# Technical Note: How to sign a CA certificate on Windows server 2008 and import certificate for SSL inspection to a FortiGate.

**Description** >> This article describes about how to Sign a CA certificate on Windows server 2008 and import the certificate for SSL inspection.

Purpose of configuring SSL inspection on FortiGate unit with CA certificate signed by Windows CA: When SSL inspection for HTTPS traffic (Deepscan) is enabled on FortiGate unit, browser will display invalid certificate error while accessing HTTPS websites.

- When SSL inspection option enabled on FortiGate unit, FortiGate unit will act as man in the middle to scan the SSL sessions. FortiGate unit will decrypt the SSL sessions and re encrypt them with its own certificate (FortiGate\_CA\_SSLProxy).
- > The client browser show an error message "invalid certificate" becuase the client browser cannot validate the certificate used to encrypt the session.
- > To overcome this behaviour, you can import the FortiGate\_CA\_SSLProxy certificate to client browser. But this may not be possible in large networks.
- > In Windows Active directory Domain environments, we can generate a CA certificate signed by the Windows CA and configure the certificate for SSL inspection.
- Since the certificate is signed by the domain controller CA, This certificate will be trusted by all workstations which are member of the domain. Manually importing the certificates on to computers is not necessary.

### Note:-

- Mozilla Firefox and other open source browsers do not depend on the local certificate store of windows. You need to import the certificate manually in these browsers.

## **Expectations and Requirements;**

To sign certificate using Windows CA, CA server should be installed on Windows AD.

## **Configuration steps**

- 1) Generate a CSR on FortiGate unit.
- 2) Sign the CSR on Windows CA and download the signed certificate from Windows CA.
- 3) Import the signed certificate on to FortiGate unit.
- 4) Configure SSL inspection to use the new certificate.

- Generate a Certificate Signing Request on FortiGate unit.
- Log in to FortiGate unit GUI >> Go to System >> Certificates >> Local Certificates >> Select "Generate"



• Enter the parameters as per your requirement, Select "Enrollment Method" as "File Based" and Click on OK to generate the certificate Signing request.

FortiGate VM	0				
Global				Generate Certificate	Signing Request
Dashboard	Certificate Name	fgt.viswa.local			
Top Sources	Subject Information				
<ul> <li>Top Destinations</li> </ul>	ID Type	Domain Name 💌			
Top Applications	Domain Name	fgt.fglab.com			
Threat History	Optional Information				
E 🛃 VDOM	Organization Unit	Fortinet	⊡		
🖲 🕮 Network	Organization	Fortinet	]		
🖶 🌃 Admin	Locality(City)	NA			
E Certificates	State/Province	NA	1		
•••• Local Certificates	Country/Region				
CA Certificates	E-mail	fgt@viswa.local			
- CRL	Subject Alternative Name				
🗉 🕎 Log Config					
	Кеу Туре	RSA 🔻			
	Key Size	2048 Bit 💌			
	Enrollment Method	⊙ File Based O Online SCEP			
				ОК	Cancel

• Go to System >> Certificates >> Local Certificates >> Select certificate created in the previous step and click on Download button to download the CSR.

Sign the CSR on Windows CA and download the signed certificate from Windows CA.

- Go to Active directory Web enrolment page on your Windows CA.
- Click on "Request a certificate"
- Select "Advanced certificate request"
- Select "Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file"
- Using text editor (notepad), open the CSR downloaded in step1.
- Copy the contents of the CSR to clipboard and paste the contents of the certificate in "Saved Request"
- In "Certificate Template", select template as "Subordinate Certifcate Authority" and Click "Submit" button.

G S ♥ Image http://localhost:8080/certsrv/certrqxt.asp
🔆 Favorites 🙀 😰 Suggested Sites 🔻 🙋 Web Slice Gallery 👻
Microsoft Active Directory Certificate Services
Microsoft Active Directory Certificate Services viswa-WIN-A0FABPCCUES-CA
Submit a Certificate Request or Renewal Request
To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by
Saved Request:
BEGIN CERTIFICATE REQUEST Base-64-encoded MIIC4DCCAcgCAQAwgYcxCzAJBgNVBAYTAklOMQswu extificate request BxMCTKEXETAPBgNVBAOTCEZvcnRpbmVOMRewDwYD (CMC or AlUEAxMPZmd0LnZpc3dhLmxvY2FsMR4wHAYJKoZI PKCS #10 or bG9jYWwwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAw PKCS #7): sUsF/KMLYS4/jX21cRpo/kv1EpE6111F2WS7W/PF
Certificate Template: Subordinate Certification Authority
Additional Attributes:
Attributes:
Submit >

• Download the certificate in next screen and save it locally on hard drive.

## Step3

- Import the signed certificate on to FortiGate unit.
- Log in to FortiGate unit GUI >> Go to System >> Certificates >> Local Certificates >> Select the certificate signing request created in step1 and click on "Import" button.

Global	👕 Delete 📑 Generate	🦉 Import 🛛 😹 View Certificate Detail 🛛 🚵 Download 🖓 Edit Comments
🗟 🕙 Dashboard	Eartinet CA SSI Proxy C =	Subject
- Status	Fortinet Factory	
Top Sources	Fortinet_Factory2	
Top Destinations	Fortinet_Firmware	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN = FortiGate, emailAddress = su
Top Applications	Fortinet_Wifi	OU = Domain Control Validated, OU = PositiveSSL, CN = auth-cert.fortinet.com
Traffic History	🗹 fgt.viswa.local	
Threat History		
🗉 🎰 VDOM		
🗉 🚊 Network		
🖻 🐻 Config		
🖶 🜃 Admin		
🖻 📧 Certificates		
······································		
···· • Remote		
• • CA Certificates		
- CRL		
🗄 📴 Log Config		

- In the Import certificate page, select Type as "Certificate" and Click on Choose file Button.
- Navigate to the Certificate downloaded from Windows CA in step 2, select the certificate and click on OK. You will get message "Upload Certificate successfully"
- Click on Return button and verify the certificate has been imported properly.

Global		Certificate Detail Information
Clobal  Clobal	Certificate Name Issuer Subject Valid From Valid To Version Serial Number	Americal DC = local DC = viswa, CN = viswa-WIN-A0FABPCCUES-CA         C = IN, ST = NA, L = NA, O = Fortinet, OU = Fortinet, CN = fgtviswa.local, emailAddress = fgt@viswa.local         2013-10-28 12:02:34 GMT         2015-10-28 12:12:34 GMT         3         1a:ba:ddt7/:00:00:00:00:00:39         Name: V509v3 Subject Key Identifier         Critical: no         Content         E2:35:E2:5AE:0:F3:CA:3A:EE:43:FE:09:E7:4E:1A:E9:2C:28:E8:3A         Name: X509v3 Authority Key Identifier         Critical: no         Content         Keylid:64:37:43:7C:4F:BE:6E:14:68:44:0D:6E:0D:A2:E6:0B:EC:55:A9:DC         Name: X509v3 CRL Distribution Points         Critical: no         Content         Full Name: URI:1dap:///CN=viswa-WIN-A0FABPCCUES-CA, CN=WIN-A0FABPCCUES, CN=CDP, CN=Public%20Key%20Services, cN=Services, CN=Content         Full Name: 4uthority Information Access         Critical: no         Content         CAlssuers - URI:1dap:///CN=viswa-WIN-A0FABPCCUES-CA, CN=AIA, CN=Public%20Key%20Services, CN=Services, CN=C         Name: 1.3.6.1.4.1.311.20.2         Critical: no         Content:         CAlssuers - URI:1dap:///CN=viswa-WIN-A0FABPCCUES-CA, CN=AIA, CN=Public%20Key%20Services, CN=Services, CN=C         Issuers - URI:1dap:///CN=viswa-WIN-A0FABPCCUES-CA, CN=AIA, CN=Public%20Key%20Services, CN=Services, CN=C <t< td=""></t<>
		Close

> Configure SSL inspection to use the new certificate.

You can select the SSL inspection certificate under: Policy >> Policy >> SSL/SSH Inspection Options >> Select the profile used in firewall policy >> CA Certificate

FortiGate VM64			
System			Edit SSL/SSH Inspection Profile
Router Policy & Objects	Name Comments	default all default services	
<ul> <li>Policy</li> <li>IPv4</li> <li>Explicit Proxy</li> <li>Do5</li> <li>Proxy Options</li> <li>SSL/SSH Inspection</li> <li>Cobjects</li> <li>Load Balance</li> <li>Monitor</li> </ul>	SSL Inspection Options Enable SSL Inspection of	<ul> <li>Multiple Clients Connecting to Multiple Servers</li> <li>Protecting SSL Server</li> </ul>	
	CA Certificate Inspection Method Inspect All Ports ONT HITPS ONT FOP3S ONT FOP3S ONT IMAPS ONT FTPS Exempt from SSL Inspect Web Categories Addresses SSH Inspection Options	fgt.viswa.local       Please Select       K       Fortinet_CA_SSLProxy       ca_cert_2       fgt.viswa.local       ssl_fg       993       990       Click to add       V	
	SSH Port SSH Port Protocol Exec Port-Forward SSH-Shell X11-Filter	Any  Specify 22  Action Block Log	
Security Profiles	Common Options Allow Invalid SSL Certificates		

> Verification.

Since the SSL inspection certificate is signed by the domain controller CA, all the hosts part of the domain will trust the CA certificate. When client access a HTTPS website with deep scan/SSL full inspection enabled on FortiGate unit, browser will not display certificate error message.

