ADTRAN

Configuration Guide

61200890L1-29.4A
May 2005

Internet-based WAN Backup Solutions using NetVanta

Overview

This configuration guide delineates the advantages of using the NetVanta product line and the Internet for wide area network (WAN) connectivity. It includes example scenarios using Internet-based backup solutions.

Introduction

WAN communication links are traditionally the weakest component in computer networking. Unlike LAN components, which are typically in the owner's direct physical and administrative control, the facilities that make up the WAN link belong to and are controlled by a third party. These facilities also cover wide geographic areas, making them more susceptible to physical harm. Such characteristics make WAN links the single largest contributor to network downtime.

When the WAN link is critical to a network's operation, it is wise to design towards WAN resiliency. In some cases, the volume and criticality of the WAN might dictate the need to completely duplicate the WAN with redundant and independent facilities. The cost of this solution can be quite high, so the benefit must be carefully weighed.

Another common solution, especially in large hub and spoke networks, is to use dial backup around the WAN provider. In this solution, should a spoke lose its WAN connectivity to the hub, it will place a call to a dial-up server located at the hub, completely bypassing the WAN. While this is a well known solution that has been used for many years, the cost of dial-up server ownership, maintenance, and long distance toll charges can be quite high.

The Internet as an Alternative

Using the stateful inspection firewall and powerful IPSec VPN capabilities provided in the NetVanta router product line, the Internet can be a useful and low cost alternative for WAN connectivity -- as a backup or even as a primary connection. Internet use eliminates the dial-up server and its ownership and maintenance expenses, in effect outsourcing management of the modem bank to local ISPs at each location. It also eliminates toll charges since each location can connect via a local ISP. A site can remain connected indefinitely for a flat fee in many areas, incurring no toll charges.

Following are descriptions and detailed examples of several Internet-based backup solutions. These solutions have been tested with AOS Version 8.0.22E.

Note that detailed firewall design and VPN design are dependent on each network's unique requirements. The examples shown here are simpified to focus on the mechanics of using a primary and backup connection.

Also note that in these examples, the NetVanta is the remote site router. A NetVanta or a third party device can be used as the central router and the central FW/VPN gateway.

Solution 1 - Primary = Frame Relay Service Provider, Alternate = ISP via Dial-up

In this scenario (see Figure 1), a Frame Relay service provider supplies the Frame Relay access line and virtual circuit that connects a NetVanta remote site directly to the central site. Since this link is entirely over a provider's Frame Relay network, no firewall or VPN is required to protect the customer's network. The central site also has a protected Internet connection and an IPSec VPN gateway for Internet-based access to the central site network. The remote site has a dial-up resource (analog modem or ISDN) and an account at a local ISP. Should the remote's Frame Relay link fail, a dial-up connection is invoked to a local ISP. An IPSec VPN connection is established across the Internet to the central site VPN gateway, re-establishing connectivity between the two sites. The NetVanta uses its stateful inspection firewall to protect the remote network while connected to the ISP. When the Frame Relay connection is re-established, the dial backup connection is dropped and the IPSec connection ages out. The dial connection to the Internet is used solely as a backup link, and general Internet access is not provided.

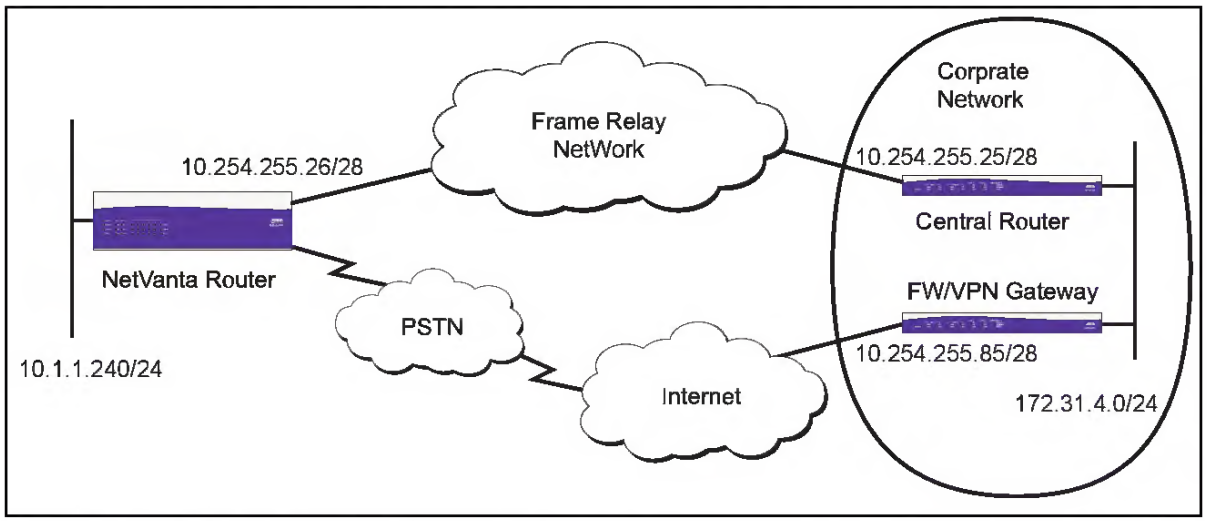

Figure 1. Primary WAN Connectivity via Frame Relay Service Provider, Backup Connectivity via IPsec VPN over Dial-up Internet Connection

Remote NetVanta Router Configuration:

```
!
!
hostname "NV_Remote"
!
ip routing
!
ip firewall
!
ip crypto
!
crypto ike policy 100
 initiate aggressive
 no respond
```



```
 local-id fqdn REMOTE
 peer 10.254.255.85
 attribute 10
  authentication pre-share
  group 2
  lifetime 300
!
crypto ike remote-id fqdn CENTRAL. preshared-key 1234567890
!
crypto ipsec transform-set dessha esp-des esp-sha-hmac
 mode tunnel
!
crypto map HOSTviaDIAL 100 ipsec-ike
 match address REMOTE_to_CENTRAL
 set peer 10.254.255.85
 set transform-set dessha
 set security-association lifetime seconds 600
 set pfs group2
!
interface eth 0/1
 ip address
 access-policy LOCALLAN
 no shutdown
!
!
interface t1 1/1
 clock source internal
 tdm-group 1 timeslots 1-24 speed 64
 no shutdown
!
interface bri 1/3
 description ISDN link to local PSTN
 isdn spid1 11111
 isdn spid2 11112
 no shutdown
!
interface fr 1 point-to-point
 description Interface to FR Service Provider - PRIMARY
 frame-relay lmi-type ansi
 no shutdown
 cross-connect 1 t1 1/1 1 frame-relay 1
!
interface fr 1.1 point-to-point
 description VC to CENTRAL
 frame-relay interface-dlci 100
```



```
 ip address  10.254.255.26  255.255.255.252
 access-policy FR

 dial-backup number 2222 digital-64k 1 1 ppp 2
! link interface ppp 2/ISDN for dial backup in case this VC is lost
!
interface ppp 2
 description Dial Backup Interface to ISP with Firewall, VPN to CENTRAL Gateway
 ip address negotiated
 access-policy DIAL
 crypto map HOSTviaDIAL
 ppp authentication chap
 username ISP_Dial_Srv password a
 ppp chap hostname ISP_Customer_Dial
 ppp chap password a
 no shutdown
!
ip access-list extended REMOTE_to_CENTRAL
 remark permits local lan subnet to central subnet
 permit ip 10.1.1.240 0.0.0.15  172.31.4.0 0.0.0.255
!
! each interface has its own policy class to allow for
! discrete destination policy control if needed
!
ip policy-class DIAL                    ! inbound on dial only allows sessions from CENTRAL
 allow reverse list REMOTE_to_CENTRAL
!
ip policy-class FR                      ! inbound on FR allows any session from CENTRAL
 allow reverse list REMOTE_to_CENTRAL
!
ip policy-class LOCALLAN                ! outbound on LAN allows any session to CENTRAL
 allow list REMOTE_to_CENTRAL
!
!
ip route 0.0.0.0 0.0.0.0 fr 1.1         ! static to primary.
ip route 0.0.0.0 0.0.0.0 ppp 2 3        ! floating static to the dial backup link should the
                                        ! fr iface go down.
!
end
```

Solution 2 - Primary = Frame Relay Service Provider, Alternate = ISP via PPPoE/DSL-Cable

In this scenario (see Figure 2), a Frame Relay service provider supplies the Frame Relay access line and virtual circuit that connects a NetVanta remote site directly to the central site. Since this link is entirely over a provider's Frame Relay network, no firewall or VPN is required to protect the customer's network. The central site has a protected Internet connection and an IPSec VPN gateway for Internet-based access to the central site network. The remote site also has a PPPoE over DSL or cable modem to a local ISP. This connection is always on and is used for local Internet access (if the corporate security policy allows such connectivity) while providing an alternate path to the central site. This link is protected by the NetVanta firewall. Should the NetVanta's Frame Relay link fail, an IPSec VPN connection is established over the PPPoE connection across the Internet to the central site's VPN gateway, re-establishing connectivity between the two sites. The NetVanta uses its stateful inspection firewall to protect the PPPoE connection to the Internet.

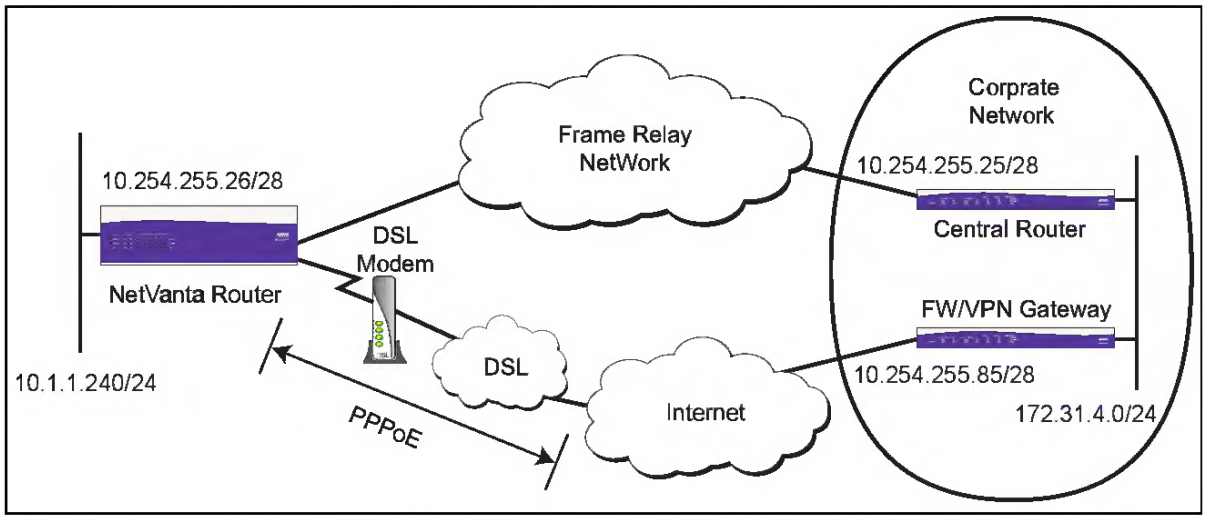

Figure 2. Primary WAN Connectivity via Frame Relay Service Provider, Backup Connectivity via IPsec VPN over PPPoE/DSL-Cable ISP Connection

Remote NetVanta Router Configuration:

```
!
hostname "NV_Remote"
!
ip routing
!
ip firewall
!
ip crypto
!
crypto ike policy 100
  initiate aggressive
  no respond
```

```
 local-id fqdn REMOTE
 peer 10.254.255.85
 attribute 10
  authentication pre-share
  group 2
  lifetime 300
!
crypto ike remote-id fqdn CENTRAL. preshared-key 1234567890
!
crypto ipsec transform-set dessha esp-des esp-sha-hmac
 mode tunnel
!
crypto map HOSTviaPoE 100 ipsec-ike
 match address REMOTE_to_CENTRAL
 set peer 10.254.255.85
 set transform-set dessha
 set security-association lifetime seconds 600
 set pfs group2
!
interface eth 0/1
 description Local Lan Interface
 ip address  10.1.1.254  255.255.255.240
 access-policy LOCALLAN
 no shutdown
!
interface eth 0/2
 description Ethernet to DSL/Cable Modem
 no ip address
 no shutdown
!
interface t1 1/1
 clock source internal
 tdm-group 1 timeslots 1-24 speed 64
 no shutdown
!
interface fr 1 point-to-point
 description Interface to FR Service Provider - PRIMARY
 frame-relay lmi-type ansi
 no shutdown
 cross-connect 1 t1 1/1 1 frame-relay 1
!
interface fr 1.1 point-to-point
 description VC to Central
 frame-relay interface-dlci 100
 ip address  10.254.255.26  255.255.255.252
```



```
 access-policy FR
!
interface ppp 1
 description PPPoE Interface to ISP with Firewall, VPN to CENTRAL Gateway
 ip address negotiated
 access-policy PoE
 crypto map HOSTviaPoE
 ppp authentication chap
 username ISP_PPPoE_Srv password a
 ppp chap hostname ISP_Customer_PPPoE
 ppp chap password a
 mtu 1492
 no shutdown
 cross-connect 2 eth 0/2 ppp 1
!
!
ip access-list extended Internet
 permit ip 10.1.1.240 0.0.0.15 any
!
ip access-list extended REMOTE_to_CENTRAL
 remark permits local lan subnet to central sub
 permit ip 10.1.1.240 0.0.0.15  172.31.4.0 0.0.0.255
!
! each interface has its own policy class to allow for
! discrete destination policy control if needed
!
ip policy-class FR                              ! inbound on FR allows any session from CENTRAL
 allow reverse list REMOTE_to_CENTRAL
!
ip policy-class LOCALLAN                        ! outbound on LAN allows any session to CENTRAL
                                                ! and outbound Internet access (with nat)
 allow list REMOTE_to_CENTRAL
 nat source list Internet interface ppp 1 overload policy PoE! Internet sessions are limited to egress
                                                             ! interfaces with the PoE policy class
!
ip policy-class PoE                             ! inbound on PoE allows any session from CENTRAL
 allow reverse list REMOTE_to_CENTRAL
!
!
Ip route 0.0.0.0 0.0.0.0 ppp 1                   ! Internet traffic
ip route 172.31.4.0 255.255.255.0 fr 1.1        ! traffic to central over primary
ip route 172.31.4.0 255.255.255.0 ppp 1 3       ! traffic to central over backup
!
end
```

Solution 3 - Primary = ISP via PPPoE/DSL-Cable, Alternate = ISP via Dial-up

In this scenario (see Figure 3), the remote site has two ISP accounts, one via PPPoE using a DSL or cable modem and another via dial-up. Both are protected by the NetVanta firewall. This PPPoE connection is always on and is used for local Internet access (if the corporate security policy allows such connectivity) as well as being used as the primary path to the central site. The central site has a protected Internet connection and an IPSec VPN gateway for Internet-based access to the central site network. The remote site uses IPSec VPN to connect to the central VPN gateway over its PPPoE interface as a primary. Should the PPPoE link fail, a dial-up connection is invoked to a local ISP. Another IPSec VPN connection is negotiated across the Internet to the central site VPN gateway, re-establishing connectivity between the two sites.

If the remote router accesses the central VPN gateway on the same IP address no matter which remote router interface is active, it is important that both devices support IKE dead peer detection. Otherwise, when the remote site switches to the other interface, the IPSec and/or IKE SA (depending on the exact configuration) have to age out naturally before a new VPN connection is established. Dead peer detection expedites this process, allowing the alternate VPN connection to be established more quickly.

Note that this configuration is shown using the NetVanta DIM Carrier Module (1200877L1), which allows the dial backup interface module (DIM) to be used without a network interface module (NIM) installed.

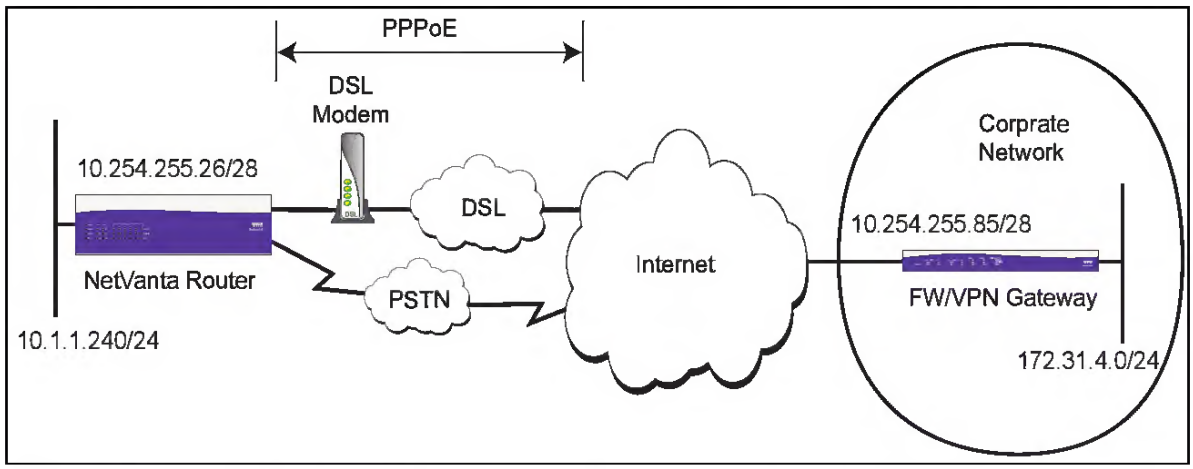

Figure 3. Primary WAN Connectivity via IPsec VPN over PPPoE/DSL-Cable ISP Connection, Backup Connectivity via IPsec VPN Dialup ISP Connection

Remote NetVanta Router Configuration:

```
!
hostname "NV_Remote"
!
ip routing
!
ip firewall
!
!
```

```
ip firewall fast-nat-failover
!
! If using the PPPoE and Dial-up ISP connections for local Internet access
! and using 'NAT source' with the address of the currently active interface, the
! previous command is necessary to allow sessions started on one interface to be
! terminated when the route to the destination switches to the other interface.
!
ip crypto
!
crypto ike policy 100
 initiate aggressive
 no respond
 local-id fqdn REMOTE
 peer 10.254.255.85
 attribute 10
  authentication pre-share
  group 2
  lifetime 300
!
crypto ike remote-id fqdn CENTRAL. preshared-key 1234567890
!
crypto ipsec transform-set dessha esp-des esp-sha-hmac
 mode tunnel
!
! separate crypto maps are used to allow for future customization of
! individual VPN connections if needed
!
crypto map HOSTviaDIAL 100 ipsec-ike
 match address REMOTE_to_CENTRAL
 set peer 10.254.255.85
 set transform-set dessha
 set security-association lifetime seconds 600
 set pfs group2
!
crypto map HOSTviaPoE 100 ipsec-ike
 match address REMOTE_to_CENTRAL
 set peer 10.254.255.85
 set transform-set dessha
 set security-association lifetime seconds 600
 set pfs group2
!!
interface eth 0/1
 description Local Lan Interface
 ip address  10.1.1.254  255.255.255.240
 access-policy LOCALLAN
```



```
 no shutdown
!
interface eth 0/2
 description Ethernet to DSL/Cable Modem
 no ip address
 no shutdown
!
interface bri 1/3
 description ISDN link to local PSTN
 isdn spid1 11111
 isdn spid2 11112
 no shutdown
!
interface ppp 1
 description PPPoE Interface to ISP with Firewall, VPN to CENTRAL Gateway - PRIMARY
 ip address negotiated no-default
 access-policy PoE
 crypto map HOSTviaPoE
 ppp authentication chap
 username ISP_PPPoE_Srv password a
 ppp chap hostname ISP_Customer_PPPoE
 ppp chap password a
 mtu 1492
 dial-backup number 2222 digital-64k 1 1 ppp 2
 no shutdown
 cross-connect 2 eth 0/2 ppp 1
!
interface ppp 2
 description Dial Backup Interface to ISP with Firewall, VPN to CENTRAL Gateway
 ip address negotiated
 access-policy DIAL
 crypto map HOSTviaDIAL
 ppp authentication chap
 username ISP_Dial_Srv password a
 ppp chap hostname ISP_Customer_Dial
 ppp chap password a
 no shutdown
!
!
ip access-list extended Internet
 permit ip 10.1.1.240 0.0.0.15  any
!
ip access-list extended REMOTE_to_CENTRAL
 remark permits local lan subnet to central sub
 permit ip 10.1.1.240 0.0.0.15  172.31.4.0 0.0.0.255
```



```
!
ip policy-class DIAL
 allow reverse list REMOTE_to_CENTRAL
!
ip policy-class LOCALLAN
 allow list REMOTE_to_CENTRAL

!
 nat source list Internet interface ppp 1 overload policy PoE
 nat source list Internet interface ppp 2 overload policy DIAL
!
! Since the Internet traffic is using 'nat source' to the active interface IP address,
! a destination policy class is included in the previous NAT policies to control which
! NAT is used. Specifying a destination policy class restricts that policy for use on
! sessions that egress an interface with the specified policy class. This in conjunction
! with 'ip firewall fast-nat-failover allows NAT to adjust quickly when the egress
! interface changes.
!
ip policy-class PoE
 allow reverse list REMOTE_to_CENTRAL
!
!
ip route 0.0.0.0 0.0.0.0 ppp 1                    ! primary default route
ip route 0.0.0.0 0.0.0.0 ppp 2 3                  ! backup default route
!
end
```