ADTRAN

Understanding IPSec Virtual Private Networking (VPN)

Introduction

This document briefly explains Virtual Private Networking (VPN), Internet Key Exchange (IKE) and provides a listing of basic VPN definitions. Links to more detailed information for configuring VPN on AOS products is also included.

What is a Virtual Private Network?

Virtual Private Networking (VPN) tunnels (encrypted data streams) enable you to securely connect computers and networks across a non-secure network (i.e. the Internet). Unlike an unencrypted connection, VPN encryption and authentication minimizes the risk of data being intercepted or altered.

Which IKE Mode should be used?

For VPN tunnels using Internet Key Exchange (IKE) there are two modes available: AGGRESSIVE MODE and MAIN MODE. Selecting the IKE mode depends on your Internet connection and how you want to establish the tunnel:

- **IKE Main Mode** allows for either location to initiate the tunnel. AOS routers use IP addresses to identify a given VPN peer, so in order for one side to both initiate and respond, each router must have a static WAN IP address. For more information on configuring an AOS product for IKE Main Mode, please see kb article # 1925.

- **IKE Aggressive Mode** requires one site to be the initiator and one site to be the responder. Since AOS routers use IP addresses to identify the VPN peer, the AOS router configured as the responder MUST have a static WAN IP address. The initiator may be configured using either static or dynamic addressing. Once the VPN tunnel is established data can flow in both directions. For more information on configuring an AOS product for for IKE Aggressive Mode, please see kb article # 1926.

What you will need

- Two ADTRAN AOS routers running Enhanced Feature Pack (EFP) VPN software, or compatible IPSec-compliant devices
- An Internet connection
- The following information from your Internet Service Provider (ISP) for each location:

    - Public IP address and subnet mask
    - Default gateway address
    - Primary domain name server (DNS) IP address
    - Secondary DNS IP address if available,
- Local Area Network (LAN) addresses and subnet masks for each location. (By default, the LAN of AOS products is 10.10.10.0 with a subnet mask of 255.255.255.0)

Considerations

- Only two devices may connect with each tunnel - two AOS routers or an AOS router and an IPSec-compliant VPN tunneling device.
- The LANs on either side of the tunnel must be on different IP networks to allow the AOS router to route between the networks.
- At least one side of the tunnel must have a static IP address:
    - If each VPN device is configured with a static IP address, either side can initiate the tunnel, and IKE Main Mode may be used.
    - If one side is configured with a dynamically assigned public IP address, then it must be configured as the initiator and IKE Aggressive Mode MUST be used.
- Both VPN devices must be set to use the same encryption, authentication, pre-shared key (if used), and Diffie-Helman Group.

Definition of IKE Terms

Item	**Description**	**Assigned By**
WAN IP Address	The Wide Area Network (WAN) IP address is the public address of the AOS router, which identifies it to the Internet. **Site A: 206.166.249.1** **Site B: 68.130.44.15**	ISP
WAN Subnet Mask	The overlay of bits that determines which part of the IP address identifies the network. For example, a Class C address licenses 256 addresses and has a netmask of 255.255.255.0 **Site A: 255.255.255.248** **Site B: 255.255.255.0**	ISP
Default Gateway	IP address of the ISP router that will act as a gateway to the Internet. **Site A: 206.166.249.2** **Site B: 68.130.44.254**	ISP
LAN Network	A private network address range used by an organization	You

<table>
<tr>
<td>Address with Subnet Mask</td>
<td>for local network traffic. ADTRAN recommends using an address from one of the reserved IP ranges:
<table>
<tr><th>NETWORK</th><th>SUBNET MASK</th></tr>
<tr><td>10.0.0.0</td><td>255.0.0.0</td></tr>
<tr><td>172.16.0.0</td><td>255.240.0.0</td></tr>
<tr><td>192.168.0.0</td><td>255.255.0.0</td></tr>
</table>
IP address of the ISP router that will act as a gateway to the Internet.
<b>Site A: 10.10.10.0 ---- 255.255.255.0</b>
<b>Site B: 192.168.0.0 ---- 255.255.128.0</b></td>
<td></td>
</tr>
<tr>
<td>Exchange Type</td>
<td>IKE exchange type. You can choose either Main Mode, or Aggressive Mode. If using Aggressive Mode, one side will be the initiator, and the other will be the Responder.
<b>Site A: MAIN MODE</b>
<b>Site B: MAIN MODE</b></td>
<td>You/ISP</td>
</tr>
<tr>
<td>Identification Type</td>
<td>Method of identification used during IKE negotiation. The options are IP Address, Fully Qualified Domain Name (FQDN), User FQDN, and DER ANS1 DN (X.500 distinguished name - using certificates) IKE exchange type. You can choose either Main Mode, or Aggressive Mode. If using Aggressive Mode, one side will be the initiator, and the other will be the Responder.
<b>Site A: FQDN - host.adtran.com</b>
<b>Site B: FQDN - remote.adtran.com</b></td>
<td>You</td>
</tr>
<tr>
<td>Encryption Algorithm</td>
<td>Encryption method determines the length in bits of the key used to encrypt and decrypt communication packets. Des is a 56-bit encryption and 3DES is a 168-bit. Either DES or 3DES may be selected as long as both sides use the same method.
<b>Site A: 3DES</b>
<b>Site B: 3DES</b></td>
<td>You</td>
</tr>
<tr>
<td>Authentication Algorithm</td>
<td>Authentication Hash Algorithm used. The choices are MD5 or SHA. Either may be selected as long as both sides use the same method.
<b>Site A: MD5</b>
<b>Site B: MD5</b></td>
<td>You</td>
</tr>
<tr>
<td>Pre-Shared Key</td>
<td>A key stored at both ends of the tunnel to authenticate the transmission as being from the claimed origin. The key can be any alphanumeric string, but must be at least 12</td>
<td>You</td>
</tr>
</table>

	characters, no more than 49 characters, and cannot contain any spaces. The pre-shared key must be the same at both locations. **Site A: Pre-SharedKey** **Site B: Pre-SharedKey**	
Lifetime of Key	Lifetime in seconds of the IKE SA, before it must be renewed. **Site A: 86400** **Site B: 86400**	You
DH Group	Diffie-Helman Group. A protocol that allows 2 parties without any initial shared secret to create one in a manner immune to eavesdropping. Group 1 is 768 bits and Group 2 is 1024 bits. Either may be used as long as both sides use the same group. **Site A: DH Group 1** **Site B: DH Group 1**	You

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.