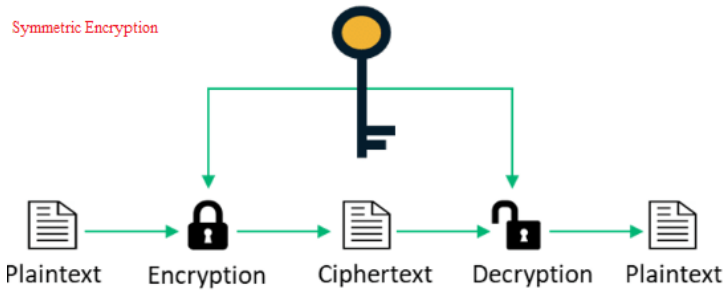
SSL Encryption and Decryption (SSL Deep Inspection)

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.

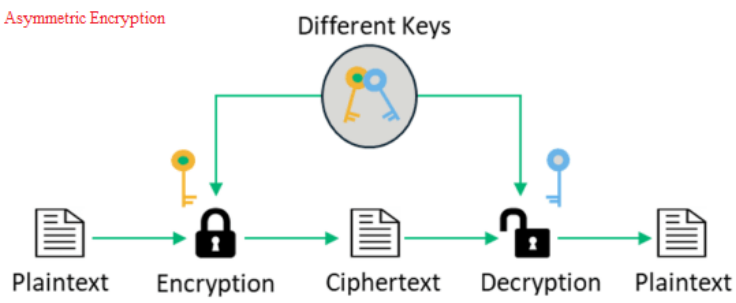
SSL Şifreleme Süreci

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 şifrelenir hem de şifreleri çözülür. Simetrik şifreleme algoritmalarına örnek olarak AES şifreleme algoritması verilebilir.

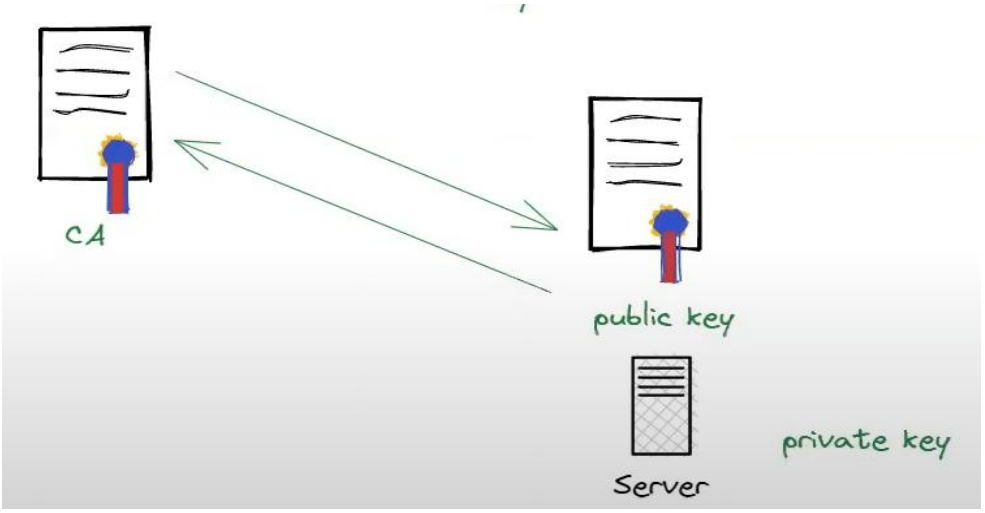


Asimetrik şifrelemede yaklaşımında ise Public ve Private olmak üzere iki farklı anahtar oluşturulur. Bu anahtarlar arasında matematiksel bir ilişkiye dayanır. Veriler Public anahtar ile şifrelenirken sadece Private key kullanılarak çözülebilir. Yani Public key kullanılarak veriyi şifreleyen taraf elinde 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.

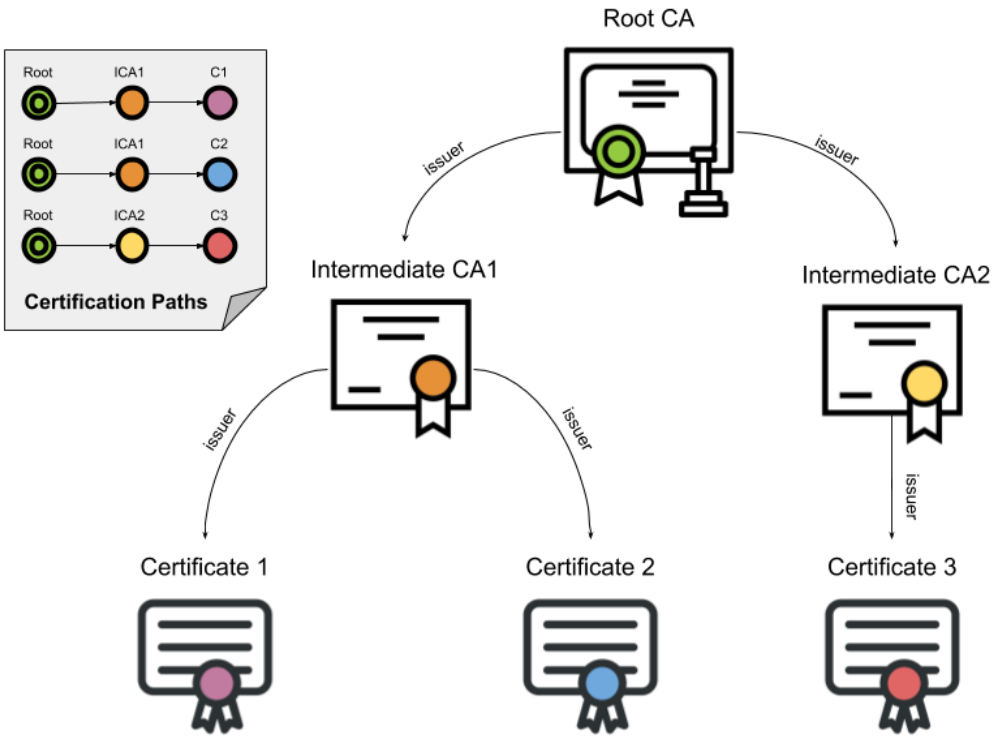


Şifreleme yaklaşımlarıyla ilgili kabaca bilgi edindikten sonra artık SSL sertifikasıyla bu sürecin nasıl gerçekleştiği açıklanmaya başlanabilir.

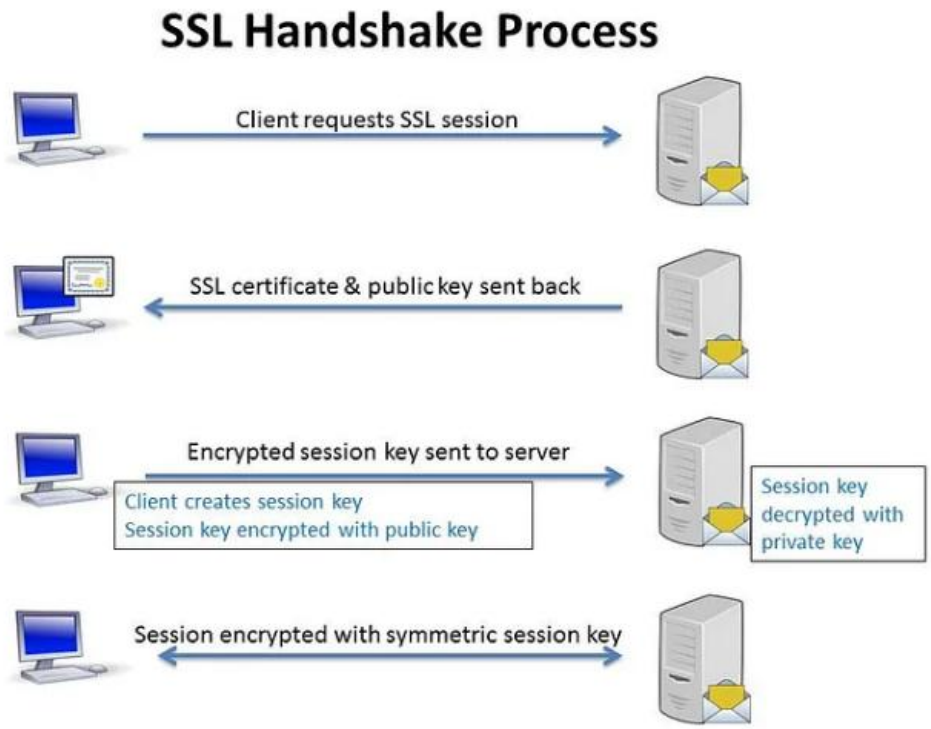
Sürece ilk olarak güvenli erişim sağlanması istenen sunucu üzerinde SSL sertifikası oluşturmak için Asimetrik şifrelemede açıklanan bir anahtar çifti (Public ve Private anahtarlar) oluşturuluyor. Sunucu üzerinde oluşturulan anahtar çiftinden Private anahtarı sunucu üzerinde kalırken, verileri şifrelemek 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.



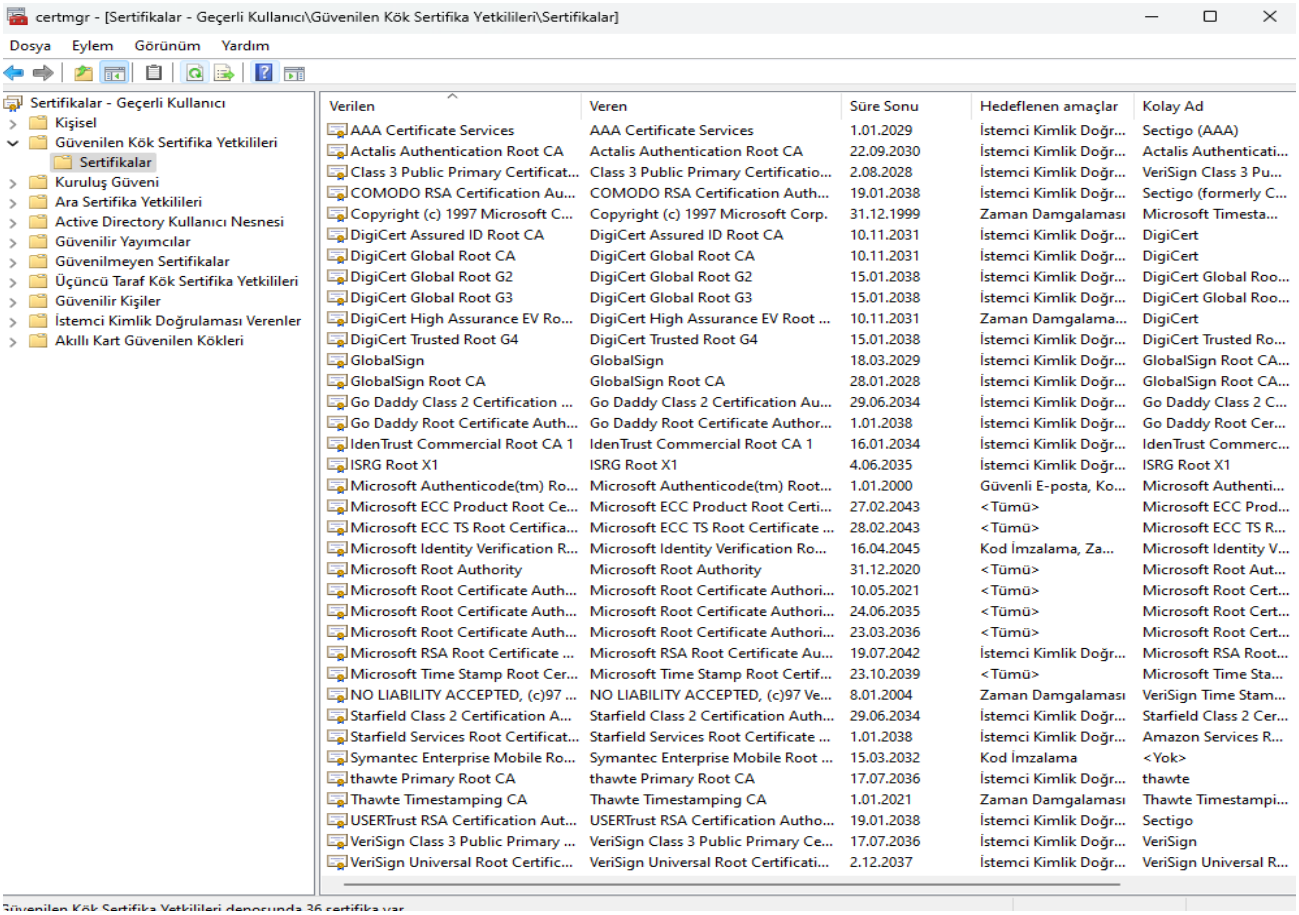
Alınan SSL sertifikası sunucuya yüklendikten sonra herhangi bir istemci tarayıcısından sunucuya HTTPS protokolü üzerinden erişmek istediğinde sunucu üzerindeki sertifika ve Public anahtar bilgisi kullanıcıya iletiliyor. İstemci sunucunun gönderdiği sertifikayı kontrol ettiğinde sertifika sağlayıcısının 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 içerisindek 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 olarka Chrome için “chrome://certificate-manager/crscerts” yazmanız yeterli).

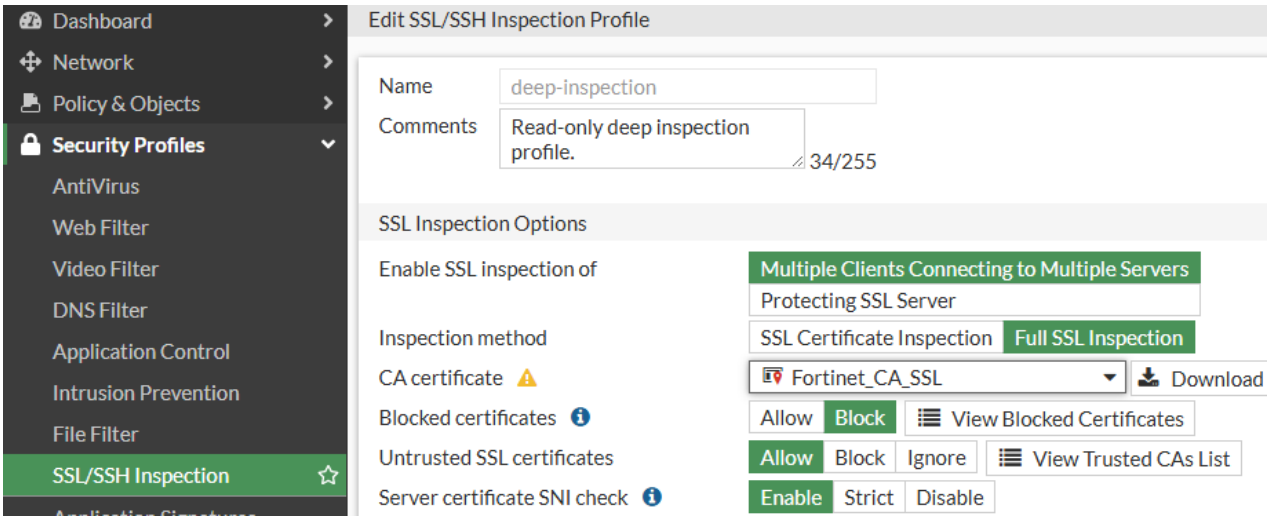


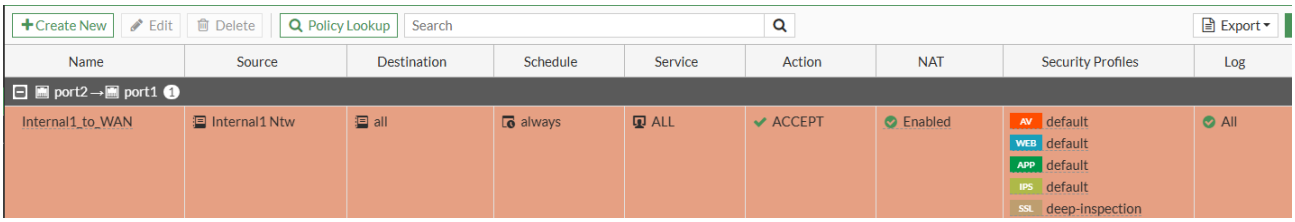
|→ Certificate Authority hizmeti veren organizasyonların önemine bakıldığında, sertifikayı herkes oluşturabilir ve istemci ile arasındaki trafiği şifrelemek için kullanabilir. Sertifikanın güvenilirliği güvenilir olmadığı takdirde istemci ile sunucu arasındaki veri trafiğinin şifresini ele geçirilip 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 çözümlenip içeriği kontrol edildikten sonra yeniden şifrelenebilmesi gerekmektedir. Bunu sağlayabilmenin iki yöntemi bulunmaktadır.

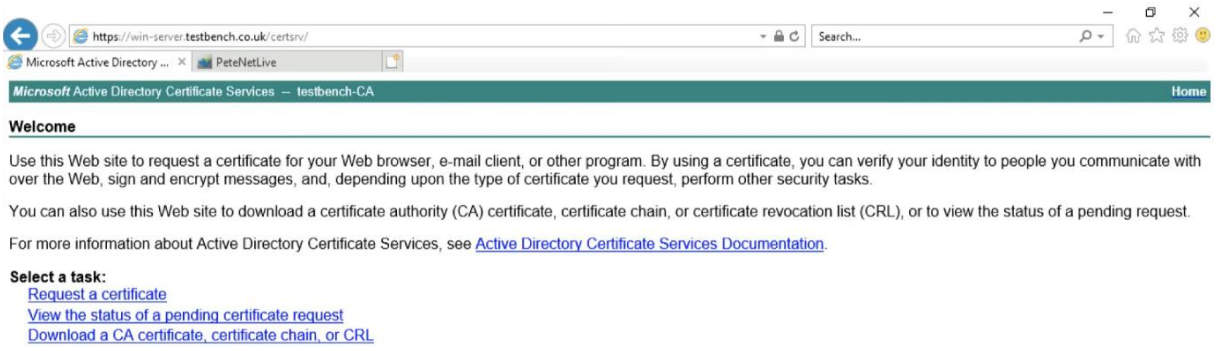
1- İlk olarak Fortigate FW üzerindeki Deep İnspection profili içerisinde kullanılan CA sertifikası, trafiği Deep Inspection profili uygulana Policy'i kullanacak bütün istemcilere yüklenebilir. Bu sayede Deep Inpection profili uygulanan Policy'lerde trafik Decrypt edilip içeriği kontrol edildikten sonra 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 içintrafikler FW'dan geçirilemeyecektir, bloklanacaktır.



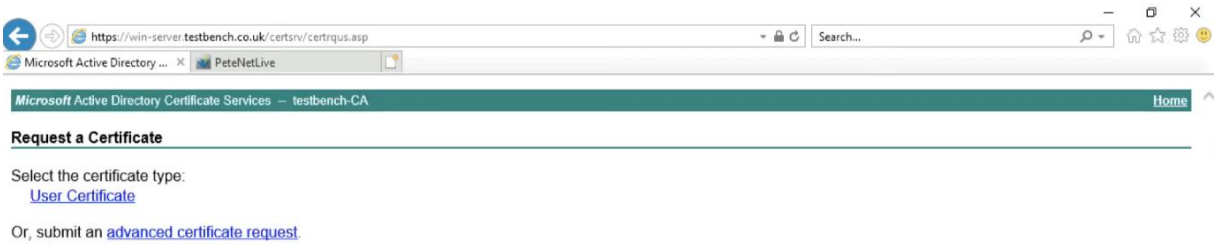


2- Microsoft Sertifika sunucusunda yeni bir sertifika oluşturulup Fortigate FW'a yüklendikten sonra SSL Inspection Profile tanımlarında kullanılması sağlanabilir. Aynı zamanda bu sertifika oluşturulan SSL Inspection profilinin kullanılacağı Policy'i kullanacak bütün istemcilere yüklenmesi gerekir. Microsoft Sertifika Sunucusunda sertifika oluşturmak için;

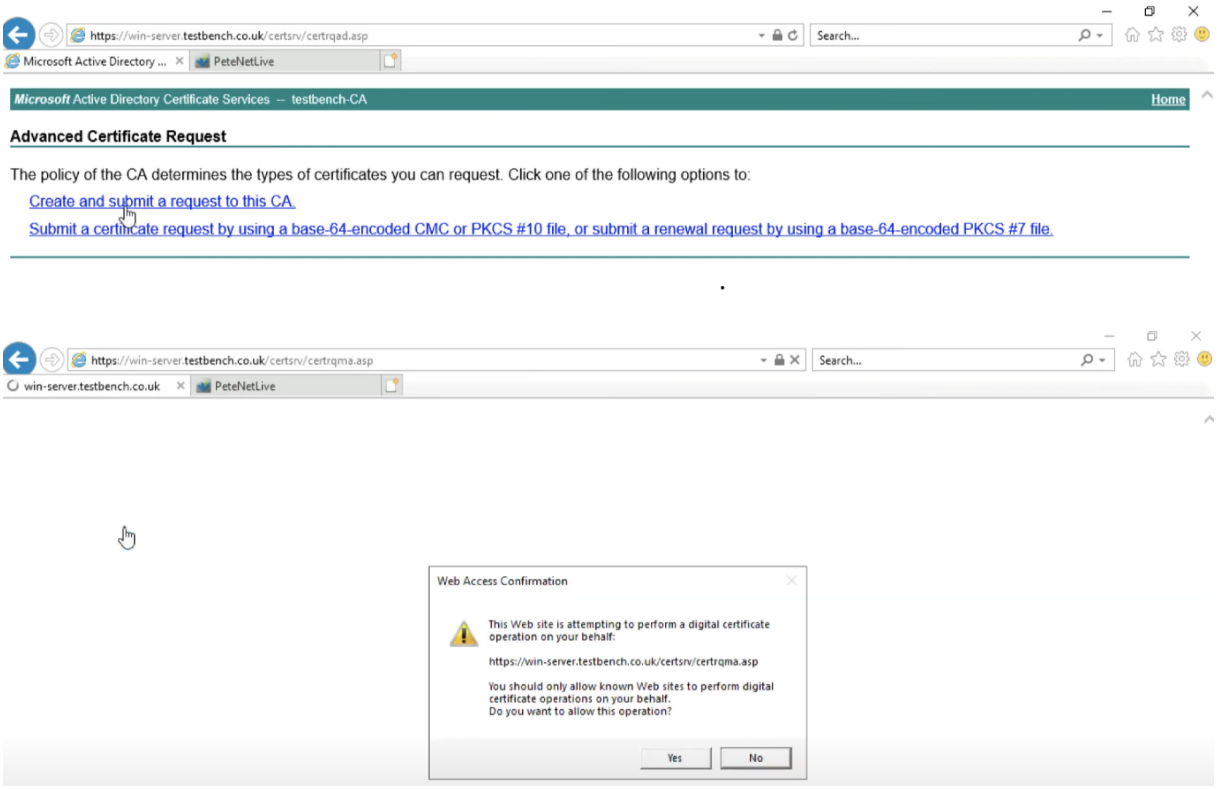
   a. İlk olarak Windows sunucusunda AD Sertifika servisinin/rolünün kurulmuş olması gerekiyor. Kurulum yapıldıktan sonra arayüzüne girildiğinde "**Request a Certificate**" seçeneği ile devam edilecektir.



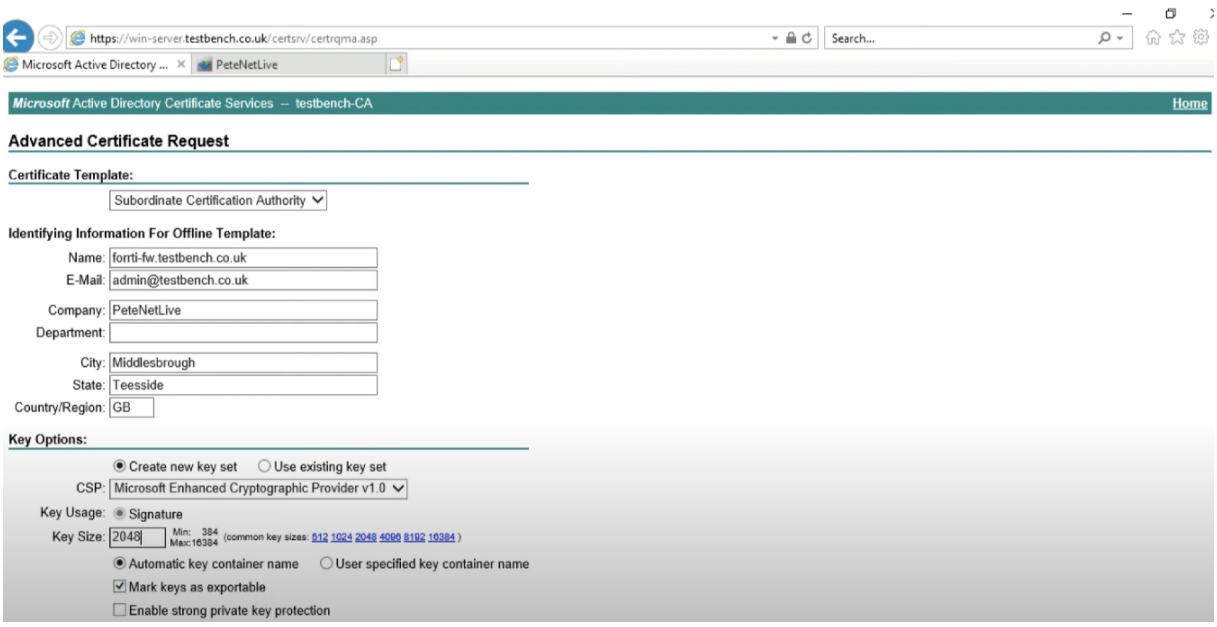
   b. Açılan sayfada "**Advanced Certificate Request**" seçeneğiyle devam ediliyor.



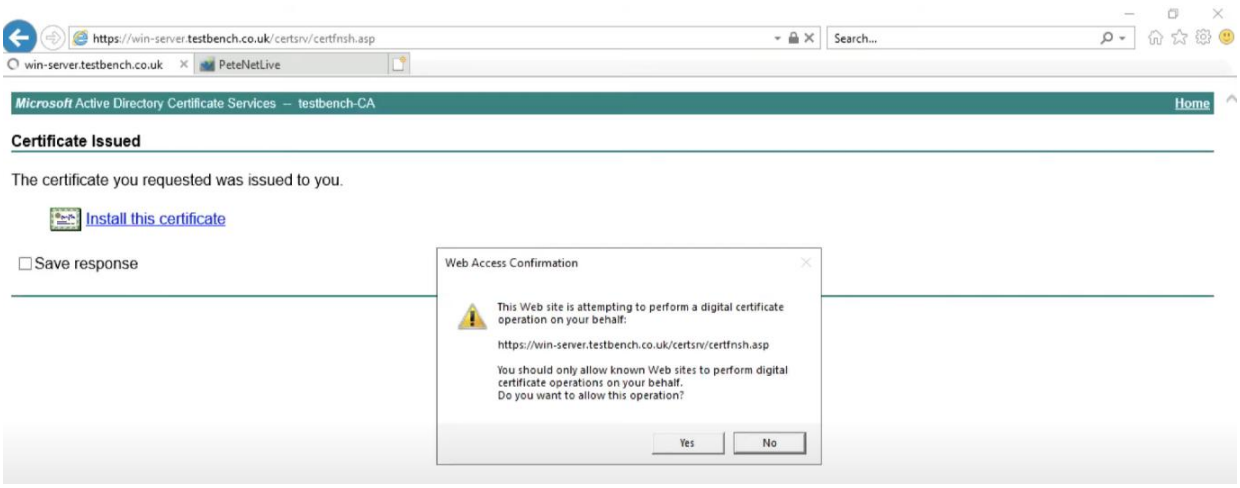
c. Acılan sayfada “**Create and Submit a Request to this CA**” seçeneğiyle devam ediliyor. Gelen uyarı kutusunu onayladıktan sonra sertifika detaylarının ayarlanacağı sayfa gelecektir.

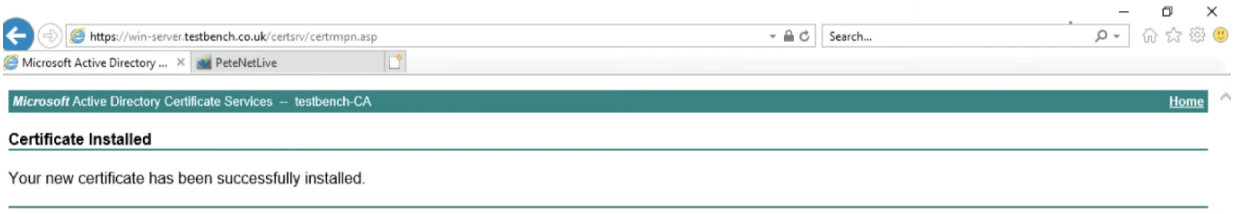


a. Açılan sayfada Template olarak “Subdomaine Certification Authority” seçeneği seçilmelidir. Ardından sertifika Template isimi, iletişim için mail adresi, lokasyon bilgisi gibi bilgiler doldurulmalıdır. Key Options kısmında daha güvenli olması adına anahtar boyutu güncellenebilir. Bu ayarlamalar yapıldıktan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

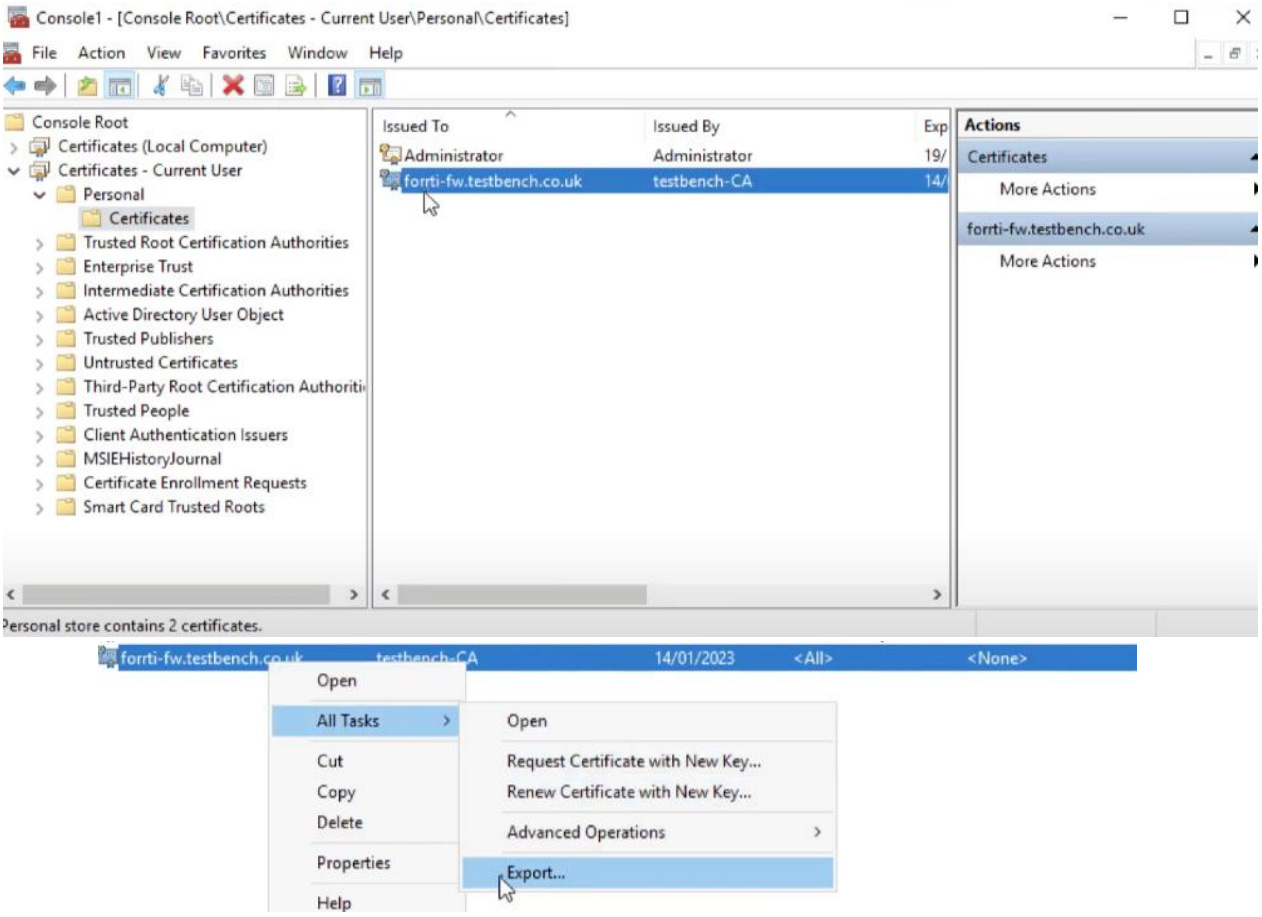


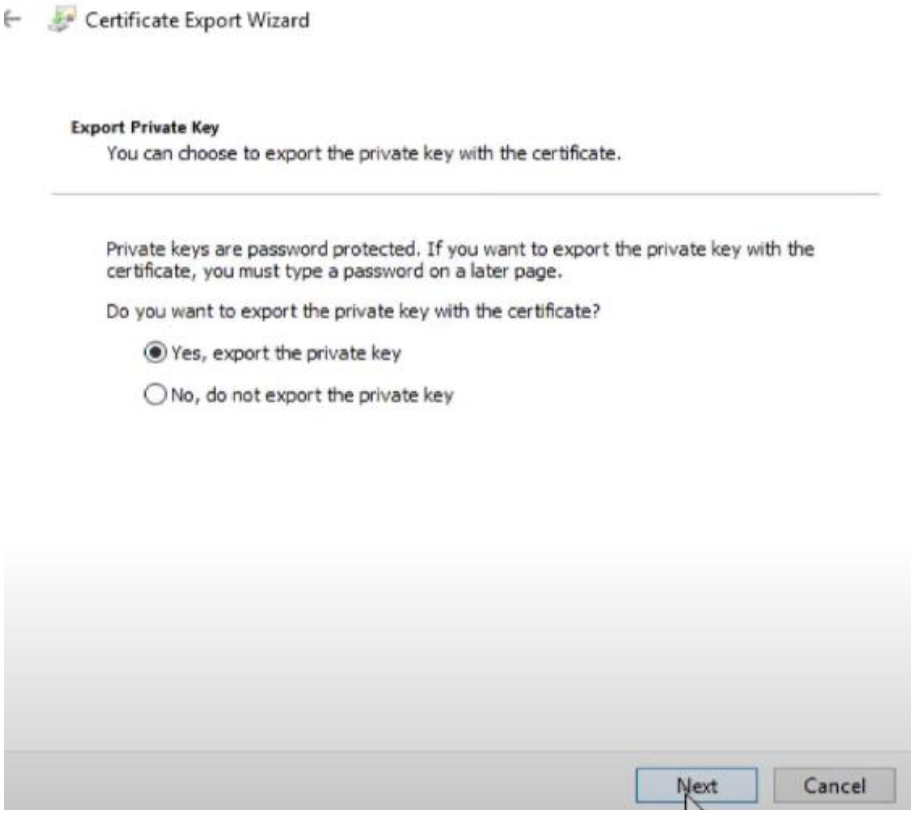
d. Sertifika oluşturulduktan sonra gelen sayfada üzerine tıklanarak sertifika sunucusuna yüklenmesi sağlanır.



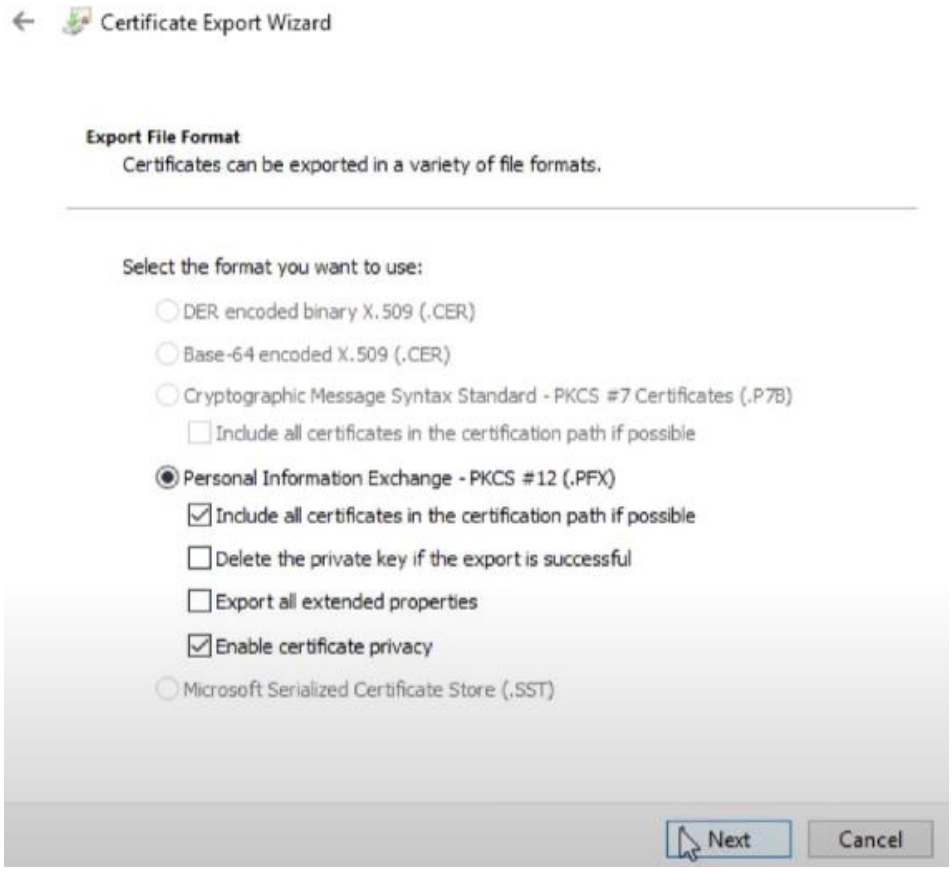


e. Sertifika AD S ertifika sunucusuna yüklendikten sor Fortigate FW ve istemcilere yüklenmek üzere Sertifika Yöneticisinden ilgili sertifika seçilerek “All Task -> Export” yolu izlenmeli ve sertifika Export edilmelidir.

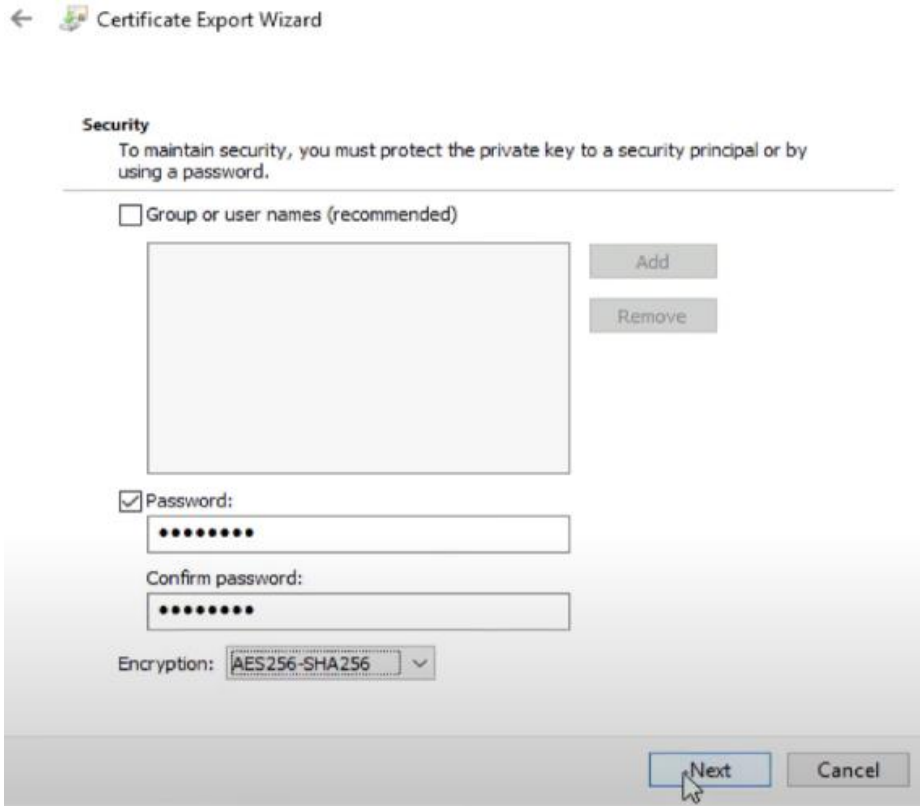




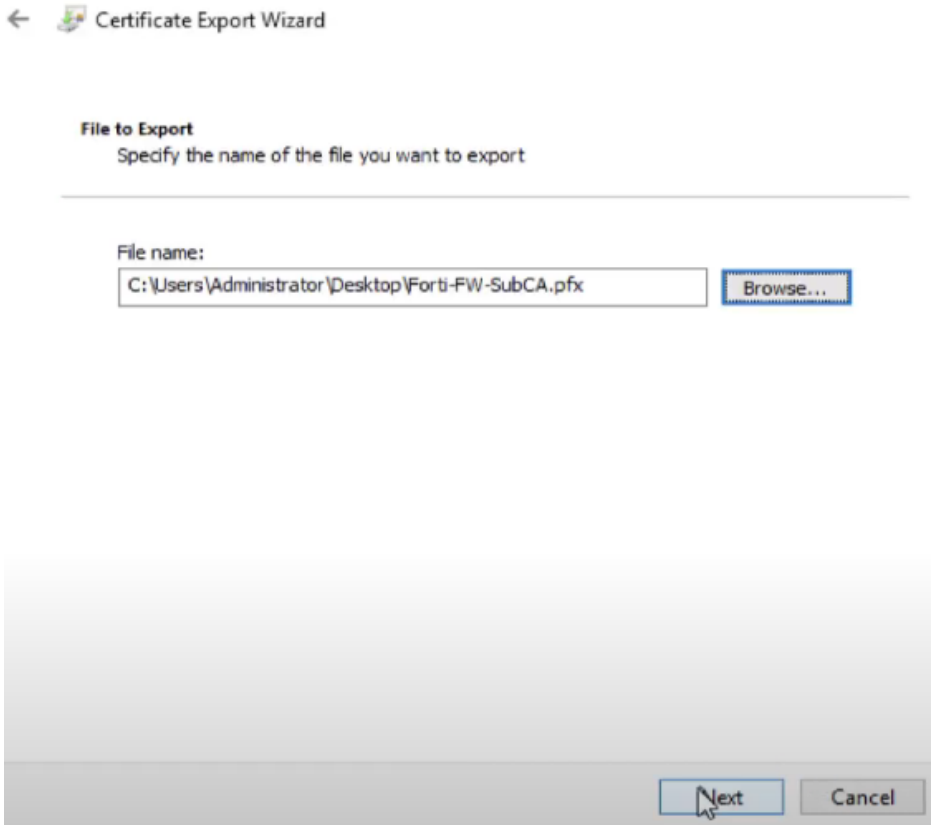
Burada dosyanın hangi formatta kodlanıp Export edilmek istendiği belirlenmelidir.

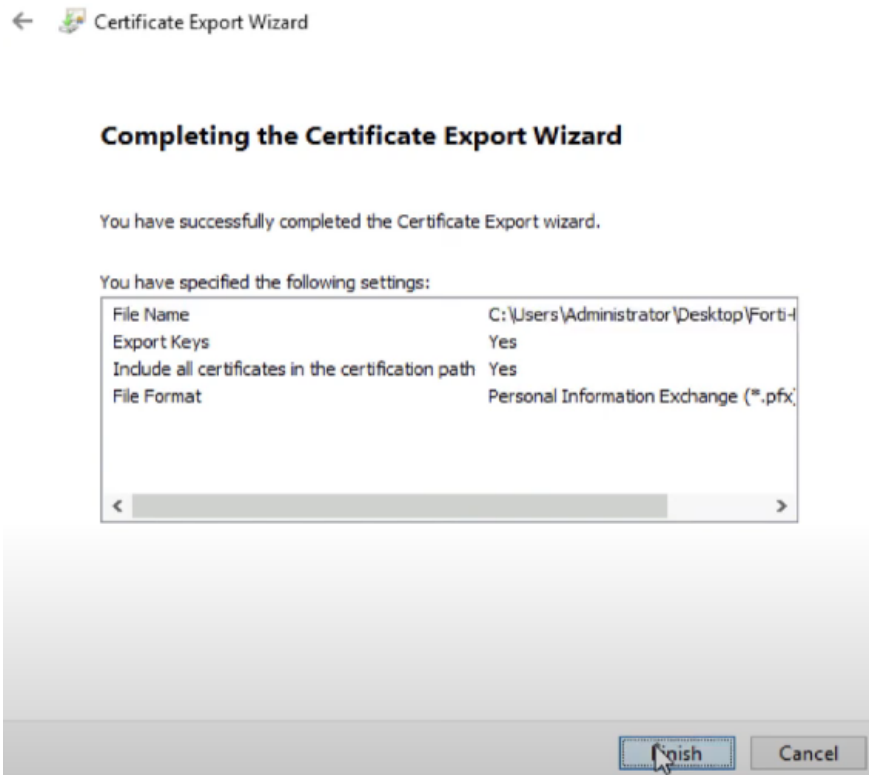


Sertifika yüklenmek istendiğinde soruacak parola bilgisidir. Paroalnın hangi şifreleme algoritmasıyla şifrelenerek tutulması istendiği de ayrıca seçilebiliyor. Yani herhangi bir parola verilebilir.

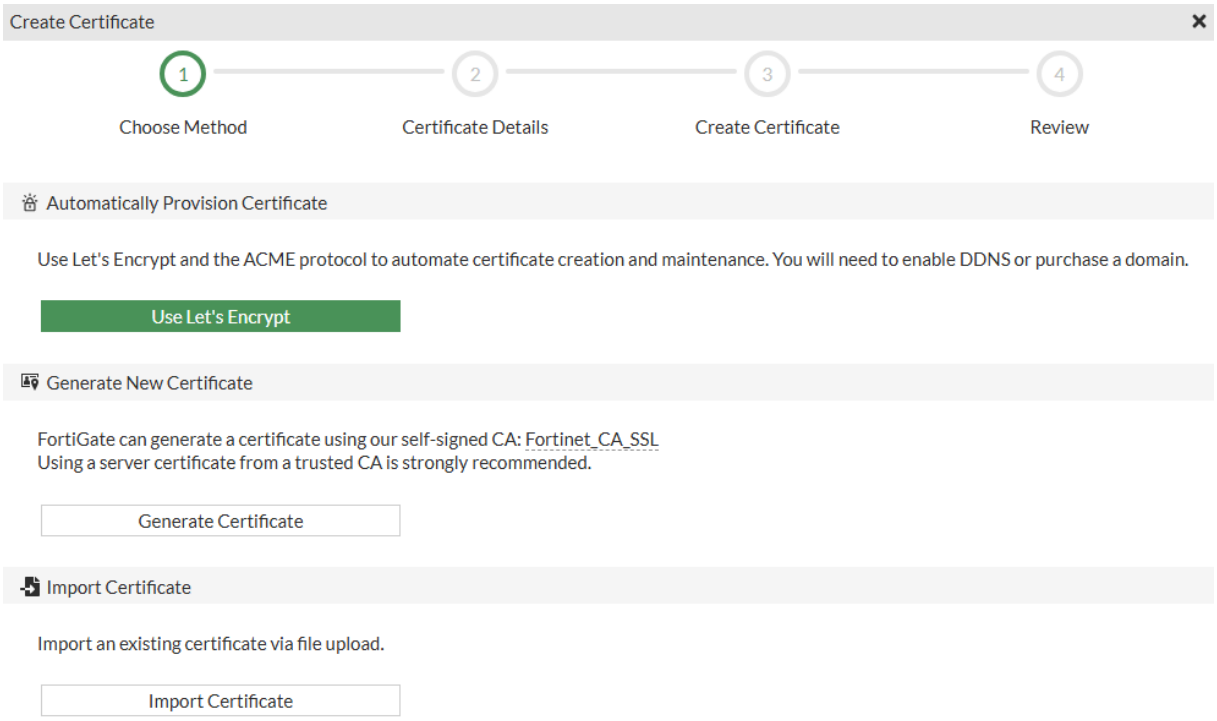


Dosyanın bilgisayar üzerinde kaydedileceği konum seçilmektedir.

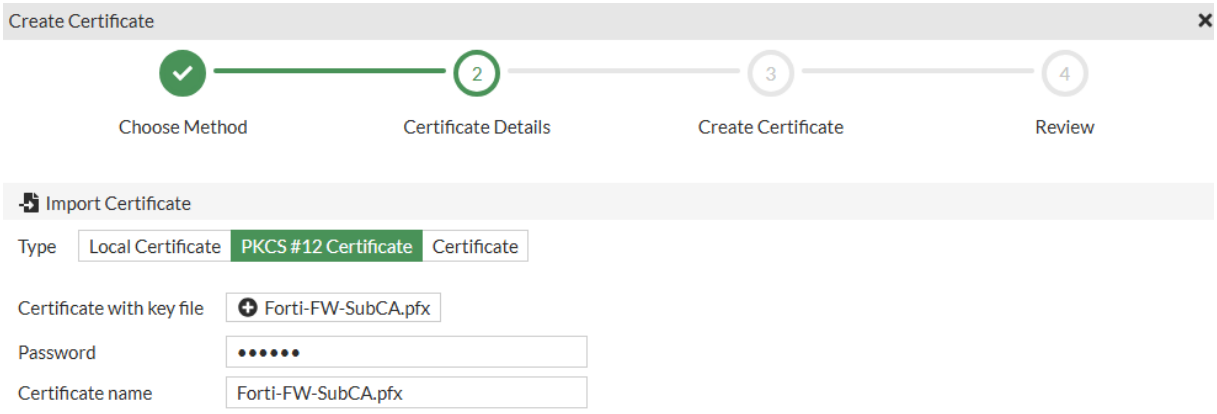




Yukarıdaki adımlar takip edilip Microsoft AD Certificate Sunucusundan sertifika oluşturulup export edildikten sonra artık Fortigate FW üzerine yüklenip SSL Inspection profili oluşturulabilir. Bu işlem için “System -> Certificate -> Creat/Import -> Certificate” yolu takip edilmelidir. Burada “Import Certificate”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

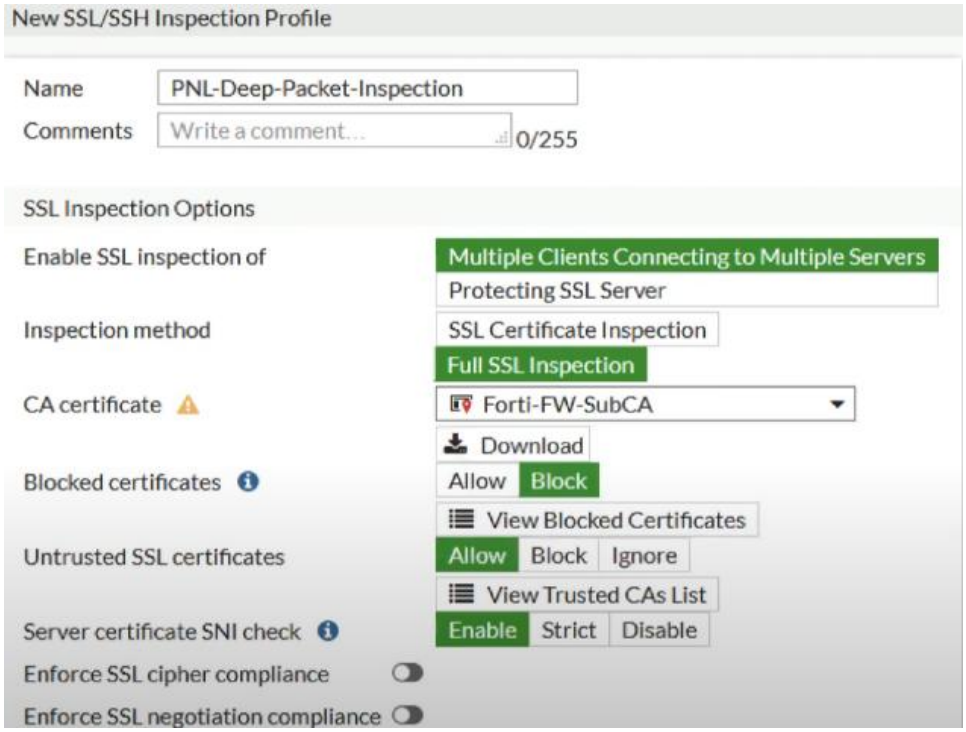


Bir sonraki sayfada “PKCS#12 Certificate” kısmına Export edilen sertifika yüklenerek Export edilirken belirlenen parola bilgisi girilmelidir.



Yükleme işlemi tamamlandıktan sonra “Local Certificarte” kısmında yüklenen sertifika görüntülenebilir.

Artık buradaki sertifika kullanılarak bir SSL Inspection tanımı oluşturulabilir. Bunun için “Security Profiles -> SSL/SSH Inspection -> Create New” yolu izlenerek yeni bir SSL Inspection profili oluşturulmalıdır. Burada sertifika olarak yüklenen sertifika seçilmelidir.



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 Fortgate 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.

Kaynkalar:

- 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=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%C3%BCp,inceler%2C%20ard%C4%B1ndan%20tekrar%20%C5%9Fifreleyerek%20iletir.