epati

SSL VPN İki Aşamalı Kimlik Doğrulama Linux İstemci Yapılandırması

Ürün: Antikor v2 - Yeni Nesil Güvenlik Duvarı

- Yapılandırma Örnekleri

title: ssl-vpn-yapilandirmasi-linux 2fa
—

SSL VPN İki Aşamalı Kimlik Doğrulama Linux İstemci Yapılandırması

SSL VPN (Secure Sockets Layer Virtual Private Network - Güvenli Yuva Katmanı Tabanlı Sanal Özel Ağ):** Herhangi bir ağa uzaktan güvenli bir şekilde erişmek için kullanılır. SSL VPN sayesinde SSL Sertifikalı şifreli bir iletişim sağlanır. IPSec VPN'de yaşanan zorluklar nedeni ile IPSec VPN'in yerini SSL VPN almıştır.

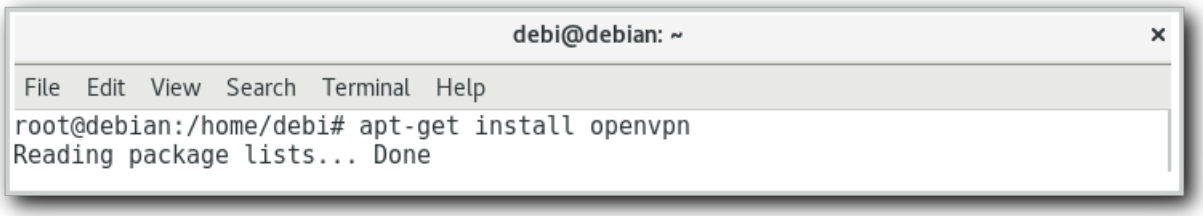
Linux tarafında Debian dağıtımı kullanılmıştır. Diğer Linux dağıtımlarında ilgili paketler yüklendiği takdirde problemsiz çalışacaktır.

Konfigürasyon

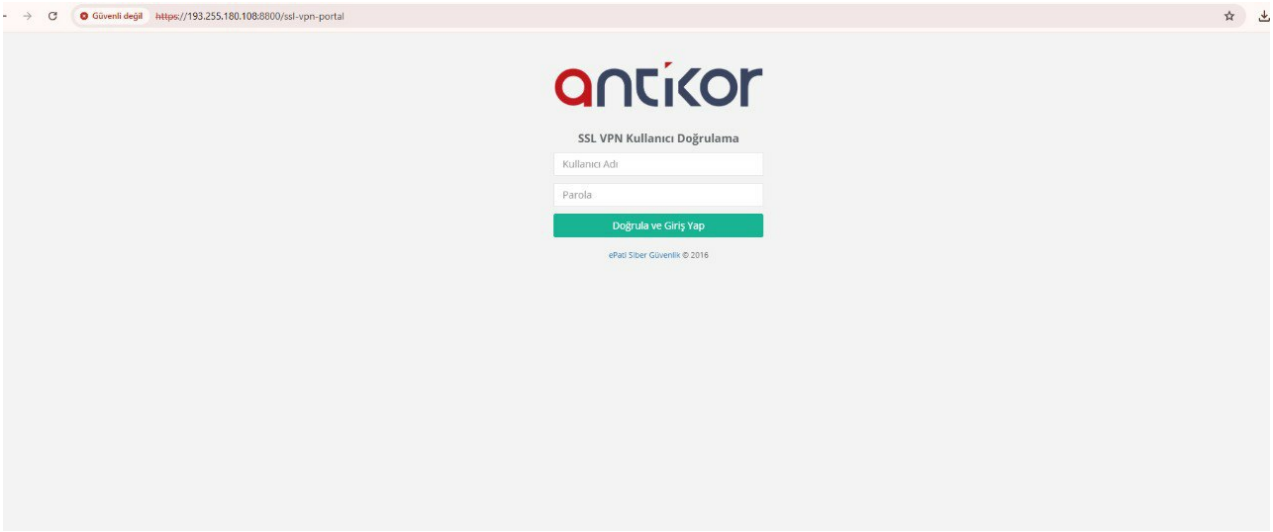
Aşağıdaki adımlar sırası ile gerçekleştirilir.

1. Terminalden apt-get update && apt-get upgrade yapılır.

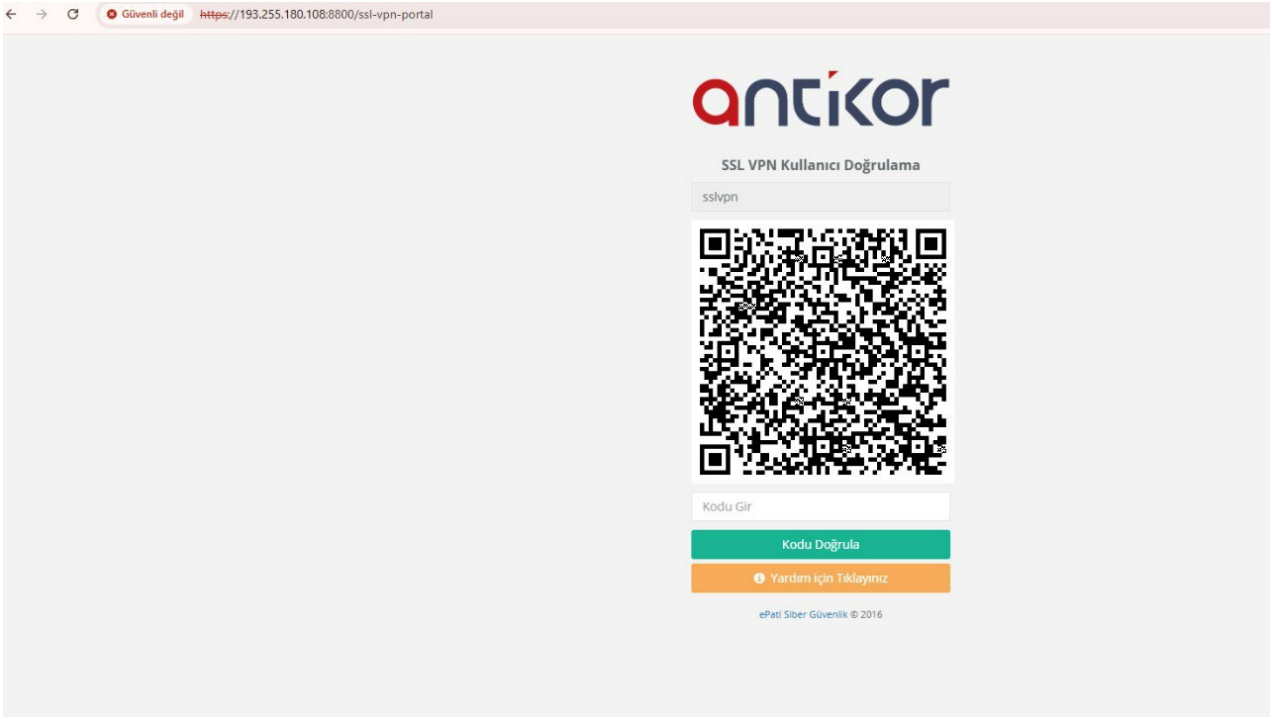
2. Terminalden apt-get install openvpn komutu kullanılarak openvpn indirilir.



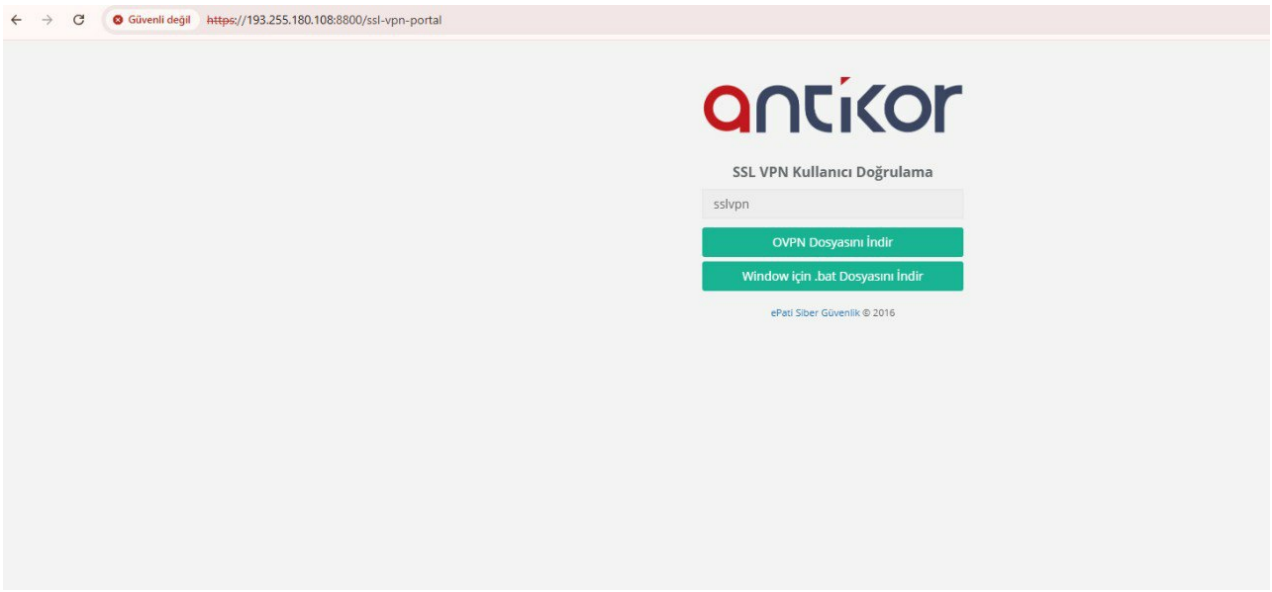
3. Antikor'dan VPN Yönetimi menüsü altında bulunan SSL VPN Ayarları sayfasında gidilir. Açılan sayfada "Ekle" butonuna tıklanarak, SSL VPN için bir kullanıcı kimliği oluşturulur. SSLVPN doğrulaması için https://ip:8800/ssl-vpn-portal



kullanıcı bilgileri doğrulaması yaptıktan sonra iki aşamalı kimlik doğrulaması için ekranda görüntülenen karekod google authenticator uygulaması ile okunur ve alınan key karekod altından yer alan kodu gir satırına girilir ve kodu doğrula butonuna tıklanır.



4. doğrulama işlemi başarılı olduğunda ekrana sertifika indir butonu gelir ve işletim sistemimize uygun sertifika indirilir.



5. istemci üzerinden openvpn –config vpnsertifikasiadi.ovpn komutu ile sslvpn bağlantısı sağlanır. komut çalıştırıldıktan sonra kullanıcı adı ve şifre girilir ardından google authenticator uygulamasından alınan kod OTP anahtarı alanına girilir

```
root@admins:/home/admins/Downloads# openvpn --config sslvpn-sslvpn.ovpn
2025-01-27 08:09:13 Note: Treating option '--ncp-ciphers' as  '--data-ciphers' (renamed in OpenVPN 2.5).
2025-01-27 08:09:13 WARNING: Compression for receiving enabled. Compression has been used in the past to break enc
ryption. Sent packets are not compressed unless "allow-compression yes" is also set.
2025-01-27 08:09:13 OpenVPN 2.5.11 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [
AEAD] built on Sep 17 2024
2025-01-27 08:09:13 library versions: OpenSSL 3.0.2 15 Mar 2022, LZO 2.10
Enter Auth Username: sslvpn
🔐 Enter Auth Password: *********
🔐 CHALLENGE: OTP Anahtarını girin ******
```

girilen bilgiler doğru ise sslvpn bağlandığı görülür.

```
2025-01-27 08:09:13 OpenVPN 2.5.11 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [
AEAD] built on Sep 17 2024
2025-01-27 08:09:13 library versions: OpenSSL 3.0.2 15 Mar 2022, LZO 2.10
Enter Auth Username: sslvpn
🔐 Enter Auth Password: *********
🔐 CHALLENGE: OTP Anahtarını girin ******
2025-01-27 08:10:06 Outgoing Control Channel Authentication: Using 160 bit message hash 'SHA1' for HMAC authentica
tion
2025-01-27 08:10:06 Incoming Control Channel Authentication: Using 160 bit message hash 'SHA1' for HMAC authentica
tion
2025-01-27 08:10:06 TCP/UDP: Preserving recently used remote address: [AF_INET]10.2.1.111:1194
2025-01-27 08:10:06 Socket Buffers: R=[212992->212992] S=[212992->212992]
2025-01-27 08:10:06 UDP link local: (not bound)
2025-01-27 08:10:06 UDP link remote: [AF_INET]10.2.1.111:1194
2025-01-27 08:10:06 TLS: Initial packet from [AF_INET]10.2.1.111:1194, sid=ae0a88e0 6e1c333f
2025-01-27 08:10:06 WARNING: this configuration may cache passwords in memory -- use the auth-nocache option to pr
event this
2025-01-27 08:10:06 VERIFY OK: depth=1, CN=ePati Cyber Security
2025-01-27 08:10:06 VERIFY KU OK
2025-01-27 08:10:06 Validating certificate extended key usage
2025-01-27 08:10:06 ++ Certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server Authenticat
ion
2025-01-27 08:10:06 VERIFY EKU OK
2025-01-27 08:10:06 VERIFY OK: depth=0, CN=antikor2-sslvpn
2025-01-27 08:10:07 Control Channel: TLSv1.3, cipher TLSv1.3 TLS_AES_256_GCM_SHA384, peer certificate: 2048 bit RS
A, signature: RSA-SHA256
2025-01-27 08:10:07 [antikor2-sslvpn] Peer Connection Initiated with [AF_INET]10.2.1.111:1194
2025-01-27 08:10:07 PUSH: Received control message: 'PUSH_REPLY,dhcp-option DNS 8.8.8.8,route-gateway 192.168.3.1,
topology subnet,ping 10,ping-restart 60,route 192.168.2.0 255.255.255.0,ifconfig 192.168.3.2 255.255.255.0,peer-id
 0,cipher AES-256-CBC'
2025-01-27 08:10:07 OPTIONS IMPORT: timers and/or timeouts modified
2025-01-27 08:10:07 OPTIONS IMPORT: --ifconfig/up options modified
2025-01-27 08:10:07 OPTIONS IMPORT: route options modified
2025-01-27 08:10:07 OPTIONS IMPORT: route-related options modified
2025-01-27 08:10:07 OPTIONS IMPORT: --ip-win32 and/or --dhcp-option options modified
2025-01-27 08:10:07 OPTIONS IMPORT: peer-id set
2025-01-27 08:10:07 OPTIONS IMPORT: adjusting link_mtu to 1625
2025-01-27 08:10:07 OPTIONS IMPORT: data channel crypto options modified
2025-01-27 08:10:07 Outgoing Data Channel: Cipher 'AES-256-CBC' initialized with 256 bit key
2025-01-27 08:10:07 Outgoing Data Channel: Using 160 bit message hash 'SHA1' for HMAC authentication
2025-01-27 08:10:07 Incoming Data Channel: Cipher 'AES-256-CBC' initialized with 256 bit key
2025-01-27 08:10:07 Incoming Data Channel: Using 160 bit message hash 'SHA1' for HMAC authentication
2025-01-27 08:10:07 net_route_v4_best_gw query: dst 0.0.0.0
2025-01-27 08:10:07 net_route_v4_best_gw result: via 10.2.1.253 dev enp2s0
2025-01-27 08:10:07 ROUTE_GATEWAY 10.2.1.253/255.255.255.0 IFACE=enp2s0 HWADDR=6c:62:6d:32:a3:f7
2025-01-27 08:10:07 TUN/TAP device tun0 opened
2025-01-27 08:10:07 net_iface_mtu_set: mtu 1500 for tun0
2025-01-27 08:10:07 net_iface_up: set tun0 up
2025-01-27 08:10:07 net_addr_v4_add: 192.168.3.2/24 dev tun0
2025-01-27 08:10:07 net_route_v4_add: 192.168.2.0/24 via 192.168.3.1 dev [NULL] table 0 metric -1
2025-01-27 08:10:07 Initialization Sequence Completed
```


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