

SSL-Proxy Solution for HTTPS Decryption

Hillstone Networks Inc.



Index

1	Reques	t Analysis	3
2	Solutior	1	4
	2.1	Require-mode SSL proxy for HTTPS websites	5
	2.2	Exempt mode SSL proxy, proxy all other websites except baidu	9
3	Result.		13



1 Request Analysis

Secure Sockets Layer (SSL) is a computer networking protocol for securing connections between network application clients and servers over an insecure network, such as the internet. Due to numerous protocol and implementation flaws and vulnerabilities, SSL was deprecated for use on the internet by the Internet Engineering Task Force (IETF) in 2015 and has been replaced by the Transport Layer Security (TLS) protocol. While TLS and SSL are not interoperable, TLS is backwardscompatible with SSL 3.0

When a Web browser tries to connect to a website using SSL, the browser will first request the web server identify itself. This prompts the web server to send the browser a copy of the SSL Certificate. The browser checks to see if the SSL Certificate is trusted - if the SSL Certificate is trusted, then the browser sends a message to the Web server. The server then responds to the browser with a digitally signed acknowledgement to start an SSL encrypted session. This allows encrypted data to be shared between the browser and the server. You may notice that your browsing session now starts with https (and not http).

In order to provide public key to client, HTTPS site is using certificate issued by CA organization, you can find in client the below information:



neral Det	ails Certification Pat	h	
ow: <al< th=""><td>></td><td>~</td><td></td></al<>	>	~	
ield		Value	^
Issuer		Symantec Class 3 Secure Serv	
Valid fro	m	Monday, August 15, 2016 8:0	
Valid to		Thursday, August 17, 2017 7:	
Subject		baidu.com, service operation	
🗐 Public k	ey	RSA (2048 Bits)	
🛐 Subject	Alternative Name	DNS Name=*.baidu.com, DNS	
Basic Co	onstraints	Subject Type=End Entity, Pat	
Enhance	ed Kev Hsane	Server Authentication (1.3.6	×
N = baidu. U = servio	com e operation departme Baidu Netcom Science	nt. Technology Co., Ltd	
= BeiJing = beijing = beijing = CN			

To assure the security of sensitive data when being transmitting over networks, more and more websites adopt SSL encryption to protect their information. The device provides the SSL proxy function to decrypt HTTPS traffic. There are three work modes: Require mode, Exempt mode, Offload mode. Here we will test the first two modes.

2 Solution

Hillstone FW deployed at network exit in routing mode, firmware: SG6000-M-5.5R3.bin



2.1 Require-mode SSL proxy for HTTPS websites

(1) Create SSL-proxy profile

sslproxy-profile "require-baidu" mode require description baidu-proxy cert-subject-name baidu.com

exit

(2) Bind this SSL-proxy profile to policy

Policy Co	onfiguration							?
Basic	Protection	Options						
	Schedule:				¥]		
	QoS:					(1-1024)		
	Log: [Deny		Session sta	rt 📃	Session end		
	SSL Proxy: [Enable	Profile:	require-baidu	v			
	Position:				*]		
	Description:					(0-255) chars		
							ок	Cancel

(3) Export CA certificate from FW and import to browser

Hillstone Eleno		Destooant	Genter	Monitor	Policy	Object	Network	System
System Internation Desice Management Social Server Upgrade Management Upgrade Management Lownee Mad Server SASS Parameters	Key Trust Domain Trust Domain Content Action:	Management Invet_domain_set_p CA Centificate Insport Esport	rsor_3146 © Local	it. Certificatis (C)	31) chars PRCS#12	0	PhCS#12-der	
(B) HA 						OK	Canter	

Import the root certificate to the "Trusted Root Certification Authorities" of

client

browser



lly Name)DO CA ıíz Certicá	ľ
DO CA líz Certicá	1
iz Certicá	
CION GEN	
IZ FNMT	
AIZ MTIN	
RAIZ1	
M	
ova Ljublja	
s Authentic	1
Advar	nce
	RAIZ1 DM s Authentic Advar

(4) Verify the proxy result

A. Before the proxy



百度 证 v https://www.baidu.com/	5 a + Q
File Edit View Favorites Tools Help	
苏州: 🔆 16°C 良 90 宝箱	
Certificate ×	
General Details Certification Path	
Certificate Information	Bai
This certificate is intended for the following purpose(s):	
Ensures the identity of a remote computer Refer to the certification authority's statement for details.	
Issued to: baidu.com	视频 购物
Issued by: VeriSign Class 3 Secure Server CA - G3 Valid from 12/29/2015 to 12/30/2016	
Learn more about <u>certificates</u>	
ОК	

B. After proxy



	Certifica	te 🗙	
General	Details Certification Path		
	Certificate Information		
Thi	 s certificate is intended for the All application policies 	e following purpose(s):	Baico
. III			
	Issued to: baidu.com		
	Issued by: SG-6000		见频 购物
	Valid from 12/29/2015 to 12	/30/2016	
		Issuer Statement	

Certificate		
Certificate Information	E	Bai 💩
This certificate is intended for the following purpose(s): • Ensures the identity of a remote computer		
Issued to: badu.com	视频	网络
Issued by: 56-6000 Valid from 12/29/2015 to 12/30/2016.		
Topuer Statement		



2.2 Exempt mode SSL proxy, proxy all other websites except baidu

(1) Create SSL-proxy profile

sslproxy-profile "except-baidu" mode exempt description proxy all except baidu cert-subject-name baidu.com

exit

(2) Bind this SSL-proxy profile in policy

Policy Co	onfiguration							?
Basic	Protection	Options						
	Schedule:				¥			
	QoS:					(1-1024)		
	Log: [Deny		Session star	t 📃	Session end		
	SSL Proxy: [Enable	Profile:	except-baidu	×			
	Position:				~			
	Description:					(0-255) chars		
							ОК	Cancel

(3) Export CA certificate from FW and import to browser

Hillstone E1600		Destionent	Conter	Monitor	Policy	Object	Network	System
System Information System Information Device Management State Depice Management Depice Management Lowree Lowree Mad Server SAKS Parameters	Key Trust Domen Trust Oomain Content Action:	Management trust_domain_set_p CA Centificate Import Export	atory_2048 ③ Local	ाः Certificatie ()	31) chàn PRESet2	0	PhCS#12-der	
HA Hild Agent Hild Agent Hild Interv Cloud View Hild Dagrestic Tool						DK	Caner	

Import the root certificate to the "Trusted Root Certification Authorities" of

client browser



Issued To Issued By Expiratio Friendly Name AAA Certificate Ser AAA Certificate Services 1/1/2029 COMODO CA AC Raíz Certicámar AC Raíz Certicámara 4/3/2030 AC Raíz Certicá AC RAIZ DNIE AC RAIZ DNIE 2/9/2036 DIRECCION GEN AC RAIZ FNMT-RCM AC RAIZ FNMT-RCM 1/1/2030 AC RAIZ FNMT AC1 RAIZ MTIN AC1 RAIZ MTIN 11/4/2019 AC1 RAIZ MTIN
ACEDICOM Root ACEDICOM Root 4/14/2028 EDICOM ACEDICOM Root ACRLB 5/15/2023 NLB Nova Ljublja Actalis Authenticati Actalis Authentication 6/25/2022 Actalis Authentic

(4) Verify the result

A. The proxy site:



	Certificate	
17	General Details Certification Path	
	Certificate Information	
	This certificate is intended for the following purpose(s): • All application policies	■时尚女鞋短裤 ■ 淘抢购电
	Issued to: *.tmall.com Issued by: SG-6000	W3 W P
	Valid from 12/14/2015 to 12/14/2016	All Contractions
	Issuer Statement	the the



NE NETWORKS × (https://www.facebook.com ×	
Certificate ×	
General Details Certification Path	
Certificate Information This certificate is intended for the following purpose(s): • All application policies	
Issued to: *.facebook.com	
Valid from 3/1/2016 to 6/1/2017	
Issuer Statement	
ОК	

B. Baidu is excepted for proxy



	Certificate	
Gene	al Details Certification Path	
1	Certificate Information	Ba
	his certificate is intended for the following purpose(s): • Ensures the identity of a remote computer	
	-	
	Refer to the certification authority's statement for details.	
-	Issued to: baidu.com	100 1
	Issued by: VenSign Class 3 Secure Server CA - G3	
	Issued by: VenSign Class 3 Secure Server CA - G3 Valid from 12/29/2015 to 12/30/2016	ine constanti

3 Result

(1) ssl-proxy need to check for CA certificate, and use the subject name in certificate which is cn=xxx. Such as google/facebook those different applications need to be identified by decryption



	tertificate	Exe		
General Details Certification P	ath			
Show: <all></all>	÷			
Field	Value	*		
Signature hash algorithm	shal			
Usuer Valid from	Hilstone Networks, 5G-6000 Thursday, November 3, 2016			
Valid to	Thursday, January 26, 2017 9			
Public key	RSA (2048 Bits)			
Subject Alternative Name	DNS Name =www.google.com.hk			
KN - mode con				
U * Google Inc				
5 = California				
C = 05				
1		- 1		
1	Edit Properties Copy to File			
Learn more about certificate det	ala			
22 mm		Google	con	
	0			
STONE NETWORKS ×)	• (19) Facebook /.facebook.com	X Google		
STONE NETWORKS ×	(19) Facebook .facebook.com Certificate	x Google		
STONE NETWORKS ×	(19) Facebook	x Google		
STONE NETWORKS ×	• (19) Facebook v.facebook.com Certificate ion Path	× Google		
STONE NETWORKS ×	(19) Facebook	x Google		
STONE NETWORKS ×	(19) Facebook	× Google		
STONE NETWORKS ×	(19) Facebook	× Google		
STONE NETWORKS ×	(19) Facebook /.facebook.com Certificate ion Path Value 00 a2 1c 1f 4b sha 1RSA	× Google	••••	
STONE NETWORKS ×	(19) Facebook	x Google	•••	
STONE NETWORKS ×	 (19) Facebook /.facebook.com Certificate ion Path Value 00 a2 1c 1f 4b sha1RSA m sha1 Hillstone Networks, SG- Tuesday, March 1, 201 	Coogle Coogle		
STONE NETWORKS ×	 (19) Facebook /.facebook.com Certificate ion Path Value 00 a2 1c 1f 4b sha 1RSA m sha 1 Hillstone Networks, SG- Tuesday, March 1, 201 Thursday, June 1, 201 	Google		
STONE NETWORKS ×	 (19) Facebook /.facebook.com Certificate ion Path Value 00 a2 1c 1f 4b sha 1RSA im sha 1 Hillstone Networks, SG- Tuesday, March 1, 201 Thursday, June 1, 201 *.facebook.com, Faceb PSA (20:49 Bith) 	Google	•••	
STONE NETWORKS ×	 (19) Facebook /.facebook.com Certificate ion Path Value 00 a2 1c 1f 4b sha 1RSA im sha 1 Hillstone Networks, SG- Tuesday, March 1, 201 Thursday, June 1, 201 .facebook.com, Facet RSA (2014 Rits) 	Google		
STONE NETWORKS ×	 (19) Facebook /.facebook.com Certificate ion Path Value 00 a2 1c 1f 4b sha 1RSA im sha 1 Hillstone Networks, SG- Tuesday, March 1, 201 Thursday, June 1, 201 .facebook.com, Faceb RSA (2048 Bits) 	Google		
STONE NETWORKS ×	 (19) Facebook /.facebook.com Certificate ion Path Value 00 a2 1c 1f 4b sha 1RSA wisha 1 Hillstone Networks, SG- Tuesday, March 1, 201 *.facebook.com, Faceb RS& (2048 Bits) 	Google	 *** *** 新ff 	
STONE NETWORKS Stops://www. General Details Certification General Details Certification Show: <all> Field Signature algorithm Signature hash algorith Signature hash algorith Signature hash algorith Signature hash algorith Signature hash algorith Signature hash algorith Signature hash algorith Subject Details courses CN = *.facebook.com O = Facebook, Inc. L = Menio Park S = CA C = US</all>	 (19) Facebook /.facebook.com Certificate ion Path Value 00 a2 1c 1f 4b sha 1RSA im sha1 Hillstone Networks, SG- Tuesday, March 1, 201 *.facebook.com, Facet RSA (2048 Rite) 	Google X Google X	 ●●●● ●●● ●●● ●●● ●● ● ●	
STONE NETWORKS Stops://www. General Details Certificate Show: <all> Field Signature algorithm Signature hash algorithm Signature hash algorithm Signature hash algorithm Signature hash algorithm Subject Public kew CN = *.facebook.com O = Facebook, Inc. L = Menio Park S = CA C = US</all>	 (19) Facebook /.facebook.com Certificate ion Path Value 00 a2 1c 1f 4b sha 1RSA im sha 1 Hillstone Networks, SG- Tuesday, March 1, 201 Thursday, June 1, 201 *.facebook.com, Faceb RSA (2048 Rite) 	Google X Google X	•••• 新F5	
STONE NETWORKS Stops://www. General Details Certificate Show: <all> Field Field Signature algorithm Signature hash algorithm Signature hash algorithm Signature hash algorithm Subject Public kew CN = *.facebook.com O = Facebook, Inc. L = Menio Park S = CA C = US</all>	 (19) Facebook /.facebook.com Certificate ion Path Value 00 a2 1c 1f 4b sha 1RSA im sha 1 Hillstone Networks, SG- Tuesday, March 1, 201 Thursday, June 1, 201 .facebook.com, Faceb RSA (2048 Bits) 	× Google	•••• 新FF	
STONE NETWORKS Stops://www. General Details Certification Show: <all> Field Signature algorithm Signature algorithm Signature hash algorithm Valid from Valid from Subject Valid to Subject CN = *.facebook.com O = Facebook, Inc. L = Menlo Park S = CA C = US</all>	 (19) Facebook /.facebook.com Certificate ion Path Value 00 a2 1c 1f 4b sha 1RSA im sha 1 Hillstone Networks, SG- Tuesday, March 1, 201 Thursday, June 1, 201 .facebook.com, Facet BSA (2048 Rite) 	× Google	 ●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●	
STONE NETWORKS Stops://www. General Details Certification Show: <all> Field Signature algorithm Signature algorithm Signature hash algorithm</all>	 (19) Facebook /.facebook.com Certificate ion Path Value 00 a2 1c 1f 4b sha1RSA w sha1 Hillstone Networks, SG- Tuesday, March 1, 201 Thursday, June 1, 201 .facebook.com, Facet RSA (2048 Bits) 	× Google	•••• 新FF 州1日	
STONE NETWORKS	 (19) Facebook /.facebook.com Certificate ion Path Value 00 a2 1c 1f 4b sha 1RSA v Value 00 a2 1c 1f 4b sha 1RSA im sha 1 Hillstone Networks, SG- Tuesday, March 1, 201 Thursday, June 1, 201 *.facebook.com, Facet RSA (2014R Bits) Edit Properties Co 	× Google	•••• 新FF 州市	
ONE NETWORKS × Image: Constraint of the second s	 (19) Facebook /.facebook.com Certificate ion Path Value 00 a2 1c 1f 4b sha 1RSA Im sha 1 Hillstone Networks, SG- Tuesday, March 1, 201 Thursday, June 1, 201 *.facebook.com, Facet RSA (2048 Rite) 	× Google	···· 新FF 州市	

(2) Require mode - the device perform the SSL proxy function on the communication encrypted by the specified website certificate. The communication encrypted by other website certificates will be bypassed.



(3) Exempt mode - the device does not perform the SSL proxy function on the communication encrypted by the specified website certificate. The communication encrypted by other website certificates will be proxied by SSL proxy function.