

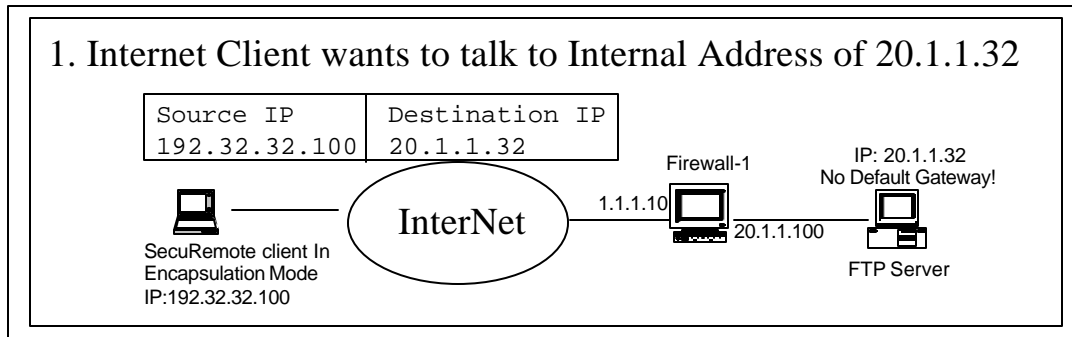
# **CheckPoint Software Technologies LTD.ä**

## ***How to Hide the Source Address of a client on the Internet behind the Firewall's Internal Address***

**Authored By: Lewis and Joe  
Date Published: November 10, 1998  
Rev 1.1**

The Purpose of this Document is to describe how to "Hide" the original source address of a packet behind the Firewalls Internal Network Interface. This will allow a path back to the original Internet Client regardless of the Internal Routing scheme used (ie. If there are no default gateways configured). This network design will be configured with SecuRemote Encapsulation turned on.

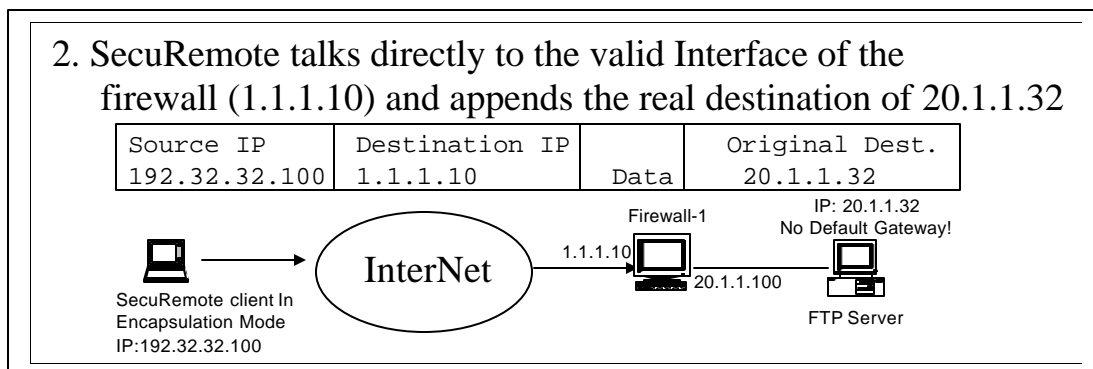
Given the Network Diagram shown below, consider the following:



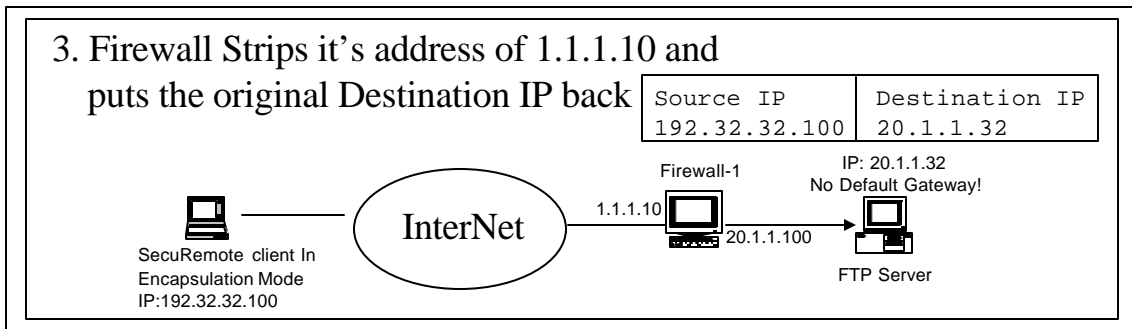
There are two problems to overcome here:

1. If the Internal Address of 20.1.1.32 is not a published Internet Address (like 10.0.0.0 networks), this problem is solved by "encapsulating" the SecuRemote connection to the Firewall first, and then route the packet to the Internal Address of 20.1.1.32.
2. The next problem with this type of network is that the Internal FTP Server of 20.1.1.32 does not have a route back to the Internet. When the SecuRemote client's packet arrives on the Internal Network, it will still have the Source Address of 192.32.32.100. This is a problem, because the FTP Server does not have a route back to the 192.32.32.0 network (or any Internet Address for that matter) as shown below.

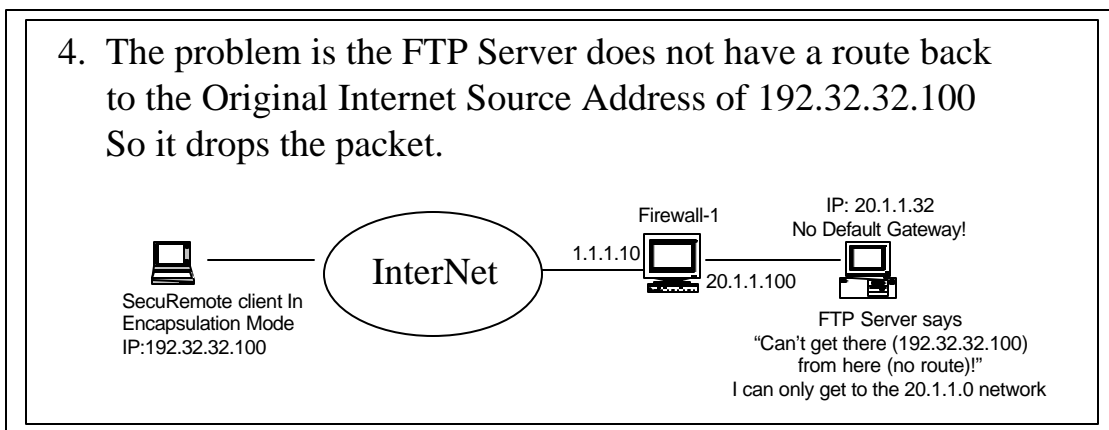
To overcome problem number 1, SecuRemote can encapsulate connections directly to the Firewall's Internet Address of 1.1.1.10. SecuRemote appends the original Destination Address of 20.1.1.32 to the end of the packet as shown below.



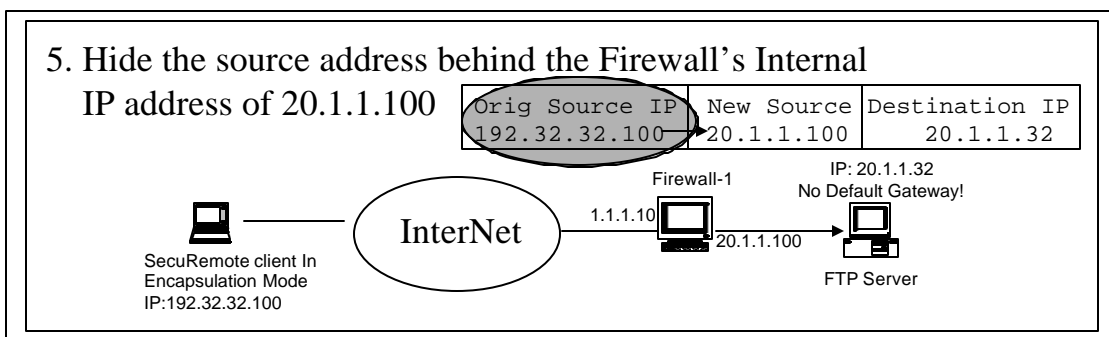
The Firewall will now strip its address of 1.1.1.10, and put the original address back in place. The Firewall then routes the packet to the FTP Server of 20.1.1.32



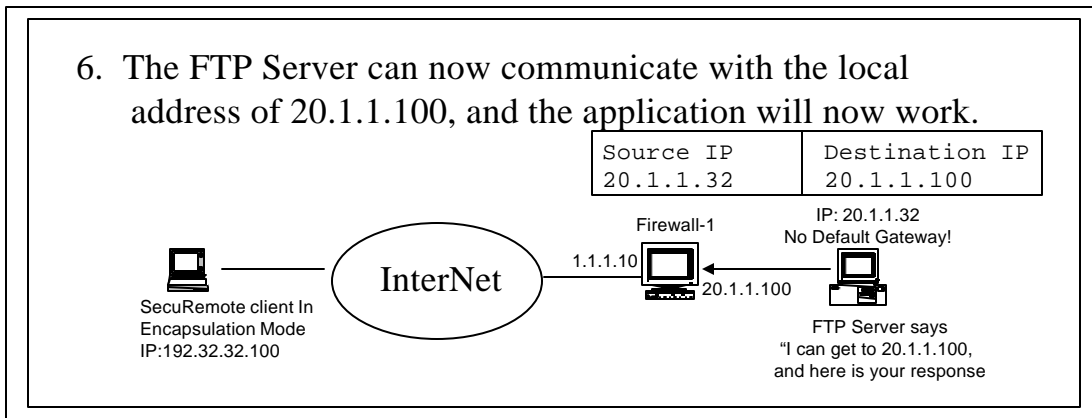
Once this packet gets to the FTP Server, the FTP Server doesn't have a route back to any Internet Address including 192.32.32.100, so the packet is simply dropped.



The solution to this problem is to hide the original source address behind the firewall's Internal Interface as shown below. This configuration is done on the Firewall Address Translation editor.



By changing the source address to 20.1.1.100, the FTP Server can then respond to the FTP Request as shown below:



The Configuration of how to “hide” the Internet behind the Firewall’s Internal Address are described below:

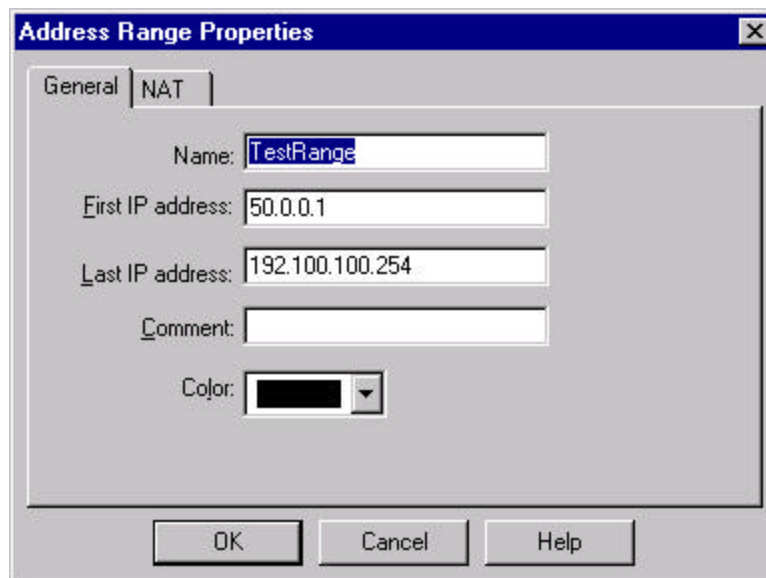
One of the important elements to hiding the SecuRemote clients is to create a range of IP Addresses for all non-internal networks, since you don't know what address the SecuRemote Internet client will be assigned. This is how the address translation rule will match the SecuRemote client's IP address.

To Create this Network Range, first click on the "**Address Translation**" Tab within the main window of the Security Policy Editor.

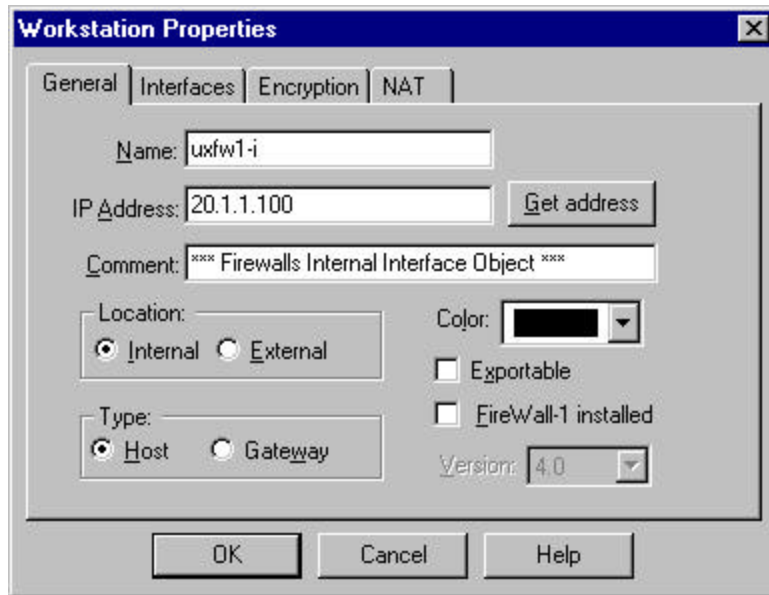
Next click on **Manage → Network Objects**

Now click on **New → Address Range**

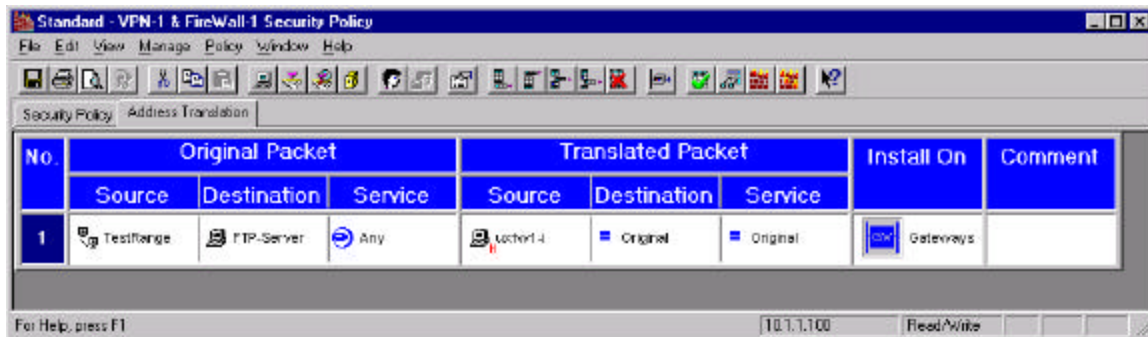
Created a Network Range object that does not conflict with the IP addresses of the ANY of the Firewall’s Interfaces (Which Is Critical) or your Internal Networks. This Range will represent the Internet based SecuRemote source addresses. You can generally identify what your source addresses of the SecuRemote Clients by the firewall-1 logviewer, or by “snooping” the Internet Interface of the firewall. In this case, the testrange object can not be used in the Security Policy, but will only be used by the Network Address Translation (NAT) Tab.



You must also create a **Manage -> Network Objects -> New -> Workstation** object to represent the internal interface for the NAT rule. Just make this a simple workstation object without Gateway or Firewall-1 Installed checked.

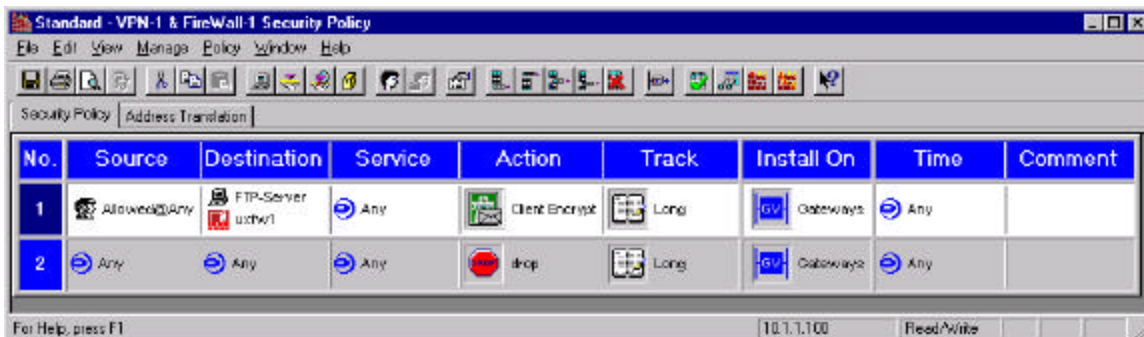


Next created the NAT rule:

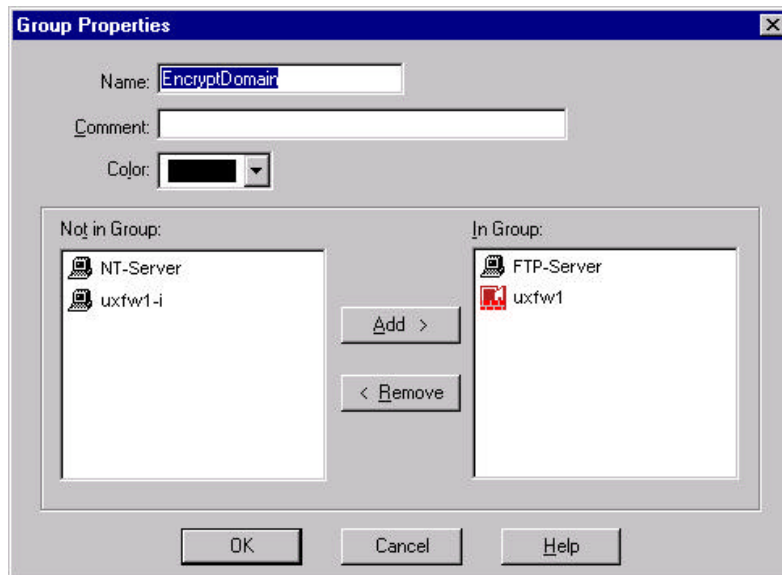


**NOTE:** The object *uxfw1-I* represents the Internal IP address of the Firewall 20.1.1.100

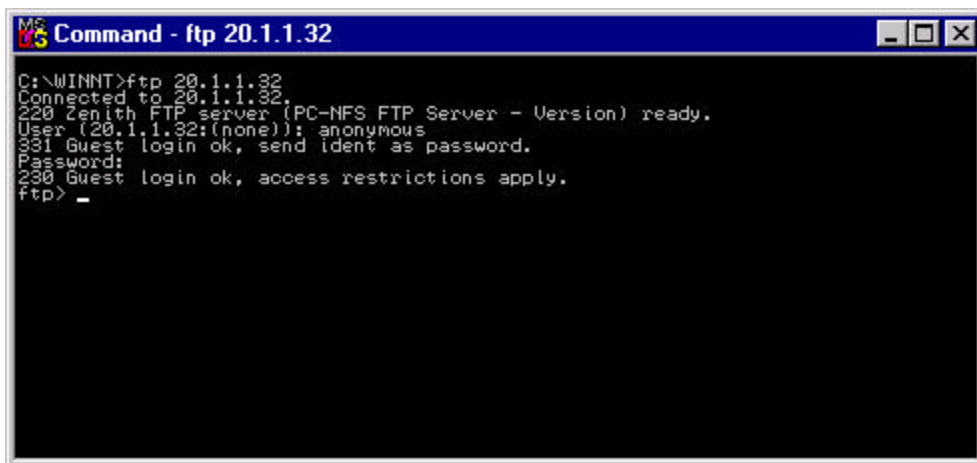
The Rule Base looks like this:



The Encryption Domain Object; (Which Included The Firewall Object & the FTP Server )



Now try and FTP from the SecuRemote client to the FTP Server, which has no route back to the SecuRemote client. The SecuRemote source address in the packets is being hidden behind the internal interface of the firewall.



The log entries reflect the proper communication:

| No. | Date      | Time     | Inter. | Origin | Type    | Action      | Service | Source        | Destination | Proto. | Rule | S_Port | User  |
|-----|-----------|----------|--------|--------|---------|-------------|---------|---------------|-------------|--------|------|--------|-------|
| 0   | 28Oct1998 | 16:42:17 | dae... | uclwrt | control | ct          |         |               |             |        |      |        |       |
| 1   | 28Oct1998 | 16:42:17 | dae... | uclwrt | control | ct          |         |               |             |        |      |        |       |
| 2   | 28Oct1998 | 16:42:33 | dae... | uclwrt | log     | decrypt     | ftp     | 192.32.32.100 | FTP-Server  | tcp    | 1    | 1082   | lewis |
| 3   | 28Oct1998 | 16:42:45 | dae... | uclwrt | log     | authcrypt   |         | 192.32.32.100 |             |        | 0    |        | lewis |
| 4   | 28Oct1998 | 16:42:48 | dae... | uclwrt | log     | key install |         | 192.32.32.100 | FTP-Server  | ip     | 0    |        |       |
| 5   | 28Oct1998 | 16:42:50 | dae... | uclwrt | log     | decrypt     | ftp     | 192.32.32.100 | FTP-Server  | tcp    | 1    | 1082   | lewis |
| 6   | 28Oct1998 | 16:43:00 | dae... | uclwrt | log     | key install |         | 192.32.32.100 | uclwrt      | ip     | 0    |        |       |
| 7   | 28Oct1998 | 16:43:04 | dae... | uclwrt | log     | decrypt     | telnet  | 192.32.32.100 | uclwrt      | tcp    | 1    | 1084   | lewis |

This particular SecuRemote client was using IKE Encapsulation, which is why you see the “key Install” log entry. Any SecuRemote Encryption Scheme will work as well including FWZ.