

epati

Kullanıcı SSH Yapılandırılması

Ürün: Antikor v2 - Yeni Nesil Güvenlik Duvarı

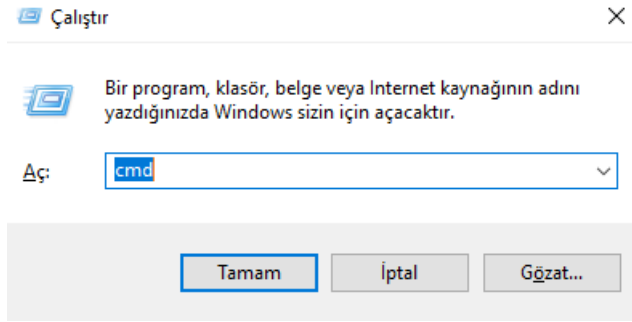
Yapılandırma Örnekleri

Kullanıcı SSH Yapılandırılması

Arayüz kullanıcılarının SSH'a erişebilmesi için ilk önce ssh-key üretmelidir.

Adım 1

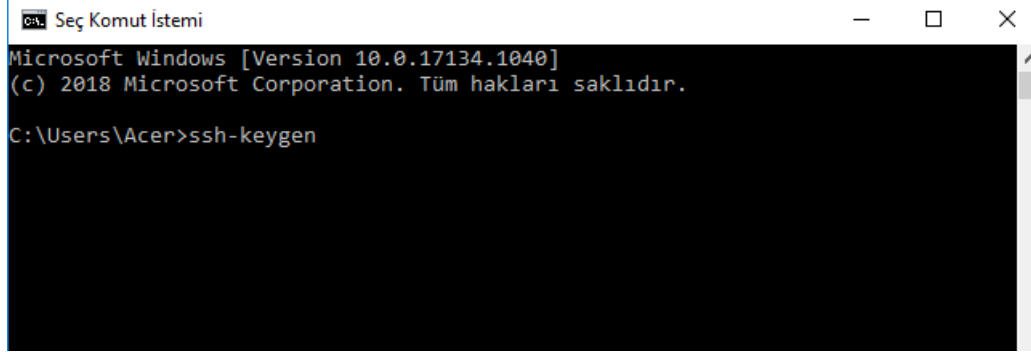
Windows+R tuşlarına basılarak Çalıştır açılır ve *cmd* yazılır.



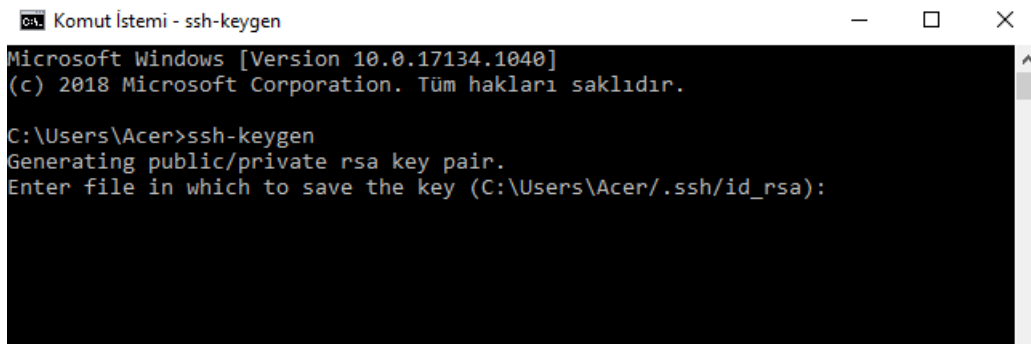
Not: Linux'da arama gezginine terminal veya uçbirim yazarak erişebilirsiniz.

Adım 2

Gelen Komut istemine *ssh-keygen* komutu yazılır.



Dosya yolu belirtilir.



Parola(passphrase) belirtilir. (SSH erişimi için)

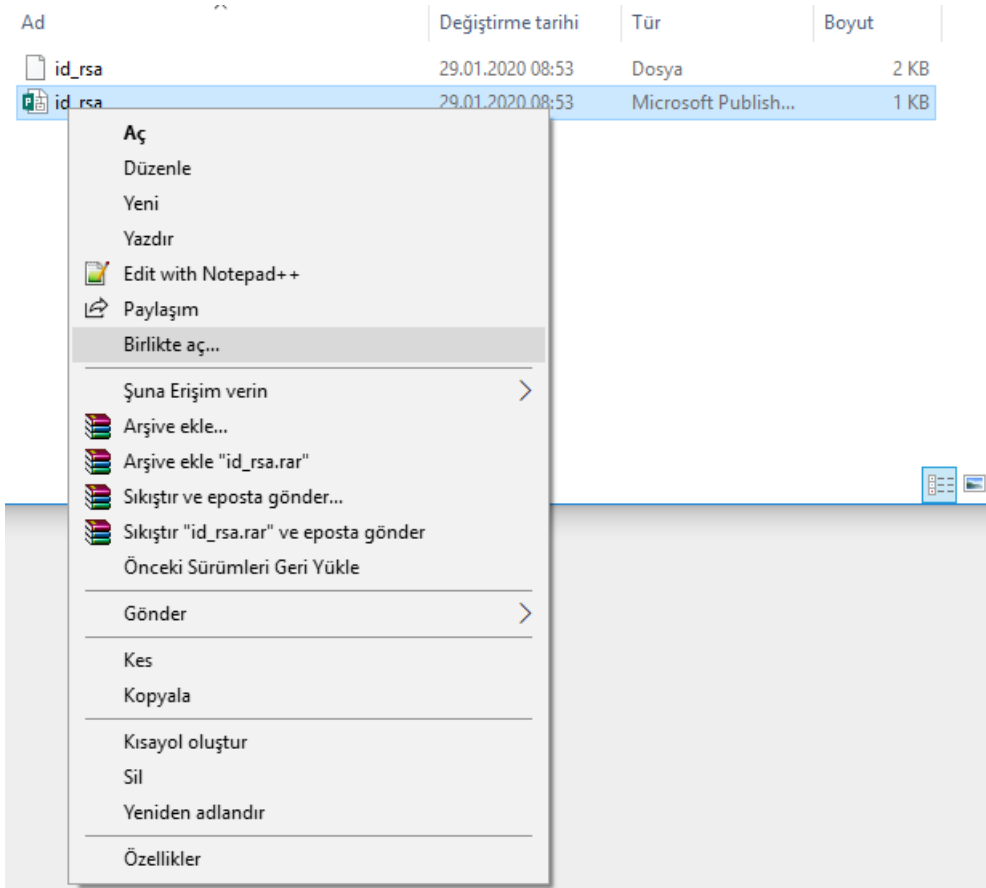
```
Komut İstemi
C:\Users\Acer>ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (C:\Users\Acer/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in C:\Users\Acer/.ssh/id_rsa.
Your public key has been saved in C:\Users\Acer/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:2jj/cS18znZw39SKq4quzvGI1noPf/vrz4Nhnru0gdo berke@berke
The key's randomart image is:
+---[RSA 2048]-----+
|
|             S          .
|          = .o ... o
|       .o = oo++++ +.
|     .ooO +.o+O+ o o
|   .o+*+E.=BXB*+
+---[SHA256]-----+
C:\Users\Acer>
```

SSH için oluşturulacak şifre belirlenir ve belirtilen dizine (C:\Users\Acer/.ssh/id_rsa) kaydedilir. (Bu dizin bilgisayardan bilgisayara değişiklik gösterebilmektedir.)

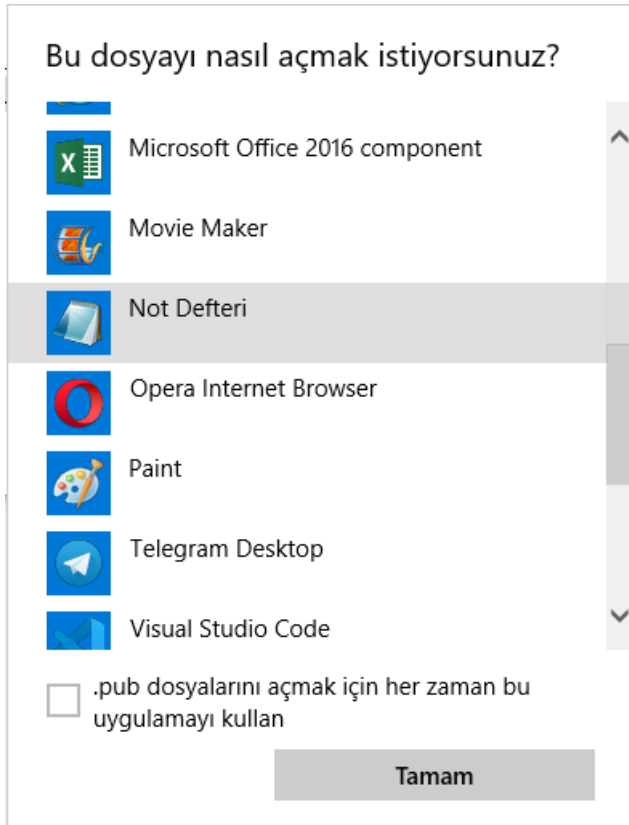
Ad	Değiştirme tarihi	Tür	Boyut
id_rsa	29.01.2020 08:53	Dosya	2 KB
id_rsa	29.01.2020 08:53	Microsoft Publish...	1 KB

Not: Aynı komutlar ile linux işletim sisteminde bulunan komut satırında da yapılabilmektedir. Komutları uyguladıktan sonra kaydedeceği dizin ise "/home/kullanıcıadı/.ssh" klasörüdür.

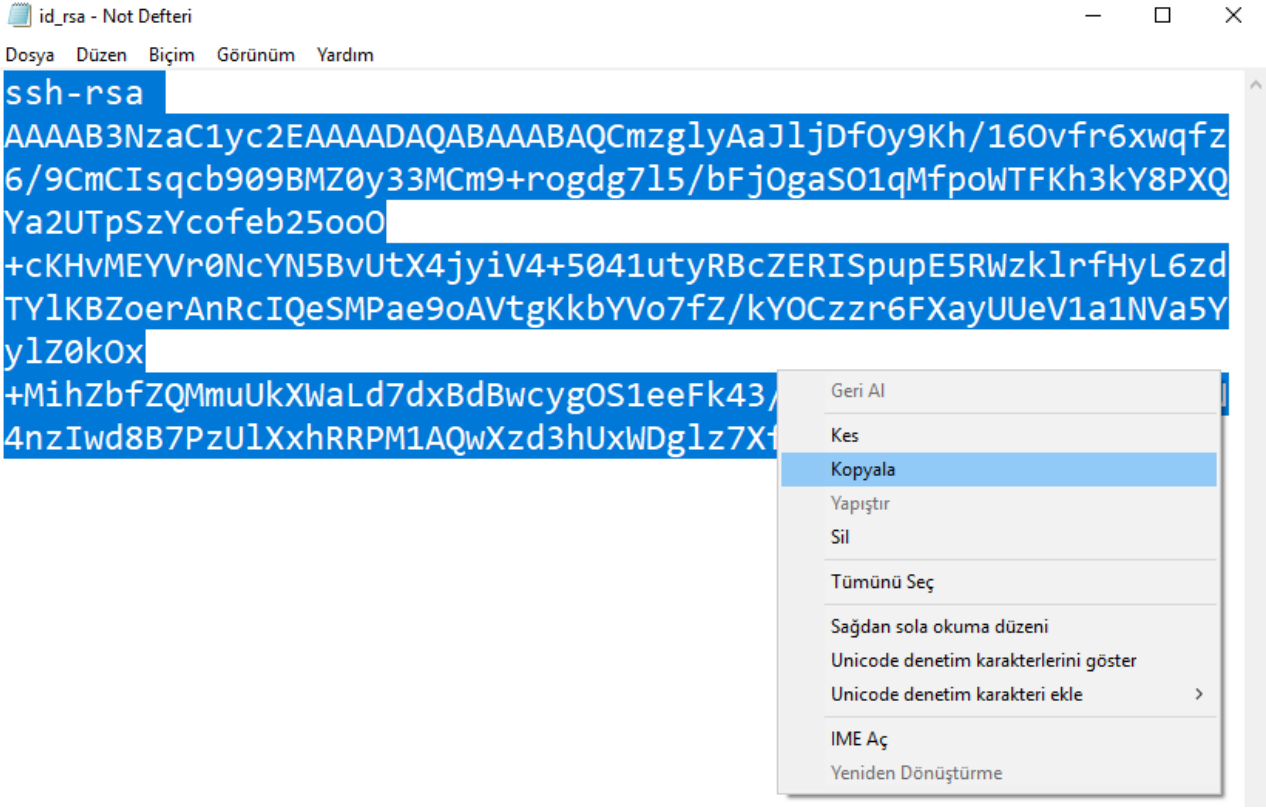
"id_rsa.pub" dosyasına sağ tıklayıp birlikte aç seçilir.



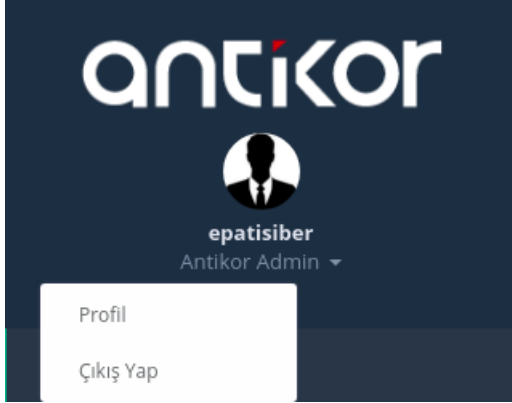
Not Defteri ile birlikte açılır.



Açılan keyin içeriğinin tamamı kopyalanır.




SSH yapacak kullanıcı için arayüze giriş yapıldıktan sonra profil'e gidilir.



"id_rsa.pub" dosyasından alıp kopyaladığımız key, profile SSH Public Key kısmına yapıştırılır.

Profil

<p>Profil Resmi</p>  <p>Kullanıcı Adı : epatisiber</p>	<p>Profil Fotoğrafı Yükle</p> <p>Profil Fotoğrafı : Yükle</p>
<p>Kullanıcı Bilgileri</p> <p>Adı : Antikor</p> <p>Soyadı : epatisiber</p> <p>Kimlik Numarası : 11111111111</p> <p>Telefon : 3243610233</p> <p>E-Posta : bilgi@epati.com.tr</p> <p>Doğum Tarihi : 2008-06-08</p> <p>İlk Giriş Tarihi : 2021-06-17 20:03:03+03</p> <p>Son Giriş Tarihi : 2021-06-17 20:29:54+03</p> <p>Kim Tarafından oluşturuldu : berke.temel.atak@epati.com.tr</p>	<p>Dil Ayarları</p> <p><input checked="" type="radio"/> tr <input type="radio"/> en <input type="radio"/> ar</p> <p>Parola Değiştir</p> <p>Kullanıcı Parolasını Değiştir</p> <p>İki Adımlı Kimlik Doğrulama</p> <p>İki Adımlı Kimlik Doğrulama Ayarları</p> <p>Gösterge Panelini Sıfırla</p> <p>Gösterge Panelini Sıfırla</p> <p>SSH Public Key</p> <p>ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQgQCkjo73Dh9d8snxtsR3dDLRyF</p> <p>Kaydet</p>

Adım 3

Arayüzde *Yönetim Paneli Kullanıcıları* kullanıcıları menüsünden ssh erişimi verilecek kullanıcı(bu yapılandırma örneği için *epatisiber* kullanıcısı) için *Düzenle* işlemine tıklanır.



Yönetim Paneli Kullanıcıları

[Yenile](#) [Ekle](#)

[XLS](#) [CSV](#) [PDF](#) [Goster/Gizle](#) Sayfa Başı Kayıt Sayısı [Tamam](#) [Filtrele](#) [Filtreyi Temizle](#)

#	Durum	Adı	Soyadı	Kullanıcı Adı	İşlemler
1	Aktif	Antikor	Admin	epatisiber	Düzenle Sil Grup Üyelikler Yetkiler ve Roller Detaylar Sertifika Yönetimi
2	Aktif	Antikor	Admin	admin	Düzenle Sil Grup Üyelikler Yetkiler ve Roller Detaylar Sertifika Yönetimi

[«](#) [<](#) [1](#) [>](#) [»](#) [Göt](#)

SSH Erişimi checkbox'ı işaretlenir.

Yönetim Paneli Kullanıcıları - Kayıt Düzeltme

Durum [Aktif](#)

Kimlik Bilgileri 111*****11 - Antikor Admin

Kullanıcı Adı epatisiber

☐ Admin Kullanıcısı ☐ Sms Doğrulama Yap ☒ SSH Erişimi

Yetkili Olduğu İstemci Grupları

Filtreleme için Yetkili Olduğu İstemci Grupları

☒ Yetkili olduğu gruplar ile aynı olsun

[İptal](#) [Kaydet](#)

Checkbox işaretlendikten sonra *SSH Yetkileri* bölümüne kullanıcı için izinli olacak SSH komutları girilir.

Durum	<input checked="" type="checkbox"/> Aktif	
Kimlik Bilgileri	111*****11 - Antikor Admin x	
Kullanıcı Adı	epatisiber	
<input type="checkbox"/> Admin Kullanıcısı	<input type="checkbox"/> Sms Doğrulama Yap	<input checked="" type="checkbox"/> SSH Erişimi
SSH Yetkileri	tcpdump, grep, top... Tümüü Seç	
Yetkili Olduğu İstemci Grupları		
Filtreleme için Yetkili Olduğu İstemci Grupları	<input checked="" type="checkbox"/> Yetkili olduğu gruplar ile aynı olsun	

İptal

Kaydet

SSH Yetkileri kısmına bir veya birden fazla komut girilebilir.

Durum	<input checked="" type="checkbox"/> Aktif	
Kimlik Bilgileri	111*****11 - Antikor Admin x	
Kullanıcı Adı	epatisiber	
<input type="checkbox"/> Admin Kullanıcısı	<input type="checkbox"/> Sms Doğrulama Yap	<input checked="" type="checkbox"/> SSH Erişimi
SSH Yetkileri	x tcpdump x Tümüü Seç	
Yetkili Olduğu İstemci Grupları		
Filtreleme için Yetkili Olduğu İstemci Grupları	<input checked="" type="checkbox"/> Yetkili olduğu gruplar ile aynı olsun	

İptal

Kaydet

Tümüü Seç butonu tüm komutları SSH yetkilerine getirecektir. (Kullanıcı SSH komutlarının hepsini kullanabilecek.)

Durum Aktif

Kimlik Bilgileri 111*****11 - Antikor Admin x v

Kullanıcı Adı epatisiber

☐ Admin Kullanıcısı ☐ Sms Doğrulama Yap ☒ SSH Erişimi

SSH Yetkileri

x tcpdump

x route

x ifconfig

x netstat

x ping

x ping6

x nslookup

x traceroute

x grep

x more

x less

x telnet

x ssh

x arp

x ndp

x radtest

x iperf

x trafshow

x adminKonsolu

x ethernet

x kullanıcı

x disk-lo

x yenidenBaslat

x poweroff

x pgsqlServer

x firewall

x uygula

x servis

x paket

x lisans

x ssh-sifresi-degistir

x radiusDebug

x ipsecPolicy

x bufferTemizle

x tabloListesi

x dhcpTara

x bootMesajlari

x sistemLoglari

x tarih

Tümünü Seç

Kullanıcı için izinli SSH komutları girildikten sonra *Kaydet* butonuna tıklanılır.

Durum

Aktif

Kimlik Bilgileri

111*****11 - Antikor Admin

Kullanıcı Adı

epatisiber



Admin Kullanıcısı



Sms Doğrulama Yap



SSH Erişimi

SSH Yetkileri

x

tcpdump

x

route

x

ifconfig

x

netstat

x

ping

x

ping6

x

nslookup

x

traceroute

x

grep

x

more

x

less

x

telnet

x

ssh

x

arp

x

ndp

x

radtest

x

iperf

x

trafshow

x

adminKonsolu

x

ethernet

x

kullanici

x

disk-io

x

yenidenBaslat

x

poweroff

x

pgsqlServer

x

firewall

x

uygula

x

servis

x

paket

x

lisans

x

ssh-sifresi-degistir

x

radiusDebug

x

ipsecPolicy

x

bufferTemizle

x

tabloListesi

x

dhcpTara

x

bootMesajlari

x

sistemLoglari

x

tarih

x

donanim-bilgisi

x

disk-bilgisi

x

disk-listesi

x

webTarayici

x

http-loglari

x

soket-yeniden-baslat

x

cluster-ceza-skoru

x

cluster-durumu

x

hotspot-kota-sifirla

x

ipsec

Tümünü Seç

Yetkili Olduğu İstemci Grupları

Filtreleme için Yetkili Olduğu İstemci Grupları

☒ Yetkili olduğu gruplar ile aynı olsun

İptal

Kaydet



Kaydedildi

Kaydınız başarıyla güncellenmiştir

OK

Yapılan ayarlar kaydedildikten sonra *Tanımları Uygula* butonuna tıklanır.

Yönetim Paneli Kullanıcıları

Tanımları Uygula 1

Yönetim Paneli Kullanıcıları

Yeni Ekle

XLS CSV PDF Göster/Gizle Sayfa Başı Kayıt Sayısı Tanımları Filtrele Filtreyi Temizle

#	Durum	Adı	Soyadı	Kullanıcı Adı	İşlemler
1	Aktif	Antikor	Admin	epatisiber	Düzenle Sil Grup Üyele Yetkiler ve Roller Detaylar Sertifika Yönetimi
2	Aktif	Antikor	Admin	admin	Düzenle Sil Grup Üyele Yetkiler ve Roller Detaylar Sertifika Yönetimi

« 1 »

Uygulanacak İşlem Listesinde *Hepsini Uygula* butonuna tıklanır.

antikor v2 NGFW Staging - STAGING Sayfa ismi girmeye başlayın...

Uygulanacak İşlem Listesi

Tanımları Uygula 2

Hepsini Uygula

SSH Kullanıcıları 1 Uygula

SSH Yetkileri 49 Uygula

Adım 4

SSH erişimi için Komut İstemi veya MobaxTerm kullanılabilir.

Terminal ile SSH Bağlantısı

Adım 1'deki işlem tekrar uygulanarak komut istemi açılır.

`ssh kullanıcıadı@antikorIPAdresi -p 22022` şeklinde komut yazılır.

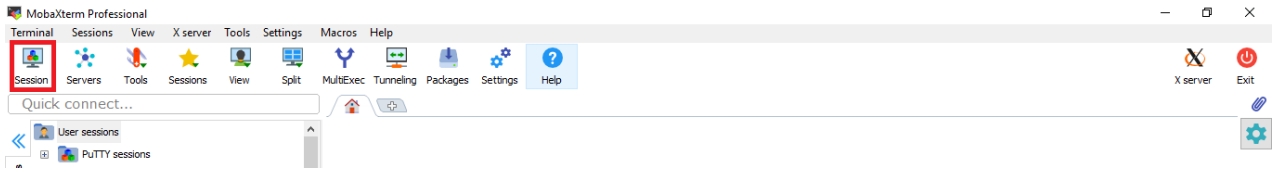
```
C:\Users\test>ssh epatisiber@10.2.3.163 -p 22022
The authenticity of host '[10.2.3.163]:22022 ([10.2.3.163]:22022)' can't be established.
ECDSA key fingerprint is SHA256:pTOPJfFnISYKrtsS5QMfNlpblnZLKEVt8qSIgYKYkDg.
Are you sure you want to continue connecting (yes/no/[fingerprint])? _
```

İlk önce “Are you sure want to continue connecting (yes/no)?” sorusuna “yes” yazıldıktan sonra **Adım 2**'de belirlenen parola (passphrase) ile açılır.

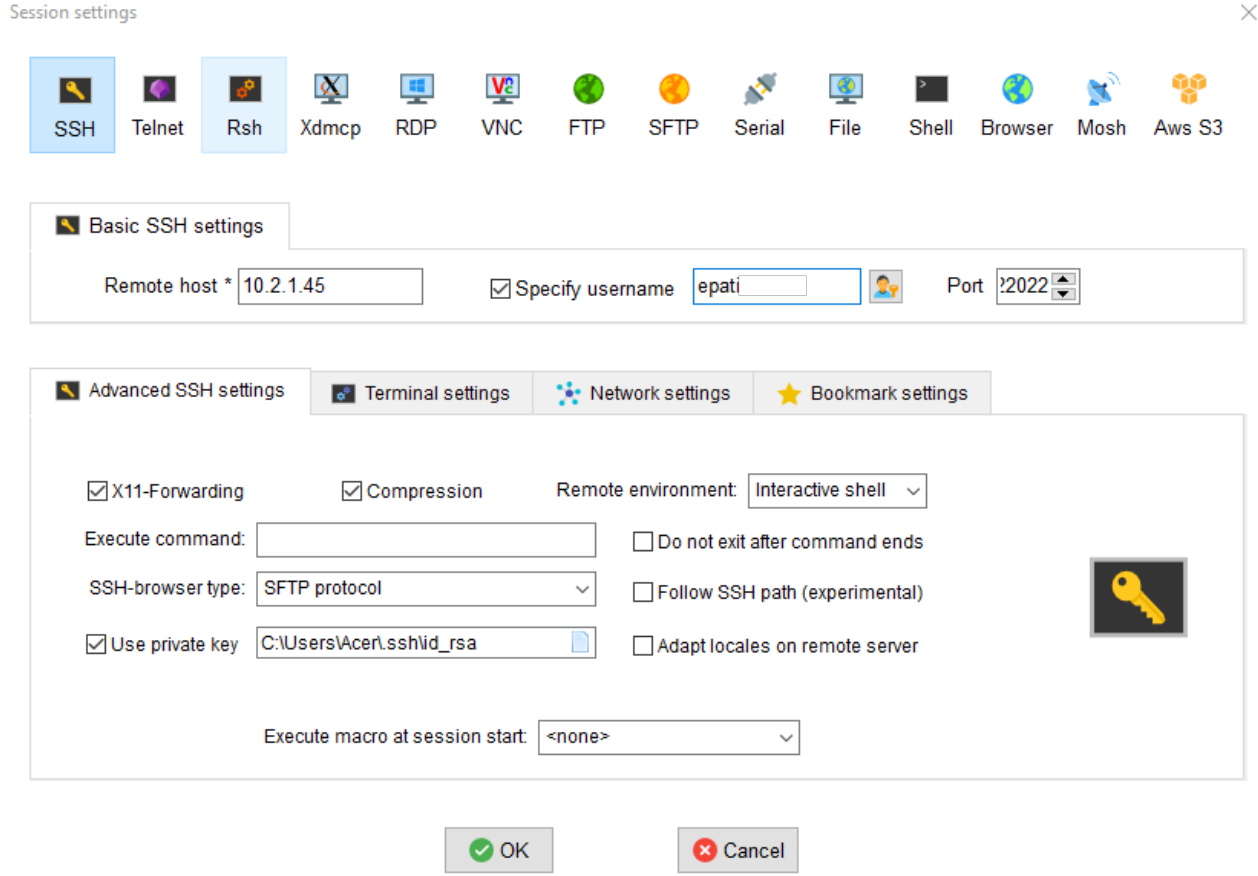
```
C:\Users\test>ssh epatisiber@10.2.3.163 -p 22022
The authenticity of host '[10.2.3.163]:22022 ([10.2.3.163]:22022)' can't be established.
ECDSA key fingerprint is SHA256:pTOPJfFnISYKrtsS5QMfNlpblnZLKEVt8qSIgYKYkDg.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.2.3.163]:22022' (ECDSA) to the list of known hosts.
Enter passphrase for key 'C:\Users\test\.ssh/id_rsa':
=====
== ePati Bilisim Teknolojileri ==
== Antikor v2 NGFW ==
=====
Komut listesi için '?' komutunu kullanabilirsiniz.
epatisiber@192.168.100.1 - ePati Siber Guvenlik A.S.:~$
```

MobaXterm ile SSH Bağlantısı

Mobaxterm programı açılıp, *Session*'a tıklanır.



Session Settings açıldıktan sonra **SSH** sekmesinde Remote host, Specify username, Port ve Use private key kısmında gereken ayarlamalar yapılır.



Remote Host kısmına Antikor IP Adresi, Specify username kısmına kullanıcı adı, Port kısmına 22022 ve Use private key kısmına **Adım 2**'de oluşturulan SSH key'in dizini (C:\Users\Acer\.ssh\id_rsa) yazılır. (Bu dizin bilgisayardan bilgisayara farklılık göstermektedir.) **OK** butonuna tıklanır.



Basic SSH settings

Remote host * 10.2.1.45

☒ Specify username epati

Port 2022

Advanced SSH settings

Terminal settings

Network settings

Bookmark settings

☒ X11-Forwarding☒ Compression

Remote environment: Interactive shell

Execute command:

☐ Do not exit after command ends

SSH-browser type: SFTP protocol

☐ Follow SSH path (experimental)☒ Use private key

C:\Users\Acer\.ssh\id_rsa

☐ Adapt locales on remote server

Execute macro at session start: <none>

OK

Cancel

IP adresi yazılı session açılır.

MobaXterm Professional

Terminal Sessions View X server Tools Settings

Session Servers Tools Sessions View Split

Quick connect...

User sessions
Putty sessions
10.2.1.45

Açılan session'a **Adım 2**'de oluşturulan parola(passphrase) girilir.



SSH bağlantısı MobaXterm programı ile kurulmuş olur.

```
• MobaXterm 10.8 •
(SSH client, X-server and networking tools)

> SSH session to epati@10.2.1.45
• SSH compression : ✓
• SSH-browser      : ✓
• X11-forwarding   : ✗ (disabled or not supported by server)
• DISPLAY          : 192.168.100.11:0.0

> For more info, ctrl+click on help or visit our website


=====
== ePati Bilisim Teknolojileri ==
== Antikor v2 NGFW ==
=====
Komut listesi icin '?' komutunu kullanabilirsiniz.
epati:~$
```

ePati Siber Güvenlik Teknolojileri A.Ş.

Mersin Üniversitesi Çiftlikköy Kampüsü

Teknopark İdari Binası Kat: 4 No: 411

Posta Kodu: 33343 Yenişehir / MERSİN

 www.epati.com.tr

 bilgi@epati.com.tr

 +90 324 361 02 33

 +90 324 361 02 39

