IPSEC VPN Configuration

Product: Antikor v2 - Next Generation Firewall

Configuration Examples

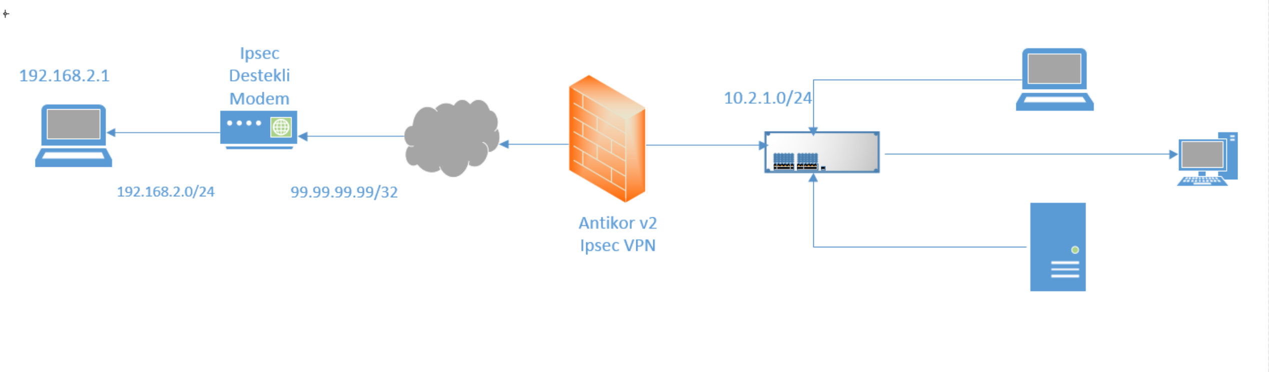
www.epati.com.tr

IPSEC VPN Configuration

Summary

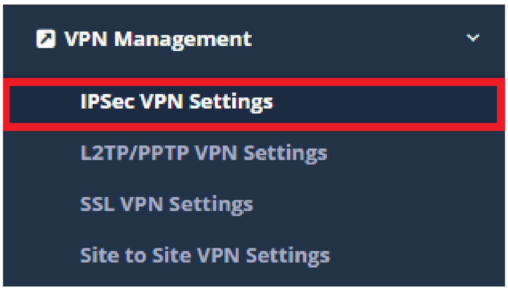
Internet Protocol Security (IPsec) is a protocol that provides protection by using authentication and encryption for each packet in communications provided using Internet Protocol (IP). IPsec has the authority to perform mutual verification and key changes during the session. It is used to protect the data flow between two computers, between the two networks and between a network and a computer.

Network Topology

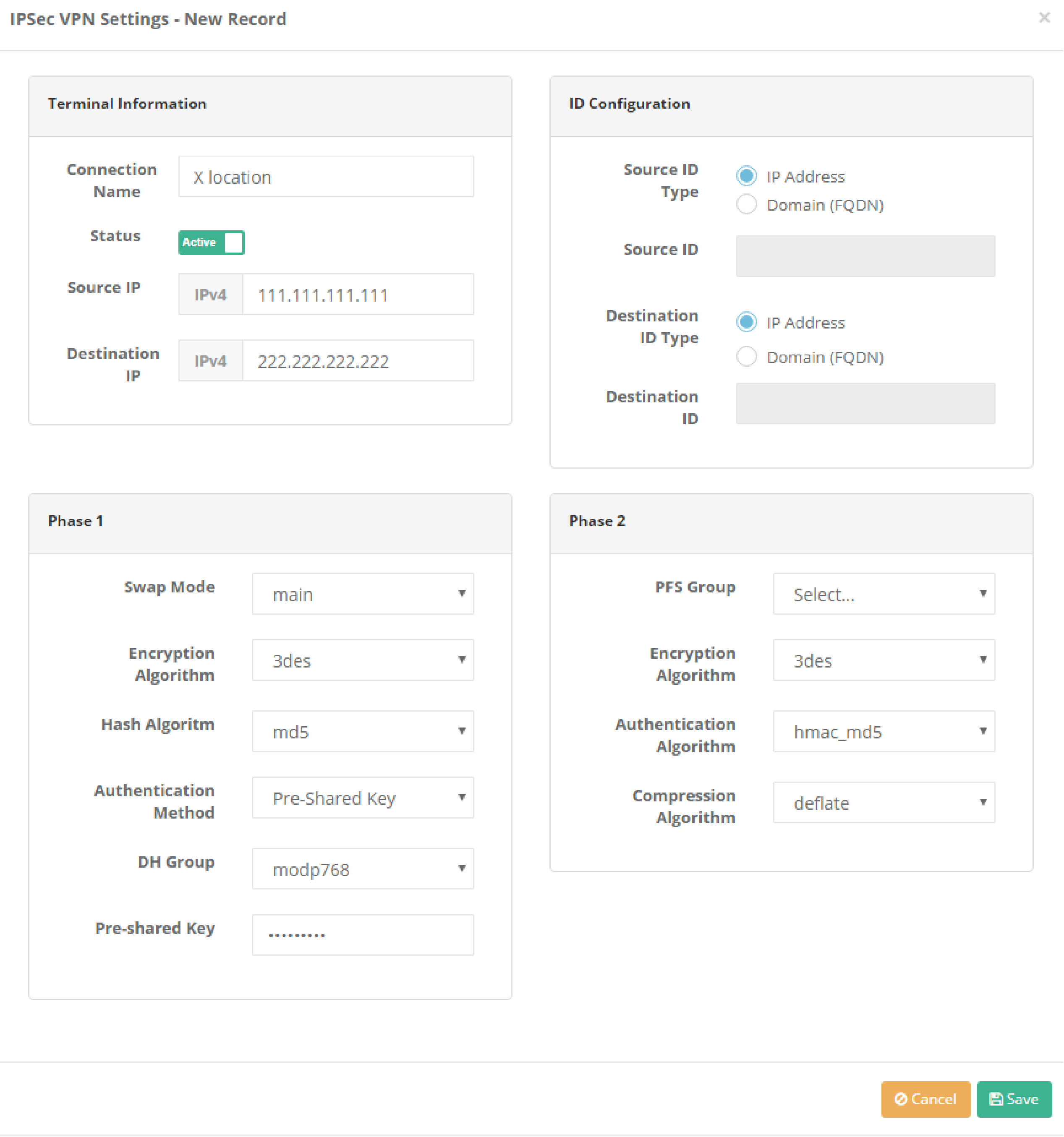


Configuration

Firstly, click the IPSEC VPN Settings under the VPN Management menu.



Click “Add” button, on the opened page.



IPSec VPN Settings - New Record

Terminal Information

Connection Name	X location
Status	Active
Source IP	IPv4 111.111.111.111
Destination IP	IPv4 222.222.222.222

ID Configuration

Source ID Type	● IP Address ○ Domain (FQDN)
Source ID	
Destination ID Type	● IP Address ○ Domain (FQDN)
Destination ID	

Phase 1

Swap Mode	main
Encryption Algorithm	3des
Hash Algoritm	md5
Authentication Method	Pre-Shared Key
DH Group	modp768
Pre-shared Key	·········

Phase 2

PFS Group	Select...
Encryption Algorithm	3des
Authentication Algorithm	hmac_md5
Compression Algorithm	deflate

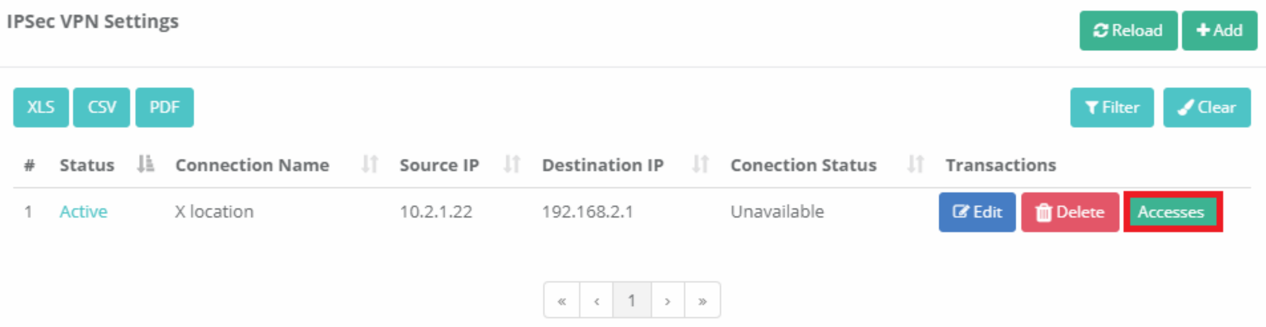
Terminal Information	Description
`Connection Name`	Any name is entered for the IPsec Vpn connection.
`Status`	Active / Passive state is set.
`Source IP`	Enter the Antikor WAN IP.
`Destination IP`	Enter the Target IP.

ID Configuration	Description
Source ID Type	If IP Addres selected, the IP that is written on the source IP is valid.
Source ID	If Domain FQDN selected, related IP is written.
Destination ID Type	If IP Address selected, the IP that is written on the target IP is valid.
Destination ID	If Domain FQDN selected, related IP is written.

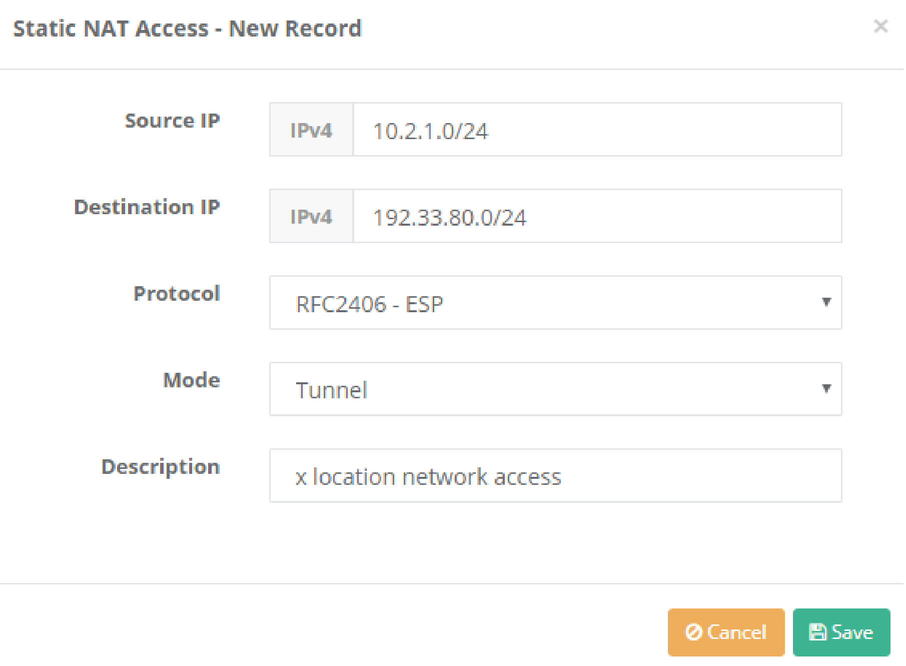
Phase 1	Description
Swap Mode	According on the settings entered on the target the main, base or aggressive is selected.
Encrytption Algorithm	According on the settings entered on the target the des, 3des etc. is selected.
Hash Algorithm	According on the settings entered on the target the sha1, md5, sha254 etc. is selected.
Authentication Method	Must be the same as Key entered on target side.
DH Group	Setting be according to the DH group entered in the destination.
Pre-shared Key	Pre-shared Key must be the same as the target.

Phase 2	Description			
PFS Group	Editing is made according to the settings entered in the target.			
Encryption Algorithm	According on the settings entered on the target the des, 3des etc. is selected.			
Authentication Algorithm	According on the settings entered on the target the hmacsha1, hmacmd5 etc. is selected.		Compression Algorithm	Deflate is selected.

After making the necessary adjustments, click the Accesses button to write the internal IPs that need to communicate.



#	Status	Connection Name	Source IP	Destination IP	Conection Status	Transactions
1	Active	X location	10.2.1.22	192.168.2.1	Unavailable	Edit Delete Accesses



Static NAT Access - New Record

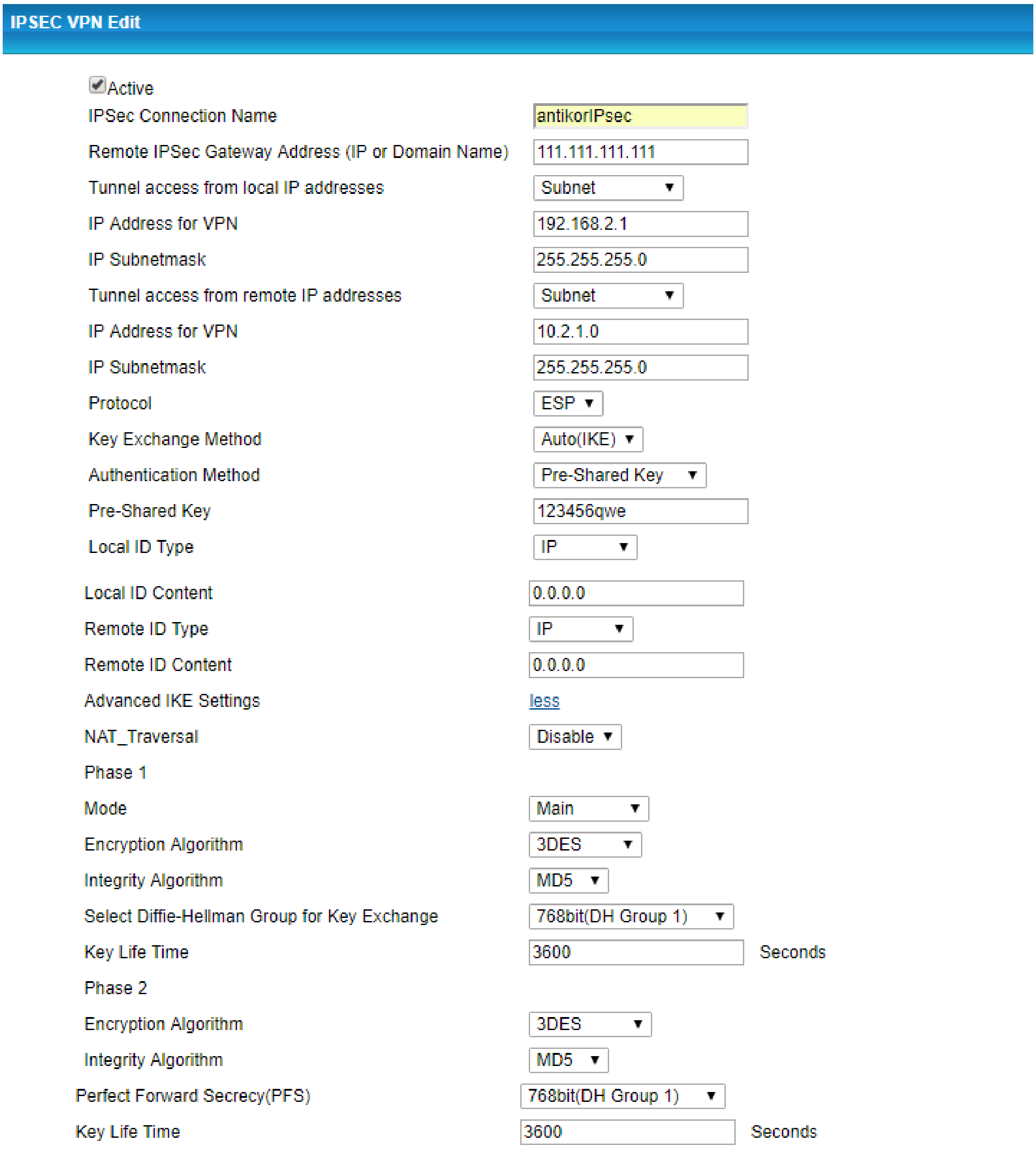
Source IP	IPv4 10.2.1.0/24
Destination IP	IPv4 192.33.80.0/24
Protocol	RFC2406 - ESP
Mode	Tunnel
Description	x location network access

After the necessary settings are made on the antibody side, Ipsec VPN Service is started from the Dashboard.

Target Side Configuration

The modem was used as the target.

The Modem and Antikor v2 settings must be the same.



IPSEC VPN Edit

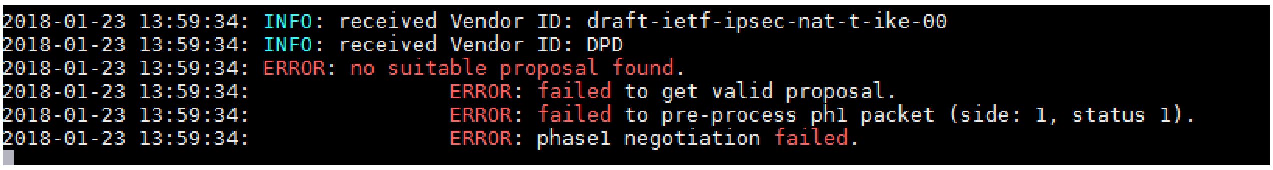
☑ Active

IPSec Connection Name	antikorIPsec	
Remote IPSec Gateway Address (IP or Domain Name)	111.111.111.111	
Tunnel access from local IP addresses	Subnet ▼	
IP Address for VPN	192.168.2.1	
IP Subnetmask	255.255.255.0	
Tunnel access from remote IP addresses	Subnet ▼	
IP Address for VPN	10.2.1.0	
IP Subnetmask	255.255.255.0	
Protocol	ESP ▼	
Key Exchange Method	Auto(IKE) ▼	
Authentication Method	Pre-Shared Key ▼	
Pre-Shared Key	123456qwe	
Local ID Type	IP ▼	
Local ID Content	0.0.0.0	
Remote ID Type	IP ▼	
Remote ID Content	0.0.0.0	
Advanced IKE Settings	less	
NAT_Traversal	Disable ▼	
Phase 1		
Mode	Main ▼	
Encryption Algorithm	3DES ▼	
Integrity Algorithm	MD5 ▼	
Select Diffie-Hellman Group for Key Exchange	768bit(DH Group 1) ▼	
Key Life Time	3600	Seconds
Phase 2		
Encryption Algorithm	3DES ▼	
Integrity Algorithm	MD5 ▼	
Perfect Forward Secrecy(PFS)	768bit(DH Group 1) ▼	
Key Life Time	3600	Seconds

Troubleshooting

1) After the settings are made, start the VPN-IPsec on the Dashboard.

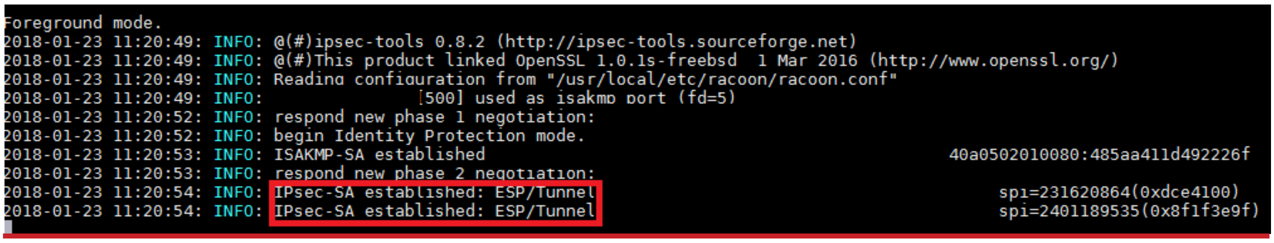
Connection status can be seen with ipsecDebug command in Antikor SSH. For example ;



```
2018-01-23 13:59:34: INFO: received Vendor ID: draft-ietf-ipsec-nat-t-ike-00
2018-01-23 13:59:34: INFO: received Vendor ID: DPD
2018-01-23 13:59:34: ERROR: no suitable proposal found.
2018-01-23 13:59:34:                ERROR: failed to get valid proposal.
2018-01-23 13:59:34:                ERROR: failed to pre-process ph1 packet (side: 1, status 1).
2018-01-23 13:59:34:                ERROR: phase1 negotiation failed.
```

As seen in the picture, there is a problem for Phase 1. Check the Phase 1 settings for the Antikor and the modem.

2) After all necessary settings have been provided, ping should be discarded. Bağlantı resmi ;



```
Foreground mode.
2018-01-23 11:20:49: INFO: @(#)ipsec-tools 0.8.2 (http://ipsec-tools.sourceforge.net)
2018-01-23 11:20:49: INFO: @(#)This product linked OpenSSL 1.0.1s-freebsd  1 Mar 2016 (http://www.openssl.org/)
2018-01-23 11:20:49: INFO: Reading configuration from "/usr/local/etc/racoon/racoon.conf"
2018-01-23 11:20:49: INFO: [redacted][500] used as isakmp port (fd=5)
2018-01-23 11:20:52: INFO: respond new phase 1 negotiation: [redacted]
2018-01-23 11:20:52: INFO: begin Identity Protection mode.
2018-01-23 11:20:53: INFO: ISAKMP-SA established [redacted] 40a0502010080:485aa411d492226f
2018-01-23 11:20:53: INFO: respond new phase 2 negotiation: [redacted]
2018-01-23 11:20:54: INFO: IPsec-SA established: ESP/Tunnel [redacted] spi=231620864(0xdce4100)
2018-01-23 11:20:54: INFO: IPsec-SA established: ESP/Tunnel [redacted] spi=2401189535(0x8f1f3e9f)
```