
Check Point Software Technologies LTD.

***FireWall-1 Version 3.0
Address Translation Quick Reference
Guide***

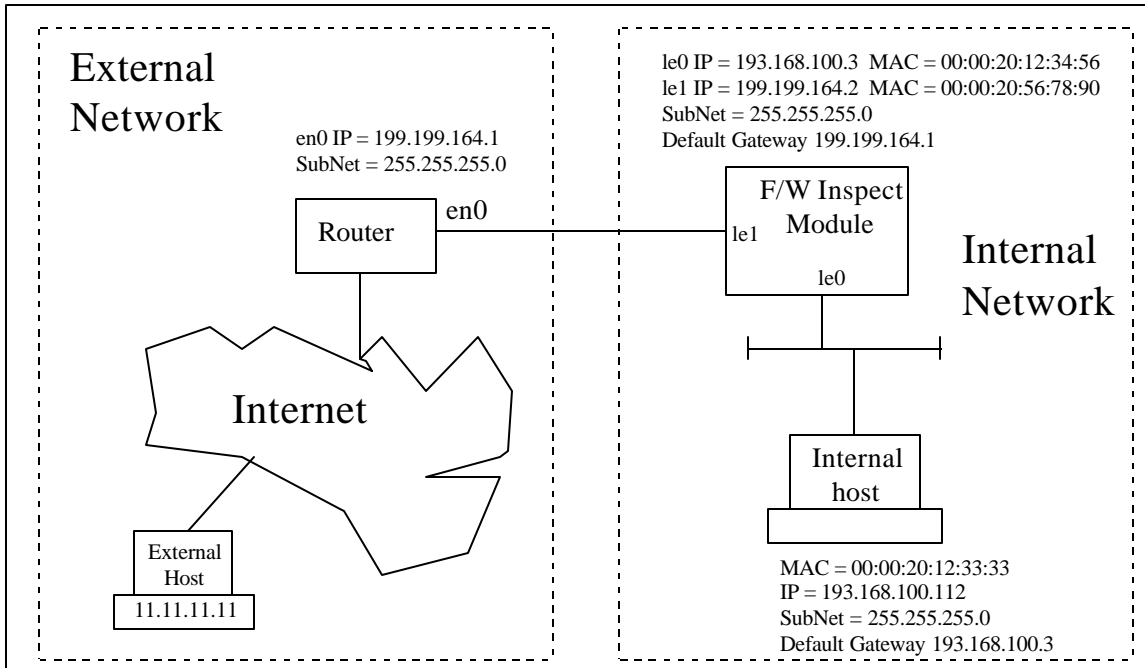
Authored By: Joe DiPietro
Date: July 11, 1997
Purpose: To describe and Document the Address Translation Features within Checkpoint Version 3.0 Firewall-1

CheckPoint Software Technologies LTD.

FireWall-1 3.0 Address Translation Quick Reference

Address Translation Example 1

Figure 1 - Network Diagram



Given Figure 1 shown above, the following is a typical goal of customers wishing to use the address translation features of version 3.0:

- Give the Internal Host, which is not a valid Internet Address, access to the Internet
- Allow communications in both directions from the Internal Host which means:
 - ◆ Communications initiated from the External Network going to the Internal Network
 - ◆ Communications initiated from the Internal Network going to the External Network

The IP address Structure for the following network is the following:

	MAC Address	IP Address	Subnet Mask	Default Gateway
Internal Host	00:00:20:12:33:33	193.168.100.112	255.255.255.0	193.168.100.3
Firewall (le0)	00:00:20:12:34:56	193.168.100.3	255.255.255.0	199.199.164.1
Firewall (le1)	00:00:20:56:78:90	199.199.164.2	255.255.255.0	199.199.164.1
Router (en0)	00:00:20:12:12:12	199.199.164.1	255.255.255.0	n/a

There are a variety of ways to configure the system in order to accomplish the goals mentioned above. These will include the following terms FWXT_DST_STATIC, FWXT_SRC_STATIC, and FWXT_HIDE.

Common Terminology

- FWXT_DST_STATIC - Communication initiated from the External Network to the Internal Network
- FWXT_SRC_STATIC - Communication initiated from the Internal Network to the External Network
- FWXT_HIDE - Communication initiated from the Internal Network to the External Network using the External IP address of the firewall in our example.

Using these terms, lets start to configure our systems in the following steps.

- Step 1. - Allow Communications initiated from the Internal Network to the External Network
- This could be an Internal Host trying to use a Web Browser to connect to www.checkpoint.com in order to look at our Web site.

- Step 2. - Allow Communications initiated from the External Network to the Internal Network
- This could be an External Host trying to ftp to your FTP server to download a file

Internal Host Configuration

The main issue with the Internal Host configuration is to point the default gateway address to the internal network interface of the firewall. In our case, the internal host should be pointed at the 193.168.100.3 address. If this machine is a Unix or NT machine, this information can be verified by using the “netstat” command as follows:

```


UNIX



```
internalhost# netstat -rn

Routing Table:
 Destination Gateway Flags Ref Use Interface

127.0.0.1 127.0.0.1 UH 0 1315 lo0
193.168.100.0 193.168.100.112 U 3 23 le0
224.0.0.0 193.168.100.112 U 3 0 le0
default 193.168.100.3 UG 0 5
internalhost#

The line “default 193.168.100.3” means that if this machine doesn’t have a route to a particular IP network, then send this information to this address (193.168.100.3), and it will figure out the correct path. If you don’t have a default router (or gateway) entry, type in the following as the root user if your machine is a UNIX host:

internalhost# route add default 193.168.100.3 1
```


```

```


WINDOWS NT



```
C:\WINDOWS>netstat -rn

Route Table

Active Routes:

 Network Address Netmask Gateway Address Interface Metric
 0.0.0.0 0.0.0.0 193.168.100.3 193.168.100.112 1
 193.168.100.0 255.255.255.0 193.168.100.112 193.168.100.112 1
 193.168.100.112 255.255.255.255 127.0.0.1 127.0.0.1 1
 193.168.100.255 255.255.255.255 193.168.100.112 193.168.100.112 1
 224.0.0.0 224.0.0.0 193.168.100.112 193.168.100.112 1

C:\WINDOWS>

The Entry of “0.0.0.0 0.0.0.0 193.168.100.3 193.168.100.112”
is the default gateway on an NT system. If this is incorrect, please go to
control panel-> network -> TCP/IP -> Default Gateway to correct this.
```


```

The above command should allow the machine to set the default route entry, or look in your workstation documentation for this setting under the “TCP/IP- Default Gateway” section of the manual.

Firewall-1 Configuration

Before configuring the address translation software, check to see if the Firewall has IP connectivity to both the Internal Host and the router.

Joe's Note: If you can't "ping" both of these devices, you must resolve this situation before you can continue. This could be a cabling issue, IP address issue (use ifconfig to check local IP addresses on UNIX, or ipconfig /all on NT), routing issue (use the netstat -rn command), or any other number of configuration issues.

You can test this part of the configuration by using the ping command as follows:

```
firewall# ping 193.168.100.112
193.168.100.112 is alive
firewall#
```

UNIX

If there is an entry in the /etc/hosts file (193.168.100.112 internalhost) or a Domain Name Server (DNS) entry that will resolve the name to IP bindings, you could have typed in the following:

WINDOWS NT

If there is an entry in the C:\winnt\system32\devices\etc\hosts (193.168.100.112 internalhost) or a Domain Name Server (DNS) entry that will resolve the name to IP bindings, you could have typed in the following:

```
firewall# ping internalhost
internalhost is alive
firewall#
```

UNIX

On Solaris 2.x machines the order of IP to name resolution can be found in the file /etc/nsswitch.conf. This file specifies the order in which to resolve names, ie /etc/hosts, DNS, etc. (files -means /etc/hosts and other local files on this host).

WINDOWS NT

DNS is configured under "Control Panels" → "Network" → "Protocols" → "TCP/IP" → "Properties" → "DNS Tab"

Use the ping command to check the IP connectivity to the router as follows:

```
firewall# ping 199.199.164.1
199.199.164.1 is alive
firewall#
```

Once the firewall can successfully ping both devices, there is one more step to verify the default gateway configuration on the firewall, before attempting to configure the address translation tables. Verify this configuration as follows:

UNIX Firewall Default Gateway

```
internalhost# netstat -rn | grep default
```

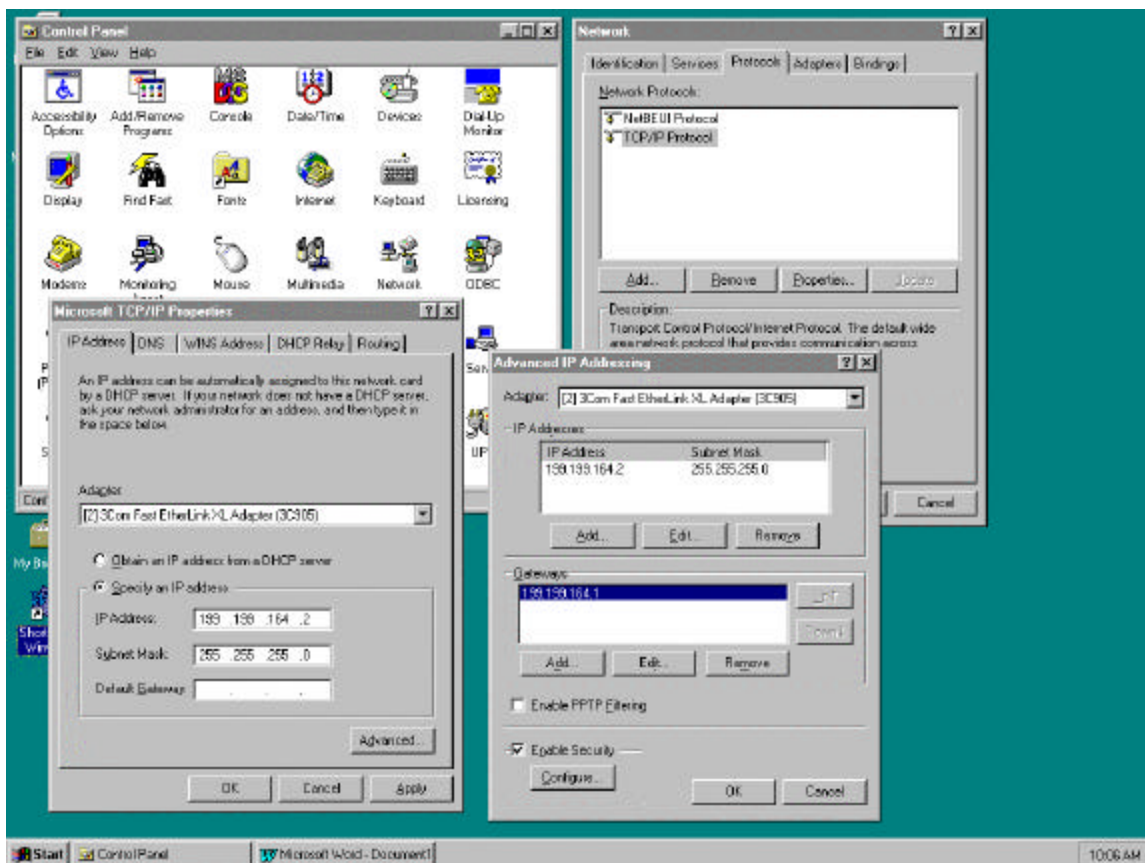
Routing Table:

Destination	Gateway	Flags	Ref	Use	Interface
default	199.199.164.1	UG	0	5	

The line “default 199.199.164.1” means that if this machine doesn’t have a route to a particular IP network, then send this information to this address (199.199.164.1), and it will figure out the correct path.

WINDOWS NT Default Gateway Configuration

Select “Control Panel” → “Network” → “TCP/IP” → “Properties” → “Advanced” → “Gateways” as shown below:



WINDOWS NT

Make sure there is only **ONE Default Gateway** Configured, or the routing will not function properly. This means that for all of the adapters that are configured, only one default gateway is defined. For this example, the default gateway for the firewall is 199 . 199 . 164 . 1

Also, verify that the “Routing” tab with TCP/IP Properties **has Routing enabled**. This must be enabled for the Firewall to pass packets from one interface to another.

Now configure the Address Translation Rules from within the “Address Translation Tab” of the “FWPOLICY” application as follows:

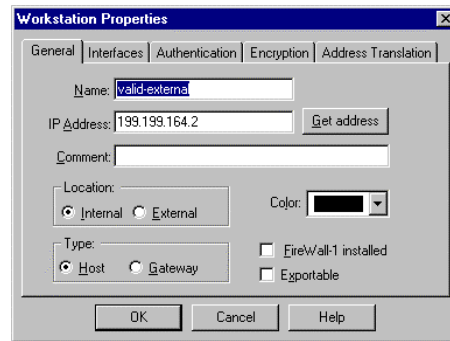
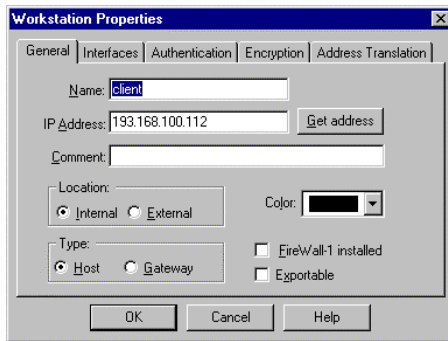
The following three pages are a Quick Reference if you are familiar with our software and understand address translation issues. If you want to understand the technical detail behind the summary presented here, read the pages after this summary.

FWXT_HIDE Configuration Summary

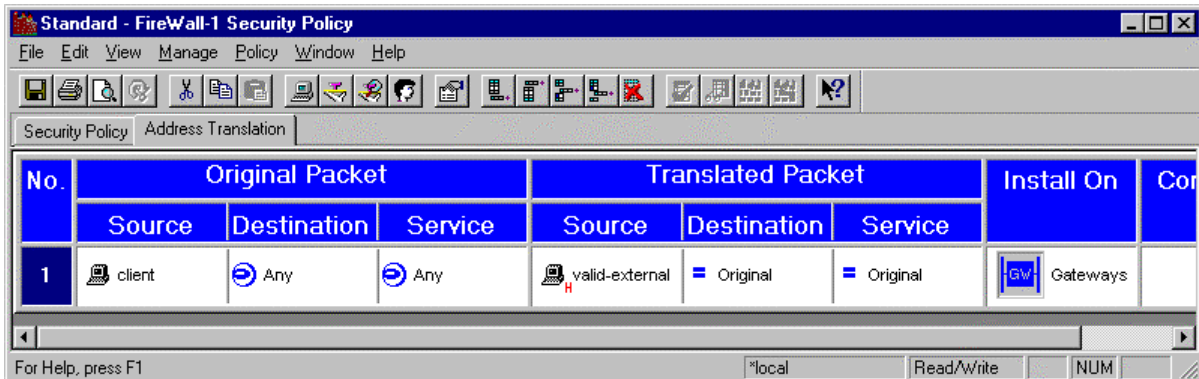
(uses the IP address of the Firewall converting from 193.168.100.112 → 199.199.164.2)

In order to allow the communications initiated from the Internal Host to communicate with the External Host using the FWXT_HIDE, four configurations steps are needed:

1. Create a “network object” in the Network Objects Manager named “client” for the IP Address of 192.168.100.112, Create another object with the name “valid-external” with the IP Address of 199.199.164.2. Do not use the “Address Translation” tab within this objects description, unless you read the pages following this quick reference.



2. Select the “Address Translation” Tab near “Security Policy” from the main window, and enter the “client” under the Original Packet “Source” field. Under the Translated Packet “Source” field enter “valid-external” using the “HIDE” method as shown below:



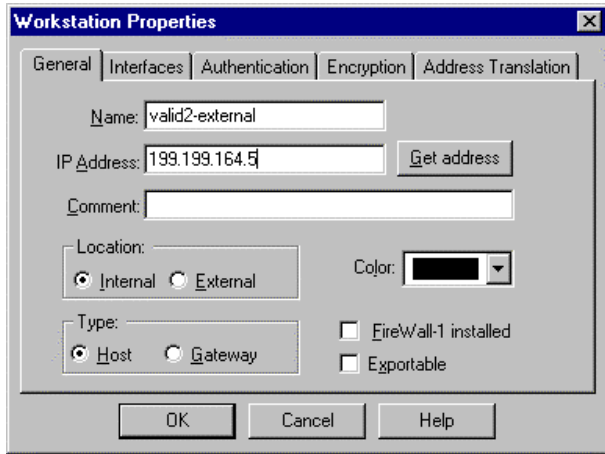
3. Make sure there is a rule entry that will accept this communications from the Internal Host to the External Host.
4. Install the Rule Base with the address translation configuration from the GUI (Policy Install) or command line:

fw load <rule filename> <firewall name or IP Address>

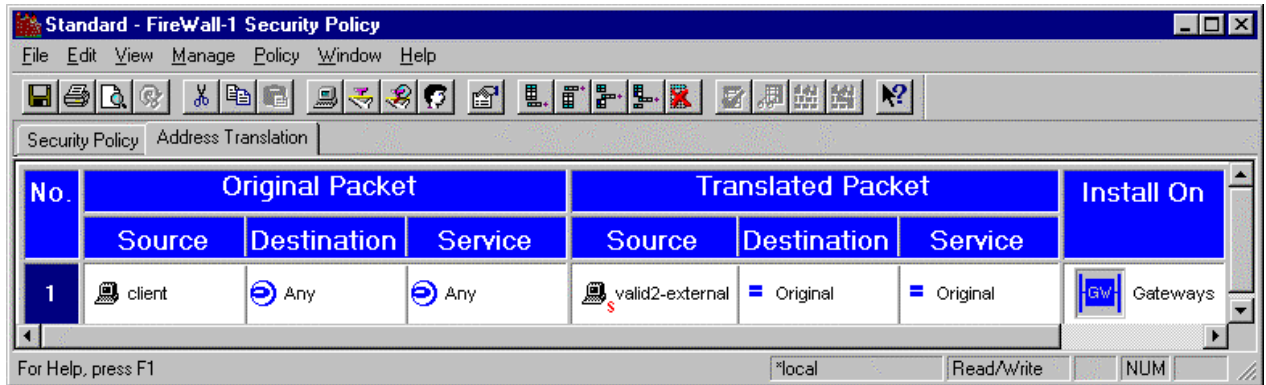
FWXT_SRC_STATIC Configuration Summary

(uses another legal IP address converting from 193.168.100.112 → 199.199.164.5)

In order to allow the communications initiated from the Internal Host to communicate with the External Host using the FWXT_SRC_STATIC configuration, five configurations steps are needed:



1. Create a “network object” in the Network Objects Manager named “valid2-external” for the IP Address of 199.199.164.5
2. Select the “Address Translation” Tab near “Security Policy” and enter the “client” under the Original Packet “Source” field. Under the Translated Packet “Source” field enter “valid2-external” using the “STATIC” method as shown below, and notice the “s” as opposed to the “h” under “valid2-external” with the Hide method:



3. Proxy ARP in the firewall or router before the firewall. Firewall configuration is shown below for NT and UNIX.

```

UNIX

arp -s 199.199.164.5 00:00:20:56:78:90 pub
    
```

```

WINDOWS NT

Create a file under C:\winnt\fw\state
File Name is “local.arp” with the following contents

199.199.164.5    00-00-20-56-78-90
    
```

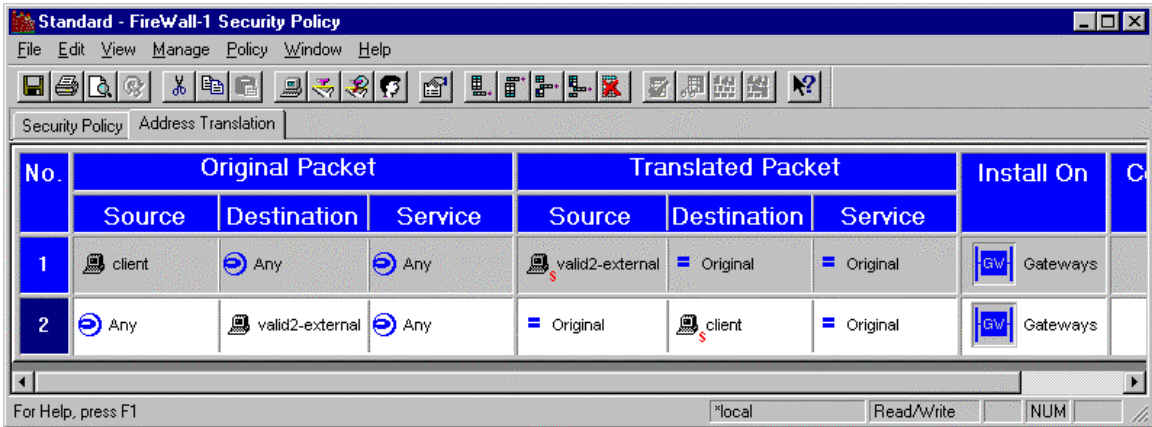
4. Make sure there is a rule entry that will accept this communications from the Internal Host to the External Host.
5. Install the Rule Base with the address translation configuration from the GUI or command line:
fw load <rule filename> <firewall name or IP Address>

FWXT_DST_STATIC Configuration Summary

(Converts from 199.199.164.5 → 193.168.100.112 in this direction)

In order to allow the communications initiated from the External Host to communicate with the Internal Host using the FWXT_DST_STATIC configuration, four configurations steps were needed:

1. Add the following entry to the Address Translation Tables as shown in Rule Number 2 with the Original Packet Destination being “valid2-external” and the Translated Packet Destination “Client”.



2. A proper routing entry in the Firewall to forward the Packet from 199.199.164.5 to 193.168.100.112
route add 199.199.164.5 193.168.100.112 1

```
UNIX  
route add 199.199.164.5 193.168.100.112 1
```

```
WINDOW NT  
route add -p 199.199.164.5 193.168.100.112  
The -p is for permanent
```

3. Make sure there is a rule entry that will accept this communications from the Internal Host to the External Host.
4. Install the Rule Base with the address translation configuration from the GUI or command line:
fw load <rule filename> <firewall name or IP Address>

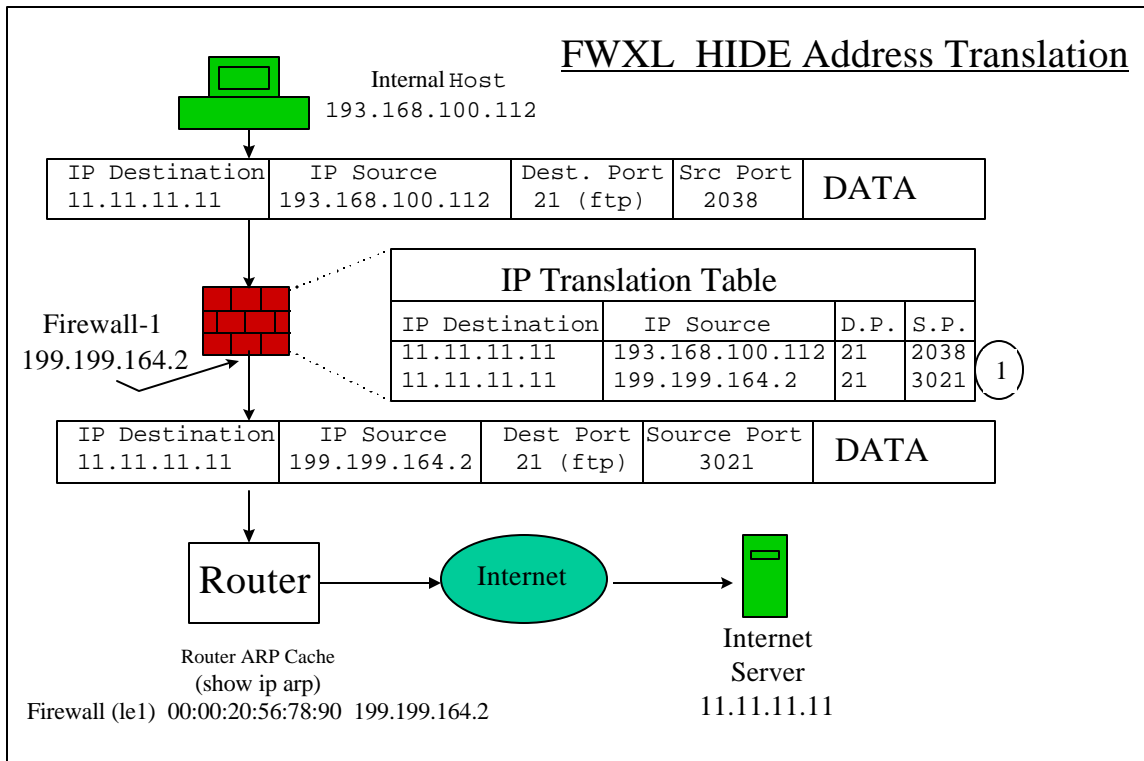
Detail Explanation of Address Translation

There are two ways to allow the communications which is initiated from the Internal Host to the External Host. FWXT_SRC_STATIC and FWXT_HIDE provide for this configuration method. Both options will be shown below:

FWXT_HIDE Configuration

The FWXT_HIDE translation will translate the Internal Host IP Address (193.168.100.112) to the IP address of the External Interface of the Firewall (199.199.164.2) as shown below.

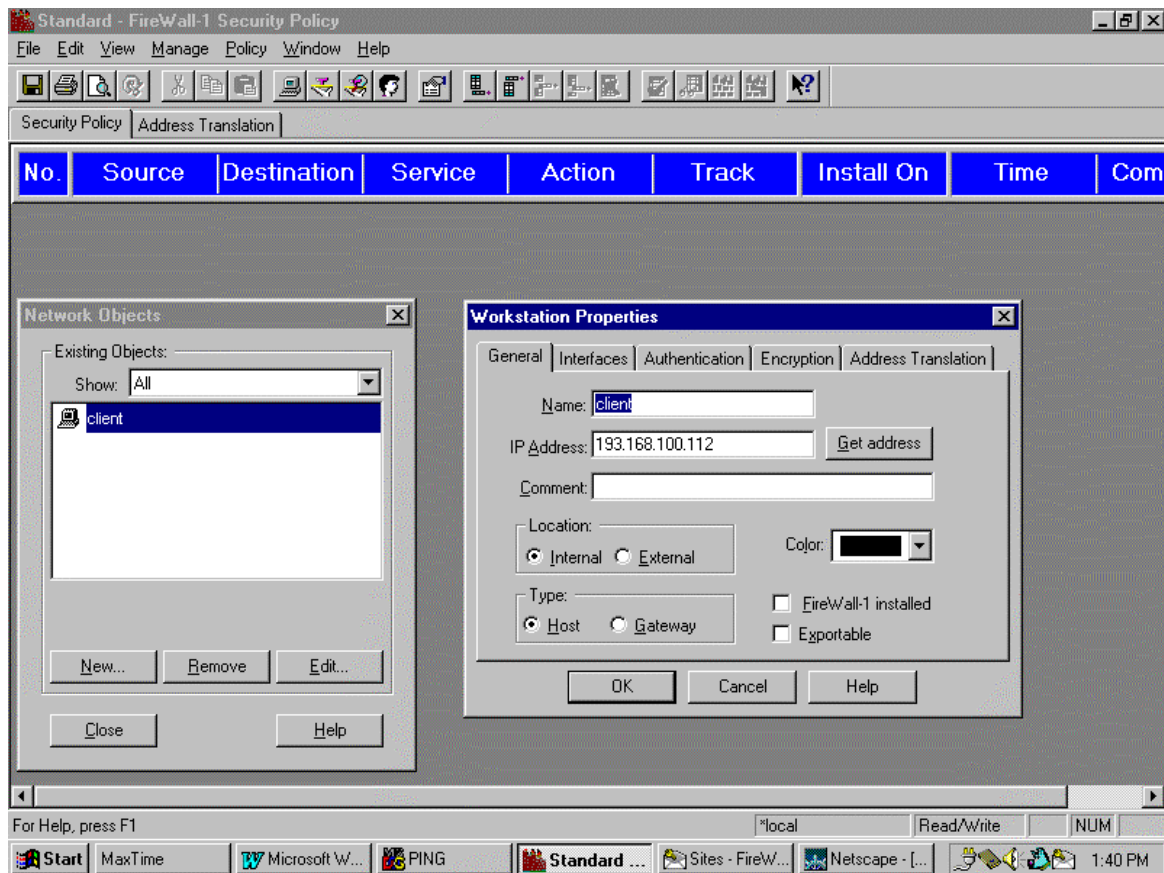
Figure 2 - FWXL_HIDE Diagram



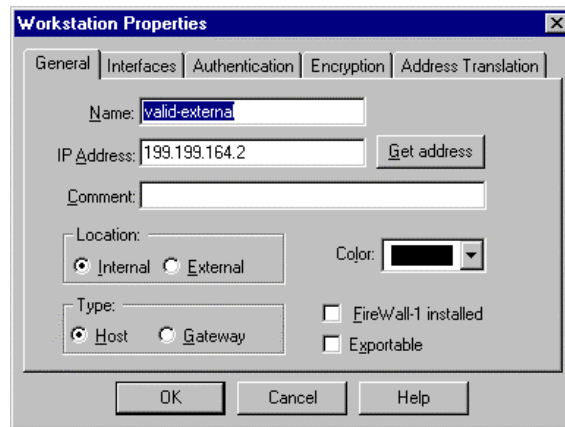
Joe's Note: Notice in this diagram that the router's arp cache will include the IP Address and the MAC address of the External Interface of the Firewall. This ARP entry will be placed in the router's cache automatically when the Firewall forwards the packet to the router, because the Firewall responds to the ARP Request of the Router. This is important so that the return packet from the External Server can be forwarded to the External Interface of the Firewall (199.199.164.2) with the appropriate MAC address (00:00:20:56:78:90).

Firewall Configuration

First, create the "internal-host" object by selecting "Manage" → "Network Objects" → "New" → "Workstation" as shown below from the Security Policy Editor. Type in the following IP address 193.168.100.112 and the name of "client" for this Internal Host object.



Second create another object, in addition to the firewall object, that will represent the external IP address of the firewall. Type in “Manage”→ “Network Objects” → “New” → “Workstation” as shown below from the Security Policy Editor. Next, enter in the name of “valid-external” for this object and the IP address 199.199.164.2.

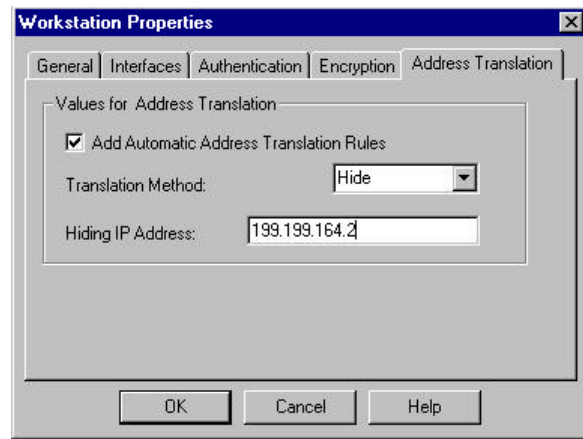


Now there are two methods to configure the address translation rule from within the GUI,

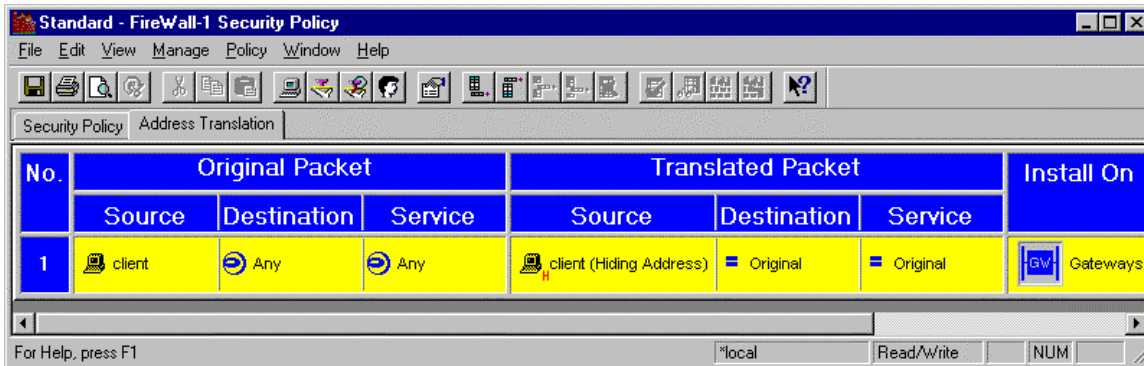
1. Let the Security Policy Editor perform the address translation for you. This method could be easier in the beginning, but you will not have the flexibility to modify the address translation tables after this has been create by the system for you. This is performed within the definition of the network object.
2. Create a separate rule-base for the address-translation table under the Security Policy Editor tab “Address Translation”, similar to the security policy. This method allows you to customize your address translation entries even after this rule has been created.

Method 1.

Select “Network Objects”→ Highlight “Client” → “edit”
Now click on the “Address-Translation” tab with this object, and select “Add Automatic...”
Now select “Hide”, and type in the IP Address of 199.199.164.2
Click → “OK” and
“Close” the “Networks Object Manger”



To verify that the address-translation rule was effectively created, select the tab “Address Translation” next to “Security Policy” from within the GUI. The following screen should appear.

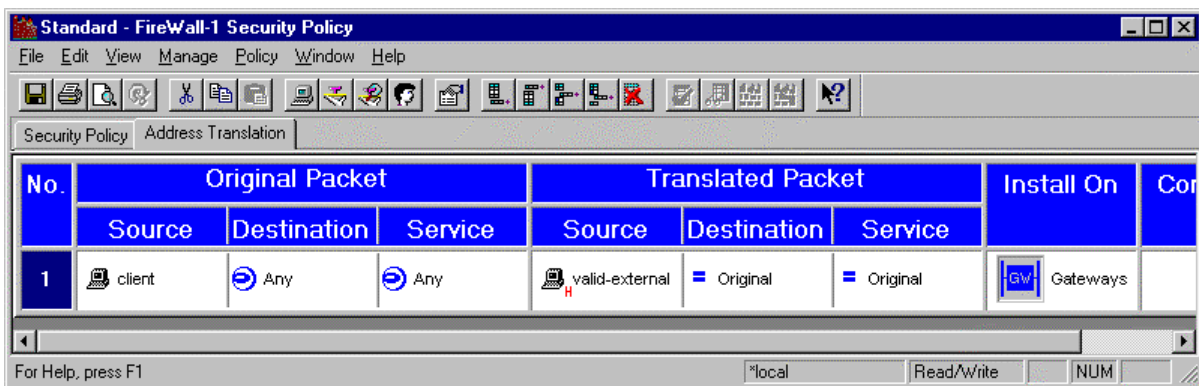


Notice that any packet with a source address of “Client” (193.168.100.112) will be modified to the Translated Packet of “Client” (Hiding address of 199.199.164.2). This rule was automatically created by the system, and can’t be modified unless you go the “Client” network object and de-select “Add Automatic Address Translation Rules”. If you have many of these rules, which are position dependent, you can modify their order unless you do this manually.

Method 2.

De-select the “Add Automatic...” from the “Client” object and click OK.

Next, select the “Address Translation” Tab near “Security Policy” from the main window, and enter the “client” under the Original Packet “Source” field. Under the Translated Packet “Source” field enter “valid-external” using the “HIDE” method as shown below:



Joe's Note: After configuring the Address Translation, you MUST install the Rule Base to the Firewall. This is because the address translation table will get compiled into the Inspect Script, and then loaded into the Firewall Virtual Inspection Machine. The loading of the rule base could be done manually as shown below, or through the GUI:

```
fw load <rule filename without .W> <firewall name or IP Address>
fw load rule23 firewall
```

After the Rule Base and the Address Translation Tables have been installed and running in the Firewall, communications can occur in the direction initiated from the Internal Host going out to the External Host. The firewall now understands by the source and destination port numbers how to uniquely identify which internal host to direct the packets back to. In our case, the ports of 2038 and 3021 create this binding with the IP Address of 193.168.100.112 in the address translation tables.

Joe's Note: To look at the currently running address translation tables you can use the "/etc/fw/bin/fw tab" command. In the response to this command, the specific table name to look for is the "table_target_list2" as shown below:

```
----- table_target_list2 -----
...
<00010001, 00000002, c1a86470, c1a86470, c7c7a402, 00000000, 00000000>
...
```

Notice that the addresses are viewed in hexidecimal
193.168.100.112 = c1.a8.64.70
199.199.164.2 = c7.c7.a4.02

FWXT_HIDE Configuration Summary

In order to allow the communications initiated from the Internal Host to communicate with the External Host using the FWXT_HIDE, three configurations steps are needed:

1. Add the "Client" to the Source Address of the Original Packet and the "valid-external" to the Source Address of the Translated Packet to the Main Address Translation window with the "hide" option.

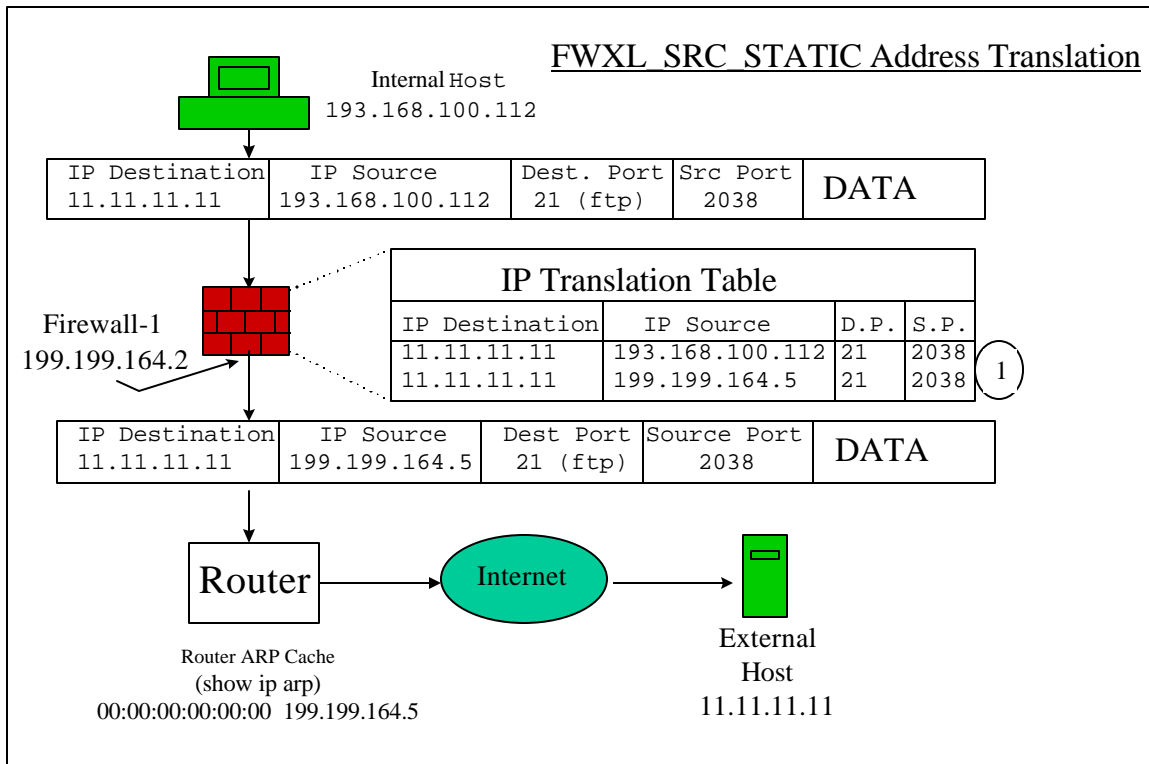
Alternatively, use the Address Translation Tab within the "Client" object's configuration menu. Select "Add Automatic Address Translation Rule", use the "Hide" Translation Method, and the Hiding IP address of 199.199.164.2.

2. Make sure there is a rule entry that will accept this communications from the Internal Host to the External Host.
3. Install the Rule Base with the address translation configuration from the GUI or command line:
fw load <rule filename> <firewall name or IP Address>

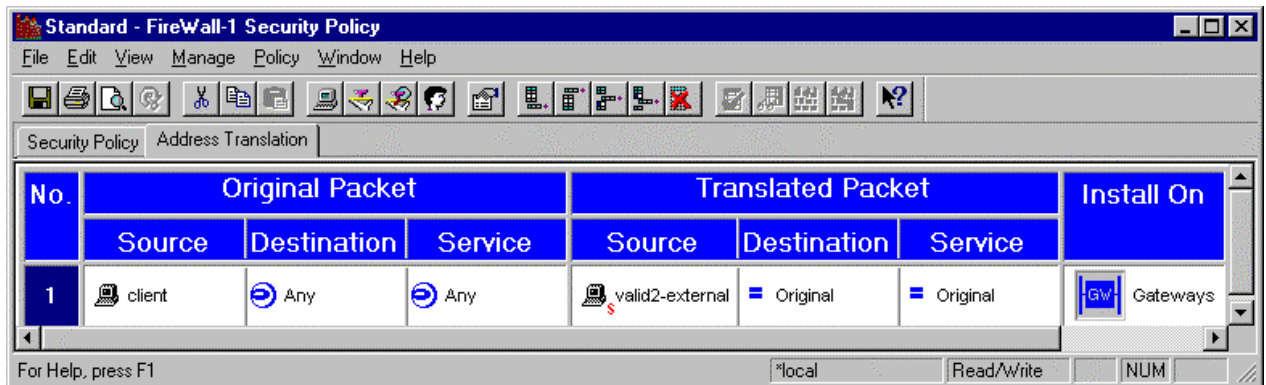
FWXT_SRC_STATIC Configuration

As an alternate method to the FWXT_HIDE, the Address Translation Software could be configured using the FWXT_SRC_STATIC. The main difference between the FWXT_HIDE and the FWXT_SRC_STATIC is that the FWXT_HIDE can use the external IP address of the firewall, whereas the FWXT_SRC_STATIC uses another legal IP address. In our example above, lets assume that another valid IP address to the Internet Exists which is 199.199.164.5. This address will be used for the FWXT_SRC_STATIC entry as follows:

Figure 3 - FWXL SRC STATIC Diagram



To create this configuration, use either Method 1 or Method 2 describe above and make sure the final entry looks like the following diagram in the main Address Translation Utility:



The above entry tells the Firewall to take the original source address of 193.168.100.112 and change it to 199.199.164.5 upon exiting the external interface of the Firewall.

Joe's Note: This utility also allows you to specify IP Address Ranges, so you could have an address range of 193.168.100.112 through 193.168.100.212 be translated to the correlating addresses of 199.199.164.5 through 199.199.164.105. This can be configured using the "Address Range Object" within the Network Object Manager.

So far the configuration of the Firewall in version 2.0 will be OK in order to take the packet from the Internal Interface with a source address of 193.168.100.112, and translate the IP source address to 199.199.164.5. It will then send this packet out of the External Interface of the Firewall to the destination of the External Host (11.11.11.11). Once this packet gets to the External Host, it will reply with the correct corresponding packet. This packet will traverse the Internet, and be received by the router. The router will then send an ARP Request for the physical address that responds with 199.199.164.5. No one will respond to the this Request at this point, until one more configuration entry is done.

Joe's Note: Notice here that in the configuration so far, there is no way for the return packet from the External Host to be sent to the firewall because the ARP resolution for 199.199.164.5 is not being answered by anyone. This is because we need to "Proxy ARP" for the address of 199.199.164.5. In this situation, there is one of two ways to handle this:

1. Statically add the ARP entry into the Firewall
2. Statically add the ARP entry into the router

Statically add the ARP entry into the Firewall

To add the ARP entry in the firewall type in the following command for the UNIX Platform:

```
arp -s 199.199.164.5 00:00:20:56:78:90 pub
```

On the NT Platform, a file called "local.arp" must be created under the \$fwdir/state directory. This is usually located under C:\winnt\fw\state if the default installation parameters have been taken during the installation process. The format of this file is as follows:

IP Address	MAC Address
------------	-------------

So in our example, the local.arp file would look like this with a "-" between MAC address characters:

199.199.164.5	00-00-20-56-78-90
---------------	-------------------

This means when someone is lookup for the IP address of 199.199.164.5, talk to the External Interface of the Firewall (00:00:20:56:78:90). This will allow the ARP Request packet for 199.199.164.5 to be resolve by the Firewall.

After adding the Proxy ARP entry into the Firewall, the full communications from the Internal Host to the External Host is completed from an IP Connectivity point of view.

WINDOWS NT

If you are using the Windows NT platform, you can verify that the local.arp file is installed on the Firewall correctly, by looking at the "arp_table" by using the "fw tab" command. The results should look similar to this:

```
----- arp_table -----  
<c7c7a405; 00002056, 00007890, 00000000>
```

Joe's Note: Remember that the Address Translation is still subject to the Rule Base of the Firewall. This means that a correct rule should be entered that allows for the communications of the Internal Host to the External host.

FWXT_SRC_STATIC Configuration Summary

In order to allow the communications initiated from the Internal Host to communicate with the External Host using the FWXT_SRC_STATIC configuration four configurations steps are needed:

1. Create an object for the address of 199.199.164.5 named “valid2-external”
2. Add the “Client” to the Source Address of the Original Packet and the “valid2-external” to the Source Address of the Translated Packet to the Main Address Translation window with the Static option.

Alternatively, use the Address Translation Tab within the “Client” object’s configuration menu. Select “Add Automatic Address Translation Rule”, use the “Static” Translation Method, and the IP address of 199.199.164.5. This will create two rules, one for FWXT_SRC_STATIC and one for FWXT_DST_STATIC.

3. Proxy ARP in the firewall or router.

```
UNIX : arp -s 199.199.164.5 00:00:20:56:78:90 pub
NT: local.arp file with “199.199.164.5 00-00-20-56-78-90 “
```

4. Make sure there is a rule entry that will accept this communications from the Internal Host to the External Host.
5. Install the Rule Base with the address translation configuration on the Firewall.

```
fw load <rule filename> <firewall name or IP Address>
```

WINDOWS NT

If you need to find out the MAC Address of the adapter for a Windows NT System, type in ipconfig /all as shown below:

```
C:\windows\IPCONFIG /all
```

```
Windows NT IP Configuration
```

```
....
....
```

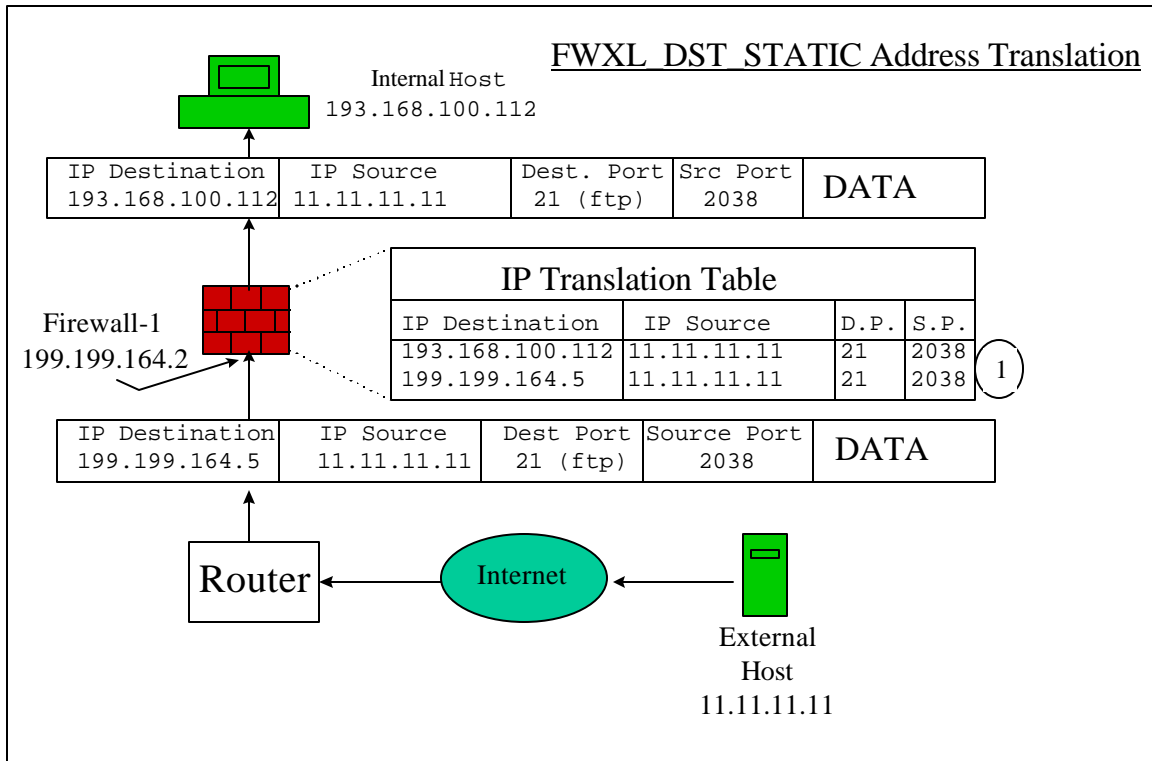
```
Ethernet adapter :
```

```
Description . . . . . : le0 Ethernet Adapter
Physical Address. . . . . : 00-00-20-56-78-90
DHCP Enabled. . . . . : No
IP Address. . . . . : 199.199.164.2
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 199.199.164.1
```

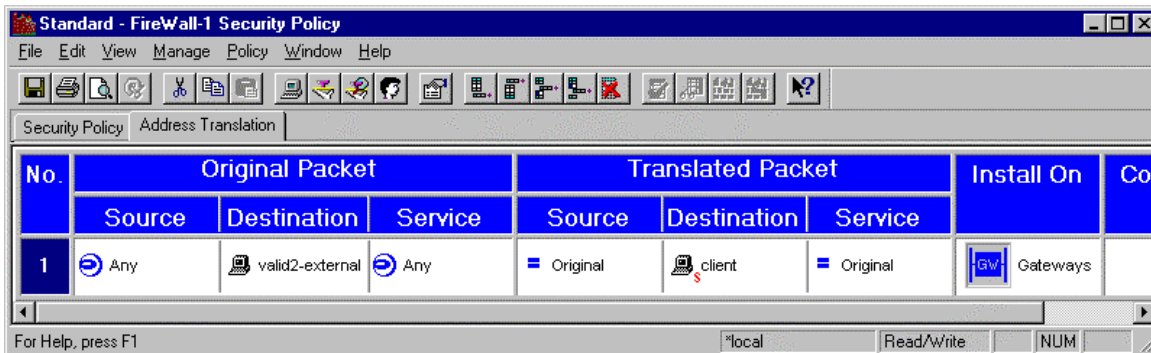
```
....
....
```

This next section deals with communications initiated from the External Host going to the Internal Host. This could be someone using FTP to connect to your company's FTP Server to download some information. For this type of configuration, we will use the FWXT_DST_STATIC configuration entry in address translation. For example, suppose that the Internal Host is also the FTP Server to allow Internet Users to download information, but we want the External Host to communicate with the IP address of 199.199.164.5 for security reasons. This configuration is shown below:

Figure 4 - FWXL DST STATIC Diagram



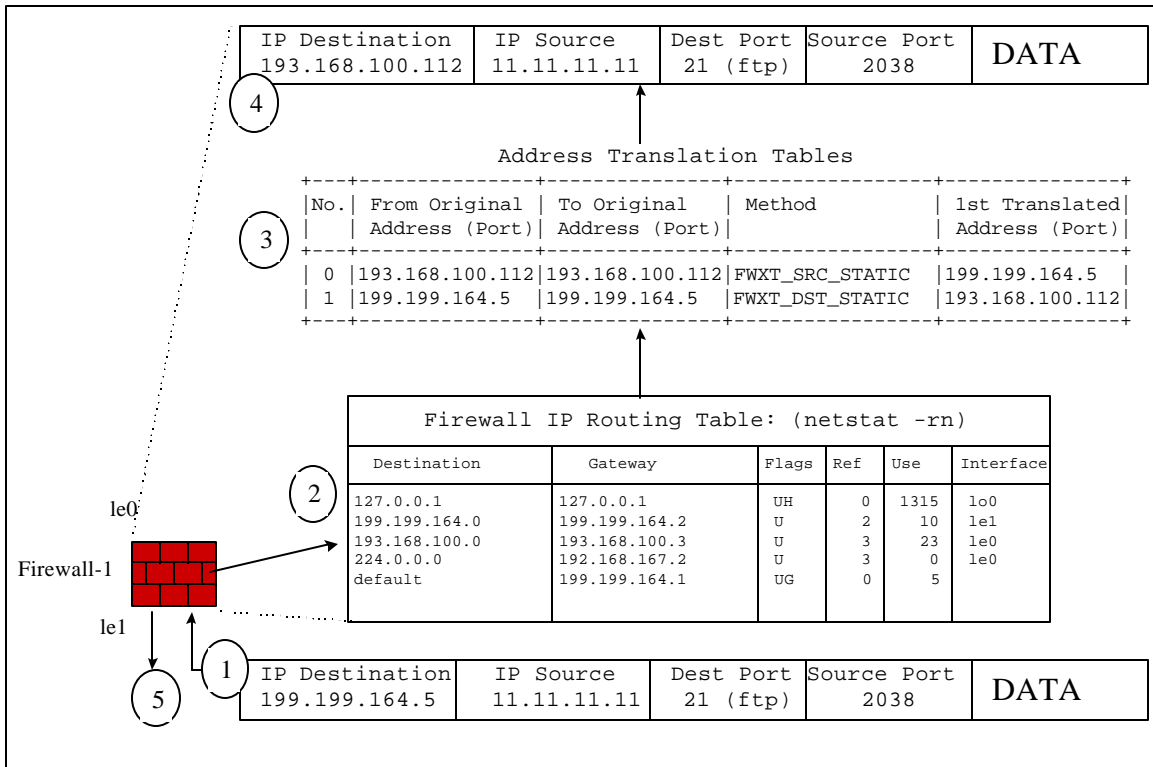
In this configuration when an External Host wants to communicate with an Internal Host, create the following entry in the Address Translation Utility as shown below.



Rule 1 tells the Firewall that when you see the IP Address of 199.199.164.5 in the destination field of the packet, convert this address to 193.168.100.112 and send it out the Internal Interface of the Firewall. In order to accomplish this, a better understanding of the Address Translation Process is needed at this point.

For this configuration, where both IP Networks (199.199.164.0 and 193.168.100.0) are directly attached to the Firewall, we need to add one more configuration step that will be described below. The address translation processes for FWXT_DST_STATIC within the Firewall-1 will be described in more detail for the address translation table shown above.

Figure 5 - Address Translation Routing Process



1. The packet is route over the Internet from the External Host, through the Router, into the Firewall-1 Host
2. The Firewall-1 host looks into the Routing Tables to see if the destination network address of 199.199.164.0 can be reached. It found an entry. This entry says to transmit packets with a destination address of 199.199.164.0 to the le1 physical interface. The packet now proceeds to the next step.
3. The address translation tables now modifies the destination address of the packet according to rule number one. This says take the address of 199.199.164.5 and replace it with the address of 193.168.100.112, which it does.
4. The packet has been modified with the new destination address, and is now ready to be transmitted
5. The packet is transmitted out the physical interface that was determined in step number 2 in the routing tables.

Joe's Note: The packet was sent out the same physical interface that it arrived on because the routing entry specified this information:

```
199.199.164.0 199.199.164.2 U 2 10 le1
```

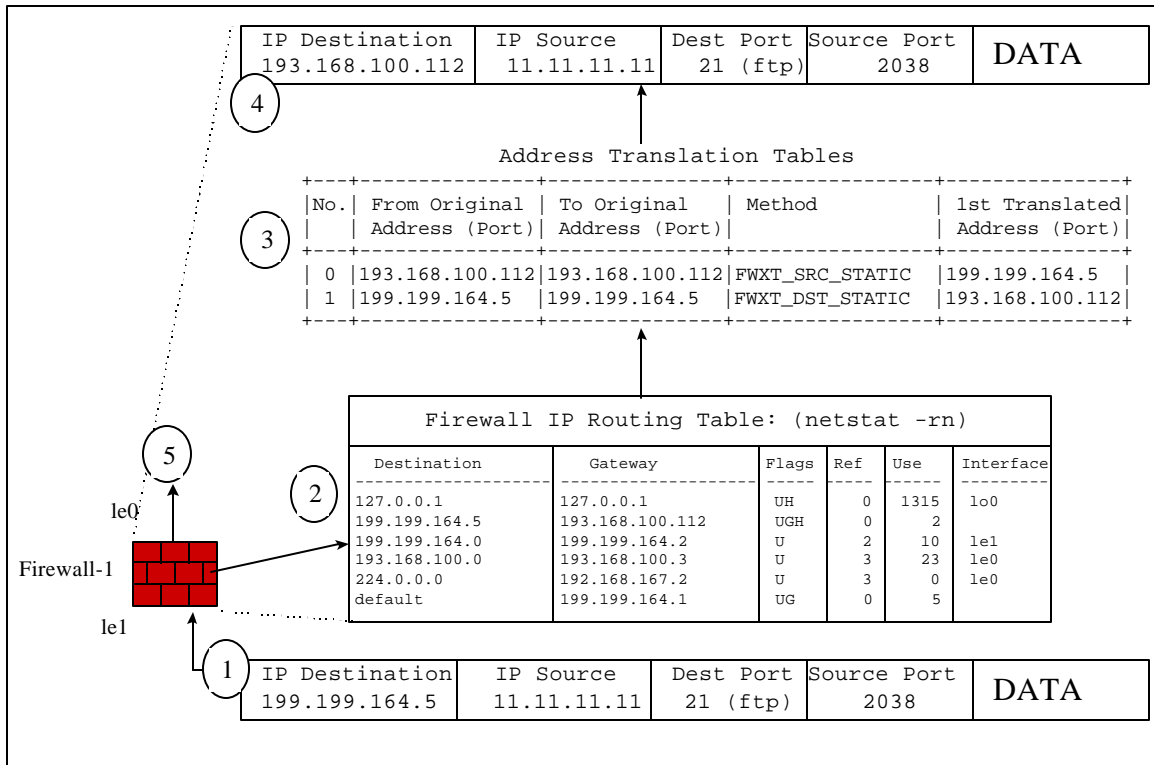
When using the FWXT_DST_STATIC make sure there is a route to force the packet to the correct physical interface. You need this there because the Address Translation of the Packet occurs after the Internal Routing process of the firewall, but before the packet gets transmitted on the wire.

To correct this situation, we need to add another route entry into the Firewall as follows:

```
route add 199.199.164.5 193.168.100.112 1 (UNIX)
route add -p 199.199.164.5 193.168.100.112 (WINDOWS NT)
```

This entry is now shown in the routing tables of the diagram below:

Figure 6 - Address Translation Routing Process Stage 2



1. The packet is route over the Internet from the External Host, through the Router, into the Firewall-1 Host
2. The Firewall-1 host looks into the Routing Tables to see if the destination network address of 199.199.164.0 can be reached. It found an entry for this specific address of 199.199.164.5. This entry says to transmit packets with a destination address of 199.199.164.5 to the le0 physical interface side of the Firewall. The packet now proceeds to the next step.
3. The address translation tables now modifies the destination address of the packet according to rule number one. This says take the address of 199.199.164.5 and replace it with the address of 193.168.100.112, which it does.
4. The packet has been modified with the new destination address, and is now ready to be transmitted
5. The packet is transmitted out the physical interface that was determined in step number 2 in the routing tables which is le0, the correct side of the Firewall.

FWXT_DST_STATIC Configuration Summary

In order to allow the communications initiated from the External Host to communicate with the Internal Host using the FWXT_DST_STATIC configuration four configurations steps were needed:

1. Add the “valid2-external” to the Destination Address of the Original Packet and the “Client” to the Destination Address of the Translated Packet to the Main Address Translation window with the Static option.

Alternatively, use the Address Translation Tab within the “Client” object’s configuration menu. Select “Add Automatic Address Translation Rule”, use the “Static” Translation Method, and the IP address of 199.199.164.5. This will create two rules, one for FWXT_SRC_STATIC and one for FWXT_DST_STATIC.

2. A proper routing entry in the Firewall to forward the Packet from 199.199.164.5 to 193.168.100.112
route add 199.199.164.5 193.168.100.112 1 (UNIX)
route add -p 199.199.164.5 193.168.100.112 (WINDOWS NT)
3. Make sure there is a rule entry that will accept this communications from the Internal Host to the External Host.
4. Install the Rule Base with the address translation configuration on the Firewall.
fw load <rule filename> <firewall name or IP Address>