Troubleshooting Site-to-Site VPNs

If your site-to-site VPN is not working correctly, try the solutions that are listed in this article.

- Ensure that the Internet connection for both systems is active.
- To verify that the VPN tunnel was initiated successfully and traffic is flowing, go to the **VPN > Site-to-Site VPN** page. Verify that green check marks are displayed in the **Status** column of the VPN tunnel.
- Double-check the VPN configuration for both systems (Lifetime, Enycrption, Hash-Method, DH-Group, Local and Remote Networks, Local and Remote Address, and Passphrase). Go to the **VPN > Site-to-Site VPN** page and verify the tunnel settings. The configurations of the peers must match or the tunnel cannot be established.
- Go to the **LOGS > VPN Log** page. Search the log for any failures and errors. Often, the problem is caused by Phase 1 and Phase 2 issues.
- From a client in the local network, ping a host in the remote network. If no host is available, try to ping the management IP address of the remote NextGen X-Series Firewall. If that does not succeed, go to the **NETWORK > IP Configuration** page on the remote X-Series Firewall and ensure that **Services to Allow: Ping** is enabled for the management IP address.
- View the the **BASIC > Recent Connections** page to verify that the correct firewall rule matches the traffic.
- Using the `tracert` and `traceroute` command-line utilities, determine where traffic is being sent. You can begin a traceroute from the **Network Connectivity Tests** section on the **ADVANCED > Troubleshooting** page. If traffic is being sent to the remote network but you are not getting a reply, verify that the gateway of the remote network is the IP address of the remote X-Series Firewall.