

CheckPoint Software Technologies LTD.ä

How to integrate Account Management and Netscape Directory Server v3.1 with VPN-1/Firewall-1 v4.1

Event: Partner Exchange Conference

Date: October 19, 1999

Revision 1.0

Author: Richard Devera, *Southern Region Technical Consultant*

Credits: Steven Yurkunas, How to configure Account Management v1.0 and a Netscape LDAP Server v3.0 – A Quick Reference Guide

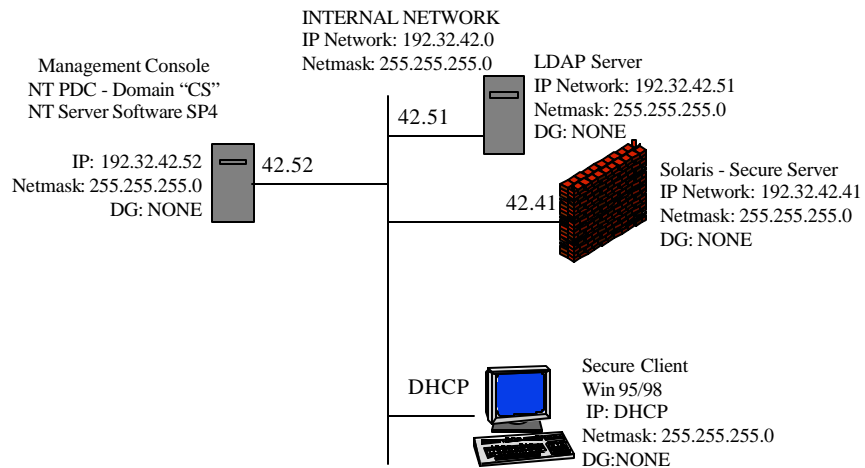
Table of Contents

<i>LDAP Model</i>	4
<i>Goal of the Demo:</i>	7
<i>Equipment Needed:</i>	7
<i>Configuration overview:</i>	8
<i>Configuration Details</i>	9
Installing Netscape Directory Server	9
Install Account Management Client	12
Creating Templates and Users	14
Configuring an Account Unit	18
Creating a Security Policy	20

How to integrate Account Management and Netscape Directory Server v3.1 with VPN-1/FW-1

This document explains the how to setup and configure SecureClient and SecureServer with Check Point VPN-1 Version 4.1. Basic knowledge of the Check Point architecture is a prerequisite. For more information on how to install all the products in this guide, please refer to the installation documentation.

Demo AMC and Netscape Directory Server



NOTE: All subnet masks are 255.255.255.0
All IP Addresses are for Subnet and Host IP Address
ie. 42.41 = 192.32.42.41
DG = Default Gateway

LDAP Model

(extracted from the VPN-1/Firewall-1 Administration Guide v4.1)

LDAP (Lightweight Directory Access Protocol) is a lightweight version of the X.500 directory access protocol. LDAP is based on a Client/Server model in which an LDAP Client makes a TCP connection to an LDAP server, over which it sends requests and receives responses.

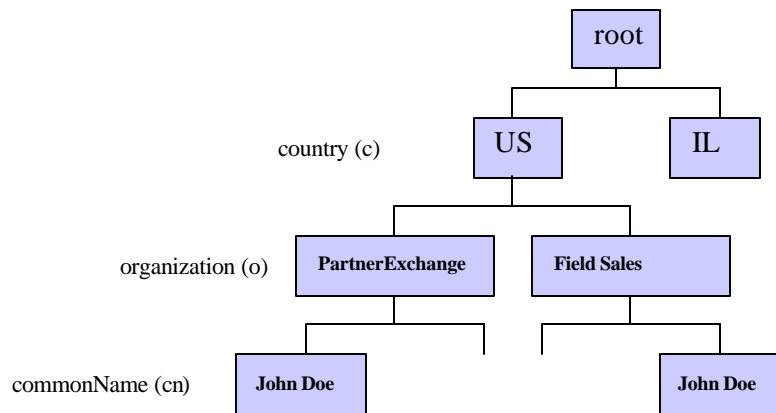
The LDAP information model is based on the entry, which contains information about some object (for example, a person). Entries are composed of attributes, which have a type and one or more values. The schema lists the attributes, their data types (for example, ASCII text, a JPEG photograph, etc.) and how those values behave during directory operations (for example, whether case is significant in comparisons).

Entries are organized in a tree structure, usually based on political, geographical, and organizational boundaries. Each entry is uniquely named relative to its sibling entries by its RDN (relative distinguished name) consisting of one or more distinguished attribute values from the entry. For example, the entry for the person John might be named with the “John Doe” value from the commonName attribute.

A globally unique name for an entry, called a DN (distinguished name), is constructed by concatenating the sequence of RDNs from the root of the tree down to the entry.

A DN is expressed in the “bottom up” sequence, that is, starting at the lowest level and moving up to the root of the tree (See Figure below for an example)

LDAP provides operations to authenticate, search for and retrieve information, modify information, and add and delete entries from the tree.



Example DN's: cn=John Doe, o=PartnerExchange, c=US is one DN which is different from Cn=John Doe, o=Field Sales, c=US.

LDAP provides operations to authenticate, search for and retrieve information, modify information, and add and delete entries from the tree.

LDAP Servers

The LDAP information model is most appropriate for directory services, that is, information which is read much more frequently than it is modified. An LDAP Server makes the data in an LDAP-compliant directory available to LDAP Clients.

An LDAP directory can be indexed, which improves performance at the cost of the directory taking up more disk space.

LDAP Schema

An LDAP schema is a description of the structure of the data in an LDAP directory.

Goal of the Demo:

- To show steps on how to deploy a VPN between a client and server.

Equipment Needed:

- Firewall-1 version 4.1 or greater (Unix or NT)
- NT 4.0 Server SP 4
- Windows 98
- Solaris 2.6
- NT or Solaris based platform 128 MB RAM, 2GB Diskspace

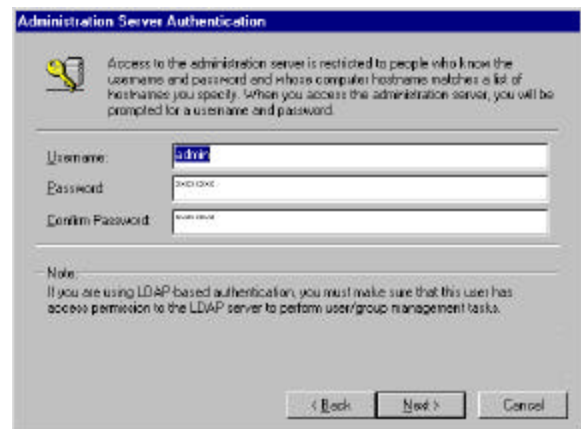
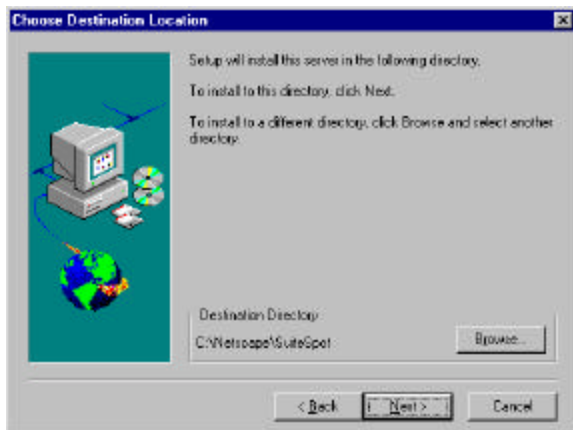
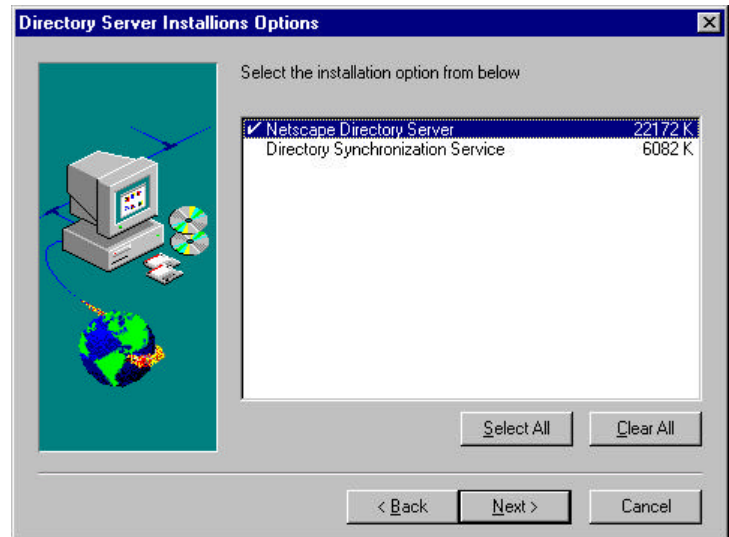
Configuration overview:

1. Interconnect systems and hubs as per topology diagram.
2. Install Windows 98 on one client, Windows NT Server for the Management console, Windows NT server platform for the LDAP server, and Solaris 2.6 for the SecureServer
3. Configure Network interfaces and routing. Verify connectivity by broadcasting a ping each host.
4. Install SecureServer on a Solaris machine
5. Install the management console on an Windows NT server machine
6. Install SecureClient on the Windows 98 machine
7. Install and Configure Netscape Directory Server on the LDAP server
8. Install Account Management Client
9. Create a SecureClient VPN rule to the SecureServer
10. Define and install a policy for the services to be tested.

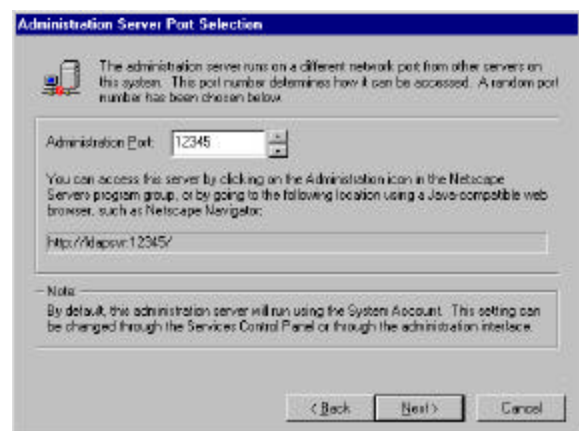
Configuration Details

Installing Netscape Directory Server

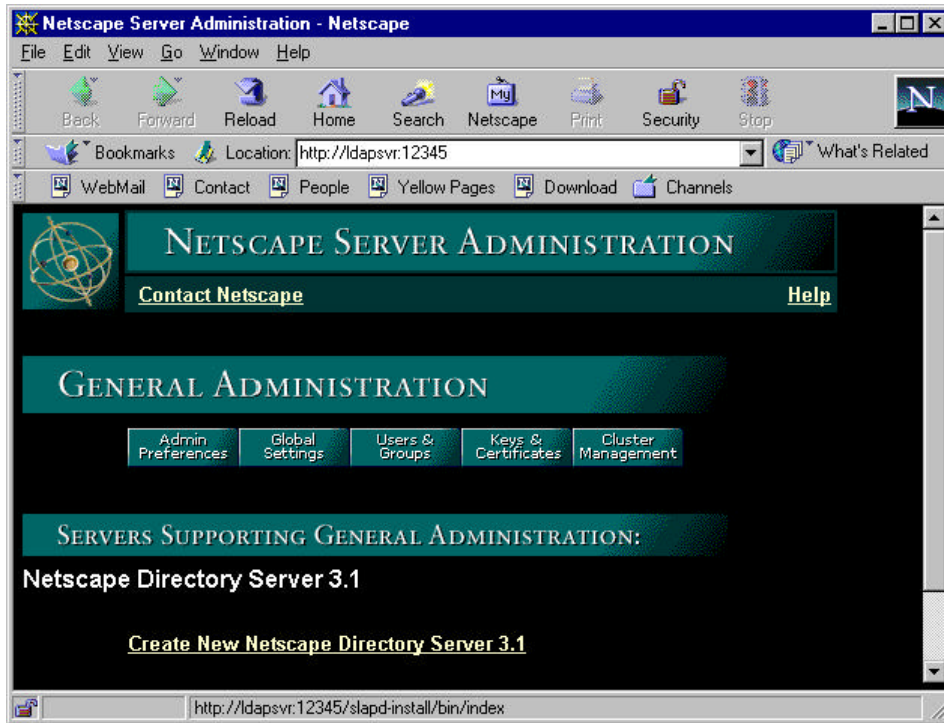
1. Install the Netscape Directory Server
2. When prompt for options, choose Netscape Directory Server
3. After accepting the license agreement, choose the default destination directory.
4. Enter the username and password for administrative access (for this demo use username: admin, password: abcd1234)
5. Enter in a unique random port number. This port is used to access the administration services of the directory server. (use 12345)



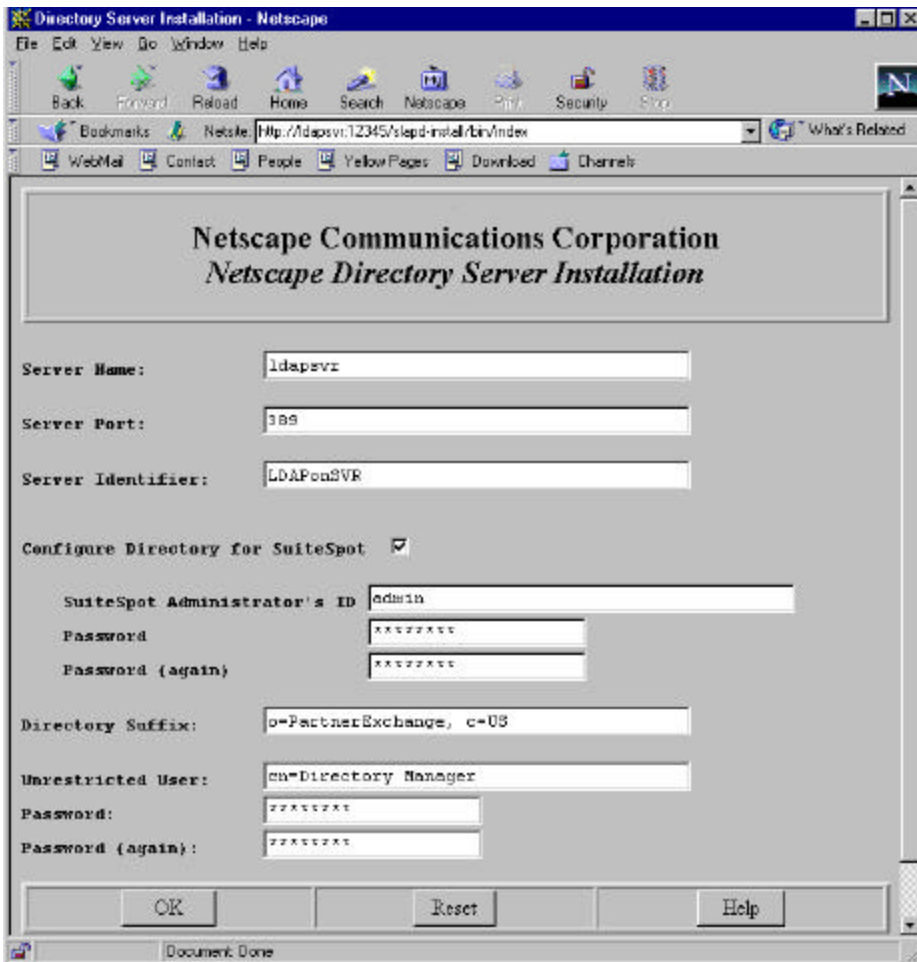
6. Netscape setup will install the directory server.
7. When completed, you will be prompted to administer the directory server. Enter the username and password you entered in the previous step.



8. Select **Create a New Netscape Directory Server 3.1**



9. When creating a directory server, you will need to input and save this information.



Enter the following:

1. Server Name: **ldapsvr**
2. Server Identifier: **LDAPonSVR**
3. SuiteSpot Administrator's ID: **admin**
4. Password: **abcd1234**
5. Directory Suffix: **o=PartnerExchange, c=US**
6. Unrestricted User: **cn=Directory Manager**
7. Password: **abcd1234**

Note: In a typical deployment the passwords between the SuiteSpot Administrator and the Unrestricted User are different

10. When creating directory has completed, to configure more about your server

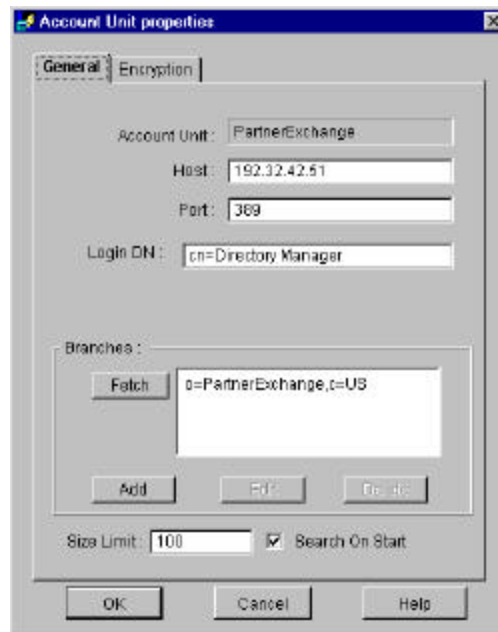
11. Directory Server Installation completed.

Install Account Management Client

1. On the LDAP Server (**ldapsvr**), and on the **Management Console (192.32.42.52)**, run **setup** to install the Account Management Client (AMC).

Note: The AMC is a standalone application that can be run on any Windows NT/98 client workstation. The AMC can also be run through the VPN-1/Firewall-1 Policy Editor.

2. After successful installation, logon to the **Management Console** and start the **Policy Editor (VPN-1/FW-1 GUI)**.
3. Select **New->Account Unit** and name it PartnerExchange. (Note: If you have more than one LDAP server, you can manage all FW-1 users through the AMC. This is recommended for several reasons, redundancy, performance, H/A).



- a) Enter **192.32.42.51** as the host (directory server)
- b) Login DN is **cn=Directory Manager**
- c) Click on **Fetch**, when fetching you will be required to enter a password for the common name cn=Directory Manager.
- d) Click **OK** to finish

Note: There are two (2) methods in importing the schema. One method is to use the *ldapmodify* command the other with the *GUI interface*. See Appendix B for more information.

4. Copy the Check Point schema from

```
$FWDIR/lib/ldap/schema.ldif
```

```
to c:\Netscape\SuiteSpot\slapd-LDAPonSVR\ldif
```

Note: This schema file is also located on the VPN-1 Certificate Manager

5. Next import the schema to the directory

Under the directory `C:\Netscape\SuiteSpot\slapd-LDAPonSVR\ldif>` run the command

Note: The **Encryption** tab is useful for securing the session between the Account Management Client (AMC) and the directory server. The session is based on SSL.

Refer to the Account Management documentation

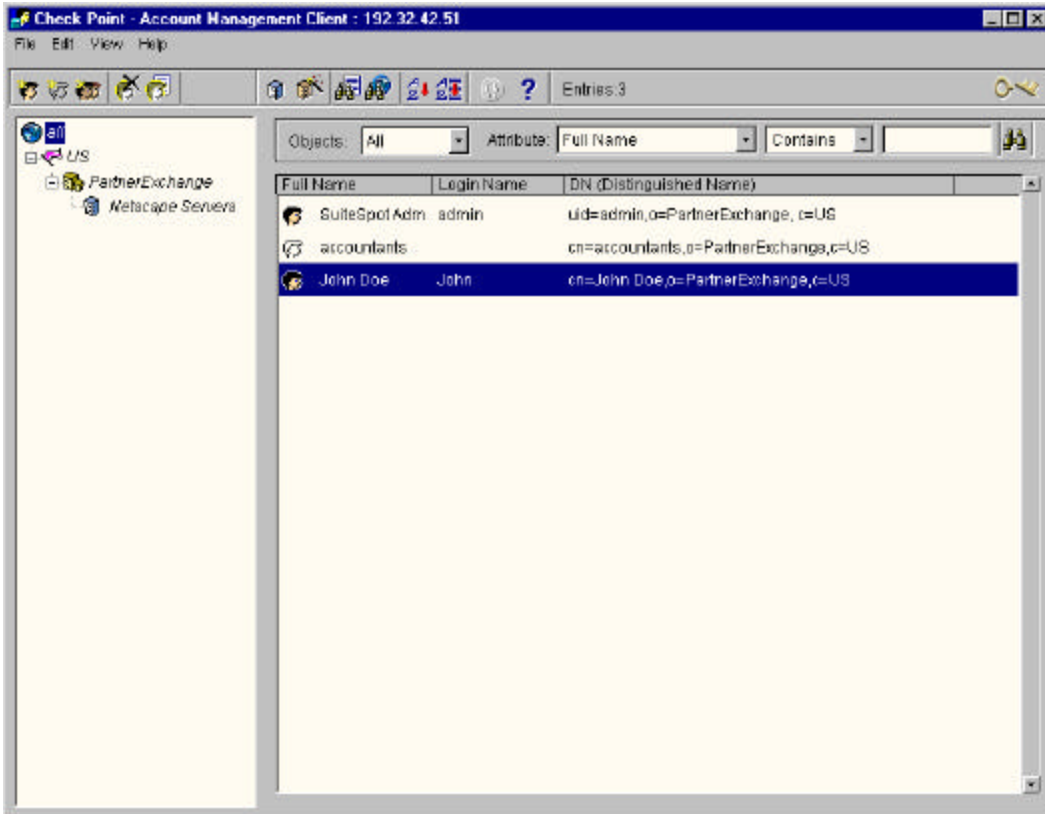
```
C:\Netscape\SuiteSpot\bin\slapd\server\ldapmodify -h ldapsvr -D  
"cn=Directory Manager" -w abcd1234 -v -f CP_schema.ldif
```

This command will add the check point schema to the directory. The schema is used to add Check Point specific attributes to the directory. This will be used to store values to an associated entry.

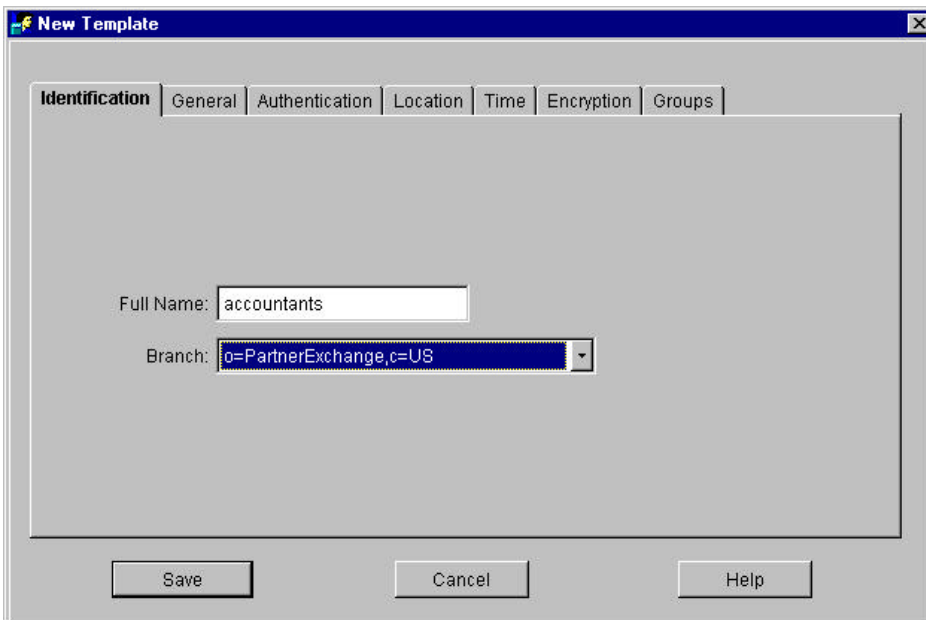
See [VPN-1/Firewall-1 Administration Guide](#) for a list of the LDAP schema.

Creating Templates and Users

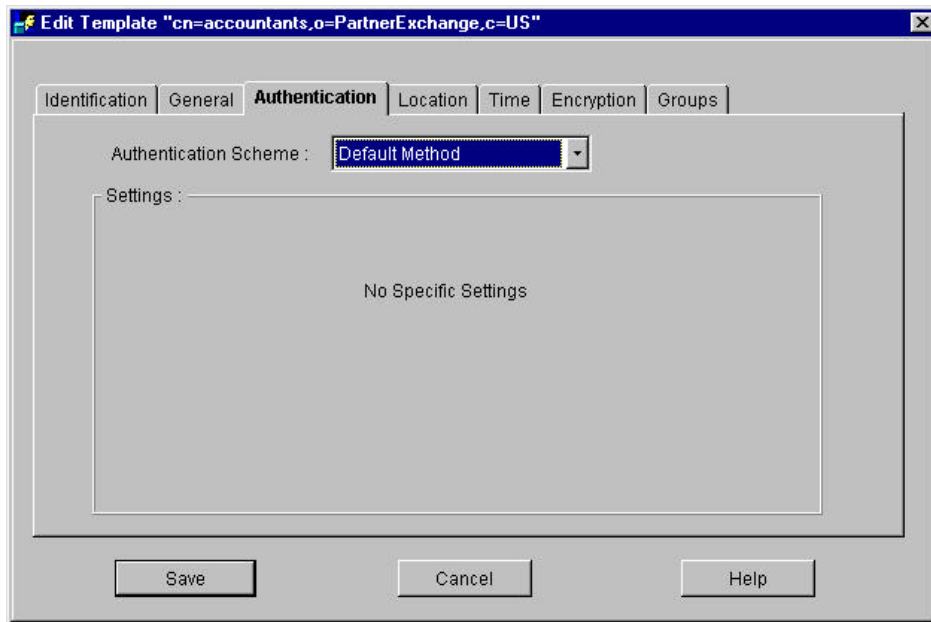
1. Startup the account management client from **Programs ->Account Management->Account Management Client**



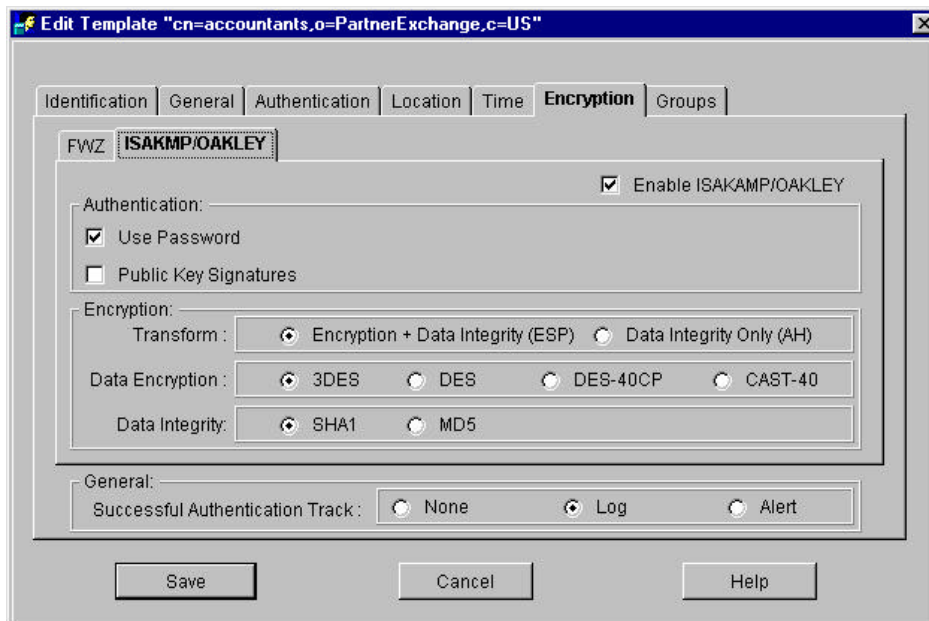
2. Go to File->New Template. A template an LDAP entry with objectclass fw1template. All templates are live links. If you modify templates, all users linked to the template will be affected.



3. Go to the authentication tab and select Default Method. Other authentication schemes are available, however for this demo we will select Default Method.



4. Select the Encryption tab and modify the settings.
 - a) Uncheck **Enable FWZ**
 - b) Enable **ISAKMP/OAKLEY**
 - c) Set Authentication to **Use Password**
 - d) Transform: **ESP**
 - e) Data Encryption: **3DES**
 - f) Data Integrity: **SHA1**
 - g) Enable **Successful Authentication Track** to **log**



5. Save Template
6. Go to **File->New User**, link this entry to the template **accountants**

New User

Identification | General | Authentication | Location | Time | Encryption | Groups

Login Name:

Last Name:

Full Name:

Branch:

Link To Template:

Save Cancel Help

7. Because most of the attributes for this entry has already been defined, click on the **Encryption** tab, **ISAKMP/OAKLEY** tab.

Edit User "cn=John Doe,o=PartnerExchange,c=US"

Identification | General | Authentication | Location | Time | **Encryption** | Groups

FWZ **ISAKMP/OAKLEY** From Template Enable ISAKMP/OAKLEY

Authentication:
 Use Password
 Public Key Signatures

Encryption:
Transform: Encryption + Data Integrity (ESP) Data Integrity Only (AH)
Data Encryption: 3DES DES DES-40CP CAST-40
Data Integrity: SHA1 MD5

General:
Successful Authentication Track: None Log Alert

Save Cancel Help

8. Click on Enter **New Password** and a **Key for Encrypting Password**
9. After updating the policy, close the application.

The screenshot shows a dialog box titled "ISAKMP" with a blue title bar. It contains two main sections: "Password:" and "Key:". The "Password:" section has a "New Password:" field and a "Re-enter Password:" field, both containing asterisks. The "Key:" section has a "Key for Encrypting Password:" field and a "Re-enter Key for Encrypting Password:" field, both containing asterisks. A red oval highlights these two key input fields, with an arrow pointing from the text box on the right to the oval. Below the input fields are "OK" and "Cancel" buttons. The "Key Last Used For Branch:" label is visible at the bottom of the key section.

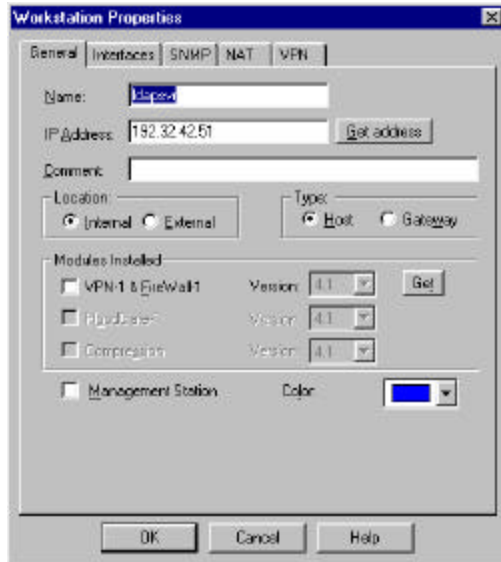
Note: Key for Encrypting Password

Enter the key to be used to encrypt users' ISAKMP pre-shared secrets on the LDAP server. This field corresponds to the **ISAKMP Key field in the Encryption tab** of the LDAP Account Unit Properties window in the FireWall-1 Windows GUI. (We will be configuring the Account Unit in the Section *Configuring an Account Unit*)

It is the same for all users on an Account Unit (even though it is defined in a User Properties window). You define this only once. Once it is defined, it appears as the default value for all other users when you open their ISAKMP Password windows

Configuring an Account Unit

1. Create a network object for the LDAP server, use IP: **192.32.42.51** and name the object **ldapsvr**
2. Modify the **Policy->Properties** and check Use **LDAP Account Management**.
3. Create a server, **Manage->Servers...** and click on **New->LDAP Account Units**
4. See **Server Object Properties** to configure.



Server Object Properties

Name — Enter the Account Unit's name, **LDAPonSVR**

Comment — descriptive text

Host — Select **ldapsvr**. This list box was created when defining network object for the LDAP server

Port — default should be 389 for non-encrypted sessions

CRL Retrieval — In this demo we will **not enable** CRL Retrieval, however, this is used for CRL retrieval, that is, it is the CRL depository for OPSEC PKI-enabled Certificate Authorities

User Management — Check this box.

User Management is enabled only if Use LDAP Account Management is checked in the LDAP tab of the Properties Setup window

Login DN — the DN (**cn=Directory Manager**) that will be used to bind (login) to the Account Unit

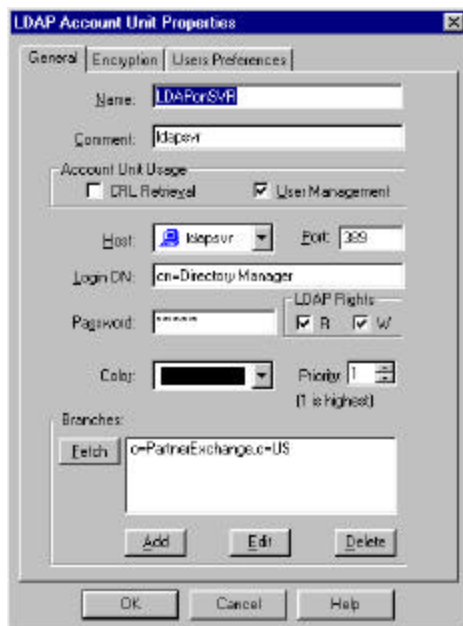
Password — **abcd1234**

(Note: The Login DN and Password was obtained when installing the Netscape Directory Server)

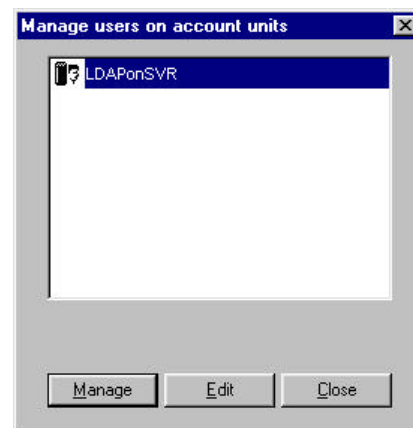
LDAP Rights — Check R and W to allow the Firewall's access privileges on the LDAP Server (Note: If the LDAP Server is a slave, uncheck W.)

Priority — leave as the default, further explanation can be found out of the VPN-1/Firewall-1 Administration Guide.

Branches — click on Fetch to get the branches available on the LDAP.



5. If needed, you can Manage Users from the Edit Users on Account Unit dialog box, by highlighting the Account Unit and clicking on Manage.
6. Next, go to **Manage->Users** and select **New->External Group**.



7. Configure the External Group with the following values:

Name – accounting

The name of the external group

Acct Unit – LDAPonSVR

The name of the account unit you defined in the previous step.

In this demo we will **select All Account-Units users**.

In practice, you can select an external users group to be a branch of a tree **SubTree** or a **Group** in a branch.

If **SubTree** is selected, enter the RDN of that branch

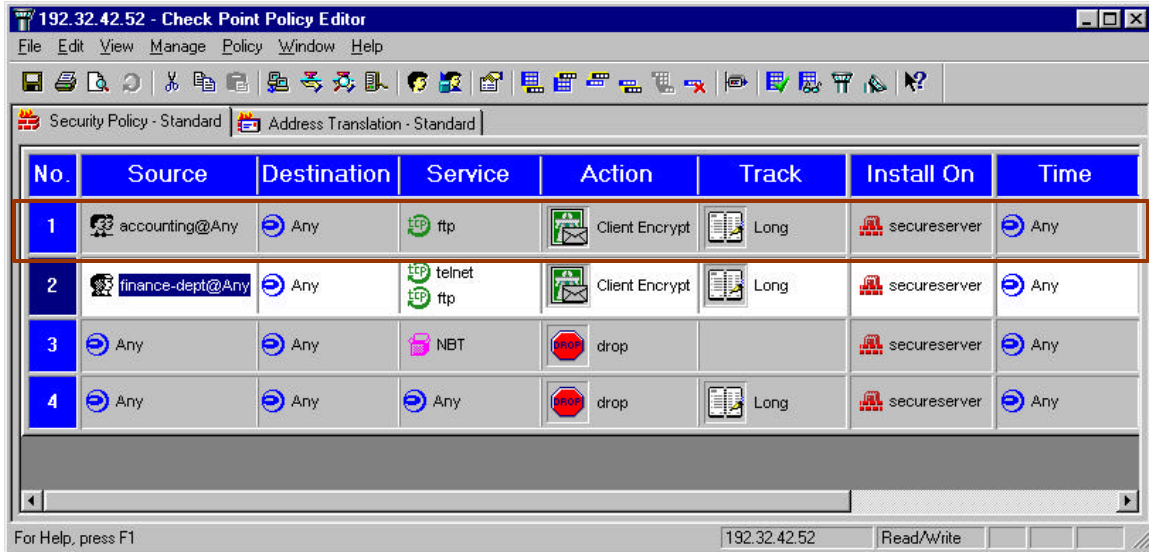
The screenshot shows the 'External User Group (LDAP)' dialog box with the following configuration:

- Name:** accounting
- Color:** Black
- Comment:** (empty)
- Acct Unit:** LDAPonSVR
- Group's Scope:**
 - All Account-Unit's Users
 - Only SubTree ([optional prefix] , branch): (disabled)
 - Only Group in branch (DN prefix): (disabled)

Buttons: OK, Cancel, Help

Creating a Security Policy

1. Create a rule that allows the External Group accounting VPN access to the *secureserver* (SecureServer) using SecureClient



2. Download the policy to secureserver.
3. To test this LDAP functionality out, logon to the Windows 98 client and attempt to access *secureserver* using the ftp client. You will be required to enter the name of the user you created in the section heading **Creating Templates and Users**
4. Setup complete.

Appendix A – Troubleshooting Tips and New Features

1. If the SecureClient or SecuRemote returns an error message “No preshared secret defined for user” and the users properties have been defined correctly. See page 15 and ensure the IKE key has been defined.
2. If you cannot import the Schema file, be sure to turn off Schema checking before doing so. See page **Error! Bookmark not defined.**
3. If you are having problems importing the Check Point schema files (CP_schema.ldif) you may need to disable schema checking. (Refer to the Netscape documentation)

Appendix B – Adding Entries using the Netscape GUI

1. Copy the schema file from the firewall \$FWDIR/lib/ldap/schema.ldif to the ldap server C:\Netscape\SuiteSpot\slapd-LDAPonSVR\ldif
2. Select the directory server LDAPonSVR and click on Database Management
3. Select Add Entries on the left hand side.
4. Enter in the directory path of the ldif file.
5. Click OK,
6. Click the Apply and restart the server.

