



Configuring Automatic VPN Initiation



Note

Before you begin, we highly recommend that you read “SAFE: Wireless LAN Security in Depth,” which you can access at <http://www.cisco.com/go/safe>

This document analyzes the best practices of implementing security for wireless LANs using VPNs. For a sample configuration demonstrating complete step-by-step instructions covering the group/user configuration on the VPN Concentrator, auto initiation configuration on the VPN Client, and wireless configuration in the Aironet, refer to the TAC technical note “Configuring Automatic VPN Initiation on a Cisco VPN Client in a Wireless LAN Environment.”

Automatic VPN initiation (auto initiation) provides secure connections within an on-site wireless LAN (WLAN) environment through a VPN Concentrator. When auto initiation is configured on the VPN Client, the VPN Client:

- Becomes active immediately when a user starts his/her PC or when the PC becomes active after being on standby or hibernating
- Detects that the PC has an IP address defined as requiring auto initiation
- Establishes a VPN tunnel to the VPN Concentrator defined for its network, prompts the user to authenticate, and allows that user network access

It is worth mentioning that although auto initiation was designed for wireless environments, you can use it in any networking environment. Auto initiation provides a generic way for the VPN Client to auto initiate a connection whether the VPN Client PC is based on specific networks or not.

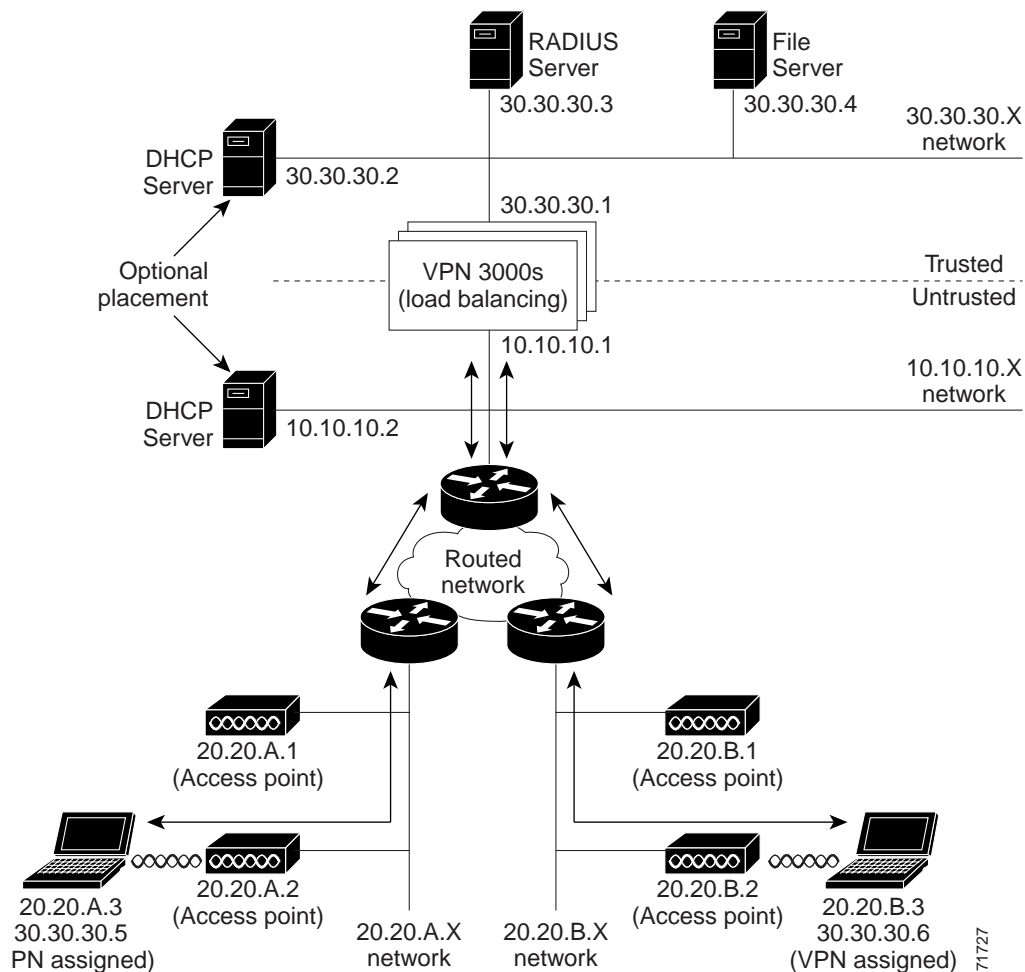
Figure 4-1 depicts a simple network configuration that employs VPN for securing on-site WLANs. The VPN 3000 Concentrators, which may or may not be using load balancing, provide the gateway between the untrusted and the trusted networks. The DHCP Server can be on either side of the VPN 3000 Concentrator. VPN Client users with laptops that have wireless NIC cards can connect through access points (APs) throughout the campus or building and tunnel to the trusted 30.30.30.x network from the untrusted 10.10.10.x network. The network administrator can set this type of scenario up to be largely transparent to the VPN Client user.



Note

You can set up auto initiation configurations that both include and exclude networks for auto initiation.

Figure 4-1 Auto Initiation Scenario



In [Figure 4-1](#) the trusted (wired) network, numbered 30.30.30, is at the top of the diagram with a VPN Concentrator separating it from other networks considered untrusted. The untrusted networks contain wireless subnets, such as 20.20.A.x and 20.20.B.x. Every device on the untrusted network must use a VPN tunnel to access resources on the trusted network. Access to a DHCP server must be available to provide the devices on the untrusted network with initial IP connectivity to the VPN Concentrator. The figure shows the placement of the DHCP server as optional, since it can be placed either on the untrusted network or on the trusted network with DHCP Relay enabled in the VPN Concentrator.

To configure auto initiation for users on the network, you add parameters to the VPN Client's global profile (vpnclient.ini). For information on how to create or use a global profile, see [“Creating a Global Profile.”](#)

Using the VPN Client GUI, users can only enable/disable auto initiation and change the retry interval. These features are available through the Options menu when auto initiation has been configured through the global profile. If auto initiation is not configured, these options do not appear in the Options menu. For a complete explanation of how auto initiation appears to the VPN Client user on a Windows system, see *Cisco VPN Client User Guide for Windows*, “Using Automatic VPN Initiation.”

The auto initiation feature can be used in WLAN environments containing NIC cards and access points from any vendor.

Creating Automatic VPN Initiation in the vpnclient.ini File

This section shows how to create or edit the vpnclient.ini file to activate auto initiation on a VPN Client.

Preparation

Before you begin, you should gather the information you need to configure auto initiation:

- The network IP addresses for the client network
- The subnet mask for the client network
- The names for all connection entries that users are using for their connections

What You Have to Do

To configure auto initiation, you must add the following keywords and values in the [Main] section of the vpnclient.ini global profile file:

- **AutoInitiationEnable**—enables or disables auto initiation. To enable auto initiation, enter 1. To disable it, enter 0.
- **AutoInitiationRetryInterval**—specifies the number of minutes to wait before retrying an auto initiation connection. The range is 1 to 10 minutes or 5 to 600 seconds. If you do not include this parameter in the file, the default retry interval is one minute.
- **AutoInitiationRetryIntervalType**—specifies whether the retry **AutoInitiationRetryInterval** parameter is displayed in minutes or seconds. The default is minutes.
- **AutoInitiationList**—provides a series of section names, each of which contains a network address, a subnet mask, a connection entry name, and optionally, a connect flag. You can include a maximum of 64 section (network) entries.
 - The section name is the name of an entry in the auto initiation list (within brackets)
 - The network and subnet mask identify a subnet
 - The connection entry specifies a connection profile (.pcf file) configured for auto initiation.
 - The connect flag, if present, indicates the action to take if there is a match. If the **Connect** parameter is set to 1, the VPN Client should auto initiate; if 0, the VPN Client should not auto initiate. The default setting is 1. This parameter is optional. You can use it to exclude certain network ranges from auto initiation. For example, you might want to address a situation where Mobile IP and VPN software clients co-exist on client PCs and you want the VPN Client to auto initiate when not on a corporate subnet.

In general, when configuring exceptions with the **Connect** parameter, you might want to place the network ranges you are excluding before those that should auto initiate. More importantly, the software processes the list in the order specified in the vpnclient.ini file. When it matches an entry in the list, the software stops searching and the **Connect** setting of that entry determines whether to auto initiate or do nothing. So if you put the **Connect = 1** entries first, the software never reaches the **Connect=0** entries.

It is also important to order the entries in the list by the uniqueness of the network and subnet mask. You should list the more unique entries first. For example, an entry with a network/mask that specifies a match on 10.10.200.* should come before a network/mask that specifies a match on 10.10.*.*. If not, the software matches 10.10.*.* and never reaches 10.10.200.*

Here is an example of an entry in an auto initiation list that excludes the network from auto initiating:

```
[Franklin]
Network=10.10.200.0
Subnet=255.255.255.0
ConnectionEntry=robron
Connect=0
```

Example 4-1 Section of vpnclient.ini File for Auto Initiation

Suppose a sales manager travels among three locations (Chicago, Denver, and Laramie) within a corporation, attending sales meetings, and wants to securely and easily initiate a wireless connection at these locations. The vpnclient.ini contains the entries shown in this example. The connection entry named in each network section points to the individual's profile (.pcf) for that on-site wireless LAN network.

```
[Main]
AutoInitiationEnable=1
AutoInitiationRetryInterval=3
AutoInitiationList=ChicagoWLAN,DenverWLAN,LaramieWLAN
[ChicagoWLAN]
Network=110.110.110.0
Mask=255.255.255.0
ConnectionEntry=Chicago (points to a connection profile named chicago.pcf)
[DenverWLAN]
Network=220.220.220.0
Mask=255.255.255.0
ConnectionEntry=Denver (points to a connection profile named denver.pcf)
[LaramieWLAN]
Network=221.221.221.0
Mask=255.255.255.0
ConnectionEntry=Laramie (points to a connection profile named laramie.pcf)
```

Example 4-2 Section of vpnclient File for Auto Initiation that excludes and includes auto initiation

In this example, the exceptions (more specific) network addresses appear first in the vpnclient.ini file followed by the connection entries for auto initiation. The connection entries for auto initiation do not need to include the Connect parameter.

```
[Main]
AutoInitiationEnable=1
AutoInitiationRetryInterval=3
AutoInitiationList=NetworkAExceptions,NetworkA,NetworkBexceptions,NetworkB
[NetworkAExceptions]
Network=192.168.0.0
Mask=255.255.255.0
ConnectionEntry=VPNprofileA1
Connect=0
[NetworkA]
Network=192.0.0.0
Mask=255.0.0.0
ConnectionEntry=VPNprofileA2
[NetworkBExceptions]
Network=161.200.100.0
Mask=255.255.255.0
ConnectionEntry=VPNprofileB1
Connect=0
[NetworkB]
Network=161.200.0.0
Mask=255.255.0.0
ConnectionEntry=VPNprofileB2
```

Verifying Automatic VPN Initiation Configuration

To verify that you have configured auto initiation correctly, open the VPN Client GUI application and perform the following steps:

-
- Step 1** Display the Options menu, and select **Automatic VPN Initiation**.
 - Step 2** On the Automatic VPN Initiation dialog, verify that Enable automatic VPN initiation is selected. If not, then click to select it.
 - Step 3** Click **Apply** to close the window.
-

Alternatively you can verify the auto initiation configuration from the command line by executing the following command:

vpnclient verify autoinitconfig

This display shows configuration information for each setting plus a list of your network entries.

```
C:\Program Files\Cisco Systems>cd UPN Client
C:\Program Files\Cisco Systems\UPN Client>vpnclient verify autoinitconfig
Cisco Systems UPN Client Version 4.0 (int_92)
Copyright (C) 1998-2003 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Windows, WinNT
Running on: 5.0.2195

Auto-initiation Configuration Information.
Enable: 1
Retry Interval: 2 minutes
List Entry 0: Network: 10.10.32.32
               Mask: 0.0.0.0
               Connect Flag: 1
               Connection Entry: "Engineering"
```

87684

