ADTRAN

TECHNICAL SUPPORT NOTE
Configuring VPN Tunnels on the 1st Generation NetVanta 2100 Using IKE Aggressive Mode with Pre-Shared Keys
Featuring the 1st Generation NetVanta 2100

Introduction

This Technical Support Note explains the configuration of VPN tunnels on the NetVanta 2100. There are several options available when setting up VPN tunnels. This Technical Support Note addresses IKE Aggressive Mode exchange using specific ID types, encryption and authentication algorithms, and policy lifetimes.

***Note:** ADTRAN's implementation of IKE Aggressive Mode requires a static WAN IP address on at least one of the NetVantas to terminate the tunnel. If one NetVanta's WAN IP address is dynamically assigned, then it must be the tunnel initiator, and the NetVanta with the static WAN IP will be the responder. Establishing a VPN tunnel requires the LAN IP addresses of the remote and local NetVantas function on unique IP networks.*

Before You Begin

This Technical Support Note assumes that the NetVanta has been installed and is performing NAT operation between the LAN and WAN interfaces.

Configuring the NetVanta 2100

Using a Web browser, log in to the NetVanta (see DLP-001).

Add the following policies:

IKE Policy

1. Select the **POLICIES** menu from the menu bar located at the top of the screen.
2. Select **VPN** from the menu list located on the left side of the screen.
3. Select **IKE** from the menu list located on the left side of the screen. The IKE Policies display box will appear. Click the **Add** button to display the IKE Policy Configuration page.

4. Enter an alphanumeric string used to identify this policy in the **Policy Name** field. Spaces are not valid characters.
5. Using the **Direction** pull-down menu, select **INITIATOR ONLY** for the initiator side and **RESPONDER ONLY** for the responder side.
6. Using the **Exchange Mode** pull-down menu, select **AGGRESSIVEMODE**.
7. Using the **Local IdType** pull-down menu, select **FQDN** to use the Fully Qualified Domain Name of the local NetVanta.
8. Enter the identification data selected for the local NetVanta in the **Local ID Data**field using the following format: **user1.domain.com**
9. Using the **Remote IdType** pull-down menu, select **FQDN** to use the Fully Qualified Domain Name of the remote users.
10. Enter the identification data selected for the remote users in the **Remote ID Data** fields using the following format: **user2.domain.com**
11. In the **Local IP Address** field of the responder NetVanta enter the local NetVanta's assigned WAN IP address. If initiator, enter **0.0.0.0**.
12. In the **Remote IP Address** field of the initiator NetVanta enter the remote NetVanta's assigned WAN IP address. If responder, enter **0.0.0.0**.
13. Using the **Encrypt Algo** pull-down menu, select **3DES** to invoke Triple-Des Encryption.
14. Using the **Auth Algo** pull-down menu, select **MD5** to invoke the Message Digest 5 authentication algorithm.
15. Using the **Auth Mode** pull-down menu, select **Pre-Shared Key**.
16. Enter a 12 to 49 character alphanumeric key in the **If Auth Mode is Pre-Shared Key enter the key** field (spaces must not be used). This key must be the same for both the local and remote NetVanta units.
17. Enter **86400** in the **Life time of key** field (24 hours).

    Note: *The values entered in the Lifetime of Key field are ADTRAN suggested values only. These values may be changed per application. When determining the appropriate value, ADTRAN recommends using a 3:1 ratio between the IKE and IPSec key lifetime values. This ratio provides for a secure network with minimal key negotiation overhead.*

18. Using the **DH Group** pull-down menu, select **Group 1** to invoke Diffie-Hellman Group 1.
19. Click the **Submit** button to register the policy.

IPSec Policy

1. Select the **POLICIES** menu from the menu bar located at the top of the screen.
2. Select **VPN** from the menu list located on the left side of the screen.
3. Select **Tunnels** from the menu list located on the left side of the screen to display the IPSec Policies Page.
4. Click the **Auto** button located on the bottom left corner of the IPSec Policies display box. The Auto Edit page is displayed.

5. Enter an alphanumeric string used to identify this policy in the **Policy Name** field. Spaces are not a valid character.
6. Using the **Status** pull-down menu, select **Enable** to configure this as an active policy.
7. Using the **Source Address** pull-down menu, select **Other**.
8. Enter the local NetVanta's assigned LAN IP Network address in the **Source Address** field. Enter 24 in the **Mask Bits** field or the appropriate mask bits.
9. Enter the remote NetVanta's assigned LAN IP Network address in the **Dest IP Address** field. Enter 24 in the **Mask Bits** field or the appropriate mask bits.
10. Using the **Source Port** pull-down menu, select **Any**.
11. Using the **Destination Port** pull-down menu, select **Any**.
12. Using the **Protocol** pull-down menu, select **All**.
13. Enter the remote NetVanta's assigned WAN IP address in the **Peer Security Gateway** field in the initiator NetVanta. If responder, enter **0.0.0.0**.
14. Using the **Perfect Forward Secrecy** pull-down menu, select **No**.
15. Using the **Security Protocol** pull-down menu, select **ESP with AUTH**.
16. Using the **AUTH Algorithm** pull-down menu, select **MD5**.
17. Using the **ESP Algorithm** pull-down menu, select **3DES**.
18. Enter **28800** in the **Life Time Secs** field (8 hours).

    Note: *The values entered in the Lifetime of Key field are ADTRAN suggested values only. These values may be changed per application. When determining the appropriate value, ADTRAN recommends using a 3:1 ratio between the IKE and IPSec key lifetime values. This ratio provides for a secure network with minimal key negotiation overhead.*

19. Using the remaining two **Security Protocol** pull-down menus, select Last Transform.
20. Click the **Add** button to register this policy.

To LAN Access Policy Configuration (Inbound Traffic)

1. Select the **POLICIES** menu from the menu bar located at the top of the screen.
2. Select **Access Policies: To LAN** from the menu list located on the left side of the screen.
3. Using the pull-down menu next to **Add**, select **Beginning**, and then click the **Submit** button to the right of the **Rule ID** field. The Internet Access Policy Configuration page will be displayed.
4. Using the **Source IP** pull-down menu, select **Other** to configure the NetVanta to forward all packets received from the specified network to the LAN network.

5. Enter the remote NetVanta's assigned LAN IP Network address in the **IP if Source IP is OTHER** field. Enter 24 in the **Mask Bits** field or the appropriate mask bits.
6. Using the **Destination IP** pull-down menu, select **OTHER**.
7. In the **IP if Dest IP is OTHER** field enter the local NetVanta's assigned LAN IP Network address. Enter 24 in the **Mask Bits** field or the appropriate mask bits.
8. Using the **Destination Port** pull-down menu, select ANY to forward all TCP/UDP ports or select the specific port to forward to the server. If the TCP/UDP port you want is not listed, select **Other** and enter the port (or port range) in the **Port Range if Port is OTHER** boxes.
9. Using the **Protocol Type** pull-down menu, select **ALL** to forward all data protocols or select the specific protocol to forward to the server. If the protocol you want is not listed, select **Other** and enter the protocol value (using decimal notation) in the **If Protocol is Other enter Protocol** value box.
10. Using the Action Type pull-down menu, select PERMIT.
11. Set **Enable Log** to **No**.
12. Set **Enable NAT** to **No**.
13. Leave the Dynamic Interface field blank.
14. Select the **Security** checkbox located at the bottom of the page. This configures the NetVanta to perform a data check when the policy is submitted. The security check ensures that all inbound data covered by this access policy has an associated VPN policy as well.
15. Click the **Submit** button to register this policy.

From LAN Access Policy Configuration (Outbound Traffic)

1. Select the **POLICIES** menu from the menu bar located at the top of the screen.
2. Select **Access Policies: From LAN** from the menu list located on the left side of the screen.
3. Using the pull-down menu next to **Add**, select **Beginning**, and then click the **Submit** button to the right of the **Rule ID** field. The Internet Access Policy Configuration page will be displayed.
4. Using the **Source IP** pull-down menu, select **Other** to configure the NetVanta to forward all packets from the specified LAN across the Internet.
5. Enter the local NetVanta's assigned LAN IP Network address in the **IP if Source IP is OTHER** field. Enter 24 in the **Mask Bits** field or the appropriate mask bits.
6. Using the **Destination IP** pull-down menu, select **OTHER**.
7. In the **IP if Dest IP is OTHER** field enter the remote NetVanta's assigned LAN IP Network address. Enter 24 in the **Mask Bits** field or the appropriate mask bits.

8. Using the **Destination Port** pull-down menu, select **ANY** to forward all TCP/UDP ports or select the specific port to forward to the server. If the TCP/UDP port you want is not listed, select **Other** and enter the port (or port range) in the **Port Range if Port is OTHER** boxes.
9. Using the **Protocol Type** pull-down menu, select **ALL** to forward all data protocols or select the specific protocol to forward to the server. If the protocol you want is not listed, select **Other** and enter the protocol value (using decimal notation) in the **If Protocol is Other enter Protocol** value box.
10. Using the **Action Type** pull-down menu, select **PERMIT**.
11. Set **Enable Log** to **No**.
12. Set **Enable NAT** to **No**.
13. Leave the **Dynamic Interface** field blank.
14. Select the **Security** checkbox located at the bottom of the page. This configures the NetVanta to perform a data check when the policy is submitted. The security check ensures that all outbound data covered by this access policy has an associated VPN policy as well.
15. Click the **Submit** button to register this policy.

Saving the Configuration

1. Select the **ADMIN** menu from the menu bar located at the top of the screen.
2. Select **Save Settings** from the menu list located on the left side of the screen.
3. Click the **Yes** button to confirm the save command.

If you experience any problems using your ADTRAN product, please contact ADTRAN Technical Support.

DISCLAIMER

ADTRAN provides the foregoing application description solely for the reader's consideration and study, and without any representation or suggestion that the foregoing application is or may be free from claims of third parties for infringement of intellectual property rights, including but not limited to, direct and contributory infringement as well as for active inducement to infringe. In addition, the reader's attention is drawn to the following disclaimer with regard to the reader's use of the foregoing material in products and/or systems. That is:

ADTRAN SPECIFICALLY DISCLAIMS ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO, MERCHANTABILITY AND

FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL ADTRAN BE LIABLE FOR ANY LOSS OR DAMAGE, AND FOR PERSONAL INJURY, INCLUDING BUT NOT LIMITED TO, COMPENSATORY, SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR OTHER DAMAGES.