Configuração de uma política de inspeção SSL no Cisco FireSIGHT System

Contents

Introduction **Prerequisites Componentes Utilizados Configurações** 1. Descriptografar e reassinar Opção 1: Usar o FireSIGHT Center como uma autoridade de certificação (CA) raiz Opção 2: Faça com que uma AC interna assine seu certificado Opção 3: Importar um certificado e uma chave CA 2. Descriptografar com chave conhecida Importando certificado conhecido (alternativa para descriptografar e reassinar) Configurações adicionais Verificação Descriptografar - Reassinar Descriptografar - Certificado conhecido Troubleshooting Problema 1: Alguns sites podem não ser carregados no navegador do Chrome Problema 2: Obtendo um aviso/erro não confiável em alguns navegadores Referências Discussões relacionadas da comunidade de suporte da Cisco

Introduction

O recurso de inspeção SSL permite bloquear o tráfego criptografado sem inspecioná-lo ou inspecionar o tráfego criptografado ou descriptografado com controle de acesso. Este documento descreve as etapas de configuração para configurar uma política de inspeção SSL no Cisco FireSIGHT System.

Prerequisites

Componentes Utilizados

- Cisco FireSIGHT Management Center
- Dispositivos Cisco Firepower 7000 ou 8000
- Software versão 5.4.1 ou superior

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.

aviso: Se você aplicar uma política de inspeção SSL no dispositivo gerenciado, ela poderá afetar o desempenho da rede.

Configurações

Você pode configurar uma política de inspeção SSL para descriptografar o tráfego das seguintes maneiras:

- 1. Descriptografar e reinar:
 - Opção 1: Usar o FireSIGHT Center como uma autoridade de certificação raiz (CA) ou
 - Opção 2: Fazer com que uma AC interna assine seu certificado ou
 - Opção 3: Importar um certificado e uma chave CA
- 2. Descriptografar com certificado conhecido:
 - Faça login no FireSIGHT Management Center e, em seguida, navegue até Objects.
 - Na página Objetos, expanda o PKI e selecione CAs internas.
- 1. Descriptografar e reassinar

Opção 1: Usar o FireSIGHT Center como uma autoridade de certificação (CA) raiz

I. Clique em Gerar CA.

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

ii. Preencha as informações relevantes

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. Clique em Gerar CA autoassinado.

Opção 2: Faça com que uma AC interna assine seu certificado

I. Clique em Gerar CA.

🕕 Health System Help 🔻	admin 🔻
💿 Generate CA 💿 Import CA 🔍 Filter	

ii. Preencha as informações relevantes.

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	

Note:Talvez seja necessário entrar em contato com o administrador da CA para determinar se ele tem um modelo para a solicitação de assinatura.

iii. Copie o certificado inteiro incluindo —BEGIN CERTIFICATE REQUEST— e —END CERTIFICATE REQUEST— e salve-o em um arquivo de texto com a extensão .req.

 Subject: 			
Common Name: InternalCA			
Organization: Sourcefire			
Organization Unit: TAC			
SR:			
BEGIN CERTIFICATE REQUEST			*
MIIB42CCAUwCAQAwZTELMAkGA1UEBhMCVVMxCz DAbDb2x1bWJpYTETMREGA1UECgwKU291cmNlZ	AJBgNVBAgMAk1EMREwDwYDVQQ miv7TEMMAaGA1UECwwDVEEDMR		
EQYDVQQDDApJbnRlcm5hbENBMIGfMA0GCSqGSI	b3DQEBAQUAA4GNADCBiQKBgQC5		
XTQixBMnyPNmGTvAXrqG7LhXPXxZ7igF6MfKxwLf Tv1cwNpr4Bnbk9kDS9iDYaftFJzOu8UJ6wKcmxa2I	h8rVwoejHhwbAUro8ju/R3Ig7 IUx80r9v1SKzSiRpr]dSBaRc	- 1	
LSHey3dI0K5SXNKtTb8vBV97RYAfX4VDR7iVDKwx	zQIDAQABoD4wPAYJKoZIhvcN		
the start when the second of the second start of the second starts of th	pLdPqzpTXGkwDAYDVR0TBAUw		
AQKOMS8WETA0BgNVHQ4EFgQUIN/JertJm2Itte3sp AwER/zANRokobkiG9w0RAOUFAAORoORibazWEeX	ilos25vxfvUo/W97uT4DeVLm9		

Note: O administrador da AC solicitou outra extensão de arquivo além do .req.

Opção 3: Importar um certificado e uma chave CA

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

- I. Clique em Importar CA.
- ii. Procure ou cole no certificado.
- iii. Navegue até ou cole na chave privada.
- iv. Marque a caixa criptografada e digite uma senha.

Import Internal Certificate Authority	? ×
Name: Win2008R2	
Certificate Data or, choose a file: Browse	
Hendeling Hendeling	•
Key or, choose a file: Browse	
BEGIN PRIVATE KEY MIIEvgIBADANBgkghkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQDOt4aQGG1QGmA3 ZA1SWMrogBs0BJg2YQgQddVQ9M4kfAQxcwpvP6jHH1Q5AZdyurxKSGY/gQAQZNQUJ gZKxa36F71aHHHk1Bm83Hmzd9oA51+eAYC98xdWeHxgXHWySy4CFxD5kU+MTVonz gIa03gUsz5IHdwagIY2IVb5+YIZINvUTJSIxgUvQxzfGFr8tczDkEky+8yGSluY AgbJEK6n9SRZpBTIHwzPLZJJcyAgMy/LE+9o9GovRkgwKQHHRObvJm2ia0NtgPo NAU/9PUpfHpCtycS5MVryZI+08U12BLaWnGg0WsShIZRIVO2Wed0E8R47TSWtoG JmD/1+AvAgMBAAECggEAZZW0zRUT8v9JNVgNG+CCphfihC7Zvg1mMKe74++EfPT4 rV39T+IY2U3U5vQE9w6Rclux8LxI3D2K06Z3HZ1VvQvBskTUICMuYCvfk6/dmE	•
S Encrypted, and the password is:	
Save	Cancel

Note: Se não houver senha, marque a caixa criptografada e deixe-a em branco.

2. Descriptografar com chave conhecida

Importando certificado conhecido (alternativa para descriptografar e reassinar)

- I. Na página Objetos à esquerda, expanda PKI e selecione Certificados internos.
- ii. Clique em Adicionar certificado interno.
- iii. Procure ou cole no certificado.
- iv. Navegue até ou cole na chave privada.
- v. Marque a caixa **Criptografado** e digite uma senha.

dd Kno	own Internal Certificat	e	? >
Name:	KnownCert		
Certifica	te Data or, choose a file:	Browse	
BEG	IN CERTIFICATE		A
MIIDOD	CCAIACCODssfBhdDsHTDANBgk	ahkiG9w0BAQUFADBeMQswCQYDVQQGEwJV	
UZELMA	kGA1UECAwCTUQxETAPBgNVB	AcMCENvbHVtYmlhMRMwEQYDVQQKDApTb3Vy	
Y2VmaX	0IMQwwCgYDVQQLDANUQUMx	DDAKBgNVBAMMA1RBQzAeFw0xNTA2MDgxNzA4	
MDZaFw	0x0DAzMDQxNzA4MDZaMF4x0	ZAJBgNVBAYTAIVTMQswCQYDVQQIDAJNRDER	
MA8GA1	UEBww1Q29sdW1iaWExEzARB	gNVBAoMCINvdXJjZWZpcmUxDDAKBgNVBAsM	
A1RBQ2	EMMAoGA1UEAwwDVEFDMIIBI	JANBgkghkiG9w0BAQEFAAOCAQ8AMIIBCgKC	
AQEAXA	kHMrRPPyyslwkgwAH0ELtiHmY	Q3/I+MgMzmQiuAhrE3A2mh7t682QrwFgK	*
Key or,	choose a file: Browse		
BEG	IN RSA PRIVATE KEY		
MIIEpAI	BAAKCAQEAxAkHMrRPPyysIwkg	wAH0ELtlHmYQ3/i+MgMzmQiuAhrE3AZm	
h7t6BZC	QrwFgKeMX1KV7LuxXnsuJfpNk	3Dp8fm33TMJQiuAZW6zpusjgOKS3yUs4E	
wG5wco	MVe/baDT2B/XQt3BLUgLsL+T	PipUgazzrFt3rOECvroPxDRCQ/fz8AzXUV	
JFX8WV	0t3SqYtjzw41vU9qai2OuVaANr	IB5iz+9NnwNTpVGvrwHx+iOI/e2ZARI1	
FrtH/eN9	9+/p66tUSILV23rUKUKM0gkh8	3IPs2mu17Upgqv3uYW2OWvnQsz41CGzht	
YonbuE	UCpEtJDWctl/P2rriWECMsumJI	v7hNfKQIDAQABAoIBAC;SNHSDhYkDNWkq	
Sm6RO2	2CO2TUaTeNFud1SO1lfrFR13I5	wqsMS8ArfWuj3rF6P4khWHBh+LDxc1UvP	*
Encry	voted, and the password is:		
		Save	Cancel

Note: Se não houver senha, deixe a caixa Criptografado em branco.

4. Navegue até Policies > SSL e clique em New Policy.

Overview Analysis Policies Devices Objects AM		🕔 Health System He	sp v admin v 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. Forneça um nome e selecione uma **Ação padrão**. A página do editor de política SSL é exibida. A página do editor de política SSL funciona da mesma forma que a página do editor de política de controle de acesso.

Note: Se não tiver certeza sobre a Ação Padrão, Não descriptografar é o ponto inicial recomendado.

6. Na página do editor de política SSL, clique em **Adicionar regra**. Na janela Adicionar regra, forneça um nome para a regra e preencha todas as outras informações relevantes.

Add Rule					? ×
Name Resign		Enabled	Insert below rule	v 1	
Action Do not decrypt	•				
Zone 🛗 Decrypt - Resign	Users Applications Po	orts Category Certificate	DN Cert Status Cipher Suite	Version	Logging
Available and Do not decrypt		Source Zones (0)	Destina	tion Zones (0)	
Sear 🗙 Block		any	any		
arrow 7010 🔀 Block with reset					
501 Monitor					
🚔 📐 External					
A Thereset	Add to				
		e			
	Add to Destinat				
				Add	Cancel

A seção a seguir descreve várias opções na janela Adicionar regra:

Ação

Descriptografar - Reassinar

 O sensor atua como um homem no meio (MitM) e aceita a conexão com o usuário e, em seguida, estabelece uma nova conexão com o servidor. Por exemplo: O usuário digita em https://www.facebook.com em um navegador. O tráfego chega ao sensor, o sensor negocia com o usuário usando o certificado CA selecionado e o túnel SSL A é criado. Ao mesmo tempo, o sensor se conecta a https://www.facebook.com e cria o túnel SSL B.

- Resultado final: O usuário vê o certificado na regra, não no facebook.
- Esta ação requer uma CA interna. Selecione Substituir chave se desejar que a chave seja substituída. O usuário receberá o certificado selecionado.

Note: Isso não pode ser usado no modo passivo.

Descriptografar - chave conhecida

- O sensor tem a chave que será usada para descriptografar o tráfego. Por exemplo: O usuário digita em https://www.facebook.com em um navegador. O tráfego chega ao sensor, o sensor descriptografa o tráfego e inspeciona o tráfego.
- Resultado final: O usuário vê o certificado do facebook
- Esta ação requer um certificado interno. Isso é adicionado em Objetos > PKI > Certificados Internos.

Note: Sua organização deve ser a proprietária do domínio e do certificado. Para o exemplo do facebook.com, a única maneira possível de fazer com que o usuário final veja o certificado do facebook seria se você realmente tivesse o domínio facebook.com (ou seja, sua empresa é o Facebook, Inc) e tivesse a propriedade do certificado do facebook.com assinado por uma CA pública. Você só pode descriptografar com chaves conhecidas para sites que sua organização possui.

A principal finalidade da descriptografia de chave conhecida é descriptografar o tráfego que vai para o servidor https para proteger os servidores contra ataques externos. Para inspecionar o tráfego do lado do cliente para sites https externos, você usará o decodificador de resignação, já que não é dono do servidor e está interessado em inspecionar o tráfego do cliente na sua rede, conectando-se a sites criptografados externos.

Note: Para que DHE e ECDHE descriptografem, devemos estar em linha.

Não descriptografar

O tráfego ignora a política SSL e continua para a Política de controle de acesso.

Certificado

A regra corresponde ao tráfego SSL usando este certificado específico.

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

DN

A regra corresponde ao tráfego SSL usando determinados nomes de domínio nos certificados.

Zones	Networks	VLAN Tags	Users	Applications	Ports	Category	Certificate	DN	Cert Status	Ciphe	r Suite	Version	Logging
Available D	Ns C			0		Subject DI	Vs (0)				Issuer	DNs (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			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 o	or CN				Enter 0	W or CN	Add

Status do certificado

A regra corresponde ao tráfego SSL com esses status 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	i:		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	lid:		Yes	No Do Not N	1atch						
Invalid Cer	tificate:		Yes	No Do Not N	1atch						
Invalid CRI	L:		Yes	No Do Not N	1atch						

Conjunto de Cifras

A regra corresponde ao tráfego SSL usando estes pacotes de cifras.



Versão

As regras se aplicam somente ao tráfego SSL com as versões selecionadas de SSL.

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

Registro

Ative o registro para ver eventos de ligação para o tráfego SSL.

7. Clique em Certificado CA confiável. É aqui que CA confiável é adicionada à política.

Rules Trusted CA Certificates Undecryptable Actions			
Available Trusted CAs 🛛 🕹	0	Selected Trusted CAs	
🔍 Search		🚍 Sourcefire Trusted Authorities	i
🚍 Sourcefire Trusted Authorities	<u> </u>		
A-Trust-nQual-01			
A-Trust-nQual-03			

8. Clique em **Ações não descriptografáveis**. Aqui estão as ações para as quais o sensor não pode descriptografar o tráfego. Você pode encontrar as definições na ajuda on-line (**Ajuda > Online**) do 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	•

- Sessão Compactada: A sessão SSL aplica um método de compactação de dados.
- Sessão SSLv2: A sessão é criptografada com SSL versão 2. Observe que o tráfego é descriptografável se a mensagem de saudação do cliente for SSL 2.0 e o restante do tráfego transmitido for SSL 3.0.
- Conjunto de Cifras Desconhecido: O sistema não reconhece o conjunto de cifras.

- Conjunto de Cifras Não Suportado: O sistema não suporta descriptografia com base no conjunto de cifras detectado.
- Sessão não armazenada em cache: A reutilização de sessão SSL está habilitada, o cliente e o servidor restabeleceram a sessão com o identificador de sessão e o sistema não armazenou esse identificador de sessão em cache.
- Erros de aperto de mão: Ocorreu um erro durante a negociação do handshake SSL.
- Erros de descriptografia: Ocorreu um erro durante a descriptografia do tráfego.

Note: Por padrão, elas herdam a Ação padrão. Se a ação padrão for Bloquear, você poderá enfrentar problemas inesperados

9. Salve a diretiva.

10. Navegue para **Políticas > Controle de acesso**. Edite sua política ou crie uma nova Política de Controle de Acesso.

11. Clique em Avançado e edite Configurações gerais.

Overview Analysis Policies Devices	Objects AM	Р							
Access Control Intrusion - Files N	letwork Discovery	SSL	Application D	etecto	rs	Users	Correlation	Actions	•
TAC Access Control Enter a description Rules Targets (1) Security Intelligence	HTTP Responses	Advance	ed						
General Settings			Ø	Tr	ansp	ort/Net	work Layer	Preproces	sor Se
Maximum URL characters to store in connection	n events		1024	I	gnore	the VLAN	header when	tracking co	nnectio
Allow an Interactive Block to bypass blocking for (seconds) 600					Detection Enhancement Settings				
SSL Policy to use for inspecting encrypted connections None					daptiv	e Profiles	;		
Inspect traffic during policy apply			Yes	Pe	erforn	nance S	ettings		
Network Analysis and Intrusion Policie	General Settings								? × t
Intrusion Policy used before Access Control r determined	Maximum URL chara connection events	cters to st	ore in	1024]
Intrusion Policy Variable Set	Allow an Interactive	Block to by	ypass blocking	600					
Default Network Analysis Policy	SSL Policy to use for	inspecting	g encrypted	SSL Po	olicy				~
Files and Malware Settings	connections	a policy pr	anlı		,				
Limit the number of bytes inspected when do	inspect traffic during	g policy ap	עוקנ	•					
Allow file if cloud lookup for Block Malware to	Revert to Defaults						ОК	Cancel	

- 12. No menu suspenso, selecione sua Política SSL.
- 13. Clique em **OK** para salvar.

Configurações adicionais

As seguintes alterações devem ser feitas nas políticas de intrusão para identificação adequada:

I. A variável \$HTTP_PORTS deve incluir a porta 443 e quaisquer outras portas com tráfego https que serão descriptografadas pela sua política (**Objetos > Gerenciamento de Objetos > Conjunto**

de Variáveis > Editar o conjunto de variáveis).

Overview Analysis Polic	ies Devices Objects AMP						() Health	i System Help v	admin v
Object Management									
							Add Variable	Set 🔍 Filter	
A 💭 Network	Name			Description					
Individual Objects Object Groups	Default Set			This Variable Set is	provided by Sourcefire.				08
Security Intelligence	Home Variables								Ø 🖯
4 🌽 Port									
Individual Objects Goups		Edit Variable HTTP_PORTS				? ×			
▲ 📎 VLAN Tag									
Individual Objects		Name: HTTP_PORTS							
Cobject Groups		Type: Port 👻							
a 🕘 URL		Available Ports 🖒	Included Ports (110)		Excluded Ports (0)				
Chiest Crowns		Search by name or value	A 36	A	none				
Application Filters		0" POP'S	2 80	a l					
S Variable Set		🧀 RADIUS	2 81	<u> </u>					
File List		🥟 RIP	📌 82	6					
Security Zones		n SIP	83	8					
ipher Suite List		JP SMTP	📌 84						
a 🥰 Distinguished Name		J SMTPS	💉 85						
Individual Objects		Je SNMP	📌 86	6					
Cobject Groups		Je SSH	87						
⊳ <i>JP</i> PKI		J ^a SYSLOG	88 🦋						
Geolocation		TCP high ports	89						
		J TELNET	📌 311						
		/* TFTP	283						
		Jahoo Messenger Messages	255						
		Vahoo Messenger Voice Chat (TCP)	Part Lord		Deut .				
		Tanoo Messenger Voice Chat (UDP)	443	Add	Enter a port	Add			
						Save Cancel			

ii. A política de análise de rede que está inspecionando o tráfego criptografado deve ter a porta 443 (e quaisquer outras portas com tráfego https que serão descriptografadas pela sua política) incluída no campo de portas das configurações do pré-processador HTTP, caso contrário, nenhuma das regras http com modificadores de conteúdo http (ou seja, http_uri, http_header, etc.) será acionada porque isso depende das portas http definidas e os buffers http no snort não serão preenchidos para o tráfego que não passa pelas portas especificadas.

iii. (Opcional, mas recomendado para melhor inspeção) Adicione suas portas https às configurações **de configuração de fluxo TCP** no campo **Executar remontagem de fluxo em ambas as portas**.

iv. Reaplique a política revisada de controle de acesso durante uma janela de manutenção programada.

Aviso: essa política modificada pode causar problemas significativos de desempenho. Isso deve ser testado fora do horário de produção para reduzir o risco de paralisação ou desempenho da rede.

Verificação

Descriptografar - Reassinar

1. Abra um navegador da Web.

Nota: O navegador Firefox é usado no exemplo abaixo. Este exemplo pode não funcionar em Chrome. Consulte a seção Solução de problemas para obter detalhes.

2. Navegue até um site SSL. No exemplo abaixo, https://www.google.com é usado. Os sites da instituição financeira também funcionarão. Você verá uma das seguintes páginas:

🛞 http:	s://www.g	joogle.com	n/?gws_rd=ssl
---------	-----------	------------	---------------

ŵ

You have a	asked Firefox to connect securely to www.google.com,	but we can't confirm
connectio	n is secure.	
Add Security	Exception	_
Server	ou are about to override how Firefox identifies this site. egitimate banks, stores, and other public sites will not	t ask you to do this.
	https://www.example.com/2mus.cd.col	Get Certificate
Location:	nttps://www.googie.com/?gws_rd=ssi	
Location: Certificate	status	
Location: Certificate This site a	e Status ttempts to identify itself with invalid information.	<u>_</u> iew

Note:Você verá a página acima se o certificado em si não for confiável e o certificado CA de assinatura não for confiável pelo navegador. Para descobrir como o navegador determina certificados de CA confiáveis, consulte a seção Autoridades de certificado confiáveis abaixo.

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	ship 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		

Note: Se esta página for vista, você regravou o tráfego com êxito. Observe a seção **Verificado por: Sourcefire**.

Could not verify this certificate because the issuer is unknown.

Issueu IO

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

Perio	d of	Val	vtibi	

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

Note: Esta é uma análise detalhada do mesmo certificado.

3. No Management Center, vá para Analysis > Connections > Events.

4. Dependendo do fluxo de trabalho, você pode ou não ver a opção de descriptografia SSL. Clique em **Table View of Connection Events**.

Connections with Application Details > Table View of Connection Events

No Search Constraints (Edit Search)

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

5. Role para a direita e procure o Status do SSL. Você deve ver opções semelhantes às abaixo:

<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

Descriptografar -	Certificado	conhecido
-------------------	-------------	-----------

1. No FireSIGHT Management Center, navegue para **Analysis > Connections > Events**.

2. Dependendo do fluxo de trabalho, você pode ou não ver a opção de descriptografia SSL. Clique em **Table View of Connection Events**.

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>	Reason

3. Role para a direita e procure o Status do SSL. Você deve ver opções semelhantes às abaixo:

<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

Troubleshooting

Problema 1: Alguns sites podem não ser carregados no navegador do Chrome

Exemplo

www.google.com não pode ser carregado com um descriptografar - reinicia usando o Chrome.

Razão

O navegador Google Chrome é capaz de detectar certificados fraudulentos para propriedades do google a fim de evitar ataques de intermediários. Se o navegador Chrome (cliente) tentar se conectar a um domínio google.com (servidor) e um certificado for retornado que não é um certificado válido do google, o navegador negará a conexão.

Solução

Se você experimentar isso, adicione uma regra **Não descriptografar** para DN=*.google.com, *.gmail.com, *.youtube.com. Em seguida, limpe o cache e o histórico do navegador.

Problema 2: Obtendo um aviso/erro não confiável em alguns navegadores

Exemplo

Quando se conecta a um site usando o Internet Explorer e o Chrome, você não recebe um aviso de segurança, mas quando usa o navegador Firefox, você precisa confiar na conexão toda vez que fechar e reabrir o navegador.

Razão

A lista de CAs confiáveis depende do navegador. Quando você confia em um certificado, isso não se propaga em navegadores e a entrada confiável geralmente só persiste enquanto o navegador está aberto, então, uma vez fechado, todos os certificados confiáveis serão removidos e, na próxima vez que você abrir o navegador e visitar o site, você deverá adicioná-lo à lista de certificados confiáveis novamente.

Solução

Neste cenário, o IE e o Chrome usam a lista de CAs confiáveis no sistema operacional, mas o Firefox mantém sua própria lista. Portanto, o certificado CA foi importado para a loja do SO, mas não foi importado para o navegador Firefox. Para evitar receber o aviso de segurança no Firefox, você deve importar o certificado de CA para o navegador como uma CA confiável.

Autoridades de certificado confiáveis

Quando uma conexão SSL é estabelecida, o navegador primeiro verifica se esse certificado é confiável (ou seja, você já esteve neste site antes e manualmente instruiu o navegador a confiar nesse certificado). Se o certificado não for fidedigno, o browser verifica o certificado da Autoridade de Certificação (AC) que verificou o certificado para este site. Se o certificado CA for confiável pelo navegador, ele o considerará um certificado confiável e permitirá a conexão. Se o certificado CA não for confiável, o navegador exibirá um aviso de segurança e forçará você a adicionar manualmente o certificado como um certificado confiável.

A lista de CAs confiáveis em um navegador depende completamente da implementação do navegador e cada navegador pode preencher sua lista confiável de forma diferente dos outros navegadores. Em geral, há duas maneiras de os navegadores atuais preencherem uma lista de CAs confiáveis:

1. Eles usam a lista de CAs confiáveis em que o sistema operacional confia

2. Eles enviam uma lista de CAs confiáveis com o software e ele é incorporado ao navegador. Para os navegadores mais comuns, as CAs confiáveis são preenchidas da seguinte forma:

- Google Chrome: Lista de ACs confiáveis do sistema operacional
- Firefox: Mantém sua própria lista de CAs confiáveis
- Internet Explorer: Lista de ACs confiáveis do sistema operacional
- Safari: Lista de ACs confiáveis do sistema operacional

Éimportante saber a diferença porque o comportamento visto no cliente varia dependendo disso. Por exemplo, para adicionar uma CA confiável para o Chrome e o IE, é necessário importar o certificado de CA para o armazenamento de CA confiável do SO. Se importar o certificado CA para o armazenamento de AC fidedigno do SO, deixará de receber um aviso ao ligar a sites com um certificado assinado por esta AC. No navegador Firefox, você deve importar manualmente o certificado CA para o armazenamento de CA confiável no próprio navegador. Depois de fazer isso, você não receberá mais um aviso de segurança ao se conectar a sites verificados por essa CA.

Referências

• Introdução às regras SSL