



## **How to configure Microsoft's Active Directory to work with Check Point NG FP2**

---

Document Title: How to configure Microsoft's Active Directory to work with Check Point NG FP2

Creation Date: 30-Jun-2002

Modified Date: 30-Jun-2002

Document Revision: 1

Product Class: FireWall-1 / VPN-1

Product and Version: NG FP2

Author: Joe Green

---

# Check Point Next Generation

## TABLE OF CONTENTS

<b>OVERVIEW</b> .....	<b>3</b>
<b>ENVIRONMENT</b> .....	<b>4</b>
<b>PROCEDURAL OUTLINE</b> .....	<b>5</b>
<b>PROCEDURE</b> .....	<b>6</b>
INSTALLING MICROSOFT'S ACTIVE DIRECTORY: .....	6
CHECK POINT VPN-1 CONFIGURATION:.....	9

# Check Point Next Generation

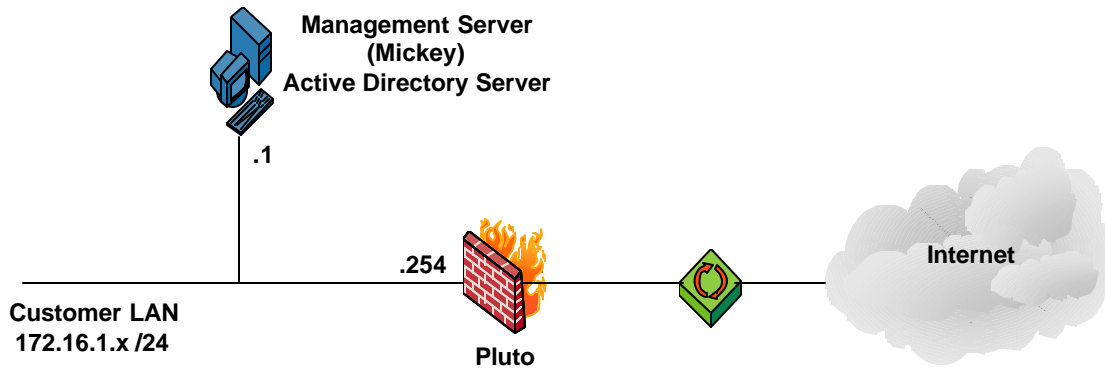
## Overview

This document assumes the following:

1. You have an understanding of installing and configuring Check Point NG in a distributed environment (Management and Module installed separately). *Note: Active Directory Integration CAN work in a Stand Alone deployment.*
2. You have a basic understanding of Active Directory and Windows 2000.

# Check Point Next Generation

## Environment



In the above configuration, the Check Point Management server is also the Active Directory Server. In a real world deployment, these two applications probably would not be running together. However, it provides an easy way to learn this set-up with the minimum amount of computers in a lab.

The DNS domain used in the above configuration is `laxlab.com`  
The Management Servers FQDN is `mickey.laxlab.com`

# Check Point Next Generation

## Procedural Outline

The following steps provide an outline of what this document covers.

1. Installation/Configuration of Active Directory
2. Installation/Configuration of Microsoft's DNS Server
3. Installation/Configuration of Microsoft's Certificate Server
4. Check Point configuration for LDAP
5. Setting up a template and managing users.

Before starting, the following should be verified:

1. Check Point NG FP2 should be installed and you should be able to push policies without any problems. (e.g. SIC is functioning, name resolution is working, etc.)
2. All machines have IP connectivity to each other.
3. The Microsoft High Encryption Pack is installed. This can be obtained at;  
<http://www.microsoft.com/windows2000/downloads/recommended/encryption/default.asp>

## Procedure

### ***Installing Microsoft's Active Directory:***

If you didn't install Microsoft's Windows 2000 Advanced Server, you need to add Active Directory to you Windows 2000 Server installation. Here's how.

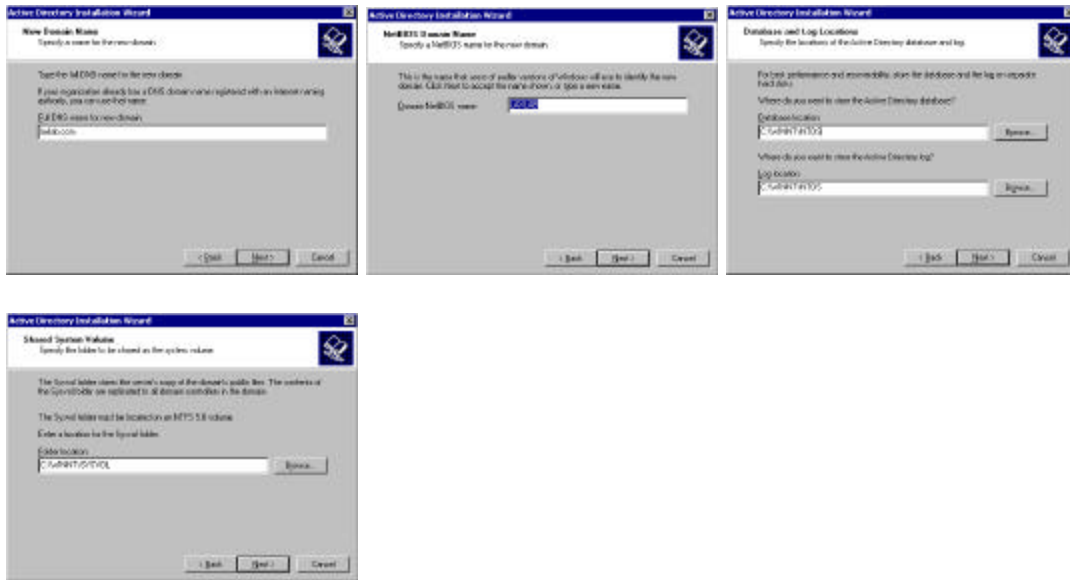
1. From within Windows, go to the Start→Run prompt, enter the command **dcpromo**. The Active Directory Wizard will start and you need to provide the following input at the prompts. (*See pictures below*)
  - a. Domain Controller for a new domain
  - b. Create a new domain tree
  - c. Create a new forest of domain trees
  - d. Type the full DNS name for the new domain **\*\*Note\*\*** This is the DNS Domain that your computer belongs to. E.g. laxlab.com
  - e. Type in the domain netbios name (this is for earlier versions of Windows. E.g. laxlab)
  - f. Specify the Database and Log locations (take the defaults)
  - g. Enter the location for the System Volume Folder (again, take the defaults)
  - h. At this point in the Active Directory installation, it will warn you that it cannot contact a DNS server for your domain (unless you have already configured DNS). Either use the existing DNS installation or have the wizard install it for you (having the Wizard install it is very easy).
  - i. Set the permissions to be compatible with your environment.
  - j. Set the password for the Directory Services restore and click next at the summary screen to complete installation of Active Directory and DNS.

*Note: When Active Directory finishes installing, it will ask you to reboot the computer, **don't reboot yet**. If you just installed DNS for your domain, the computer will take a long time present you with the logon screen after reboot. The computer is trying to contact a DNS to resolve the domain that was just created. To avoid this, make the Primary DNS server of your computer, the local computer itself. Now, reboot.*

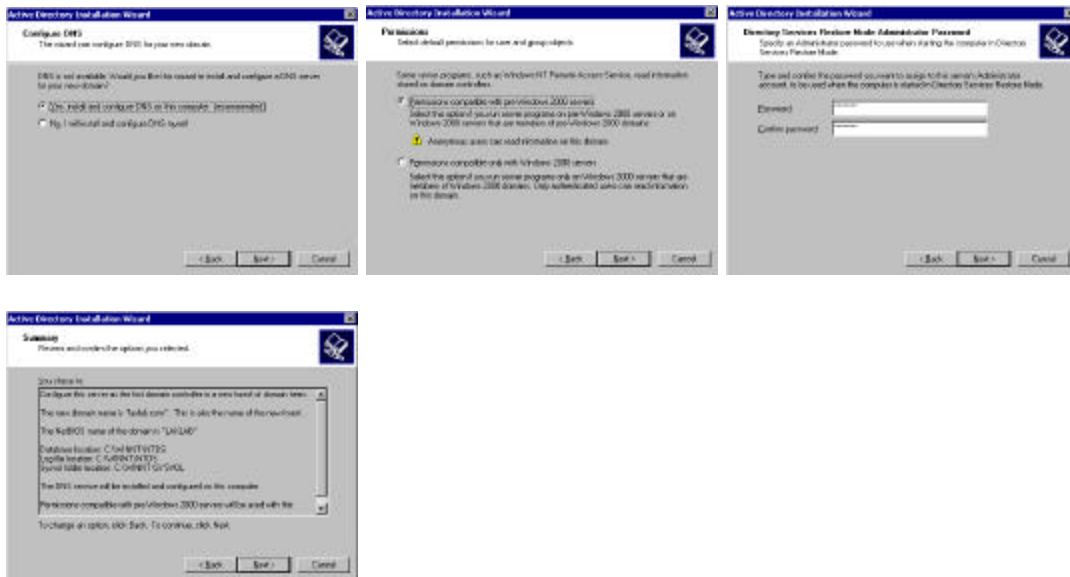
### DCPROMO:



# Check Point Next Generation



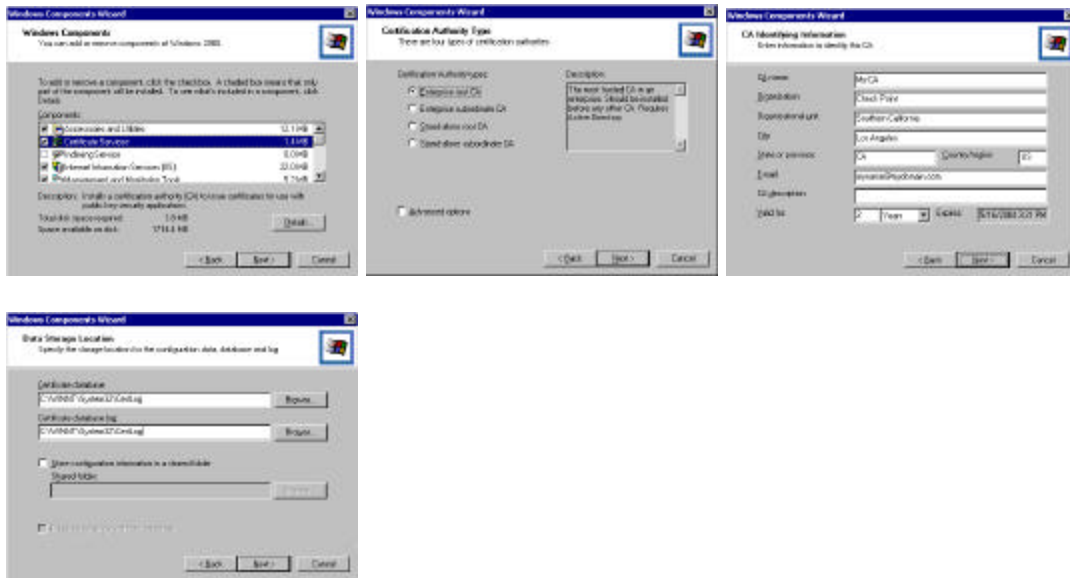
## DNS Install:



2. Upon reboot, you need to install Microsoft's Certificate Server. This is required for SSL communication between the Active Directory Server and the Check Point Management console.
  - a. This is installed through the Windows Control Panel → Add/Remove Components → **Add/Remove Windows Components**.
  - b. Select the Certificate Services option and click next. Then choose the following options.
    - i. Select **Enterprise Root CA**
    - ii. Fill in the CA Identifying Information fields. Note: This is the information that will be part of your certificate.
    - iii. Take the Data Storage Location defaults.
    - iv. Certificate Server is now installed (no reboot necessary).

# Check Point Next Generation

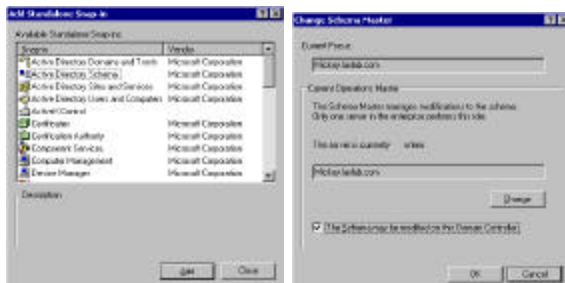
## Certificate Server:



3. Next, you need to allow the schema to be viewed and modified by the Microsoft Management console (MMC). This is easily done through the GUI in Windows 2000.

- Register the schema DLL. Go to Start→Run, and type **regsvr32 schmmgmt.dll** (you should see a message stating that the operation was successful).
- Go to Start→Run→and type **mmc**.
- From within the MMC, click on the **Console** menu, then click **Add/Remove Snap-In...**
- Click **add** and select **Active Directory Schema**, click **add**, click **close** and click **ok** to return to the MMC.
- Expand the Active Directory Schema (click on the + symbol).
- Right click on the A.D. Schema in the MMC and select **Operations Masters**.
- Place a check in the box titled “**The schema may be modified on this domain controller.**”
- Exit the MMC and reboot.

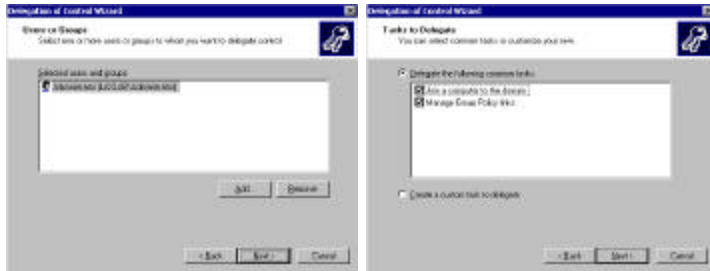
## MMC:



## Check Point Next Generation

4. Next, you need to delegate control of the directory so that the administrator can make changes.
  - a. Go to Start→Programs→Administrative Tools→**Active Directory Users and Computers**.
  - b. Right click on you city's domain and choose **delegate control**.
  - c. Add the administrator account (or administrators group) and check both of the boxes in the next screen. Click **ok** and then exit.

### Delegation:



5. To enable SSL communication between FireWall-1 and Active Directory, the following needs to be done:
  - a. Got to Start→Programs→Administrative Tools→**Domain Security Policy**.
  - b. Go to Security Settings→Public Key Policies→**Automatic Certificate Request Settings**, right click and select **New Automatic Certificate Request**.
  - c. Select **Domain Controller** from the window, then select your **CA**.

### SSL:



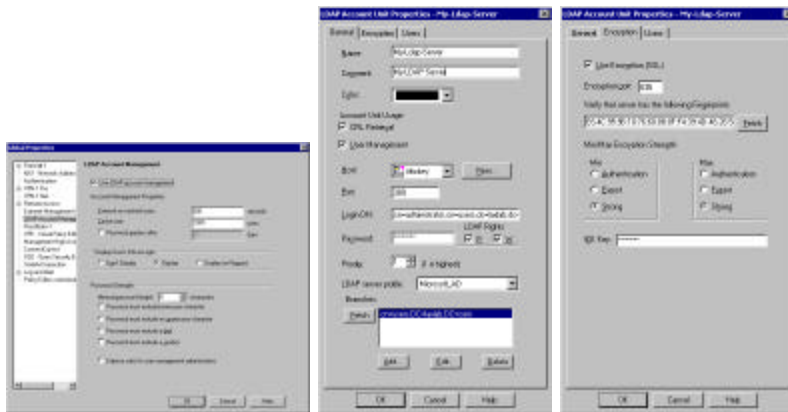
### Check Point VPN-1 Configuration:

1. Log into the Check Point Policy Editor.
2. Go to the **Policy Menu→Global Properties**.
  - a. From the **LDAP Account Management** branch, select **Use LDAP Account Management** and click **ok**.
  - b. Next, go to the **Manage Menu→Servers**. Create a **LDAP Account Unit** Object. Use the following parameters:
    - (General Tab)
    - i. Name=a descriptive name.
    - ii. Check the boxes “User Management” and “CRL Retrieval”

# Check Point Next Generation

- iii. Host=Your Management server.
- iv. Login DN: cn=admin,dc=laxlab,dc=com (Note:substitute your DNS domain for laxlab)
- v. Enter the administrator's password.
- vi. Set the LDAP type to Microsoft\_AD and fetch the branch. (Encryption Tab).
- vii. Use SSL.
- viii. Click Fetch for Fingerprint.
- ix. Set Encryption to strong and strong for Min and Max.
- x. Type in the IKE password (the same as the administrators password) Click ok.

## Check Point:



3. Close the Policy Editor and extend the Active Directory schema.
  - a. Using Wordpad, open the file \$FWDIR\lib\ldap\schema\_microsoft\_ad.ldif and replace all instances of DOMAINNAME with you domain name. e.g. **dc=laxlab,dc=com**.
  - b. Next (from the DOS prompt), using the ldapmodify command (all on one line), run the command:  
**E.g. ldapmodify -c -h mickey.laxlab.com -D "cn=admin,dc=laxlab,dc=com" -w password -f c:\winnt\fw1\ng\lib\ldap\schema\_microsoft\_ad.ldif**

*Note: In the above syntax, substitute your hostname and DNS Domain Name for mickey.laxlab.com.*

*The output of the ldapmodify command should look like;  
[Begin example]*

*adding new entry CN=fw1auth-method,CN=Schema,CN=Configuration,dc=laxlab,dc=com*

*adding new entry CN=fw1auth-server,CN=Schema,CN=Configuration,dc=laxlab,dc=com*

*adding new entry CN=fw1pwdlastmod,CN=Schema,CN=Configuration,dc=laxlab,dc=com*

*adding new entry CN=fw1key-number,CN=Schema,CN=Configuration,dc=laxlab,dc=com*

*adding new entry CN=fw1key-seed,CN=Schema,CN=Configuration,dc=laxlab,dc=com*



# Check Point Next Generation