HTTPS terminálása Server Name Indication TLS kiterjesztés használatával *Zorp Gateway*-en

2022. július 28.

Célunk a <u>Zorp Gateway</u> konfigurálása HTTPS Secure Sockets Layer (SSL) terminálására úgy, hogy Server Name Indication (SNI) Transport Layer Security (TLS) kiterjesztést is használunk.



Szerzői jog © 1996-2022 BalaSys IT Ltd.

Tartalom

1. A probléma bemutatása	3
2. A megoldás bemutatása	4
3. Technikai megvalósítás	5
4. Konklúzió	8

1. A probléma bemutatása

Ha nem megoldható, hogy a HTTPS-en érkező kéréseket webszerverünk SSL terminálja, lehetőségünk van *Zorp Gatewayel* ezen kapcsolatok SSL terminálására. Ilyen esetben egyre gyakrabban van szükség az SNI TLS kiterjesztés használatára. SNI alkalmazása esetén egyazon IP cím és port használata esetén is lehetőségünk van különböző tanúsítványt felmutatni a kliens által elérni kívánt host név alapján.

2. A megoldás bemutatása

Zorp Gatewayen Encryption policyban SNI alapú tanúsítvány (SNI-based certificate) generátor használatával SSL terminálni tudjuk a HTTPS-en érkező kéréseket.

3. Technikai megvalósítás

- 1. Hozza létre vagy importálja a megfelelő tanúsítványokat a *Zorp Management Console (ZMC)* Public Key Infrastructure (PKI)-ban.
- 2. Hozzon létre egy Encryption policyt.
- 3. Konfigurálja a *client_certificate_generator* paramétert az SNI alapú tanúsítvány (SNI-based certificate) használatával.

🍐 😫 😫 🔍 🔄 📽) 6	2	Z	i 📝 🙈										
Firewall Rules Services Policies Proxies Instar	nces Ac	dvance	d											
Policy Description Authentication policy		Polic	у											
Authentication provider		q	ass:	ClientOnlyEncryptio	n					<u>•</u>				
Authorization policy		F	Param	eter	Туре		Value			<u>*</u>				
Detector Policy		C	dient_	certificate_generato	or dass_type_	_certificategenerator_instance	SNIBasedCertificate(hostname_certificate_map=(RegexpMatcher(ignore_case=TRUE, match_ist=("download.domain.com")): Certificate(certificate_fie_path=do							
 Encryption policy 	- 11	c	dient_	verify	dass_type_	_clientcertificateverifier_instance	xe ClientNoneVerifier()							
Matcher policy	- 11	C	dient g	ssl_options	dass_type_	_clientssloptions_instance	ClientSSLOptions(cipher=SSL_CIPHERS_HIGH, cipher_server_preference=FALSE, timeout=300, disable_ttsv1=TRUE, disable_ttsv1_1=FALSE, disable_ttsv1_2=F.							
NAT policy			ZMC - Edit class X											
Resolver policy			Edit value of client partificate nanerator											
Stacking provider			Eait value of chenit_certaricate_generator											
				Class: SNIBas	edCertificate									
				Parameter	1	Туре		Value	_					
				hostname_cer	tificate_map	hash_SNIBasedCertificate_hostna	ime_certificate_ma;	 (RegexpMatcher(ignore_case=TRUE, r Contificate(contificate, file, path=numu)) 	natch					
				Geradic		bass_type_certceruncate_instan		ceruncate(ceruncate_ne_paur=www)						
									*					
				<					•					
				<u>/</u> Edit	Select	variable 🔐 Unset								
				-										
								Cancel <	¢ [®] ок					
	Ŧ	4		. [~ I			_					
New Delete			2	Edit Sele	ct variable	Unset Unset								

1. ábra - Client Certificate Generator szerkesztése

4. Állítsa be a domain tanúsítvány párokat a *RegexpMatcher* segítségével.

<



2. ábra - Domain tanúsítvány párok

5. Állítsa be a default tanúsítványt.

۵ 😭 😫 🛛 کې ا) [🛃] [8	3	2 🔗									
Firewall Rules Services Policies Proxies Instan	ces Adva	anced											
Policy Description Authentication policy		Policy	_										
Authentication provider		Class:	Cler	tOnlyEncryption									
Authorization policy		Para	meter	Туре	Va	alue		<u> </u>					
Detector Policy		dient	t_certi	ficate_generator dass_typ	e_certificategenerator_instance SN	NIBasedCertificate	e(hostname_certificate_map={RegexpMate	cher(ignore_case=TRUE, match_list=("download.domain.com")): Certificate(certificate_file_path=dc					
 Encryption policy 		dient	t_verif	y dass_typ	e_clientcertificateverifier_instance Cl	ientNoneVerifier())						
Matcher policy		dient	t_ssl_o	ptions dass_typ	e_clientssloptions_instance Cl	entSSLOptions(ci	pher=SSL_CIPHERS_HIGH, dpher_server_	preference=FALSE, timeout=300, disable_tbsv1=TRUE, disable_tbsv1_1=FALSE, disable_tbsv1_2=F.					
NAT policy			0	ZMC - Edit class				×					
Resolver policy													
Stacking provider		Edit value of client_certificate_generator											
		Class: SNIBosedCerbficste											
				Parameter	Туре		Value						
				hostname_certificate_map	hash_SNIBasedCertificate_hostname	_certificate_map	{RegexpMatcher(ignore_case=TRUE, ma	std i					
				default	class_type_certcertificate_instance		Certificate(certificate_file_path=www)						
				<u> </u>									
				<u>∕</u> Edit <u>S</u> elec	t variable								
		1					🧏 Cancel 🥰						
1	7		2010	[Barrin [Q., .								
New Selete ZEdit		-	Edit	≥eiect variable	Unset								

3. ábra - Default tanúsítvány beállítása

6. Használja fel a létrehozott Encryption policyt egy tűzfal szabályban.

w w w w w w w w w w w w w w w w w w w	<u> </u>	. 😭 🛃 🎯 🛙 🛃	🧭 📝 🙈														
ne	Firewall Rules Services Polici	es Proxies Instances Advances	ced														
Wt Source lifes: Index local Index local Index local Index local Source Part Source Zone / Subret Dest. Unce. Dest. Hore. Source Note Note Value Value Value Value Value Value Value Value Value Value Value Value Value Value Value Value Value Value Value Value Value Value Value Value Value Value Value Value Value Value Value Value Value Value Value Value Value Value Value Value Value Value <td colspan="6" th="" value<=""><th>None</th><th>· · · · · · · · · · · · · · · · · · ·</th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th></td>	<th>None</th> <th>· · · · · · · · · · · · · · · · · · ·</th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th>						None	· · · · · · · · · · · · · · · · · · ·									
IC 4% etcroit internet total total total IV 20% 4% etcroit internet total total IV 20% 24% etcroit internet total total IV 20% 24% etcroit Internet total total IV 10% 4% etcroit Internet total total IV 10% 10% 10% 10% total total total IV 10% 10% 10% 10% 10% 10% total total total IV 10%	Id VPN Source Iface	. Source Iface. Group	Protocol ICMP type	ICMP code Source	Port Dest. Port	Source Zone / Subnet	Dest. Zone / Subnet	Dest. Iface.	Dest. Iface. Group	Service	Instance						
Image: With Today: Image: With Today: Image: With To	1		TCP		443	internet	internet			test	https						
New Children Pitte		ZMC - Edit ru Enabled Description: Condition: Service: Description: Class: Description: Proyr class Encryption: Routing Router: Chainer: Limit: NAT Source I Destina Run In this ins	ule ervice Tage Lunits ovvided by this rule g service g service g service francementRouter() francementRoute		Authentication Authentication Authentication Authentication Advanced	n poley: poley: 	X Create new										
	New Delete	ZEdit									ictive coor						

4. ábra - Encryption policy használata

4. Konklúzió

A fenti leírás segítségével, a *Zorp Management Console (ZMC)* felületen tudunk SNI TLS kiterjesztés használatával HTTPS SSL terminálást beállítani a *Zorp Gateway* tűzfalunkon.

A funkcióról bővebb leírás a *How to configure HTTPS proxying* dokumentációban angol nyelven található.