Application Notes for IPSec Policy supporting Apple iPhone VPN Connectivity

For NETGEAR Security Products
Version 1.0

4/12/2010
1. Introduction
This document is a reference for router administrators to configure a mode-config policy to accept Apple iPhone's native VPN client connections. This is applicable for Apple iPhone 2G, 3G, 3GS.

1.1. Intended Audience and Scope
This document is targeted towards router administrators using the NETGEAR VPN Firewall platforms including both ProSafe and ProSecure lines.

1.2. Acronyms, Abbreviations and Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LAN</td>
<td>Local Area Network</td>
</tr>
<tr>
<td>WAN</td>
<td>Wide Area Network</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network</td>
</tr>
</tbody>
</table>
2. Router Configuration

The IPSec VPN client policy required on the router to accept Apple iPhone VPN connections consists of a mode config record and a corresponding IKE policy. It is not required to know the IP address of the iPhone in advance in order to create a client policy on the router that will allow the VPN client to be authenticated.

2.1. Mode Config Record

Use mode config to create a pool of IP addresses to assign the remote iPhone VPN clients. Note that one or more IKE policies may use the same mode config record; a unique record for iPhone VPN clients is not required.

After defining the IP address range, use the default encryption and integrity for security the traffic tunnel. The required security settings for the mode config record are as follow:

<table>
<thead>
<tr>
<th>Encryption Algorithm</th>
<th>AES-128</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integrity Algorithm</td>
<td>SHA-1</td>
</tr>
<tr>
<td>Local IP Address</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>Local Subnet Mask</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>PFS Key Group</td>
<td>DH Group2</td>
</tr>
<tr>
<td>SA lifetime</td>
<td>3600</td>
</tr>
</tbody>
</table>

One key configuration requirement for the iPhone VPN client is that the Local IP Address and Local Subnet Mask must not specify an address or network. By settings these fields to 0, the associated policy will be anonymous.
2.2. IKE Policy

Once the mode config record for the VPN client is created, create a IKE policy with the following parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exchange Mode</td>
<td>Main</td>
</tr>
<tr>
<td>Remote Identifier Type</td>
<td>FQDN</td>
</tr>
<tr>
<td>Remote Identifier data</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>Encryption Algorithm</td>
<td>AES-128</td>
</tr>
<tr>
<td>Authentication Algorithm</td>
<td>SHA-1</td>
</tr>
<tr>
<td>Authentication Method</td>
<td>Pre-shared key</td>
</tr>
<tr>
<td>Diffie-Hellman (DH) Group</td>
<td>DH Group2</td>
</tr>
<tr>
<td>XAUTH Configuration</td>
<td>Edge Device</td>
</tr>
</tbody>
</table>

Note that “Aggressive” exchange mode is not supported by the iPhone VPN client. As well the Remote Identifier data must be 0.0.0.0 as the iPhone VPN client’s IP address is typically not known by the router admin or consistent.
3. Apple iPhone VPN client Configuration

The Apple iPhone VPN client will require the IKE policy settings to match on the client side.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>Router’s WAN IP address</td>
</tr>
<tr>
<td>Account</td>
<td>Username in the local User Database</td>
</tr>
<tr>
<td>Password</td>
<td>Password to authenticate Username</td>
</tr>
<tr>
<td>Use Certificate</td>
<td>Off</td>
</tr>
<tr>
<td>Group Name</td>
<td>Group for Username if configured</td>
</tr>
<tr>
<td>Secret</td>
<td>Pre-shared key from the IKE SA</td>
</tr>
<tr>
<td>Proxy</td>
<td>Off</td>
</tr>
</tbody>
</table>