NETGEAR, INC.

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

Term	Description
LAN	Local Area Network
WAN	Wide Area Network
VPN	Virtual Private Network

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:

Encryption Algorithm	AES-128
Integrity Algorithm	SHA-1
Local IP Address	0.0.0.0
Local Subnet Mask	0.0.0.0
PFS Key Group	DH Group2
SA lifetime	3600

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.

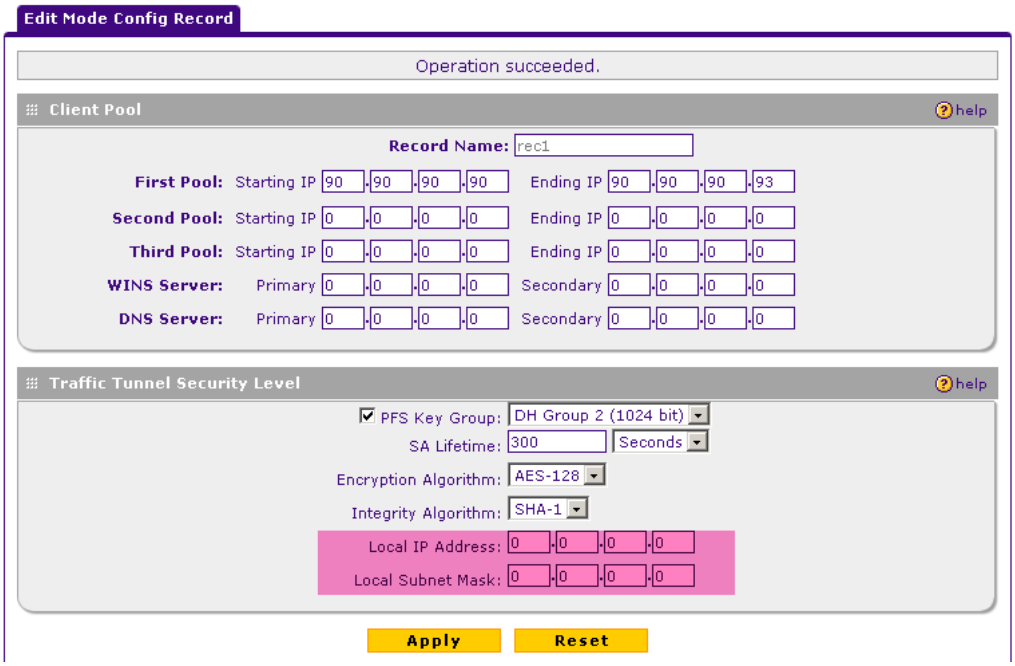

Figure 1: Require Local IP address and subnet to be all 0 in mode config record

2.2. IKE Policy

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

Exchange Mode	Main
Remote Identifier Type	FQDN
Remote Identifier data	0.0.0.0
Encryption Algorithm	AES-128
Authentication Algorithm	SHA-1
Authentication Method	Pre-shared key
Diffie-Hellman (DH) Group	DH Group2
XAUTH Configuration	Edge Device

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.

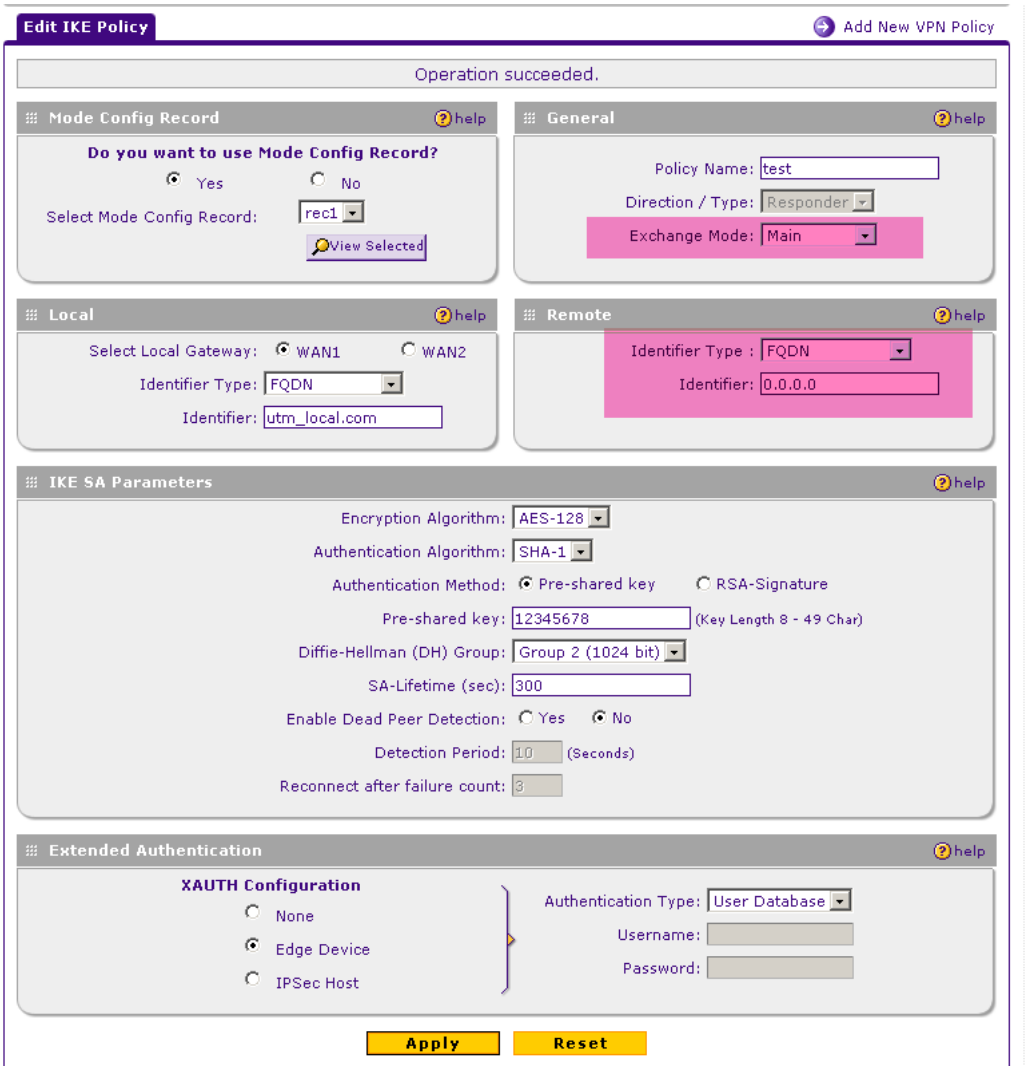

Figure 2: Exchange mode = Main and Remote identifier type settings for IKE Policy

3. Apple iPhone VPN client Configuration

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

Server	Router's WAN IP address
Account	Username in the local User Database
Password	Password to authenticate Username
Use Certificate	Off
Group Name	Group for Username if configured
Secret	Pre-shared key from the IKE SA
Proxy	Off