Troubleshooting Client-to-Site VPNs

https://campus.barracuda.com/doc/14713475/

If your client-to-site VPN is not working as expected, try the solutions that are provided in this article for the following scenarios:

You Receive a Timeout Error on the Client

- The client might not be able to reach the public listen IP address of the Barracuda NextGen Firewall X-Series. Try to ping the public listen IP address of the appliance from the client.
- Go to the **VPN > Client-to-Site VPN** page and verify that the tunnel is configured correctly.

You Receive an Authentication Error on the Client

- Go to the **VPN > Client-to-Site VPN** page and verify that the correct user authentication method is selected.

- Go to the **Users > External Services** page and verify that the external authentication method is correctly configured.
- Ensure that the correct username and password are being used to log in.
- Verify that special characters are not being used in the password. If there are any special characters, change the password and then try to connect.

You are Able to Connect but Cannot Reach the Published Networks

- On the client, see if traffic is being sent into the tunnel. You can either check the routing table of the client machine or use the `tracert` and `traceroute` command-line utilities.
- Go to the **VPN > Client-to-Site VPN** page and verify that the **VPN Access Policies** are configured correctly.
- Ensure that the firewall rule for the VPN is allowing the traffic into the networks.

Verify the VPNCLIENTS-2-LAN Rule Matches Client-to-Site VPN Traffic

Per default the **VPNCLIENTS-2-LAN** access rule allows traffic from the client-to-site VPN to all networks in the **Trusted LAN** network object**.** Verify that the rule matches by pinging a computer in the **Trusted LAN** from a connected VPN client. If the ping goes trough you are able to reach the

internal network through the client-to-site VPN. If the ping does not work, go to **BASIC > Active Connections**:

1. Find the connection of your ping by matching protocol (ICMP), source and destination.
2. If the access rule listed in the **firewall rule** column for the connection is not VPNCLIENTS-2-LAN move the VPNCLIENTS-2-LAN rule above the rule which is currently handling the VPN traffic. For more information, see Firewall Rules Order.