Configuraciones

Puede configurar una política de inspección SSL para descifrar el tráfico de las siguientes maneras:

- 1. Descifrar y renunciar:
 - Opción 1: Utilice FireSIGHT Center como autoridad de certificación (CA) raíz, o
 - Opción 2: Que una CA interna firme su certificado o
 - Opción 3: Importar un certificado de CA y una clave
- 2. Descifrar con certificado conocido:
 - Inicie sesión en FireSIGHT Management Center y, a continuación, navegue hasta Objetos.
 - En la página Objetos, expanda la PKI y seleccione CA internas.
- 1. Descifrar y renunciar

Opción 1: Utilice FireSIGHT Center como autoridad de certificados raíz (CA)

i. Haga clic en Generar CA.

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

ii. Rellene la información pertinente

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. Haga clic en Generar CA autofirmada.

Opción 2: Tenga una CA interna que firme su certificado

🕕 Health	System	Help 🔻	admin 🔻
Generate CA 💽 💽 Impor	t CA	Filter	

i. Haga clic en Generar CA.

ii. Introduzca la información pertinente.

InternalCA	
US	
MD	
Columbia	
Sourcefire	
TAC	
InternalCA	
	InternalCA US MD Columbia Sourcefire TAC InternalCA

Nota:Es posible que deba ponerse en contacto con el administrador de la CA para determinar si tiene una plantilla para la solicitud de firma.

iii. Copie todo el certificado, incluidas —BEGIN CERTIFICATE REQUEST— y —END CERTIFICATE REQUEST— y, a continuación, guárdelo en un archivo de texto con la .req extensión.

enerate Internal Certificate Authority	? X
Subject:	
Common Name: InternalCA	
Organization: Sourcefire	
Organization Unit: TAC	
:SR: BEGIN CERTIFICATE REQUEST MIIB4zCCAUwCAQAwZTELMAkGA1UEBhMCVVMxCzAJBgNVBAgMAk1EMREwDwYDVQQH DAhDb2x1bWJpYTETMBEGA1UECgwKU291cmNiZmlyZTEMMAoGA1UECwwDVEFDMRM EQYDVQQDDApJbnRicm5hbENBMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC5 XTQjxBMnyPNmGTvAXrqG7LhXPXxZ7igF6MfKxwLh8rVwoejHhwbAUro8ju/R3Ig7 Ty1cwNpr4Bnbk9kDS9jDYqftFJzOu8UJ6wKcmxg2IUx80r9y1SKzSiRprJdSBaRc LSHey3dI0K5SXNKtTb8vBV97RYAfX4VDR7iVDKwxzQIDAQABoD4wPAYJKoZIhvcN AQkOMS8wLTAdBgNVHQ4EFgQUih/JeYfJm2itIE3spLdPqzpTXGkwDAYDVR0TBAUw AwER/zANBakabkiG9w0BAOUFAAORaOBibazWFeXilos25vxfvLio/W9ZuI4DeVLm9	v Î
	al

Nota: El administrador de CA solicita otra extensión de archivo además de .req.

Opción 3: Importar un certificado de CA y una clave

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

- i. Haga clic en Importar CA.
- ii. Busque o pegue el certificado.
- iii. Busque o pegue la clave privada.
- iv. Marque la casilla cifrada y escriba una contraseña.

Import Int	ternal Certificate Authority	? ×
Name: W	Win2008R2	
Certificate 0	Data or, choose a file: Browse	
H-BEGIN (MIDYTCCA MRMwEQ// ALUEAXMN MINAMEMX8 MRYwEAYD MIBCgKCA X9UEgO3cr ob8YExLr0;	CERTIFICATE AkmgAwIBAgIOCT2sLHNRsZxB6e0Z2AMMojANBokohkiG9w0BAQUFADBD KCZImiZPyLGOBGRYDY29tMRQwEgYKCZImiZPyLGOBGRYEemVyZzEWMBQG iemVyZy1XSU4wOC1DOTAeFw0xNTA1MzEwNzA2MJNaFw0yMDA1MzEwNzE2 EzARBgo3kiaJk/IsZAEZFoNib20xFDA5BooJkiaJk/IsZAEZFoR6ZXJn DVOODEw16ZXJnLVdJTjA4LUNBMIBIJANBgkohkiG9w0BAQEFAAOCAO8A AQEAzreGkBhtUBogN+wNUJK6BobDyCYNmEKinVUPTOJHwEL3MKbz+ox r0ZykhmP4DgDuzUJSamSsWt+he9Whxx5NQZytNx5s3faAOSPngGAvfMXV IsuAhVw+ZFPJE1aJ86iGtN6ILM+\$B3cGgoomNIEW+fmJe4zclEyUpcYE	* *
Key or, cho	oose a file: Browse	
BEGIN I MIEvoIBAC 7A15W/Moi aZKxa36FZ ala03aUsz5 AabJEK6n9 NAU/9PUp JmD/1+AvA rv39T+1y21	PRIVATE KEY DANBgkghkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAODOt4aQGG1QGmA3 JGBs0BJg2YQgQd7VQ9M4kfAQxcwpvP6JHH1QSA7dyuryKSGY/gQAQ7NQU 71aHHHk1Bm83Hmzd9oA5I+eAYC98xdWeHxgXHW/Sy4CEXD5kU+MTVonz 5IHdwagiY2IVb5+YI7YVUTJSIxgUvQwzfGEr8tczDkEky+8yGSluY 9SR7pBTIHwzPLZJJcvAgMy/LEe9o9GovRkgwKQfHnRObvJm2ia0NtgPo ifHpCtycS5MVivZJ+08U12BLaWnG0WS5hI7RIVO2Wed0E8R47TSiWtoG AgMBAAECggEAZZW0ZRUT8y9JNVgNG+CCphfihC72xg1mMKe74++EfPT4 UJ3U5vQE9w6Rcjux8LxI3D2K06Z3HZ1VvOe8skTUJCMuYCvfk6/dmE	÷
Encrypte	ted, and the password is:	
	Save	e Cancel

Nota: Si no hay contraseña, marque la casilla cifrada y déjela en blanco.

2. Descifrar con clave conocida

Importación de certificado conocido (alternativa a descifrar y renunciar)

- i. En la página Objetos de la izquierda, expanda PKI y seleccione Certificados internos.
- ii. Haga clic en Agregar certificado interno.
- iii. Busque o pegue el certificado.
- iv. Busque o pegue la clave privada.
- v. Marque la casilla **Encrypted** y escriba una contraseña.

dd Kn	own Internal Certificat	e	? :
Name:	KnownCert		
Certifica	ate Data or, choose a file:	Browse	
BEG	IN CERTIFICATE		A
MIIDOD	CCAIACCODssfBhdDsHTDANBgk	qhkiG9w0BAQUFADBeMQswCQYDVQQGEwJV	
UZELMA	kGA1UECAwCTUQxETAPBgNVB	AcMCENvbHVtYmlhMRMwEQYDVQQKDApTb3Vy	
Y2VmaX	OIMQwwCgYDVQQLDANUQUMx	DDAKBgNVBAMMA1RBQzAeFw0xNTA2MDgxNzA4	
MDZaFw	v0xODAzMDQxNzA4MDZaMF4x0	ZAJBgNVBAYTAIVTMQswCQYDVQQIDAJNRDER	
MASGAI	LUEBww1Q29sdW1iaWExEzARB	gNVBAoMCINvdXJjZWZpcmUxDDAKBgNVBAsM	
A1RBQ2	EMMAoGA1UEAwwDVEFDMIIBI	JANBgkghkiG9w0BAQEFAAOCAQBAMIIBCgKC	
AQEAXA	kHMrRPPyyslwkgwAH0ELtiHmY	Q3/i+MgMzmQiuAhrE3AZmh7t6BZQrwFgK	*
Key or,	choose a file: Browse		
BEG	IN RSA PRIVATE KEY		
MIIEpAI	BAAKCAQEAxAkHMrRPPyysIwk	wAH0ELtlHmYQ3/i+MgMzmQiuAhrE3AZm	
h7t6BZ0	QrwFqKeMX1KV7LuxXnsuJfpNk	3Dp8fm33TMJQiuAZW6zpusjgOKS3yUs4E	
wG5wco	qMVe/baDT2B/XQt3BLUqLsL+T	PipUgazzrPt3rOECvroPxDRCQ/fz8AzXJV	
JFX8WV	0t3SqYtjzw41vU9qai2OuVaANr	IB5iz+9NnwNTpVGvrwHx+iOI/e2ZARI1	
FrtH/eN	9+/p66tUSILV23rUKUKM0gkh8	IPs2mu17Upgqv3uYW2OWvnQsz41CGzht	
YonbuE	UCpEtJDWctl/P2mWECMsumJ	v7hNfKQIDAQABAo1BACISNHSDhYkDNWkq	
Sm6RO/	ZCOZTUaTeNFud1SO1lfrFR13I5	wqsMS8ArfWuj3rF6P4khWHBh+LDxc1UvP	*
Encry	ypted, and the password is:	•••••	

Nota: Si no hay contraseña, deje el cuadro Cifrado en blanco.

4. Navegue hasta **Políticas > SSL** y luego haga clic en **Nueva política**.

Overview Analysis Policies Devices Objects AMP	🐠 Health System Help 🕶 admin 🕶
Access Control Intrusion • Files Network Discovery SSL Application Detectors Users Correlation	Actions •
	Compare Policies New Policy
SSL Policy	Last Modified
SSL Policy	2015-06-02 03:43:44
New SSL Policy	7 X
Name:	
Description:	
Default Action: O not decrypt Block Block with reset	
Save	Cancel

5. Proporcione un nombre y seleccione una **Acción predeterminada**. Aparecerá la página del editor de políticas SSL. La página del editor de políticas SSL funciona igual que la página del editor de directivas de control de acceso.

Nota: Si no está seguro de la Acción predeterminada, No descifrar es el punto de inicio recomendado.

6. En la página del editor de políticas SSL, haga clic en **Agregar regla**. En la ventana Agregar regla, proporcione un nombre para la regla y rellene toda la información pertinente.

Add Rule					? ×
Name Resign		✓ Enabled	Insert below rule	▼ 1	
Action Do not decrypt	~				
Zone 🙆 Decrypt - Resign	Users Applications Ports	Category Certificate	DN Cert Status Cipher Suite	Version	Logging
Available Do not decrypt		Source Zones (0)	Destina	ation Zones (0)	
Sear 🗙 Block		any	any		
📇 701(💢 Block with reset					
5 701(↓ Monitor					
🚔 📐 External					
A Internal	Add to				
	Source				
	Add to Destination				
				Add	Cancel

En la sección siguiente se describen diversas opciones de la ventana Agregar regla:

Acción

Descifrar - Renuncia

• El sensor actúa como Man in the Middle (MitM) y acepta la conexión con el usuario y, a continuación, establece una nueva conexión con el servidor. Por ejemplo: El usuario escribe en https://www.facebook.com en un navegador. El tráfico alcanza el sensor, el sensor luego negocia con el usuario mediante el certificado de CA seleccionado y se genera el túnel SSL A. Al mismo tiempo, el sensor se conecta a https://www.facebook.com y crea el túnel SSL B.

- Resultado final: El usuario ve el certificado en la regla, no en Facebook.
- Esta acción requiere una CA interna. Seleccione Reemplazar clave si desea reemplazar la clave. El usuario recibirá el certificado que seleccione.

Nota: Esto no se puede utilizar en modo pasivo.

Descifrar: clave conocida

- El sensor tiene la clave que se utilizará para descifrar el tráfico. Por ejemplo: El usuario escribe en https://www.facebook.com en un navegador. El tráfico alcanza el sensor, el sensor descifra el tráfico y, a continuación, inspecciona el tráfico.
- Resultado final: El usuario ve el certificado de facebook
- Esta acción requiere un certificado interno. Esto se agrega en Objetos > PKI > Certificados internos.

Nota: Su organización debe ser el propietario del dominio y del certificado. Para el ejemplo de facebook.com, la única manera posible de que el usuario final vea el certificado de facebook sería si realmente es propietario del dominio facebook.com (es decir, su empresa es Facebook, Inc) y tiene la propiedad del certificado de facebook.com firmado por una CA pública. Solo puede descifrar con claves conocidas los sitios que posee su organización.

El objetivo principal de descifrar la clave conocida es descifrar el tráfico que se dirige a su servidor https para proteger sus servidores de ataques externos. Para inspeccionar el tráfico del lado del cliente a los sitios https externos, utilizará el comando descrypt resign, ya que no posee el servidor y está interesado en inspeccionar el tráfico del cliente en su red que se conecta a los sitios cifrados externos.

Nota: Para que DHE y ECDHE descifren debemos estar en línea.

No descifrar

El tráfico omite la política SSL y continúa con la política de control de acceso.

Certificado

La regla coincide con el tráfico SSL usando este certificado en particular.

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

DN

La regla coincide con el tráfico SSL utilizando determinados nombres de dominio en los certificados.

Zones	Networks	VLAN Tags	Users	Applications	Ports	Category	Certificate	DN	Cert Status	Ciphe	r Suite	Version	Logging
Available DNs 🖒 🔘			Subject D	Subject DNs (0)									
🔍 Search	by name or va	lue				any					any		
Source	fire Undecrypt	able Sites											
🚍 CN=*./	citrixonline.com	n											
🚍 CN=*.4	fata.toolbar.ya	hoo.com											
	edoraproject.o	rg											
🚍 CN=*.3	tunes.apple.co	m		A	dd to								
🚍 CN=*.J	iogmein.com												
	mozilla.org												
🚍 CN=*./	rhn.redhat.com	1											
🚍 CN=*.4	sls.microsoft.c	om											
🚍 CN=*u	pdate.microsol	t.com											
CN=ac	count.live.com												
👼 Google													
						Enter DN (or CN				Enter D	N or CN	Add

Estado del certificado

La regla coincide con el tráfico SSL con estos estados de certificado.

Zones	Networks	VLAN Tags	Users	Applications	Ports	Category	Certificate	DN	Cert Status	Cipher Suite	Version
Revoked:			Yes	No Do Not N	1atch						
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	ier:		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 CRL	.:		Yes	No Do Not N	1atch						

Suite Cipher

La regla coincide con el tráfico SSL usando estos conjuntos de aplicaciones Cipher.



Versión

Las reglas sólo se aplican al tráfico SSL con las versiones seleccionadas de SSL.

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											

Registro

Habilite el registro para ver los eventos de conexión para el tráfico SSL.

7. Haga clic en **Certificado de CA de confianza**. Aquí es donde se agrega CA de confianza a la política.



8. Haga clic en **Acciones descifrables**. Estas son las acciones para las cuales el sensor no puede descifrar el tráfico. Puede encontrar las definiciones en la ayuda en línea (**Ayuda > Online**) del 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	hake Errors	Inherit Default Action	~
Decryp	otion Errors	Block	•

- Sesión comprimida: La sesión SSL aplica un método de compresión de datos.
- Sesión SSLv2: La sesión se cifra con la versión 2 de SSL. Observe que el tráfico es descifrable si el mensaje hello del cliente es SSL 2.0 y el resto del tráfico transmitido es SSL 3.0.

- Conjunto Cipher Desconocido: El sistema no reconoce el conjunto de cifrado.
- Conjunto de Cipher no compatible: El sistema no admite el descifrado según el conjunto de cifrado detectado.
- Sesión no almacenada en caché: La sesión SSL tiene activada la reutilización de la sesión, el cliente y el servidor restablecieron la sesión con el identificador de sesión y el sistema no almacenó en caché ese identificador de sesión.
- Errores de intercambio de señales: Se ha producido un error durante la negociación de intercambio de señales SSL.
- Errores de descifrado: Se ha producido un error durante el descifrado del tráfico.

Nota: De forma predeterminada, heredan la Acción predeterminada. Si su acción predeterminada es Block (Bloquear), puede experimentar problemas inesperados

9. Guarde la política.

10. Navegue hasta **Políticas > Control de acceso**. Edite la directiva o cree una nueva política de control de acceso.

11. Haga clic en Avanzado y edite la Configuración general.

Overview Analysis Policies Devices	6 Objects AM	Р					
Access Control Intrusion - Files N	Network Discovery	SSL	Application D	etectors	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 F	Preprocessor S
Maximum URL characters to store in connection	n events		1024	Ignor	e the VLAN	I header when t	racking connectio
Allow an Interactive Block to bypass blocking for (seconds)				Deteo	ction Enh	ancement Se	ettings
SSL Policy to use for inspecting encrypted con	nections		None	Adapt	ive Profile	s	
Inspect traffic during policy apply			Yes	Perfo	rmance S	Settings	
Network Analysis and Intrusion Policie	General Settings	5					? × 1
Intrusion Policy used before Access Control r determined	Maximum URL chara	acters to st	ore in	1024			
Intrusion Policy Variable Set	Allow an Interactive	Block to by	vnass blocking	600			
Default Network Analysis Policy	for (seconds)		,y	000			
Files and Malware Settings	SSL Policy to use for connections	r inspecting	g encrypted	SSL Policy			· · · ·
Limit the number of bytes inspected when do	Inspect traffic durin	ig policy ap	pply				
Allow file if cloud lookup for Block Malware ta	Revert to Defaults					ок	Cancel

- 12. En el menú desplegable seleccione su política SSL.
- 13. Haga clic en Aceptar para guardar.

Configuraciones adicionales

Para una identificación adecuada, deben introducirse los siguientes cambios en las políticas de intrusión:

 i. Su variable \$HTTP_PORTS debe incluir el puerto 443 y cualquier otro puerto con tráfico https que será descifrado por su política (Objetos > Administración de Objetos > Conjunto de Variables > Editar el conjunto de variables).

Overview Analysis Polic	cles Devices Objects AMP	🕕 Health System Help v admin v
Object Management		
		🕲 Add Variable Set
A 🔜 Network	Name	Description
Individual Objects	Default Set	This Variable Set is provided by Sourcefire.
Object Groups Security Intelligence	Home Variables	25
Port		
Individual Objects		
📇 Object Groups	Edit Variable HTTP_PORTS	? ×
▲ 📎 VLAN Tag		
Individual Objects	Name: HTTP_PORTS	
Object Groups	Type: Port	
Individual Objects	Available Ports 🖒 🔘 Included Ports (110	Excluded Ports (0)
Cobject Groups	Search by name or value	
Application Filters	🖉 POP*3 🔺 🧩 80	6
\$ Variable Set	ADIUS 👷 81	6
i File List	/* RIP 2 82	
Security Zones	SIP 83	G Contraction of the second seco
Cipher Suite List	P SMTP 84	
Distinguished Name Distinguished Name	SMIPS Include 2 85	8
Chiect Groups	P SSH	
Þ 🖉 PKI	₽ SYSLOG	
Geolocation	TCP high ports	
	2 TELNET	
	P Yahoo Messenger Messages	5
	Je Yahoo Messenger Voice Chat (TCP)	
	Port 443	Add Port Enter a port Add
		Save

ii. La política de análisis de red que inspecciona el tráfico cifrado debe tener el puerto 443 (y cualquier otro puerto con tráfico https que será descifrado por su política) incluido en el campo de puertos de la configuración del preprocesador HTTP; de lo contrario, ninguna de las reglas http con modificadores de contenido http (es decir, http_uri, http_header, etc.) se activará porque esto depende de los puertos http definidos los búfers http en snort no se rellenarán para el tráfico que no pasa por los puertos especificados.

iii. (Opcional pero recomendado para una mejor inspección) Agregue los puertos https a la configuración de **TCP Stream Configuration** en el campo **Realizar reensamblado de flujo en ambos puertos**.

iv. Vuelva a aplicar la directiva de control de acceso revisada durante una ventana de mantenimiento programada.

Advertencia: Esta política modificada puede causar importantes problemas de rendimiento. Esto debe probarse fuera de las horas de producción para reducir el riesgo de interrupción o rendimiento de la red.

Verificación

Descifrar - Renuncia

1. Abra un navegador web.

Nota: El explorador Firefox se utiliza en el ejemplo siguiente. Es posible que este ejemplo no funcione en Chrome. Consulte la sección Resolución de problemas para obtener más información.

2. Acceda a un sitio web de SSL. En el ejemplo siguiente https://www.google.com se utiliza, los sitios web de las instituciones financieras también funcionarán. Verá una de las páginas

thtps://www.google.com/?gws_rd thtps://	=ssl v C Q Search
	This Connection is Untrusted You have asked Firefox to connect securely to www.google.com, 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
	Certificate Status This site attempts to identify itself with invalid information. Unknown Identity The certificate is not trusted because it hasn't been verified as issued by a trusted authority using a secure signature.

Nota:Verá la página anterior si el certificado en sí no es de confianza y su navegador no confía en el certificado de la CA de firma. Para saber cómo determina el explorador los certificados de CA de confianza, consulte la sección Autoridades de certificados de confianza que aparece a continuación.

F

```
☆ 自 🖡
```

Gmail Images

Goo	ogle	
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 owner: Verified by: Sourcefire		
		View Certificate
Privacy & History		
Have I visited this website prior to today?	Yes, 277 times	
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		

Nota: Si se ve esta página, se ha refirmado correctamente el tráfico. Observe la sección **Verificado por: 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	ot	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

Nota: Este es un primer plano del mismo certificado.

3. En el Management Center vaya a Analysis > Connections > Events.

4. Dependiendo del flujo de trabajo, puede o no ver la opción de descifrado SSL. Haga clic en **Vista de tabla de eventos de conexión**.

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. Desplácese a la derecha y busque el estado SSL. Debería ver opciones similares a las

siguientes:

<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

Descifrar - Certificado conocido

1. En FireSIGHT Management Center, vaya a **Analysis > Connections > Events**.

2. Dependiendo del flujo de trabajo, puede o no ver la opción de descifrado SSL. Haga clic en **Vista de tabla de eventos de conexión**.

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. Desplácese a la derecha y busque el estado SSL. Debería ver opciones similares a las siguientes:

<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

Resolución de problemas

Problema 1: Es posible que algunos sitios web no se carguen en el navegador Chrome

Ejemplo:

www.google.com no puede cargar con un Decrypt - Resign usando Chrome.

Motivo

El buscador de Google Chrome puede detectar certificados fraudulentos para propiedades de Google con el fin de evitar ataques de intermediarios. Si el explorador Chrome (cliente) intenta conectarse a un dominio (servidor) de google.com y se devuelve un certificado que no es un certificado de google válido, el navegador denegará la conexión.

Solución

Si experimenta esto, agregue una regla **No descifrar** para DN=*.google.com, *.gmail.com, *.youtube.com. A continuación, borre la caché del explorador y el historial.

Problema 2: Obtención de una advertencia/error no fiable en algunos navegadores

Ejemplo:

Cuando se conecta a un sitio mediante Internet Explorer y Chrome, no recibe una advertencia de seguridad; sin embargo, cuando utiliza el explorador Firefox, debe confiar en la conexión cada vez que cierra y vuelve a abrir el explorador.

Motivo

La lista de CA de confianza depende del explorador. Cuando confía en un certificado, esto no se proclama entre los exploradores y la entrada de confianza normalmente sólo persiste mientras el explorador está abierto, por lo que una vez que se cierre, se eliminarán todos los certificados de confianza y la próxima vez que abra el explorador y visite el sitio, deberá agregarlo a la lista de certificados de confianza de nuevo.

Solución

En este escenario, tanto IE como Chrome utilizan la lista de CA de confianza en el sistema operativo, pero Firefox mantiene su propia lista. Por lo tanto, el certificado de CA se importó al almacén del sistema operativo pero no al explorador Firefox. Para evitar recibir la advertencia de seguridad en Firefox, debe importar el certificado de CA al explorador como una CA de confianza.

Autoridades de certificados de confianza

Cuando se realiza una conexión SSL, el navegador verifica primero si este certificado es de confianza (es decir, antes ha estado en este sitio y le ha dicho manualmente al navegador que confíe en este certificado). Si el certificado no es de confianza, el explorador verifica el certificado de la autoridad certificadora (CA) que verificó el certificado para este sitio. Si el explorador confía en el certificado de CA, lo considera un certificado de confianza y permite la conexión. Si el certificado de CA no es de confianza, el explorador muestra una advertencia de seguridad y le obliga a agregar manualmente el certificado como certificado de confianza.

La lista de CA de confianza en un explorador depende completamente de la implementación del explorador y cada navegador puede rellenar su lista de confianza de forma diferente que otros exploradores. En general, hay 2 maneras en que los exploradores actuales rellenan una lista de CA de confianza:

- 1. Utilizan la lista de CA de confianza en la que confía el sistema operativo
- 2. Envían una lista de CA de confianza con el software y está integrada en el explorador.

Para los exploradores más comunes, las CA de confianza se rellenan de la siguiente manera:

- Google Chrome: Lista de CA de confianza del sistema operativo
- Firefox: Mantiene su propia lista de CA de confianza
- Internet Explorer: Lista de CA de confianza del sistema operativo
- Safari: Lista de CA de confianza del sistema operativo

Es importante conocer la diferencia porque el comportamiento visto en el cliente variará según esto. Por ejemplo, para agregar una CA de confianza para Chrome e IE, debe importar el

certificado de CA al almacén de CA de confianza del sistema operativo. Si importa el certificado de CA al almacén de CA de confianza del sistema operativo, ya no recibirá una advertencia cuando se conecte a sitios con un certificado firmado por esta CA. En el explorador Firefox, debe importar manualmente el certificado de CA al almacén de CA de confianza en el propio explorador. Después de hacerlo, ya no recibirá una advertencia de seguridad cuando se conecte a sitios verificados por esa CA.

Referencias

• Introducción a las reglas SSL