

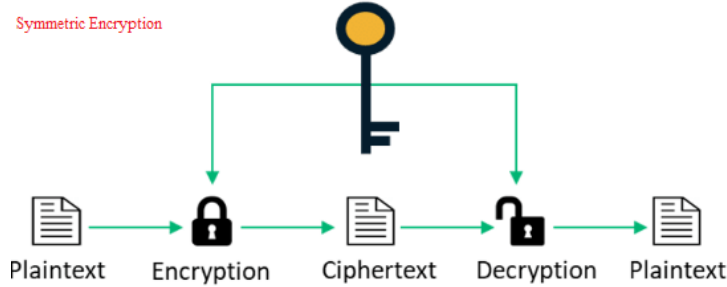
# SSL Encryption and Decryption (SSL Deep Inspection)

Bir istemci tarayıcıdan bir HTTPS protokolüyle bir web sayfasına erişmek istediğinde paketi hedef Web sunucusuna gönderirken, gönderim sürecinde paket içerisindeki verilerin gizliliğini sağlayabilmek için SSL sertifikasını kullanarak paketi şifreler. Bu şifre paket hedef Web sunucusuna iletilene kadar ki süreçte içeriği kontrol edilemez. Bu durumda kurumsal networklerde bulunan istemciler için bakıldığında, trafiği SSL sertifikası ile şifreleyerek gönderilen paketler kurumundaki Firewall'dan geçmesi gerektiğinde içeriği kontrol edilemeyeceği için sağlıklı aksiyon alamayacaktır. Bu süreci daha iyi açıklayabilmek için SSL sertifikasıyla şifreleme sürecinin nasıl gerçekleştiğinden ve Firewall üzerinde konfigürasyonlarının nasıl yapıldığına bakmak gerekecektir.

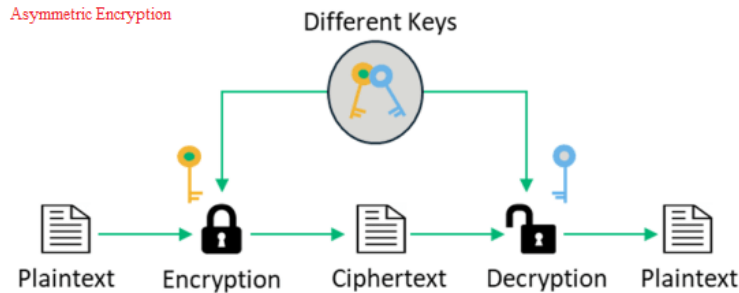
## SSL Şifreleme Süreci

SSL şifreleme sürecinden bahsetmeden önce şifreleme yaklaşımlarından bahsetmek gerekecektir. Şifreleme algoritmaları temelde Simetrik ve Asimetrik şifreleme olarak iki gruba ayrılmaktadır.

Simetrik şifreleme yaklaşımında büyük boyutlarda tek bir şifreleme anahtarı kullanılır. Veriler oluşturulan tek bir anahtar ile hem şifrenir hem de şifreleri çözülür. Simetrik şifreleme algoritmalarına örnek olarak AES şifreleme algoritması verilebilir.

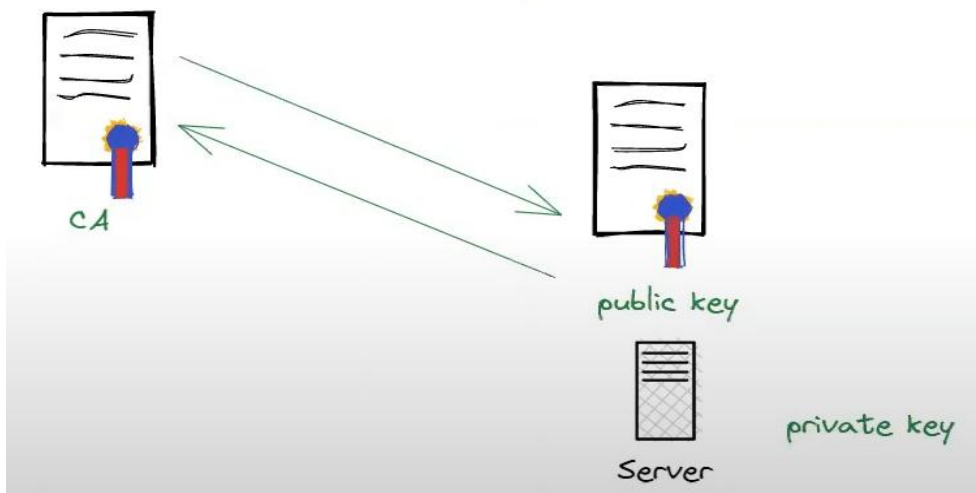


Asimetrik şifrelemede yaklaşımında ise Public ve Private olmak üzere iki farklı anahtar oluşturulur. Bu anahtarlar arasında matematiksel bir ilişkiye dayanır. Veriler Public anahtar ile şifrenirken sadece Private key kullanılarak çözülebilir. Yani Public key kullanılarak veriyi şifreleyen taraf elinde Private key bulundurmadığı sürece şifrelediği veriyi tekrar çözümleyemez. Simetrik şifreleme yaklaşımına Asimetrik şifrelemede göre çok daha fazla işlem gücü ve zaman harcanmaktadır. Asimetrik şifreleme yaklaşımına örnek olarak RSA, DSA ve ECDSA gibi algoritmalar verilebilir.

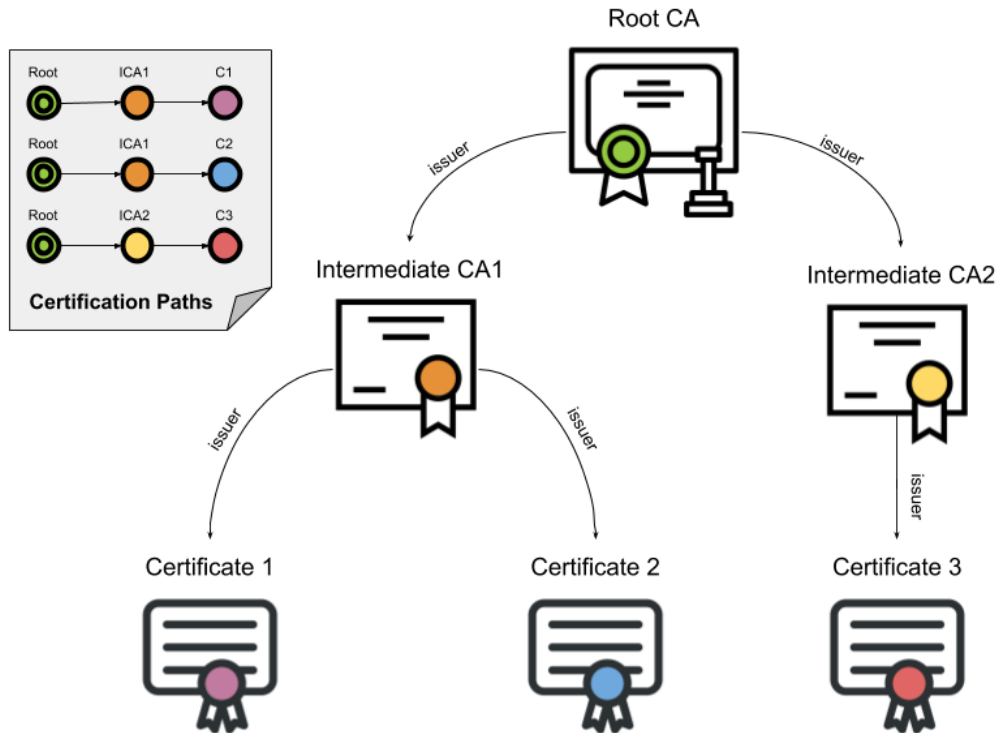


Şifreleme yaklaşımlarıyla ilgili kabaca bilgi edindikten sonra artık SSL sertifikasıyla bu sürecin nasıl gerçekleştiği açıklanmaya başlanabilir.

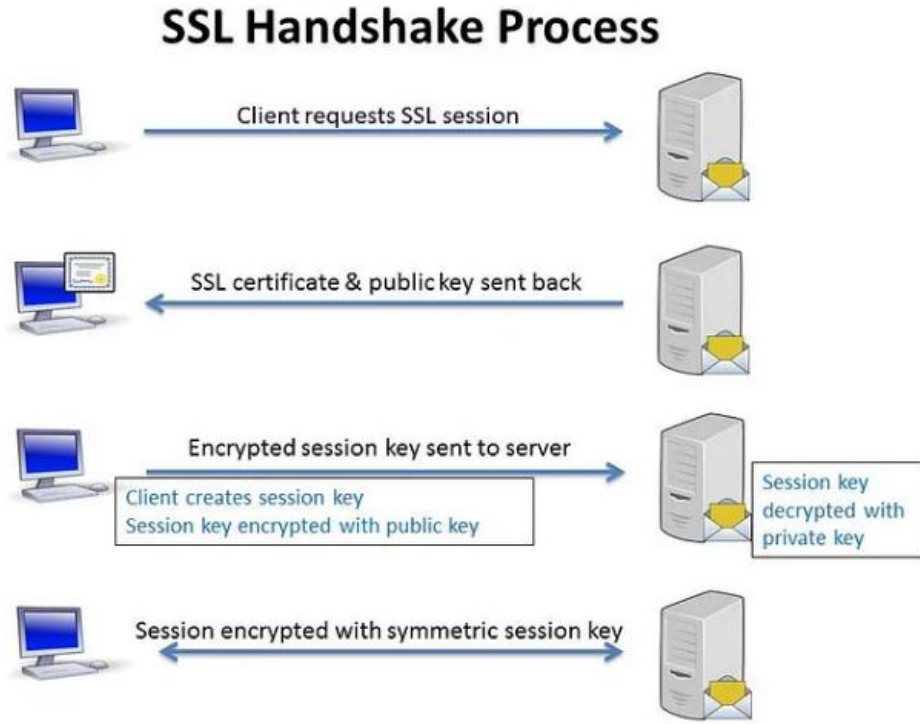
Sürece ilk olarak güvenli erişim sağlanması istenen sunucu üzerinde SSL sertifikası oluşturmak için Asimetrik şifrelemede açıklanan bir anahtar çifti (Public ve Private anahtarlar) oluşturuluyor. Sunucu üzerinde oluşturulan anahtar çiftinden Private anahtarı sunucu üzerinde kalırken, verileri şifrelemek için kullanılacak olan Public anahtarı Certificate Authority hizmeti veren organizasyonlardan birisinde tanımlayarak bir SSL sertifikası alınır ve sunucuya yüklenir.



|→ Dünyada bilindik ve güvenilir kabul edilen sertifika sağlayıcı organizasyonlar bulunmaktadır. Bu organizasyonlar CA (Certificate Authority) olarak da isimlendirilmektedir. Sertifika sürecinde de hiyerarşik bir düzen bulunmaktadır. Günün sonunda her sertifika kök sertifikaya bağlıdır. Kök sertifikadan sertifika yetkilendirme hizmeti veren kurum/organizasyonlar aracılığıyla sertifika doğrulaması gerçekleştirilir.



Alınan SSL sertifikası sunucuya yüklendikten sonra herhangi bir istemci tarayıcısından sunucuya HTTPS protokolü üzerinden erişmek istediğinde sunucu üzerindeki sertifika ve Public anahtar bilgisi kullanıcıya iletiliyor. İstemci sunucunun gönderdiği sertifikayı kontrol ettiğinde sertifika sağlayıcısının bilindik Certificate Authority organizasyonlarından birisinden sağlandığını gördüğünde sunucuya güvenilir bir şekilde bağlantı kurulabileceğine karar veriyor.



- Bu süreçte sunucuya erişim için simetrik şifreleme algoritmasında kullanılacak anahtar bilgisini sunucudan gönderilen Public anahtar ile şifreleyerek sunucuya gönderiyor.
- Sunucuda Private anahtar ile istemcinin gönderdiği Simetrik şifreleme algoritmasında kullanılacak anahtar bilgisi çıkarıp içerisindeki Simetrik şifrelemede kullanılacak anahtar bilgisini elde ediyor.
- Simetrik şifreleme algoritmasında kullanılacak anahtar bilgisi kullanılarak istemci ile arasında veri transferi Simetrik şifreleme algoritmalarıyla gerçekleştirilmeye başlanıyor.

| → İstemci ve sunucu arasındaki haberleşme süreci aslında Simetrik şifreleme algoritmaları kullanılarak gerçekleştiriliyor. Bunun nedeni Simetrik şifreleme algoritmalarının Asimetrik şifreleme algoritmalarına kıyasla daha az zaman harcanıyor olmasıdır. Konunun başında da açıklandığı üzere her ne kadar Simetrik şifreleme daha hızlı olsa da arada kullanılacak anahtar bilgisini karşı tarafa ulaştırma sürecinin güvenli bir şekilde yapılabilmesi adına ilk adıma asimetrik şifreleme algoritmalarından yardım alınıyor. Asimetrik şifreleme ile Simetrik şifrelemede kullanılacak anahtar bilgisi her iki tarafla da paylaşıldıktan sonra haberleşme sürecinin daha hızlı olması adına Simetrik şifrelemeye algoritmalarıyla devam ediliyor.

| → Burada istemci sertifikanın güvenilirliğine kara verme işlemini üzerinde varsayılanda yüklü gelen “Güvenilir Kök Sertifika Yetkilileri” içerisindeki sertifikalara bakarak bulundurarak karar veriyor. Bu sertifikaları bilgisayarın arama kısmına “Kullanıcı Sertifikalarını Yönetin” yazarak inceleyebilirsiniz (veya kullandığınız tarayıcıda da görüntüleyebilirsiniz. Örnek olarak Chrome için “chrome://certificate-manager/crscerts” yazmanız yeterli).

certmgr - [Sertifikalar - Geçerli Kullanıcı\Güvenilen Kök Sertifika Yetkilileri\Sertifikalar]					
Dosya Eylem Görünüm Yardım					
Sertifikalar - Geçerli Kullanıcı					
<ul style="list-style-type: none"> <li>Sertifikalar - Geçerli Kullanıcı <ul style="list-style-type: none"> <li>Kişisel</li> <li>Güvenilen Kök Sertifika Yetkilileri <ul style="list-style-type: none"> <li>Sertifikalar</li> <li>Kuruluş Güveni</li> <li>Ara Sertifika Yetkilileri</li> <li>Active Directory Kullanıcı Nesnesi</li> <li>Güvenilir Yayımcılar</li> <li>Güvenilmeyen Sertifikalar</li> <li>Üçüncü Taraf Kök Sertifika Yetkilileri</li> <li>Güvenilir Kişiler</li> <li>İstemci Kimlik Doğrulaması Verenler</li> <li>Akıllı Kart Güvenilen Kökleri</li> </ul> </li> </ul> </li> </ul>					
Verilen	Veren	Süre Sonu	Hedeflenen amaçlar	Kolay Ad	
AAA Certificate Services	AAA Certificate Services	1.01.2029	İstemci Kimlik Doğr...	Sectigo (AAA)	
Actalis Authentication Root CA	Actalis Authentication Root CA	22.09.2030	İstemci Kimlik Doğr...	Actalis Authenticati...	
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	2.08.2028	İstemci Kimlik Doğr...	VeriSign Class 3 Pu...	
COMODO RSA Certification Au...	COMODO RSA Certification Auth...	19.01.2038	İstemci Kimlik Doğr...	Sectigo (formerly C...	
Copyright (c) 1997 Microsoft C...	Copyright (c) 1997 Microsoft Corp.	31.12.1999	Zaman Damgalaması	Microsoft Timesta...	
DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	10.11.2031	İstemci Kimlik Doğr...	DigiCert	
DigiCert Global Root CA	DigiCert Global Root CA	10.11.2031	İstemci Kimlik Doğr...	DigiCert	
DigiCert Global Root G2	DigiCert Global Root G2	15.01.2038	İstemci Kimlik Doğr...	DigiCert Global Roo...	
DigiCert Global Root G3	DigiCert Global Root G3	15.01.2038	İstemci Kimlik Doğr...	DigiCert Global Roo...	
DigiCert High Assurance EV Ro...	DigiCert High Assurance EV Root ...	10.11.2031	Zaman Damgalama...	DigiCert	
DigiCert Trusted Root G4	DigiCert Trusted Root G4	15.01.2038	İstemci Kimlik Doğr...	DigiCert Trusted Ro...	
GlobalSign	GlobalSign	18.03.2029	İstemci Kimlik Doğr...	GlobalSign Root CA...	
GlobalSign Root CA	GlobalSign Root CA	28.01.2028	İstemci Kimlik Doğr...	GlobalSign Root CA...	
Go Daddy Class 2 Certification ...	Go Daddy Class 2 Certification Au...	29.06.2034	İstemci Kimlik Doğr...	Go Daddy Class 2 C...	
Go Daddy Root Certificate Auth...	Go Daddy Root Certificate Author...	1.01.2038	İstemci Kimlik Doğr...	Go Daddy Root Cer...	
IdenTrust Commercial Root CA 1	IdenTrust Commercial Root CA 1	16.01.2034	İstemci Kimlik Doğr...	IdenTrust Commer...	
ISRG Root X1	ISRG Root X1	4.06.2035	İstemci Kimlik Doğr...	ISRG Root X1	
Microsoft Authenticode(tm) Ro...	Microsoft Authenticode(tm) Root...	1.01.2000	Güvenli E-posta, Ko...	Microsoft Authent...	
Microsoft ECC Product Root Ce...	Microsoft ECC Product Root Certi...	27.02.2043	<Tümü>	Microsoft ECC Prod...	
Microsoft ECC TS Root Certifica...	Microsoft ECC TS Root Certificate ...	28.02.2043	<Tümü>	Microsoft ECC TS R...	
Microsoft Identity Verification R...	Microsoft Identity Verification Ro...	16.04.2045	Kod İmzalama, Za...	Microsoft Identity V...	
Microsoft Root Authority	Microsoft Root Authority	31.12.2020	<Tümü>	Microsoft Root Aut...	
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	10.05.2021	<Tümü>	Microsoft Root Cert...	
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	24.06.2035	<Tümü>	Microsoft Root Cert...	
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	23.03.2036	<Tümü>	Microsoft Root Cert...	
Microsoft RSA Root Certificate ...	Microsoft RSA Root Certificate Au...	19.07.2042	İstemci Kimlik Doğr...	Microsoft RSA Root...	
Microsoft Time Stamp Root Cer...	Microsoft Time Stamp Root Certif...	23.10.2039	<Tümü>	Microsoft Time Sta...	
NO LIABILITY ACCEPTED, (c)97 ...	NO LIABILITY ACCEPTED, (c)97 Ve...	8.01.2004	Zaman Damgalaması	VeriSign Time Stam...	
Starfield Class 2 Certification A...	Starfield Class 2 Certification Auth...	29.06.2034	İstemci Kimlik Doğr...	Starfield Class 2 Cer...	
Starfield Services Root Certificat...	Starfield Services Root Certificate ...	1.01.2038	İstemci Kimlik Doğr...	Amazon Services R...	
Symantec Enterprise Mobile Ro...	Symantec Enterprise Mobile Root ...	15.03.2032	Kod İmzalama	<Yok>	
thawte Primary Root CA	thawte Primary Root CA	17.07.2036	İstemci Kimlik Doğr...	thawte	
Thawte Timestamping CA	Thawte Timestamping CA	1.01.2021	Zaman Damgalaması	Thawte Timestampi...	
USERTrust RSA Certification Aut...	USERTrust RSA Certification Autho...	19.01.2038	İstemci Kimlik Doğr...	Sectigo	
VeriSign Class 3 Public Primary ...	VeriSign Class 3 Public Primary Ce...	17.07.2036	İstemci Kimlik Doğr...	VeriSign	
VeriSign Universal Root Certific...	VeriSign Universal Root Certificati...	2.12.2037	İstemci Kimlik Doğr...	VeriSign Universal R...	

Güvenilen Kök Sertifika Yetkilileri denetiminde 36 sertifika var

| → Certificate Authority hizmeti veren organizasyonların önemine bakıldığında, sertifikayı herkes oluşturabilir ve istemci ile arasındaki trafiği şifrelemek için kullanabilir. Sertifikanın güvenilirliği güvenilir olmadığı takdirde istemci ile sunucu arasındaki veri trafiğinin şifresini ele geçirilip trafik içeriğine erişim sağlanabilir.

## Fortigate FW üzerinde SSL Decryption

Fortigate FW üzerinden geçen trafiğin ilgili Policy üzerinde uygulanan güvenlik özelliklerinin sağlıklı bir şekilde uygulanabilmesi için SSL ile şifrelenen istemci trafiğinin FW üzerinde şifresinin çözülmesi için içeriği kontrol edildikten sonra yeniden şifrelenmesi gerekmektedir. Bunu sağlayabilmenin iki yöntemi bulunmaktadır.

- 1- İlk olarak Fortigate FW üzerindeki Deep Inspection profili içerisinde kullanılan CA sertifikası, trafiği Deep Inspection profili uygulana Policy'i kullanacak bütün istemcilere yüklenebilir. Bu sayede Deep Inspection profili uygulanan Policy'lerde trafik Decrypt edilip içeriği kontrol edildikten sonra yeniden Encrypt edilerek hedef sunucuya iletilmesi sağlanabilir. Bunun için;
  - a. Fortigate FW'da "SSL/SSH Inspection" sekmesindeki "deep inspection" profili içerisindeki sertifika indirilerek bu profilin uygulanacağı Policy'leri kullanacak bütün istemcilere yüklendikten sonra ilgili Policy'lere uygulana güvenlik politikaları sorunsuz şekilde çalışmaya başlayacaktır.
  - b. Policy yazarken SSL Inspection kısmında "Deep Inection" profili seçilmesine rağmen bu Deep Inspection profilinde kullanılan sertifika, istemcilerde de yüklü olmasa bu durumda istemci trafiklerinin içeriği kontrol edilemediği için trafikler FW'dan geçirilemeyecektir, bloklanacaktır.

**Edit SSL/SSH Inspection Profile**

Name: deep-inspection

Comments: Read-only deep inspection profile. 34/255

**SSL Inspection Options**

Enable SSL inspection of: Multiple Clients Connecting to Multiple Servers

Inspection method: SSL Certificate Inspection Full SSL Inspection

CA certificate: Fortinet\_CA\_SSL Download

Blocked certificates: Allow Block View Blocked Certificates

Untrusted SSL certificates: Allow Block Ignore View Trusted CAs List

Server certificate SNI check: Enable Strict Disable

Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log
Internal1_to_WAN	Internal1 Ntw	all	always	ALL	ACCEPT	Enabled	AV: default WEB: default APP: default IPS: default SSL: deep-inspection	All

- 2- Microsoft Sertifika sunucusunda yeni bir sertifika oluşturulup Fortigate FW'a yüklendikten sonra SSL Inspection Profile tanımlarında kullanılması sağlanabilir. Aynı zamanda bu sertifika oluşturulan SSL Inspection profilinin kullanılacağı Policy'i kullanacak bütün istemcilere yüklenmesi gerekir. Microsoft Sertifika Sunucusunda sertifika oluşturmak için;
- İlk olarak Windows sunucusunda AD Sertifika servisinin/rolünün kurulmuş olması gerekiyor. Kurulum yapıldıktan sonra arayüzüne girildiğinde **"Request a Certificate"** seçeneği ile devam edilecektir.

Microsoft Active Directory Certificate Services — testbench-CA

**Welcome**

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

**Select a task:**

- [Request a certificate](#)
- [View the status of a pending certificate request](#)
- [Download a CA certificate, certificate chain, or CRL](#)

- Açılan sayfada **"Advanced Certificate Request"** seçeneğiyle devam ediliyor.

Microsoft Active Directory Certificate Services — testbench-CA

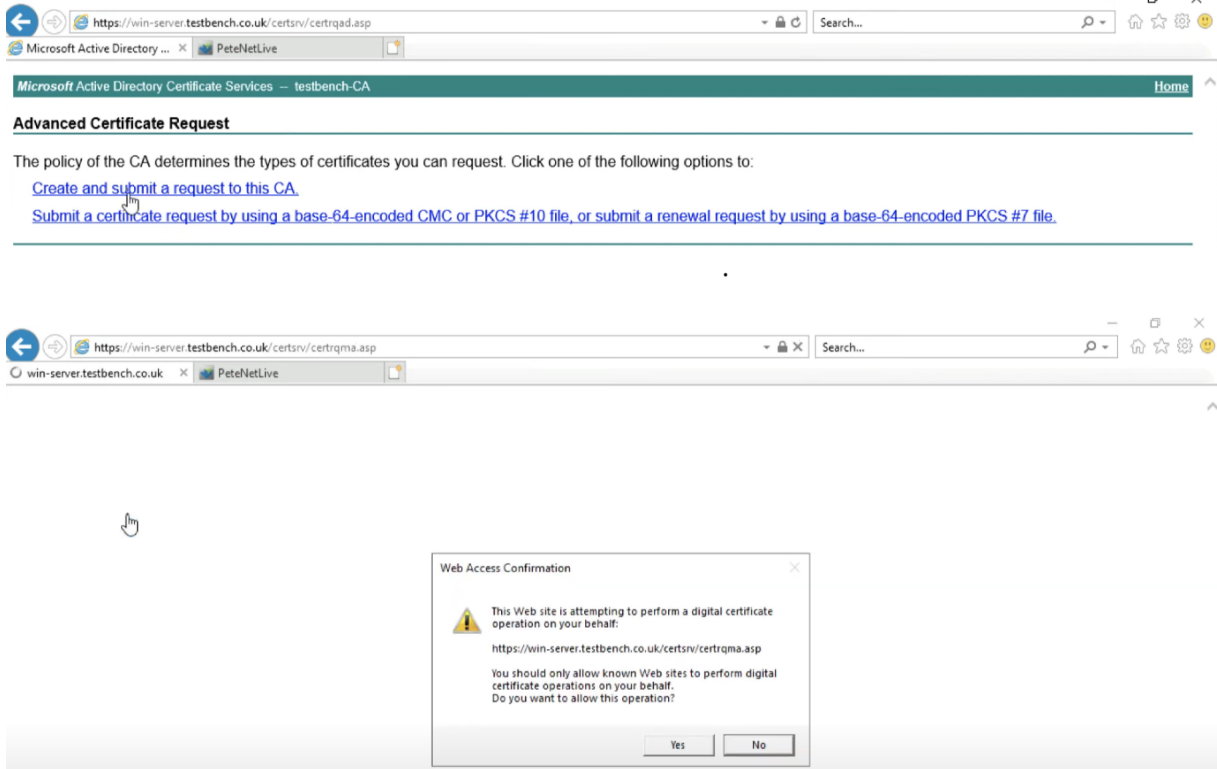
**Request a Certificate**

Select the certificate type:

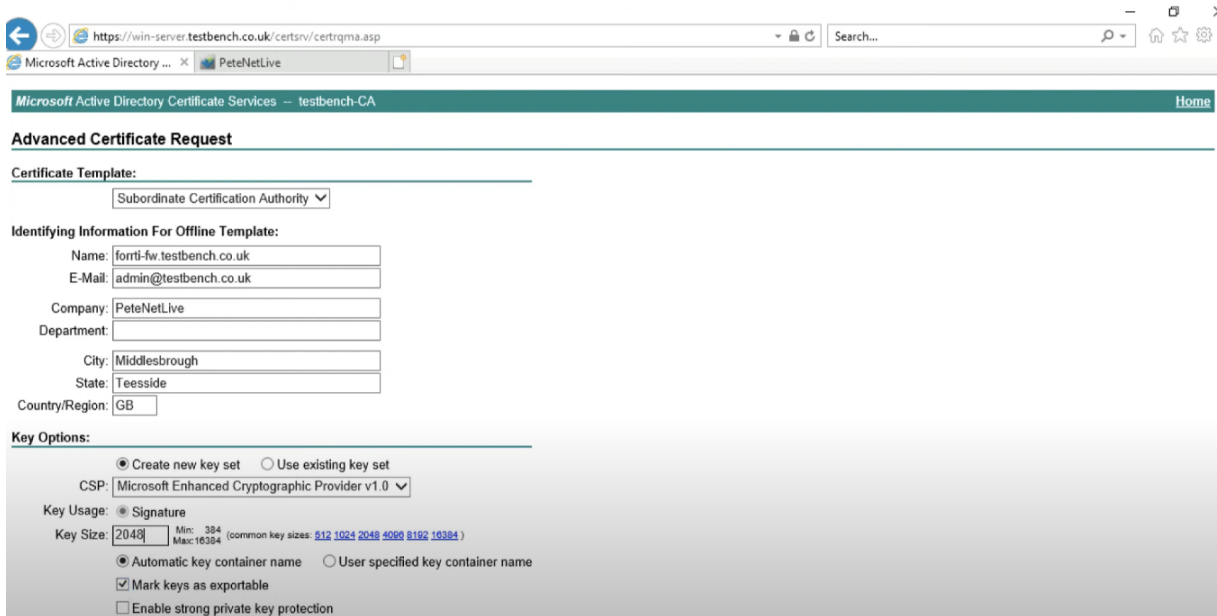
- [User Certificate](#)

Or, submit an [advanced certificate request](#).

- c. Açılan sayfada “**Create and Submit a Request to this CA**” seçeneğiyle devam ediliyor. Gelen uyarı kutusunu onayladıktan sonra sertifika detaylarının ayarlanacağı sayfa gelecektir.

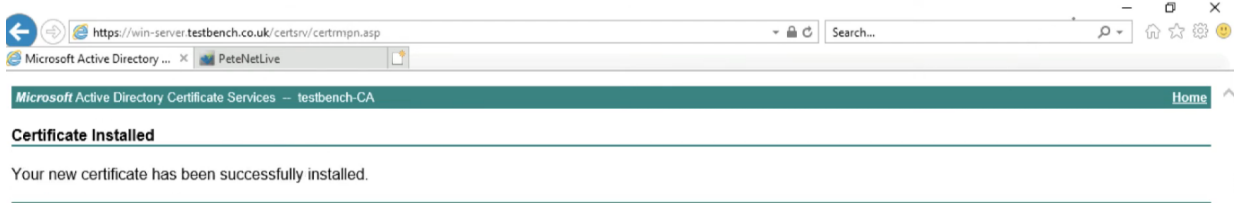
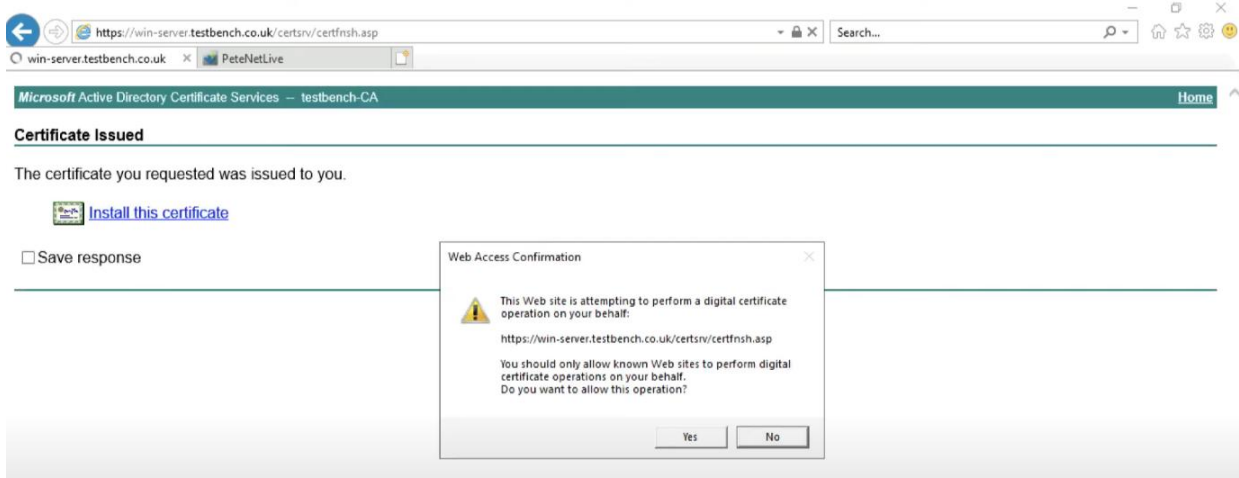


- a. Açılan sayfada Template olarak “Subdomaine Certification Authority” seçeneği seçilmelidir. Ardından sertifika Template isimi, iletişim için mail adresi, lokasyon bilgisi gibi bilgiler doldurulmalıdır. Key Options kısmında daha güvenli olması adına anahtar boyutu güncellenebilir. Bu ayarlamalar yapıldıktan sonra sayfanın altında bulunan “Submit” butonuyla sertifika oluşturulur.

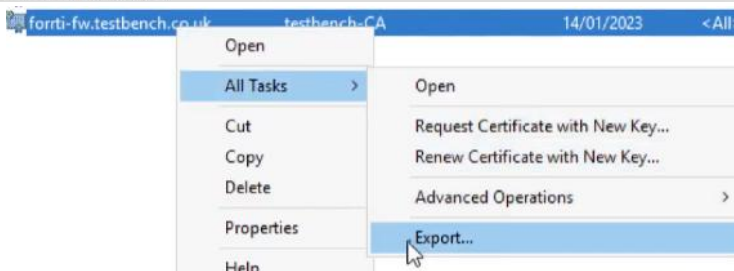
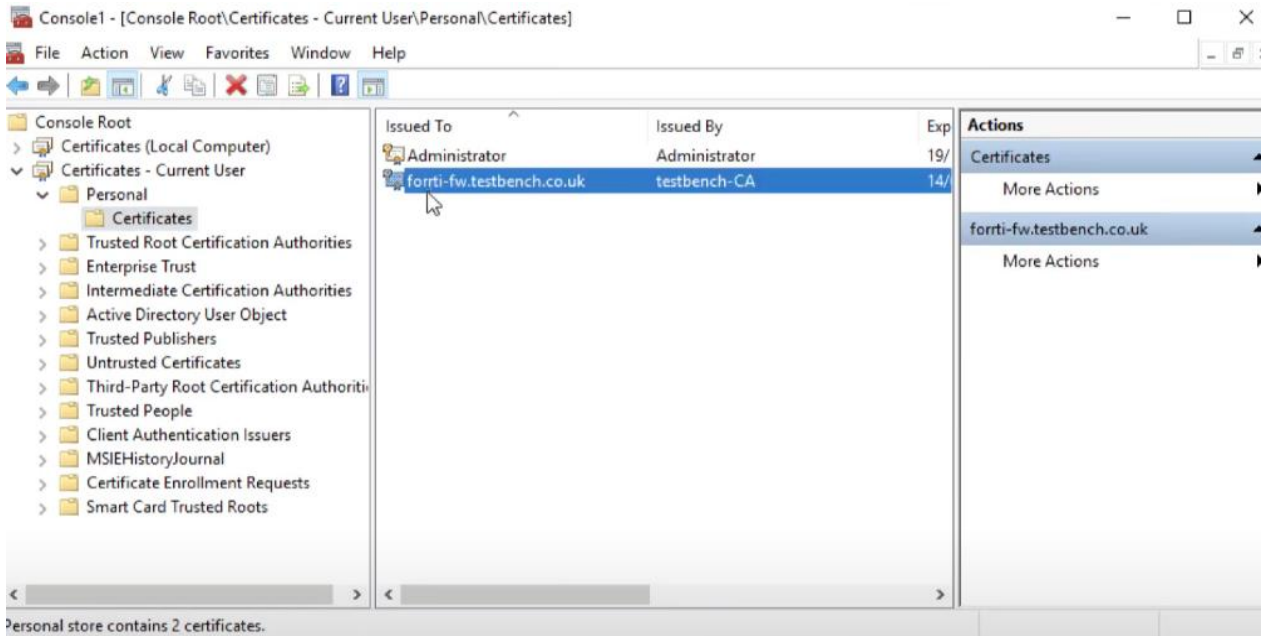




- d. Sertifika oluşturulduktan sonra gelen sayfada üzerine tıklanarak sertifika sunucusuna yüklenmesi sağlanır.



- e. Sertifika AD Sertifika sunucusuna yüklendikten sonra Fortigate FW ve istemcilere yüklenmek üzere Sertifika Yöneticisinden ilgili sertifika seçilerek "All Task -> Export" yolu izlenmeli ve sertifika Export edilmelidir.



← Certificate Export Wizard

**Export Private Key**

You can choose to export the private key with the certificate.

Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

Do you want to export the private key with the certificate?

- ☒ Yes, export the private key  
☐ No, do not export the private key

Next

Cancel

Burada dosyanın hangi formatta kodlanıp Export edilmek istendiği belirlenmelidir.

← Certificate Export Wizard

**Export File Format**

Certificates can be exported in a variety of file formats.

Select the format you want to use:

- ☐ DER encoded binary X.509 (.CER)  
☐ Base-64 encoded X.509 (.CER)  
☐ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)  
☐ Include all certificates in the certification path if possible  
☒ Personal Information Exchange - PKCS #12 (.PFX)  
☒ Include all certificates in the certification path if possible  
☐ Delete the private key if the export is successful  
☐ Export all extended properties  
☒ Enable certificate privacy  
☐ Microsoft Serialized Certificate Store (.SST)

Next

Cancel

Sertifika yüklenmek istendiğinde soruacak parola bilgisidir. Parolanın hangi şifreleme algoritmasıyla şifrelenerek tutulması istendiği de ayrıca seçilebiliyor. Yani herhangi bir parola verilebilir.



← Certificate Export Wizard

**Security**

To maintain security, you must protect the private key to a security principal or by using a password.

☐ Group or user names (recommended)

Add

Remove

☒ Password:

••••••••

Confirm password:

••••••••

Encryption: AES256-SHA256

Next

Cancel

Dosyanın bilgisayar üzerinde kaydedileceği konum seçilmektedir.

← Certificate Export Wizard

**File to Export**

Specify the name of the file you want to export

File name:

C:\Users\Administrator\Desktop\Forti-FW-SubCA.pfx

Browse...

Next

Cancel

## Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

You have specified the following settings:

File Name	C:\Users\Administrator\Desktop\Forti-
Export Keys	Yes
Include all certificates in the certification path	Yes
File Format	Personal Information Exchange (*.pfx)



Yukarıdaki adımlar takip edilip Microsoft AD Certificate Sunucusundan sertifika oluşturulup export edildikten sonra artık Fortigate FW üzerine yüklenip SSL Inspection profili oluşturulabilir. Bu işlem için “System -> Certificate -> Creat/Import -> Certificate” yolu takip edilmelidir. Burada “Import Certificate” seçeneğiyle devam edilmelidir.

Create Certificate

1

2

3

4

Choose Method

Certificate Details

Create Certificate

Review

🔧

Automatically Provision Certificate

Use Let's Encrypt and the ACME protocol to automate certificate creation and maintenance. You will need to enable DDNS or purchase a domain.

Use Let's Encrypt

🔑

Generate New Certificate

FortiGate can generate a certificate using our self-signed CA: [Fortinet\\_CA\\_SSL](#)  
Using a server certificate from a trusted CA is strongly recommended.

Generate Certificate

📁

Import Certificate

Import an existing certificate via file upload.

Import Certificate

Bir sonraki sayfada “PKCS#12 Certificate” kısmına Export edilen sertifika yüklenerek Export edilirken belirlenen parola bilgisi girilmelidir.



Son adımda ise oluşturulan SSL Inspection profile tanımı “Policy&Objects” sekmesinde güvenlik özellikleri (Web Filter, Application Control, Antivirus, IPS...) uygulanan Policy'lere uygulanarak trafiklerin sağlıklı şekilde kontrol edilebilmesini sağlayacaktır. Burada oluşturulan SSL Inspection profilinin uygulandığı Policy'i kullanacak her bir istemciye oluşturduğumuz sertifikanın yüklenmesi gerektiği unutulmamalıdır. Aksi takdirde trafiği FW'da engellenecektir.

**Sonuç olarak** ,Fortigate FW ve istemci bilgisayarlarına aynı sertifikanın yüklenmesi sayesinde istemci bir trafik oluşturduğunda aynı sertifika Fortigate üzerinde de bulunduğu için istemci trafiğini Decrypt ederek trafiğin içeriğini derinlemesine inceleyecektir. Zararlı bağlantılara, dosyalara ve daha birçok tipte zararlı aktivite oluşturulacak trafikleri daha etkili şekilde engelleyebilecektir.

SSL trafiği, istemci ile sunucu arasında güvenli bir bağlantı sağlamak için asimetrik şifreleme (public/private key) kullanır. Sunucu, Public key'i istemciye gönderir ve istemci bu anahtarla verisini şifreler. Ancak SSL Decryption işlemi sırasında FortiGate'in yaptığı şey, ortadaki adam (man-in-the-middle) gibi davranarak, istemci ile sunucu arasındaki veriyi kendi kendine şifreleyip çözmesidir. FortiGate, istemciye kendi sertifikasını sunar ve bu sertifikaya karşılık gelen private key ile SSL trafiğini deşifre eder.

FortiGate, SSL trafiğinin şifresini çözmek için kendi sertifikasını istemciye sunar. Bunu istemcinin tarayıcısı üzerinde kilit işaretine tıkladığınızda sertifikayı sağlayan kurumun Fortigate olduğunu (Fortigate'in üzerine yüklediğimiz sertifika) görüntüleyebilirsiniz. Bunun nedeni Fortigate İstemci bir sunucuya gitmek için Fortigate'e geldiğinde Fortigate arada Proxy görevi görüp kendisi doğrudan sunucuyla oturum başlatmaktadır. Bu sayede sunucuya kendisi veri gönderip gelen dönüşlerin içeriğini açıp kontrol edebiliyor. Kontrol sonrası trafiğin engellenmesi gerekmiyorsa trafiği istemciye yeniden şifreleyerek gönderiyor. İstemci üzerinde Fortigate üzerindeki SSL sertifikası ile aynı sertifika Güvenilir Kök Sağlayıcı kategorisinde yüklü olduğu için sorun oluşturmuyor (**Özetle ve anladığım kadarıyla/hatalı olabilir** konunun başında bahsettiğimiz simetrik ve asimetrik şifreleme süreçleri önce istemci Fortigate ile arasında gerçekleşiyor. Ayrıca Fortigate ile istemcinin gitmek istediği sunucu ile arasında da ayrıca gerçekleştiriliyor. Günün sonunda Fortigate aradaki trafiğin içeriğini inceleyebiliyor).

İstemcinin Sertifika Kabulü: İstemci, FortiGate'in sunduğu sertifikayı tanımazsa (yani, istemcide FortiGate'in sertifikası yüklü değilse), istemci bir güvenlik uyarısı gösterir ve kullanıcı, sertifikayı kabul etmeye ya da bağlantıyı reddetmeye karar verebilir. Genelde, organizasyonlarda FortiGate'in sertifikası, istemcinin güvenlik duvarına veya ağ geçidine dağıtılır, böylece kullanıcılar uyarı almazlar.

FortiGate Sertifikası İstemciye Sunulur: SSL trafiği FortiGate üzerinden geçerken, istemciyle iletişim kuran FortiGate, istemciye kendi sertifikasını sunar ve istemci bu sertifikayı kullanarak verileri şifreler. FortiGate, bu veriyi çözerek içeriği inceleyebilir ve sonra sunucuya iletebilir.

**SSL/SSH Inspection kısmında bulunan Certificate Inspection ile Full Inspection arasındaki farklara bakıldığında;**

- **Certificate Inspection** seçilen bir Policy'de yalnızca sertifika bilgisini incelenrek trafik denetlenir. Yan, SSL/TLS şifrelemesini açmaz, sadece sertifikaları kontrol eder ve şüpheli veya güvenilir olmayan sertifikalar tespit edilirse trafiği engelleyebilir.

- **Full SSL Inspection** seçilen bir Policy'de şifreli trafik çözümlenip (decrypt) içeriği analiz ederek daha derinlemesine bir güvenlik denetimi sağlar. Yani trafik hedefine gönderilmeden önce Firewalla geldiğinde Firewall, trafiği önce kendi açar, inceler, ardından tekrar şifreleyerek iletir. Paketin içeriği çözümlenemediği durumda (sertifika yüklü olmayan bir istemci trafik oluşturmaya çalıştığında) trafiğin içeriği incelenemediği için engellenir.

Fortigate üzerindeki SSL Inspection profili oluşturulurken değiştirilebilecek ayarların detayları bir sonraki yazıda açıklanacaktır.

#### Kaynaklar:

- [https://www.youtube.com/watch?v=kRrsM4A\\_8ZA](https://www.youtube.com/watch?v=kRrsM4A_8ZA) \*\*\*\*
- <https://www.youtube.com/watch?v=0iZcpLFTKDs> \*\*\*\*
- <https://docs.fortinet.com/document/fortigate/7.4.0/best-practices/598577/ssl-tls-deep-inspection>
- <https://www.youtube.com/watch?v=sukgxQ162co>
- <https://www.youtube.com/watch?v=KsR7mVmtJO0>
- <https://www.youtube.com/watch?v=H7g0WqJwtnw>
- [https://www.youtube.com/watch?v=X8s5\\_YkNn5Q](https://www.youtube.com/watch?v=X8s5_YkNn5Q)
- <https://www.youtube.com/watch?v=0IlwKfAb8oQ>
- <https://emanetemre.medium.com/ssl-nedir-ve-nas%C4%B1l-%C3%A7al%C4%B1%C5%9F%C4%B1r-a50c9208cc87>
- <https://www.hosting.com.tr/bilgi-bankasi/ssl-nedir-nasil-calisir/>
- <https://www.kaspersky.com.tr/resource-center/definitions/what-is-a-ssl-certificate>
- <https://tr.linkedin.com/pulse/fortigate-ssl-inspection-ile-full-farklar%C4%B1-ural-tekin-ts3sf#:~:text=Bu%20y%C3%B6ntem%2C%20%C5%9Fifreli%20trafi%C4%9Fi%20%C3%A7%C3%B6z%20ard%C4%B1ndan%20tekrar%20%C5%9Fifreleyerek%20iletir.>