

epati

Linux Side Site to Site VPN Configuration

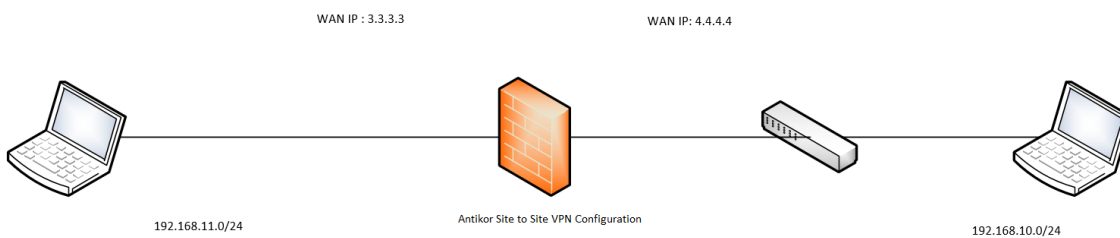
Product: Antikor v2 - Next Generation Firewall
Configuration Examples

Linux Side Site to Site VPN Configuration

Summary

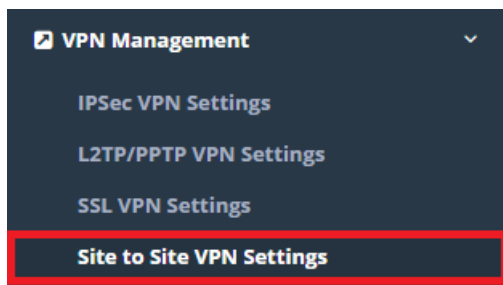
Site to site VPN is a common network used to provide secure communication between organizations for remote location offices or with any organization.

Network Topology



Antikor side Site To Site VPN Configuration

Click the Site to Site VPN under the VPN Management menu.



Firstly, click "Add" button and then the necessary configurations must be completed.

Status Active

Protocol GRE

Connection Name Linux-SitetoSite

Address Family IPv4 IPv6

Source IP Address IPv4 10.2.1.22

Destination IP Address IPv4 192.168.2.1

Source Serial IP Address IPv4 10.2.1.50

Destination Serial IP Address IPv4 192.168.2.2

Destination Network 0.0.0.0/0 × ::/0 ×

Cancel

Save

Field	Explanation
Status	Active or Passive status is selected.
Protokol	Choose IPv4 or GRE protocol.
Connection Name	Enter Connection Name.
Address Family	Choose IPv4 or IPv6 Address Family.
Source IP Address	Enter Source IP Address.
Destination IP Address	Enter destination WAN IP Address.
Source Serial IP Address	Enter Source Serial IP Address.
Destination Serial IP Address	Enter Destination Serial IP Address.
Destination Network	Enter the IP block to be accessed.

Start the "Site-to-site" VPN on the Dashboard page.

Site to Site VPN Service Running ▶ ■ ⌂

Settings on Linux Side

In the `/etc/network/interfaces` directory ;

```
auto tun1
iface tun1 inet static
    address <192.168.2.1>
    netmask <255.255.255.0>
    pre-up iptunnel add tun1 mode gre local <10.2.1.50> remote <10.2.1.22> ttl 255
    up ifconfig tun1 multicast
    pointopoint <10.2.1.50>
    post-down iptunnel del tun1
```

After, both connections are pinged to Source / Destination IP addresses and Source / Destination serial IP addresses.

```
teknik@epati: ~
File Edit View Search Terminal Help
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 0 bytes 0 (0.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1 (Local Loopback)
    RX packets 185 bytes 15000 (14.6 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 185 bytes 15000 (14.6 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

tun1: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST> mtu 1476
    inet 192.168.2.1 netmask 255.255.255.255 destination 192.168.2.2
    inet6 fe80::5efe:a02:110 prefixlen 64 scopeid 0x20<link>
    unspec 0A-02-01-10-30-30-30-3A-00-00-00-00-00-00-00-00 txqueuelen 1 (U
NSPEC)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 24 bytes 1344 (1.3 KiB)
    TX errors 2 dropped 0 overruns 0 carrier 2 collisions 0

root@epati:/home/teknik#
```

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
info@epati.com.tr
+90 324 361 02 33
+90 324 361 02 39

