6AOSSG0016-42A
August 2014

ADTRAN

Interoperability Guide

Configuring VPN Tunnel Failover for the NetVanta 7000 Series

This interoperability guide provides instructions for configuring virtual private network (VPN) tunnel failover on redundant wide area network (WAN) connections for the NetVanta 7000 Series. This guide includes the description of the solution and its operation and a device configuration overview for VPN tunnel failover and generic routing encapsulation (GRE) over VPN.

This guide consists of the following sections:

Solution Overview

In order to minimize WAN downtime, many NetVanta 7000 Series units are deployed with redundant (primary and secondary) WAN connections to provide WAN failover. In these deployments, the NetVanta 7000 Series is configured to monitor the primary WAN interface and automatically route traffic to the secondary WAN interface should the primary WAN fail.

This solution provides VPN failover for NetVanta 7000 Series deployments using redundant WAN connections. VPN tunnels enable you to securely connect computers and networks across a non-secure network, providing a simulated point-to-point connection between two sites through the Internet. Unlike an unencrypted connection, VPN encryption and authentication minimizes the risk of data being intercepted or altered. Like in the redundant WAN connections, the NetVanta 7000 Series must be configured to monitor the primary WAN interface and automatically route the VPN tunnel through the secondary WAN connection should the primary WAN fail.

This solution also provides optional GRE tunneling over the redundant VPN tunnels. GRE over VPN provides significant advantages over traditional VPN tunnels. These advantages are discussed in the following section.

GRE Over VPN Overview

To reduce the cost of point-to-point connections, the industry is adopting IPSEC VPN tunnels in lieu of dedicated circuits. However, traditional VPN tunnels have the following significant limitations: (1) all traffic that needs to traverse a VPN tunnel must be specified in the configuration, (2) discontinuous subnets require separate VPN tunnels, (3) VPN tunnels do not count as a routable interfaces, and (4) routing protocols cannot operate across VPN tunnels.

The best solution to simulate a dedicated point-to-point connection is a GRE tunnel. This kind of tunnel has the following advantages over VPN tunnels: (1) by default it has no limitations on the traffic that traverses it, (2) it can route multiple subnets without multiple tunnels, (3) it counts as a routable interface, and (4) it can have routing protocols operate across it. However, unlike VPN tunnels, GRE tunnels are not secure.

The ultimate solution is to merge the two processes by protecting the GRE tunnel with a VPN tunnel. This solution allows the GRE tunnel traffic to traverse the VPN tunnel, allowing traffic limitations to be dictated by the GRE tunnel instead of the VPN tunnel. Additionally, this solution has the benefit of creating a single IPSEC association regardless of how the GRE tunnel is used.

Hardware and Software Requirements and Limitations

The NetVanta 7000 Series VPN tunnel failover solution was tested and verified using a NetVanta 7100 running firmware version R10.11.0.HA.E.

Table 1. Verification Test Equipment and Firmware Versions

Product	Firmware/Software Version
ADTRAN NetVanta 7100	R10.11.0.HA.E

The use of General Routing Encapsulation (GRE) on a WAN VPN degrades the bandwidth performance of the connection. When using GRE, this solution supports a maximum symmetric bi-directional bandwidth of 6 Mbps (12 Mbps aggregate link bandwidth). Aggregate bandwidths above 12 Mbps can cause performance degradation and should be considered with caution.

Configuring NetVanta 7000 Series VPN Redundancy

The following sections provide an overview for the steps required to configure VPN tunnel failover and GRE over VPN tunneling features. They reference existing ADTRAN documents that provide additional detailed instructions.

Configuring VPN Tunnel Failover

Use the steps below to configure VPN tunnel failover. The steps reference sections from *Configuring Redundant VPN Tunnel Fail-Over in AOS* available online at https://supportforums.adtran.com:

1. Configure redundant VPN tunnels (refer to **Redundant VPN Tunnel Configuration**). This requires two WAN IP addresses be configured on the NetVanta 7000 Series as well as two WAN IP addresses on the remote router. In most cases, the Ethernet 0/0 port will be used for one WAN port while one of the LAN ports configured with a WAN VLAN will be used for the other WAN port.
2. Configure link state detection for the primary WAN connection (refer to **Link State Detection**), dynamic VPN tunnel removal (refer to **Dynamic Removal of a VPN Tunnel**), and VPN keep-alive (refer to **VPN Keep-Alive**). Link state detection allows the NetVanta 7000 Series to detect that the primary WAN connection is down and switch to the secondary WAN connection. It also allows the NetVanta 7000 Series to detect when the primary connection becomes available again and to switch traffic back to the primary. Dynamic VPN tunnel removal prevents the unit from initiating a VPN connection to the peer's primary WAN connection when the primary WAN is down. VPN keep-alive periodically sends traffic over the secondary WAN VPN tunnel, which keeps the connection open and minimizes downtime during the transition to failover.

> NOTE
> *In order to detect when the primary VPN tunnel fails, a pingable IP address must exist on the remote side while the primary VPN tunnel is operational. This IP address is used to determine if the primary tunnel is functioning properly.*

Configuring GRE Over VPN Tunnels

Use the steps below to configure GRE tunnels over the primary and secondary WAN VPN tunnels. The steps reference sections from *Configuring a GRE over IPSEC VPN Tunnel in AOS* available online at https://supportforums.adtran.com:

1. Configure the VPN tunnels on each WAN connection to use GRE tunnel endpoints (Refer to the **VPN Tunnel Configuration** section).
2. Configure the GRE tunnel (refer to the **GRE Tunnel Configuration** section).
3. Configure the firewall for the GRE tunnel (refer to the **GRE Tunnel Firewall Setup (Optional)** section).
4. Configure routing to direct desired traffic over the tunnel (refer to the **Routing Settings** section).