



## SSL VPN Settings

Product: Antikor v2 - Next Generation Firewall  
Guides

# SSL VPN Settings

SSL VPN (Secure Sockets Layer Virtual Private Network): It is used to securely access any network remotely. Thanks to SSL VPN, an encrypted communication with SSL certificate is provided. Due to the difficulties experienced in IPsec VPN, IPsec VPN has been replaced by SSL VPN.

The page where SSL VPN settings are made.

SSL VPN Configuration

Settings

WAN IP Address

IPv4 10.2.4.202

VPN Network Address

IPv4 192.168.1.0/24

DNS Settings

☒ Set Manually
 ☐ Use Split Tunnel DNS Service

DNS Server

IPv4 8.8.8.8

Authentication Digest

SHA1

Crypto Algorithm

AES-256-CBC

Protocol

UDP

Port Number

1194

Accessible Networks

0.0.0.0/0 × ×

Operation Mode

User Authentication

Multiple Sessions Per User

☐ Single Session
 ☒ Multiple Sessions

Save

Portal addresses:

- https://10.2.4.202:8800/ssl-vpn-portal
- https://10.10.50.1:8801/ssl-vpn-portal

Use Split Tunnel DNS

Refresh

Add

#	Domain Name	Domain Name Server	Transactions

«

»

FIELD	DEFINITIONS
WAN IP Address	The WAN IP address of the users connected to the VPN is determined. If left blank the Antikor will use the WAN IP address.
VPN Network Address	IP address block which will be used when VPN connected.
DNS Settings	Select “Manually Adjust” or “Use Split Tunnel DNS Service”.
DNS Server	Enter DNS address for users who will be connected to the VPN. If “set manually” is selected, this field will be active.
Use Split Tunnel DNS Service	If “Use Split DNS Service” is selected, the field shown on the right will be active and the records are entered here.
Protocol	The protocol should be selected.
Port Number	Specify the VPN Port.
Accessible Networks	IP blocks accessible via the SSL VPN are opened in the internal network. 1-If blank is left empty, Internet goes on VPN and all internal network will be accessible. </br> 2-IP address want to be accessed is written.</br>
User Authentication	The button must be activated to use authentication with User name and Password during the VPN connection phase.
Certificate Authentication	If the user name and password are not requested with the certificate downloaded from the portal, it must be activated.
User Authentication and two factor authentication	It must be activated if it is requested to be verified with the username, password and QR code during the connection.
Multiple Sessions Per User	For the SSL VPN record created, this is the setting required for one or more users to connect.

Certificate Management

User Setting Assignment

ReloadAdd

XLSCSVPDFShow/HideRecords Per PageOKFilterReset Filter

#	Status	Username	Reserved IP Address	Accessible Networks	Description	Transactions
1	Active		1.255.255.10	192.168.58.0/24	test	EditDelete

<<1>>

Go

**ePati Cyber Security Technologies Inc.**  
Mersin Universitesi Ciftlikkoy Kampusu  
Teknopark Idari Binasi Kat: 4 No: 411  
Zip Code: 33343 Yenisehir / MERSIN / TURKIYE

[www.epati.com.tr](http://www.epati.com.tr)  
[info@epati.com.tr](mailto:info@epati.com.tr)  
+90 324 361 02 33  
+90 324 361 02 39

