

---

# SecuRemote Version 3.0 Quick Reference Guide

**Authored By:** Joe DiPietro  
**Date:** October 24, 1997/Updated 12/16/1999  
**Purpose:** To describe and Document Client Virtual Private Network (VPN) within Checkpoint Version 3.0 Firewall-1 and SecuRemote version 3.0

---

The Goal of using SecuRemote is to encrypt data from the PC to the Firewall. This can be useful to provide privacy of data over a public network. This technology is also called a Virtual Private Network (VPN). This paper will describe how a SecuRemote user will retrieve their Email over the Internet.

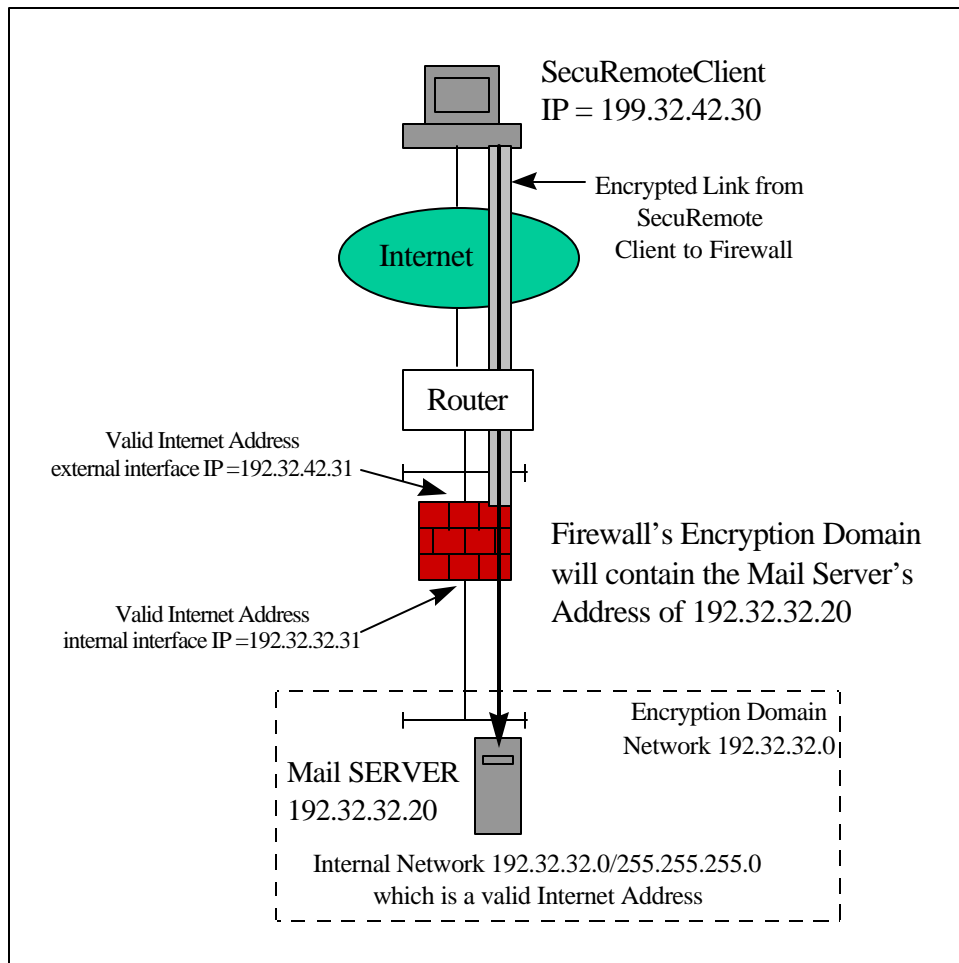


Figure 1. SecuRemote with Valid Internet Addresses

There are three methods to accomplish this task. The first method is to use a Valid Internet IP Address scheme as shown above. This means the SecuRemote Client as well as the Mail Server have valid IP Addresses on the Internet.

The Second Method is to use Address Translation on the Firewall, in addition to SecuRemote to gain access to the Internal Host as shown in Figure 2. In this method, all internal hosts that need to be accessed from the Internet must have a corresponding Valid Internet IP Address to make a connection. So if your employees needed to connect to 50 Internal Hosts (Mail, FTP, Telnet, Web, etc.) , you would need 50 Valid Internet IP Addresses.

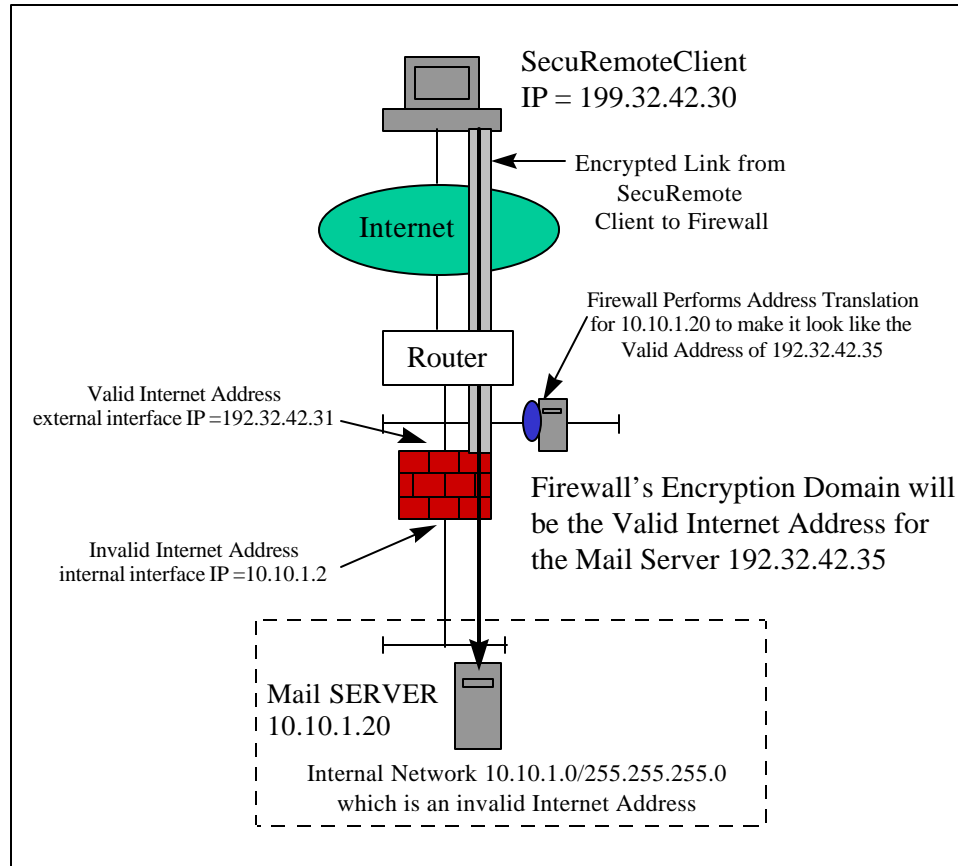


Figure 2 - SecuRemote with Invalid IP Addresses and Address Translation

The third method is to encrypt and “encapsulate” the data from the PC to the Firewall, and then Route the packet to the host on the internal network. This means that you do not need to have a Valid Internet Address for the Internal Host, because the SecuRemote Client only talks to the Firewall. This method could also be called “encapsulation”, “tunneling”, or “deferred-routing”, because the actual routing to the destination takes place after the firewall decrypts the packet. This is shown below in Figure 3:

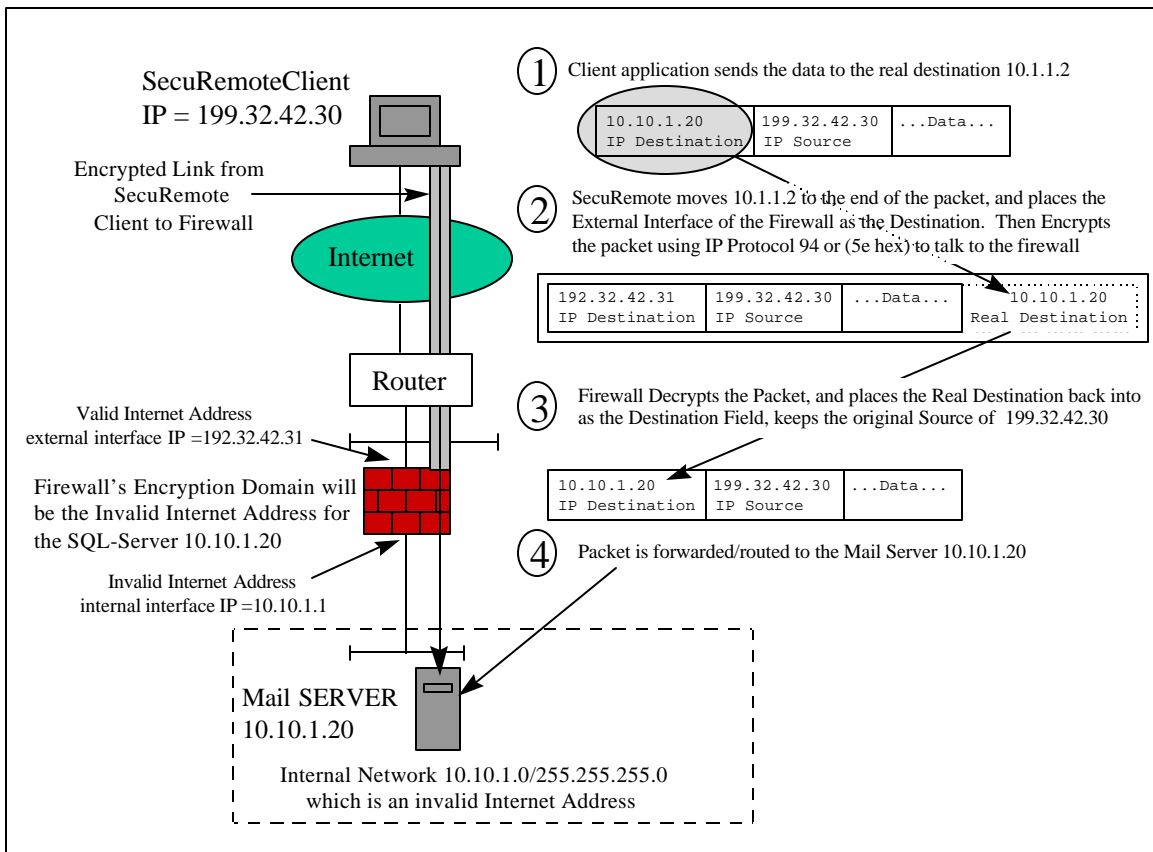
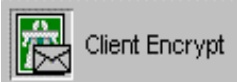



Figure 3. Encapsulation with SecuRemote to Invalid Internet Address

This encapsulation technique allows connectivity from the Internet to Invalid IP Addresses, without having to publish valid Internet Addresses for every machine that is required remote access.

### Configuration

There will be three steps needed to load and configure SecuRemote.

1. Configure a rule on the Firewall that allows for the  in the Action field. (See Page 4)
2. Load and install the SecuRemote software on the Client PC (See Page 11)
3. Configure the SecuRemote Software by double clicking on the envelope , in the bottom right hand corner of the screen, and adding the appropriate Certificate Authority (CA) site. This will be where the Management Station of the firewall will reside. Most times this is the firewall itself. (See Page 12)

Step 1. Configure a Rule for  on the Firewall.

Launch the Security Policy Editor as follows:

**Start → Program → Firewall-1 → Security Policy**

After the Security policy has been loaded you will need to create the following items:

1. Network Object defining the Encryption Domain
2. Firewall Object
3. Users to Authenticate the SecuRemote Session
4. A Rule that Allows SecuRemote

This Security Policy will be based on the Diagram in Figure 1 to allow the SecuRemote Client on the Internet (any IP Address) to access the SQL-Server at 192.32.32.20.

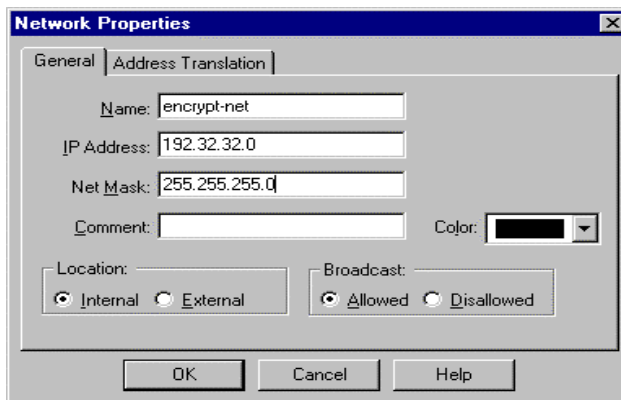
From the Security Policy, create the encryption domain of 192.32.32.20 using the Network Object Manager as follows.

**Manage → Network Objects**



Now Select **New → Network**

Now add            **“encrypt-net”**  
IP Address        **192.32.32.0**  
Subnet Mask      **255.255.255.0**  
Click              **“OK”**



The Encryption Domain is used by the Firewall to define those addresses which will be encrypted/decrypted by the SecuRemote Client. It is necessary to define this object first, because the definition of the Firewall Object Definition will use the Encryption Domain Information.

Next Define the Firewall object as follows:

Select **New → Workstation**

Add the Firewall Name: **firew**  
IP Address: **192.32.42.31**

Note: Use the Get Address button to fill in the IP Address. If this doesn't fill in the IP address make sure the name "firew" is the official host name of the computer by typing in "hostname". If this is the official host name, make sure that its IP Address is in the /etc/hosts file for unix machines, or the \winnt\system32\drivers\etc\hosts file for NT machines (create this ascii file if needed).

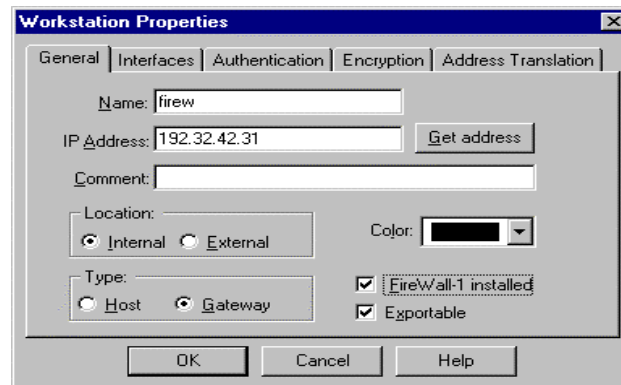


Make sure that the following options are selected from the "General" Tab on the right:

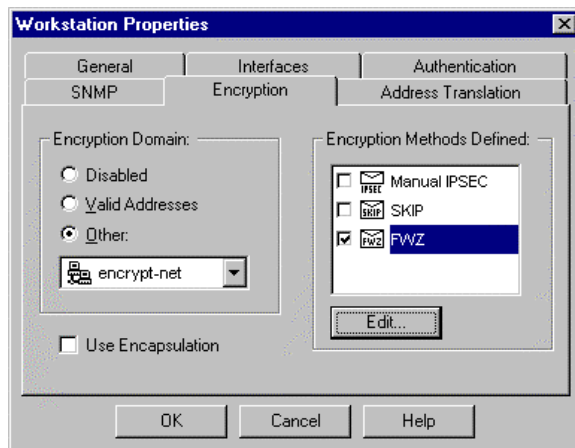
- Type **Gateway**
- **Firewall-1 Installed**
- **Exportable**

The "Gateway" option tells Firewall-1 there is more than one physical Interface.

The Firewall-1 Installed identifies this machine as a Check Point Firewall.



Exportable option allows the "encryption-domain" information to be "exported" to the SecuRemote Clients. This is a very important option, and if not selected, SecuRemote will not work correctly at the SecuRemote Client. The symptoms will be that the SecuRemote client does not pop-up the Username, and Password Dialog box, when sending data to anywhere within the encryption domain (192.32.32.0).



Next, Select the → **"Encryption" Tab** within the "firew" object.

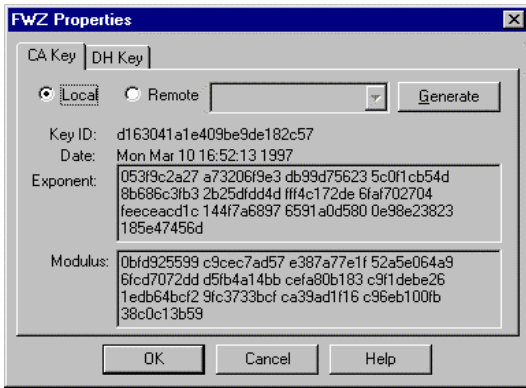
Select the following under the Encryption Domain:

→ **Other**, and then select → **"encrypt-net"** by clicking on the arrow to the right of the blank space under "other".

This tells the firewall that everything to this network, the "encrypt-net" will be Decrypted from the SecuRemote Client. Also, everything that is sent to the SecuRemote Client, will be Encrypted.

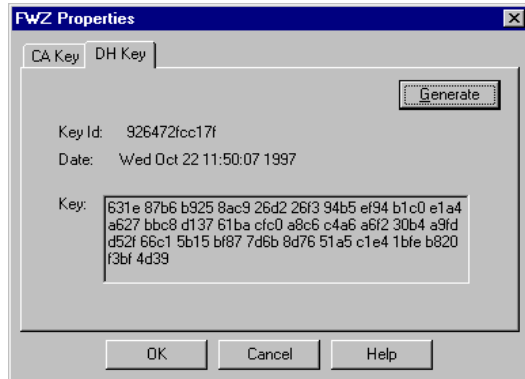
For purposes of this configuration, do not select the Encapsulation option. The "Use Encapsulation" box will be used when we configure SecuRemote for Figure 3 (page 3) which is the encapsulation mode. This option allows the SecuRemote Client to "Tunnel" or "Encapsulate" the encrypted session to the firewall.

Next Click on → **"FWZ"** as the encryption method and Select → **"EDIT"**



Select the → **“CA TAB”** and select → **“LOCAL”**. This is defining a Certificate Authority (someone who will validate the authenticity of the keys that will be generated on the Firewall.) This CA function is handled by the Management Server function, which is located as a daemon process on the Firewall in our design. This is why you select local.

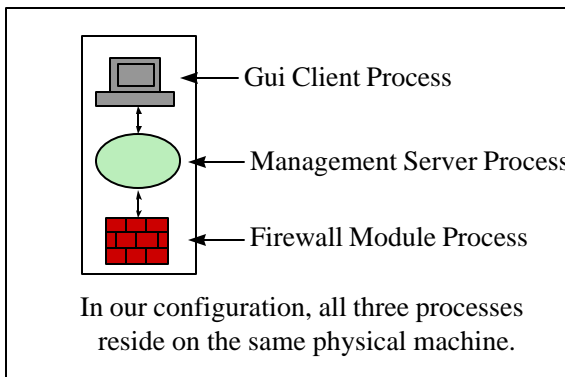
Next Click on the → **“Generate”** function which should fill in something similar to the diagram on the left.



Next, Select the → **“DH Key”** Tab. This is where the Diffie-Hellman key will be generate. This is used to “Exchange Keys” with the SecuRemote Client.

Select → **“Generate”**

This will Generate and store the Diffie-Hellman Key on the Management Station, and download this information to the Firewall Module(s) when using a Management Server that is De-Coupled from the Firewall Module, the CA will still be defined as local.

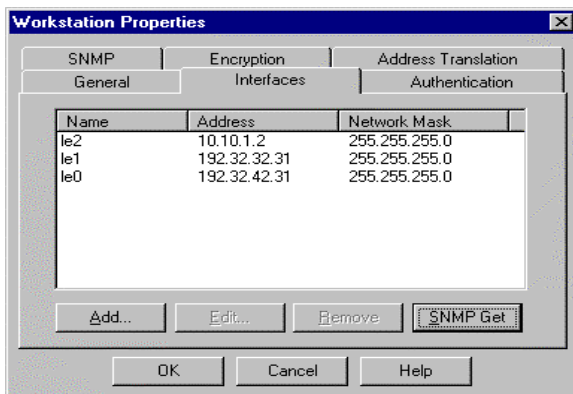


The Diagram on the left shows the different functional elements to the firewall system.

In our example, all three processes reside on the same machine.

Click → **“OK”** when the DH Key has been generated.

Next Click on the → **“Interfaces”** Tab of the Firewall Network Object.



Click on the **“SNMP Get”** function to retrieve the Interface Definitions. This will tell the Firewall Software to Inspect Packets on all of the Physical Interfaces in the Firewall.

Note: If the SNMP Get function fails on an NT System, make sure you have loaded the optional SNMP module from the NT CDROM.

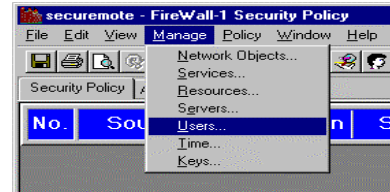
It is very important that the Interface Definitions be filled out correctly so that the Software will be able to inspect the packets properly on all Interfaces.

Click → **“OK”** to complete the definition of the Firewall Object.

Click → **“Close”** to end the Network Objects portion of the configuration.

Define the SecuRemote User in the User Section of the Security Policy. To accomplish this, select the following from the Main Security Policy window:

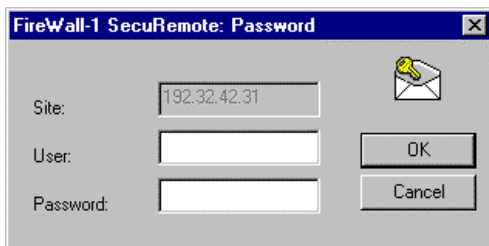
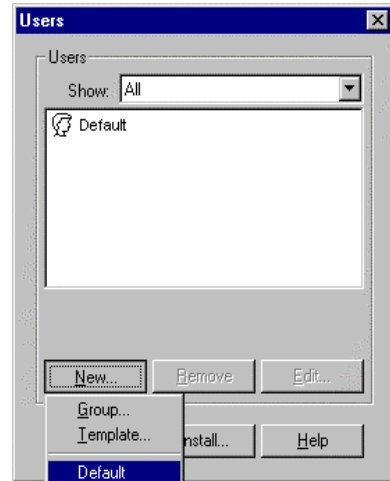
**Manage → Users**



Add a New User to the system by typing the following:

**New → Default**

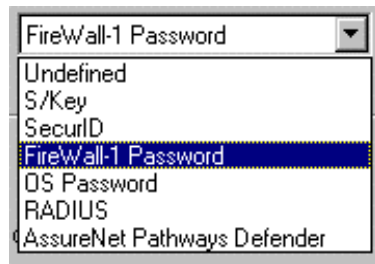
This will be the name of the user and the password information that is used for the SecuRemote Screen that pops up on the SecuRemote Client machine.



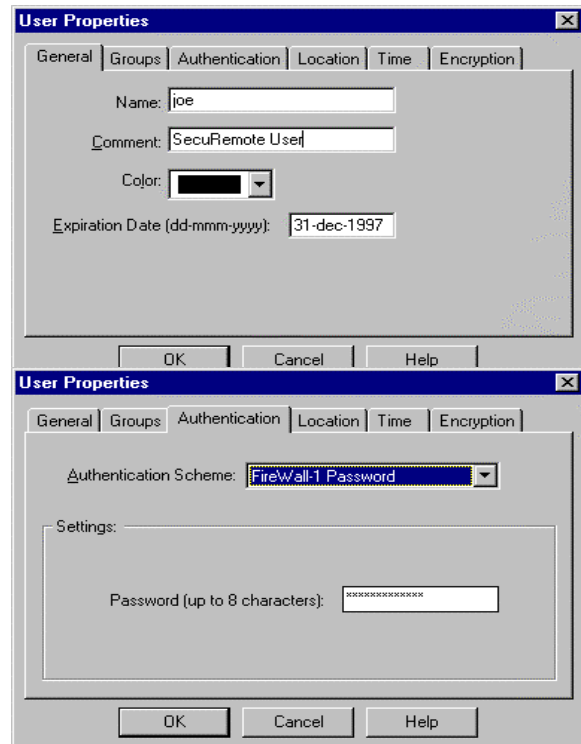
Add the User as Follows:

Enter the User Name **“Joe”**  
 Validate the Expiration Date Information  
**31-Dec-1997**

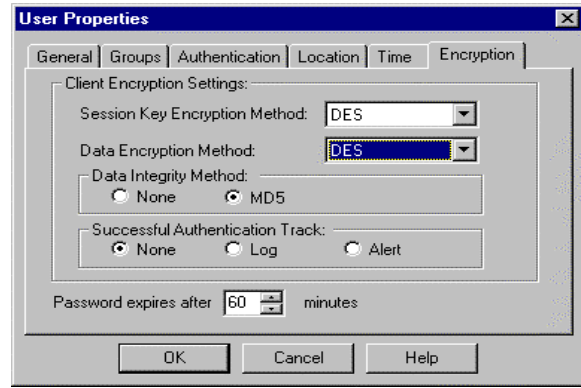
Now Select what Method to Authenticate the User  
**“Joe”**, by Clicking  
**→ “Authentication” TAB**  
 You can select from the following in version 3.0B:



For our purposes we will select the **“Firewall-1”** password. Type in a password with up to 8 characters.



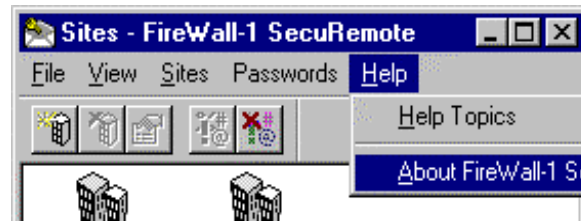
Next, select the → **“Encryption” Tab** and select the Method of encryption. In our Case, this will be **“DES”**.



\*\*\*\*\* Joe’s NOTE \*\*\*\*\*

To Find out what Encryption Type the SecuRemote Client is capable of,

select **Help** → **“About Firwall-1 SecuRemote”** On the SecuRemote Client.



For our SecuRemote Client, It has the **“DES”** version of encryption as shown to the right.

This must match the **“Encryption”** settings defined in the User Profile Definition on the firewall as Shown Above.....

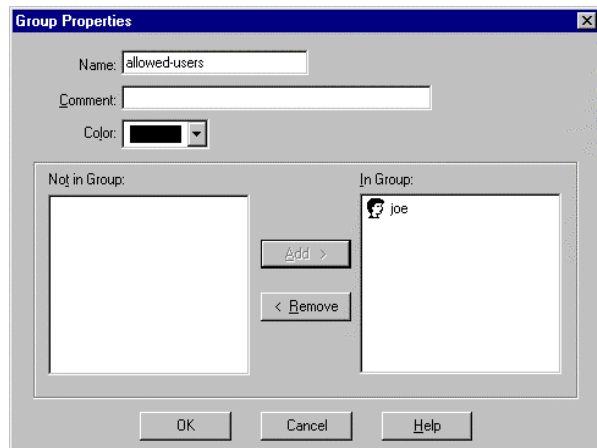


Now we must create a group for the User **“Joe”** to belong to. Select

**New** → **Group** and type in **“allowed-users”**

Select **“Joe”** and **“add”** him to this Group.

**Click** → **OK**



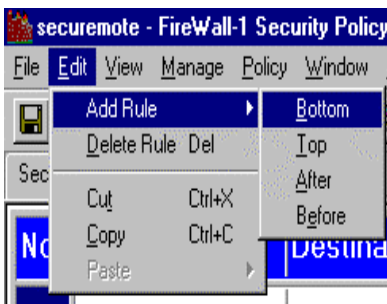
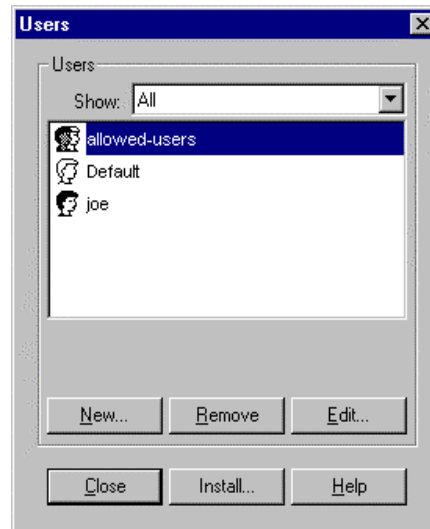
This will complete the User Definitions at the firewall, and the screen should look like the diagram on the right.

Click “Close” at this point.

Now we must add the rule that will define Where the SecuRemote clients are allowed access to. From the Security Policy Editor,

Select **Edit → Add Rule → Bottom.**

As shown below.

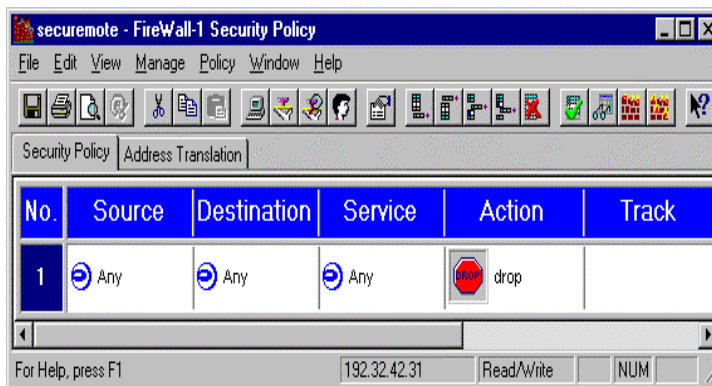


Next, change rule 1 in the Security Policy shown below from:

Source	Destination	Service	Action
any	any	any	drop

-----**To**-----

Source	Destination	Service	Action	Track
allowed-users@any	encrypt-net	anyClient-Encrypt	long	



To accomplish this, click with your right mouse button in the Source Field Column, to → “Add User Access”

Now Select → “Allowed-Users”

Select “OK”

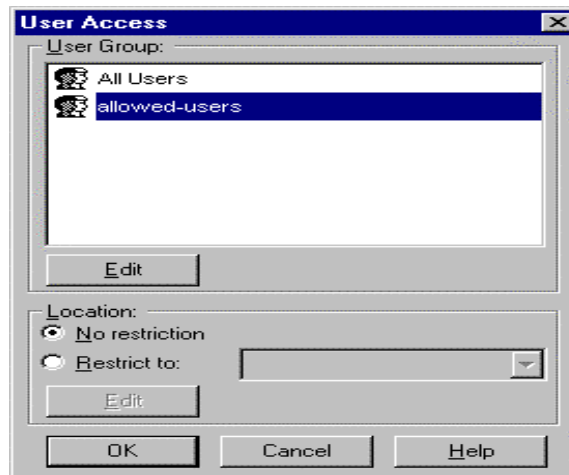
In the Destination Field Select

“add→ encrypt-net” and Select → “OK”

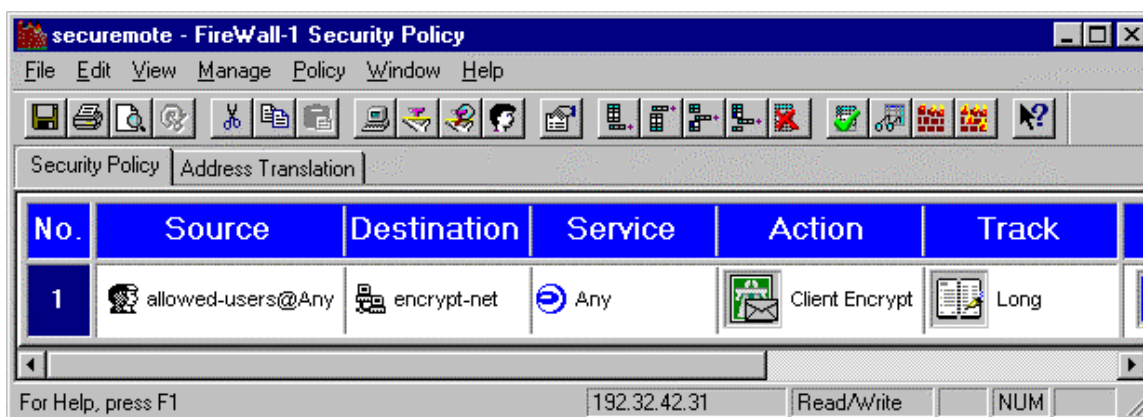
Allow all services, and select

→ “client-encryption” in the Action Field.

Select → “Long-Log” in the Track Field



You rule should now look like the following Diagram:



This will allow all the SecuRemote Users defined in “Allowed-users” to access any device on the “encrypt-net” using any services (ie. Telnet, FTP, Mail, HTTP, etc.).

The Track Column will allow the Logging of the Authentication of the SecuRemote User as well as the Connection information.

Now we must Install the Security Policy on the firewall. To Perform this action

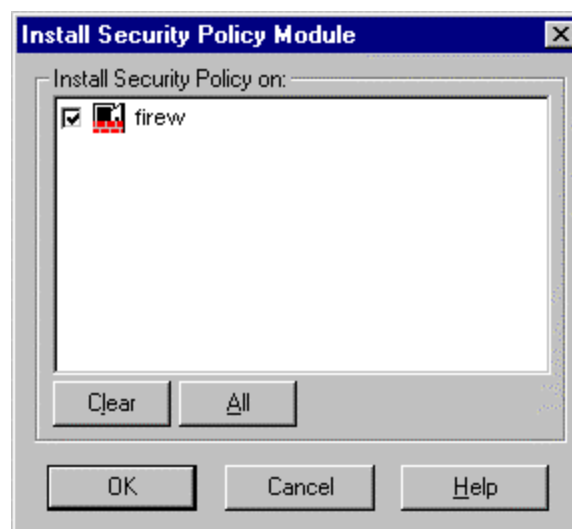
Select **Policy** → **Install**

The Screen to the Right will Show up with the Firewall Object “Firew” in the window.

If there is no object in this window, you have not defined the “Firew” object correctly (you need to make sure Firewall-1 Installed is selected in the object definition).

Click → **OK**

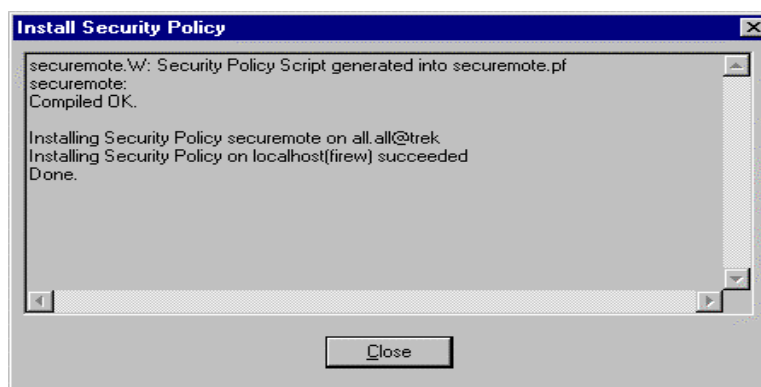
To Install this policy on the firewall



This Screen should show up as the Security Policy is saved in Inspect Script, and Compiled into machine language code to be downloaded to the Firewall Module. This is functionally what is happening here.

If you see “succeeded”, then the security Policy is successful.

Now onto the SecuRemote Client.....

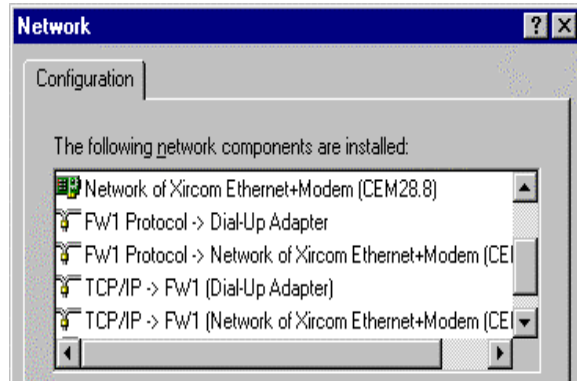


## Step 2. Load and Install the Software on the SecuRemote Client

In order to load the software on the Client PC, simply execute the “setup.exe” file on the SecuRemote Floppy Disk or wherever the software has been downloaded to on the Hard Disk. In our case, the software has been loaded on the hard disk under the C:\temp\securemote subdirectory. Simply type in “setup” at this point from the C:\temp\securemote directory. This will step you through a very simple installation process.

\*\*\*\*\* NOTE \*\*\*\*\*

The most important part of the Software installation is to know what LAN Adapter, or DIAL-UP Adapters will be used for SecuRemote Encryption. SecuRemote will provide you with the option of using either both the Dial-up and LAN adapters, or only the Dial-up adapters at installation. If you are using a Dial-up connection to the Internet, you will only need the Dial-up Adapter configured for SecuRemote. If you work at your office on a Local Area Network (LAN), and use SecuRemote to access other remote sites, then you will need to install it on Both the Dial-up adapter and the LAN Adapter.



These settings can be found under the **Control Panels** → **Network**. The Diagram shown Above is after SecuRemote Installation.

If installed on both Dial-Up Adapters and LAN Adapters, SecuRemote will modify the original settings

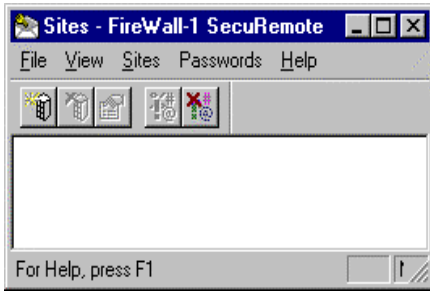
FROM	TO
TCP/IP → Dial-Up Adapter	TCP/IP → FW1 (Dial-Up Adapter) FW1 Protocol → Dial-Up Adapter
TCP/IP → LAN Adapter	TCP/IP → FW1 (LAN Adapter) FW1 Protocol → LAN Adapter

SecuRemote inserts a “SHIM” between the Adapter Layer and the TCP/IP Layer of the Operating System. No TCP/IP Communication can occur unless it passes through the SecuRemote Layer. This is where it will be decided to encrypt the packet, or not to encrypt the packet before forwarding it.

After installing the SecuRemote software, you must reboot your PC for the Drivers to take effect.

Now that the SecuRemote Software has been loaded on the PC, now we must configure it.

Step 3. Configure the SecuRemote Software by double clicking on the envelope icon, in the bottom right hand corner of the screen.



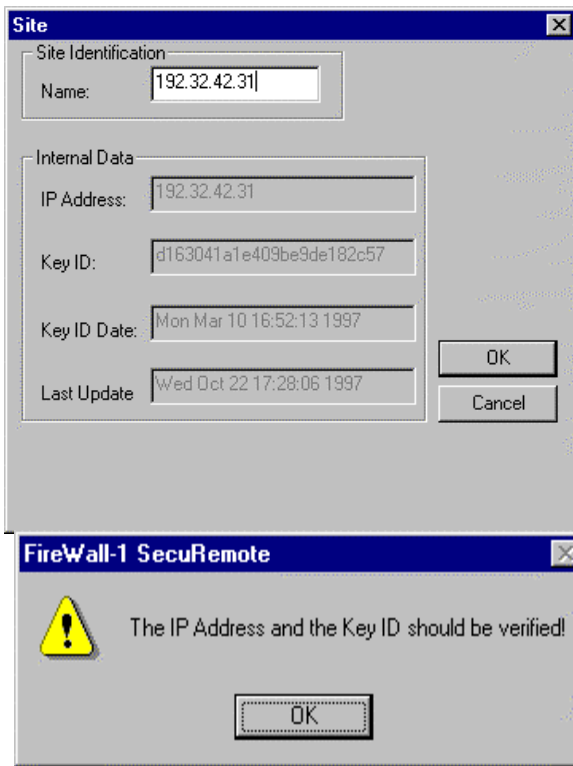
This will bring up the Screen shown at the left.

Now Select **Site** → **Make New**



The Screen Below will now be displayed

Now, enter the IP Address, or a Name that can be resolved to an IP Address. In our case, this must be the IP Address of the External Interface of the Firewall, because it is the Certificate Authority for the Firewall. → **192.32.42.31** was entered, and click **“OK”**



You should now see communications from the SecuRemote client to the Firewall, and the Grayed portion of the screen labeled “Internal Data” will be filled in Automatically.

**NOTE:** If you ever change the “encrypted Domain Information on the Firewall, you must “UPDATE” this site so that SecuRemote knows to encrypted the data to the new Encryption Domain Locations. This is done by Double Clicking on the Site and Selecting the “UPDATE” Button.

If you are successful, the next screen will show up, specifying that the IP Address and Key ID should be verified with the Firewall Administrator. This is to validate that the Key information is actually from the Firewall itself, and no-one spoofed this data. This is also a good way to verify if the SecuRemote user has the latest Encryption Domain Information. This can be obtained by looking at the Last Updated Date.

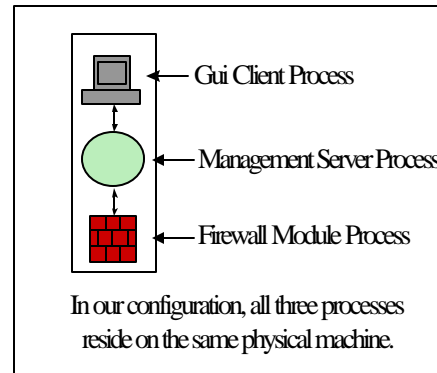
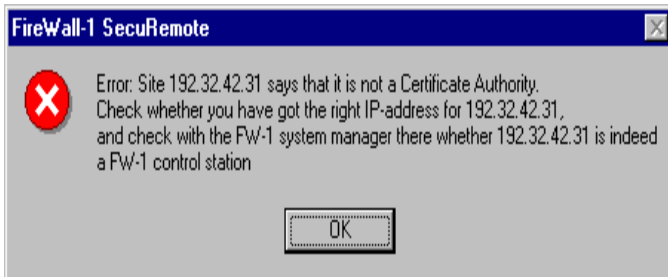
**NOTE:** If you are not successful, try and PING the IP address of the Firewall to make sure you can communicate with this site. Communications to the Firewall will be needed before trying to “Make a New Site” in SecuRemote. For Dial-up Adapter users, make sure you have a valid Internet Connection before trying to make a new site in SecuRemote. You might also want to ping another site as well (www.yahoo.com for example) to see if your Internet connections is properly configured. If you can’t ping the IP Address of the Firewall, you must fix this communications problem before you continue.

\*\*\*\*\* NOTE \*\*\*\*\*

If you Receive the Error Message below, make sure the firewall has the proper license for a "CA" by typing in the following:

From Unix:  
/etc/fw/bin/fw printlic

From Windows NT:  
\\winnt\fw\bin\fw printlic

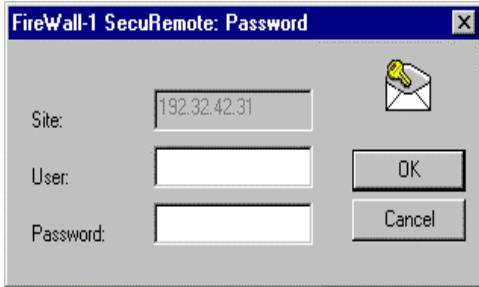


If you have a valid license, make sure the Certificate Authority (CA) is not De-coupled from the Firewall Module machine, and placed on the Management Server machine (ie. Control Station). If this is the case, you must type in the address of the Management Server Machine in the SecuRemote Window for Making a New Site, and not the Firewall's IP Address

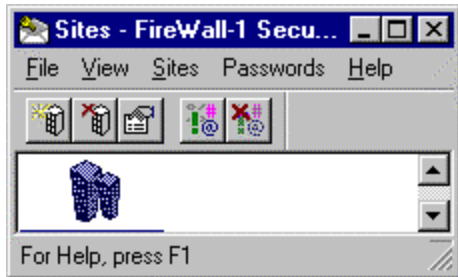


If you receive this error message on the left, please get a "SecuRemote" license. SecuRemote has to be licensed in order to get the topology download and the site definition. You can contact your reseller or Check Point Representative for this "free" license.

Now you should be ready to test the SecuRemote Encryption. Simply use your normal application to connect to the Mail Server, and the following window will pop-up. This is where you enter your User Name and Password as defined in Firewall. In my case, I typed in "joe" with a password of "xxxxx".

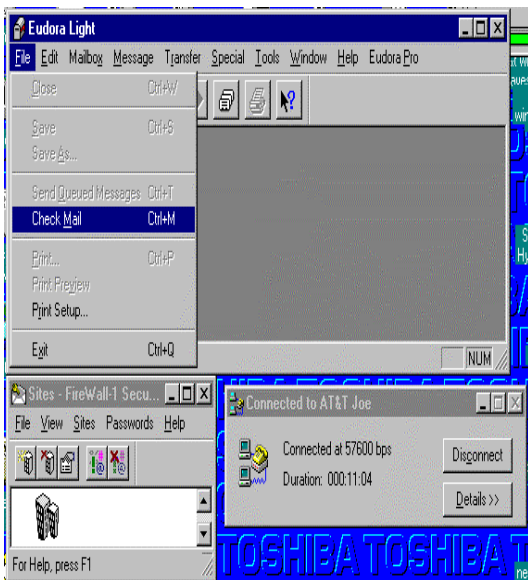


You might also want to position the SecuRemote Screen so as to see the bottom section (where it says **For Help, Press F1**). This should now change to the **"Exchanging Keys with a Firewall"**, after you hit the "OK" button for the User and Password box on the left.



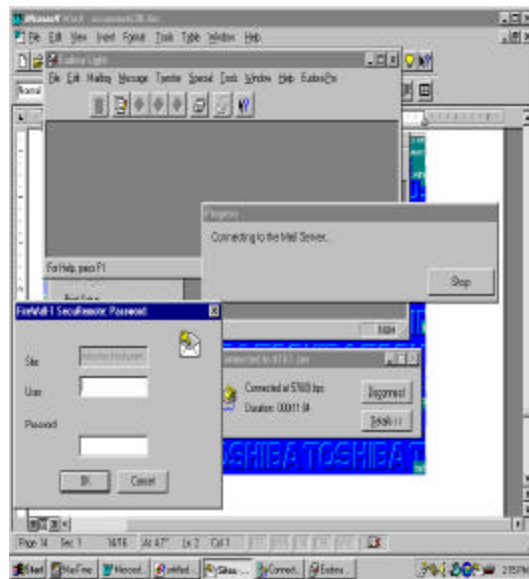
If you were using SecuRemote in addition to checking your email, it might look like the following diagram(s) on the next page.....

Step 1. Check Mail

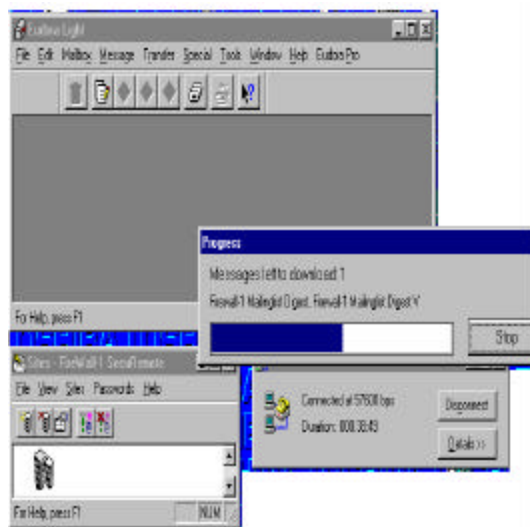
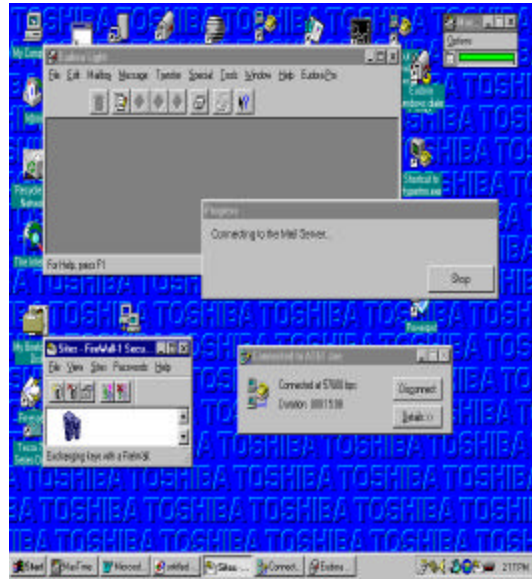
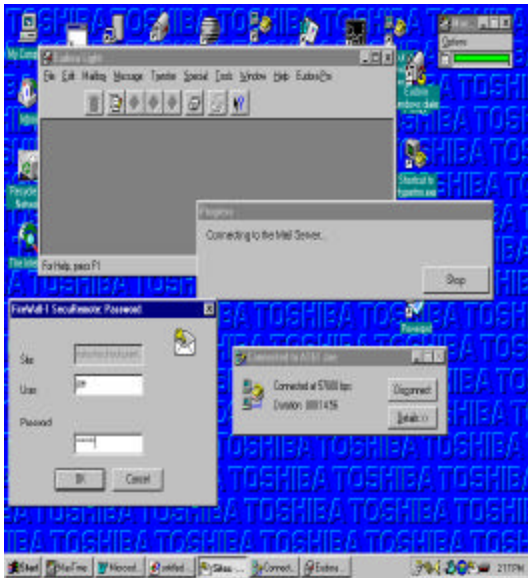


Step 3. Enter Username and Password

Step 2. SecuRemote Pops Up



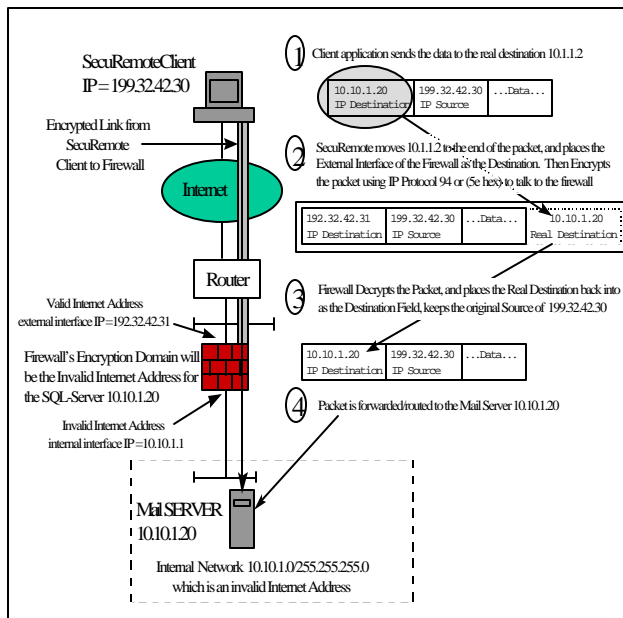
Step 4. SecuRemote Exchanges Key with Firewall and establishes Encrypted Link to Firewall.



Step 5. User is Authenticated at the firewall, and Eudora Session is connected to the Mail Server retrieving their mail over an encrypted link over the Internet.

This Process is transparent to any application, because SecuRemote is a Shim in between Layers 2 (Data Link) and Layer 3 (Network). You can use other applications such as Telnet and FTP to test your particular situation.

### Tunneling With SecuRemote



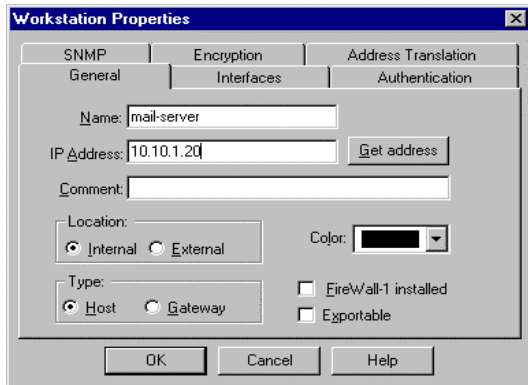
Given the Diagram on the left, we will now use SecuRemote to “encapsulate” from the client (199.32.42.30) to the firewall (192.32.42.31), and then route to the Illegal IP Address of the Server (10.10.1.20). We will use Telnet on the client to access the Mail Server for administrative purposes.

The following additional Firewall configurations must now be added:

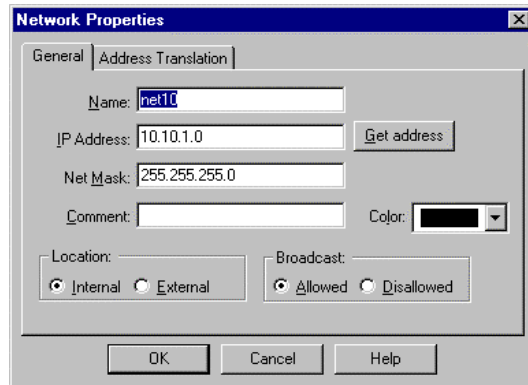
1. Add the following Objects to the Firewall:
  - ◆ Mail Server (10.10.1.20)
  - ◆ Net10 (10.10.1.0/255.255.255.0)
  - ◆ Group “encrypt-zone” with Net10
2. Add Net10 to the Encryption Domain on the Firewall (to encrypt to Mail Server)
3. Select “Encapsulation” in the Encryption Tab on the Firewall Object “firew”.

## Configuration Steps

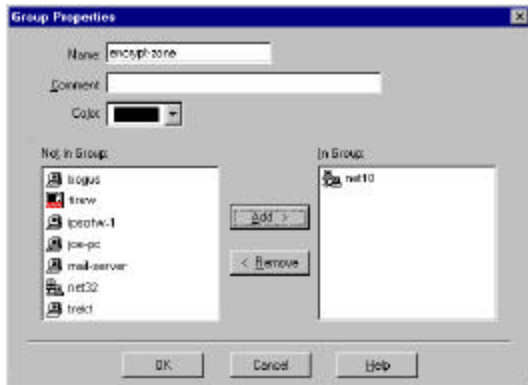
1. Create the Mail Server Object (10.10.1.20)

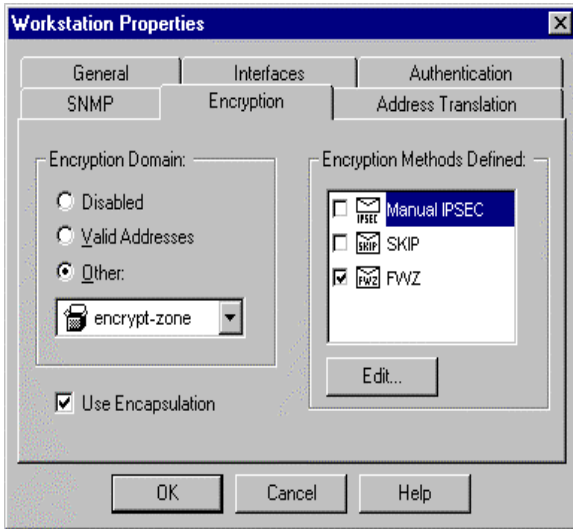


2. Create the Network object 10.10.1.0 Network



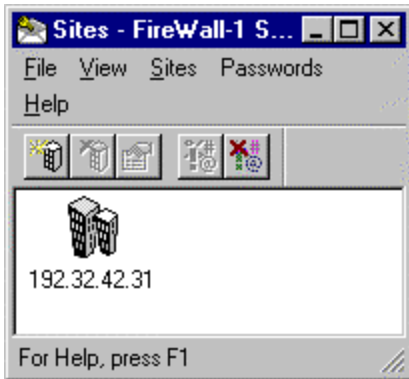
3. Create a Group Object “encrypt-zone” with “net10” as a member of this group. This will allow the firewall to encrypt/decrypt anything to this network



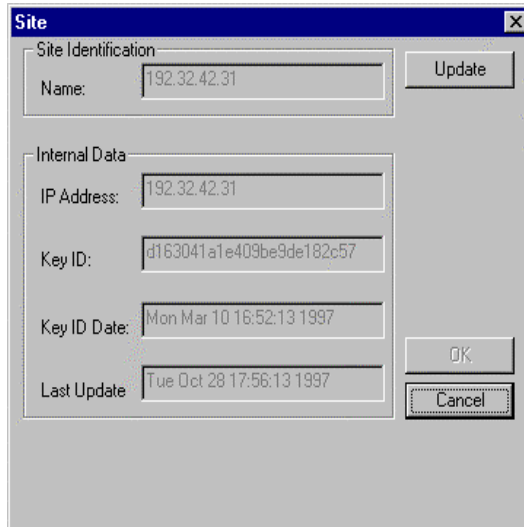


1. Add **“Encrypt-Net”** to the Encryption Domain on the Firewall Object **“firew”** as shown to the left.
2. Select **“Use Encapsulation”** as shown to the left.
3. Click **“OK”**
4. Now Download the Security Policy to the Firewall at this point.  
**Policy → Install**

**On SecuRemote Machine.**



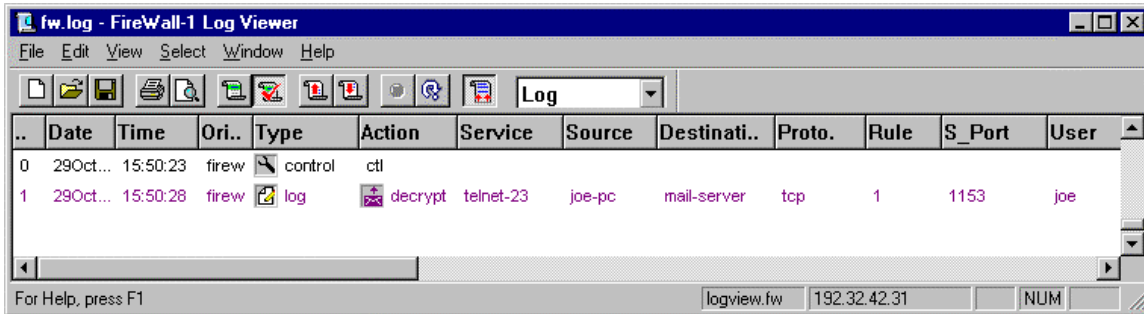
1. Now **Double Click on the “192.32.42.31”** Icon to update the site. We need to update the site to tell the SecuRemote Client that there is new encryption domain information (10.10.1.0/255.255.255.0), and to encapsulate the traffic.
2. Next, Update the site by clicking on the **“Update”** button.



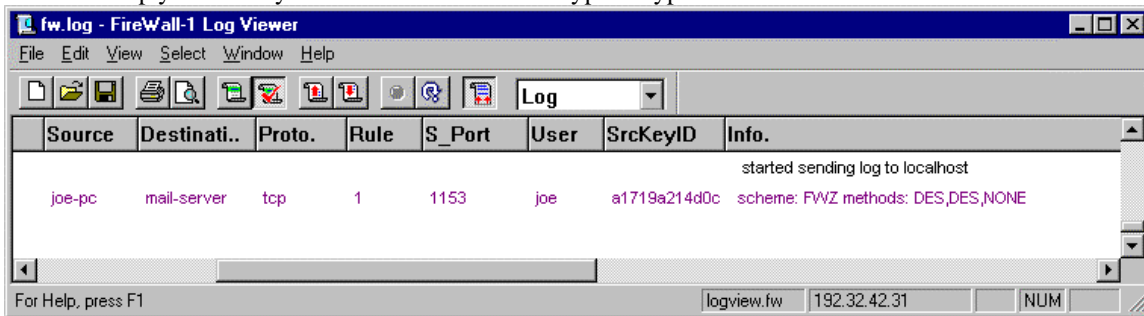
Now we can try and Telnet to the 10.10.1.20 Mail Server from the SecuRemote Client.

You will see the **“Snoop”** traces and Log Viewer of the results on the next page.

The Log-Viewer on the Firewall Shows the Telnet Session from the user “joe” located on the “joe-pc” (199.32.42.30) machine going to the destination of the Mail Server (10.10.1.20).



By Scrolling over in the Log Viewer, notice the Encryption Method in the Info Field. (DES, DES, None) This will help you identify the machines and the encryption types.



By using the “Snoop” command on the Solaris Firewall, we can look at the Packet Traces from the two Interfaces.

#### External Interface (192.32.42.31)

```

firew# snoop -d le0
Using device /dev/le (promiscuous mode)
199.32.42.30 -> firew IP D=192.32.42.31 S=199.32.42.30 LEN=810,
ID=46616
firew-> 199.32.42.30 IP D=192.32.42.30 S=192.32.42.31 LEN=366,
ID=49409
firew-> 199.32.42.30 IP D=192.32.42.30 S=192.32.42.31 LEN=121,
ID=49410
199.32.42.30 -> firew IP D=192.32.42.31 S=199.32.42.30 LEN=49,
ID=46360
199.32.42.30 -> firew IP D=192.32.42.31 S=199.32.42.30 LEN=121,
ID=46872
firew-> 199.32.42.30 IP D=192.32.42.30 S=192.32.42.31 LEN=49, ID=893
....
....
....
199.32.42.30 -> firew IP D=192.32.42.31 S=199.32.42.30 LEN=45,
ID=47128
firew-> 199.32.42.30 IP D=192.32.42.30 S=192.32.42.31 LEN=60, ID=894
199.32.42.30 -> firew IP D=192.32.42.31 S=199.32.42.30 LEN=48,
ID=47384
firew-> 199.32.42.30 IP D=192.32.42.30 S=192.32.42.31 LEN=45, ID=895
firew#
  
```

#### Internal Interface (10.10.1.1)

```

trek# snoop -d le1
Using device /dev/le (promiscuous mode)
199.32.42.30 -> mail-srv TELNET C port=1169
mail-srv -> 199.32.42.30 TELNET R port=1169
199.32.42.30 -> mail-srv TELNET C port=1169
199.32.42.30 -> mail-srv TELNET C port=1169
mail-srv -> 199.32.42.30 TELNET R port=1169
199.32.42.30 -> mail-srv TELNET C port=1169
....
....
....
199.32.42.30 -> mail-srv TELNET C port=1169
199.32.42.30 -> mail-srv TELNET C port=1169
mail-srv -> 199.32.42.30 TELNET R port=1169
mail-srv -> 199.32.42.30 TELNET R port=1169
firew#
  
```

The Snoop trace on the External Interface shows the “Encapsulated” Packet from the SecuRemote Client. The Address of “firew” is 192.32.42.31. The Column on the Right shows the packet after it has been decrypted, and un-encapsulated and routed to the Mail Server. Notice that you can identify the “Telnet” application within the packet trace after it has been decrypted by the firewall. This packet is using the Telnet Port which is port 23.

The details of one of the encapsulated packets are shown below. Please notice that this packet is using IP Protocol “94” to encapsulate the original packet into this format.

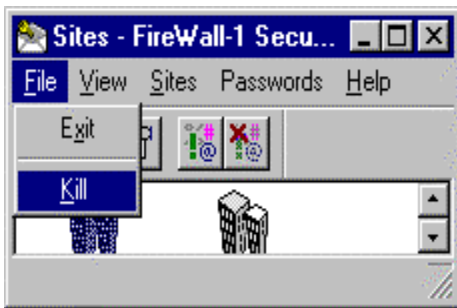
```
firew# snoop -d le0 -v
Using device /dev/le (promiscuous mode)
ETHER: ----- Ether Header -----
ETHER:
ETHER: Packet 1 arrived at 16:06:54.03
ETHER: Packet size = 849 bytes
ETHER: Destination = 8:0:20:7b:d2:45, Sun
ETHER: Source = 0:80:c7:73:fe:8d, Xircom Inc.
ETHER: Ethertype = 0800 (IP)
ETHER:
IP: ----- IP Header -----
IP:
IP: Version = 4
IP: Header length = 20 bytes
IP: Type of service = 0x00
IP:   xxx. .... = 0 (precedence)
IP:   ...0 .... = normal delay
IP:   .... 0... = normal throughput
IP:   .... .0.. = normal reliability
IP: Total length = 835 bytes
IP: Identification = 41752
IP: Flags = 0x0
IP:   .0.. .... = may fragment
IP:   ..0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 32 seconds/hops
IP: Protocol = 94 ()
IP: Header checksum = 1fc3
IP: Source address = 199.32.42.30, 199.32.42.30
IP: Destination address = 192.32.42.31, firew
IP: No options
IP:
```

<\*\*\*\*\* IP Protocol 94 is used for SecuRemote Encapsulation \*\*\*\*\*>

---

**Troubleshooting:** if you can't connect to the Mail Server:

1. Validate that there is IP Connectivity between your SecuRemote Client and the Fire wall



If you are having trouble connecting to the firewall, try “Killing” SecuRemote by clicking File → Kill. This will disable SecuRemote, so that you can validate the machine can actually PING the firewall for connectivity. Then SecuRemote can be reinstalled by clicking Start → Programs → Firewall-1 → SecuRemote

If you have been able to Define the site and retrieve the keys, this will eliminate the lack of IP Connectivity Issue, and there is another problem.

2. If the SecuRemote Client, does not pop-up when you try and connect to the Mail Server, Validate the Encryption Domain on the Firewall. This will tell the SecuRemote Client when to start the Authentication process for the Encrypted Destinations.
3. If the Encryption Domain looks OK, make sure the SecuRemote Client has “Updated” its information. There is also a file on the SecuRemote PC named “userc.c” that will show the encryption domain.
4. Check out the Log Viewer, and see if there is any connectivity from the SecuRemote client.
5. Make sure the Fire wall can communicate to the mail server
6. Validate the Security Policy to make sure that communications is allowed to/from the proper devices.

7. Run the “Snoop” trace to see the packets to and from the SecuRemote Client. On Windows NT, use the Monitor Application.