NetVanta 2000 Series Technical Note

Site-to-Site VPN Tunnel is up but not passing traffic

NOTE *This document is applicable to NetVanta 2600 series, 2700 series, and 2800 series units.*

Problem Definition:

A site-to-site IPSec VPN tunnel consists of two phases:

- Phase I: IKE (Internet Key Exchange)
- Phase II: IPSec (IP Security)

In Phase I, IKE creates an authenticated, secure channel between the two NetVanta 2000 Series UTM appliances (IKE peers). This is done over UDP port 500. In Phase II, IKE negotiates the IPSec security associations and generates the required key material for IPSec. This can be done either over IPSec Protocol 50 or over UDP port 4500. The latter is called NAT Traversal.

After configuring a Site to Site VPN policy between the NetVanta 2000 Series UTM appliance and another device, the tunnel may come up but no traffic may traverse the tunnel from a host behind one device to a host behind the other device. This could be due to various reasons, some of which are:

- Local or Destination network mismatch (VPN policy > Network Tab)
- The Zone or Type of the Local or Destination network is incorrectly configured
- Static Route
- Default gateway of the computers not pointing to the NetVanta 2000 Series.
- Multi-homed computers.
- AV Enforcement on VPN Zone.
- Intrusion Prevention Service (IPS), Windows Firewall or other AV application blocking ping.
- Access Rules
- Misc Troubleshooting

This integrated article tries to list the most probable causes and their resolution. For the purpose of this article the devices assumed to be used on both sides are NetVanta 2000 Series UTM appliances with Enhanced OS firmware.

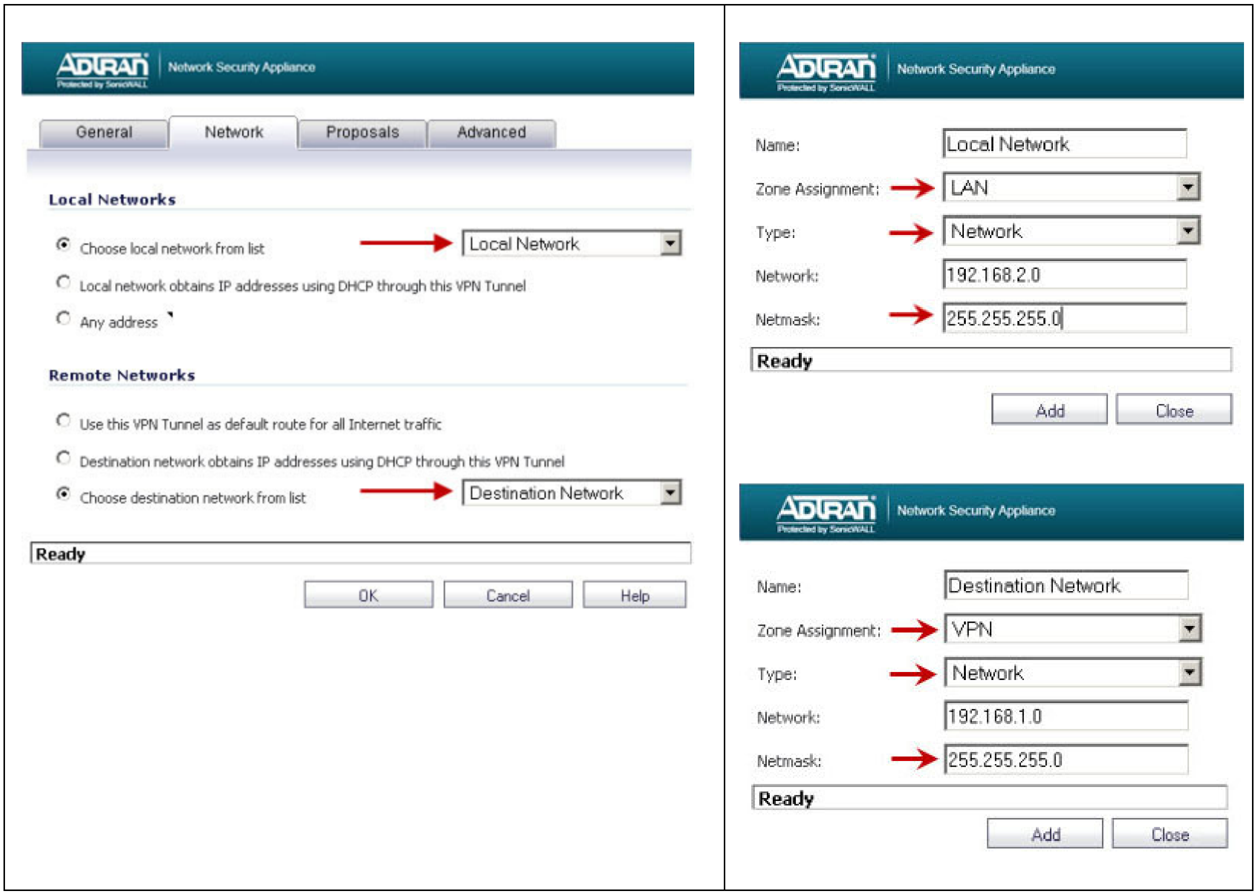
Troubleshooting:

Local and Destination Network mismatch

This is the most common reason for traffic failing to traverse a VPN tunnel. This is accompanied by an error in the NetVanta 2000 Series Log. The following errors can be seen in the log:

- Proposal does not Match
- Invalid Cookies

When configuring the VPN, the Local and Destination Network needs to be defined on each device. Make sure that the Local Network chosen matches the Destination Network chosen on the other site.



Local Networks

● Choose local network from list: Local Network

○ Local network obtains IP addresses using DHCP through this VPN Tunnel

○ Any address

Remote Networks

○ Use this VPN Tunnel as default route for all Internet traffic

○ Destination network obtains IP addresses using DHCP through this VPN Tunnel

● Choose destination network from list: Destination Network

Ready

Name: Local Network
Zone Assignment: LAN
Type: Network
Network: 192.168.2.0
Netmask: 255.255.255.0
Ready

Name: Destination Network
Zone Assignment: VPN
Type: Network
Network: 192.168.1.0
Netmask: 255.255.255.0
Ready

The Zone or Type of the Local or Destination Network is incorrectly configured

The zone assignment of a local or destination network is crucial for traffic to be routed through the tunnel. Although creating an **Address Object** for a local network is scarcely required, if a requirement arises to create an Address Object, ensure the zone assignment is **LAN** or **DMZ** as the case maybe.

When creating Address Objects for destination network/s ensure the zone assignment is **VPN**. If selecting more than one subnet add them to an Address Group. When creating an Address Object for an entire subnet for either local or destination network, it is advisable to have the Type set as Network rather than range. Make sure the subnet mask is correctly configured.

Static Route

Sometimes a tunnel does not come up or it comes up but no traffic passes through, if a static route is defined in the Network > Routes page which conflicts with the Local or Destination Network defined in the VPN Policy. By default, Static Routes on a NetVanta 2000 Series will overrule VPN Tunnel routes. If a Static Route has been defined for the Destination Network, the NetVanta 2000 Series will use this route instead of passing the traffic on to the VPN Tunnel.

With the introduction of the Enhanced OS 4.0, a new option "Allow VPN path to take precedence " has been introduced.

By means of the Diagnostic utility "Find Network path" on the System > Diagnostics page, it can easily be determined if the NetVanta 2000 Series has been configured with an overlapping route. Note all VPN destination networks defined in the Network tab of the VPN policies. Test each network using the Find Network Path diagnostic tool. If the network is not a static route that may override the VPN tunnel, the utility will report that the network is located on the WAN, either behind the Remote Gateway IP address, or behind your Default Router. This test may not be conclusive if the overlapping Static Route is pointing to the Default Gateway.

Default Gateway not pointing to the NetVanta 2000 Series.

In some networks, there are multiple paths to the internet from the LAN, and a host whose Default Gateway is not configured or wrongly confgured will be able to participate in the VPN traffic. The problem computer may not have a Default Gateway set at all (common on platforms which don't offer GUI methods for setting gateways like Windows, and when the server historically has only been reached by local hosts on the same network).

The answer is simply to configure a Default Gateway on the computer (or a route of last resort in a LAN router) pointing to the NetVanta 2000 Series LAN IP address

Multi-homed computers or computers with dual NICs.

Certain servers could have multiple NICs installed in them to communicate with multiple networks. At times this could pose problems for a host on the other side of the VPN tunnel to communicate with the server over the VPN tunnel. The request from the host may reach the server but the reply may go out through the NIC not participating in the VPN tunnel. To rectify this bahaviour make sure the routes in the servers are configured properly.

AV Enforcement on VPN Zone

It is normal, even advisable, to enforce the Security Services of the NetVanta 2000 Series on the VPN zone. An exception to this would be AV Enforcement on the VPN zone. If this is enabled, the NetVanta 2000 Series would drop traffic from any host communicating to another host over the VPN if Mcafee Client AV is not installed in it. Unless this is a requirement it is advisable to disable Client AV Enforcement on the VPN zone.

IPS blocking Ping

The most common way to test whether traffic is passing through the VPN tunnel is using the ping command. However if Low Priority Attacks under the NetVanta 2000 Series Intrusion Prevention Service is globally enabled or ICMP / Ping is individually enabled for prevention, ICMP packets would be dropped by the NetVanta 2000 Series. Check the logs for a message indicating the same.

Ping can be blocked by personal firewall applications like Windows Firewall and by Anti-virus applications.

Access Rules

The NetVanta 2000 Series GUI provides easy-to-configure VPN Policy interface which enables users to define VPN parameters without having to worry about the access rules and routes which are created automatically behind the scenes. However, on rare instances these rules don't get automatically created and needs to created manually. The screenshot below is an example of a LAN to VPN and VPN to LAN rule.

Misc Troubleshooting

If all of the above fail to resolve the issue, the following could be tried:

* Upgrade both units to the latest firmware if not already done.

* Disable the VPN policies on both sides, reboot the NetVanta 2000 Series and re-enable the policies.

* Delete the existing policies and re-create them.