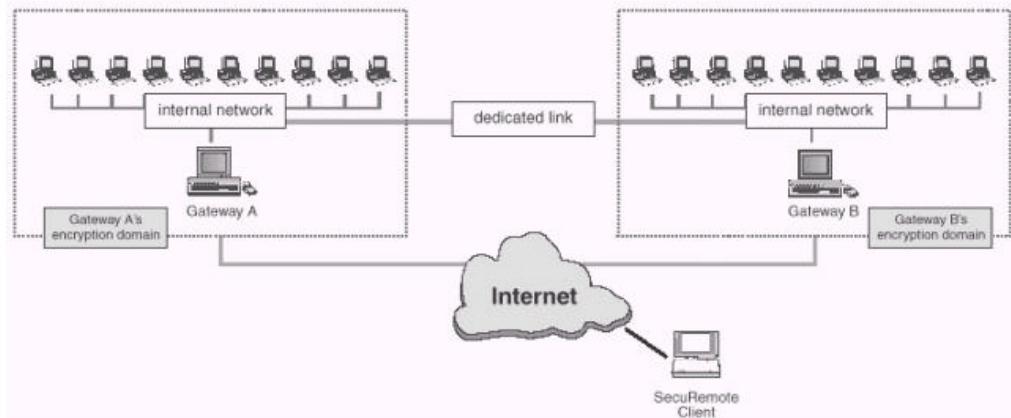


# **CheckPoint Software Technologies LTD.ä**

## ***How to Configure the Firewall to use Multiple Entry Point (MEP) & Overlapping Encryption Domains***

**Event: Partner Exchange Conference**  
**Date: November 16, 1999**  
**Revision 1.1**  
**Author: Bill Cooper**  
**Credits: Victor Bojorquez, Dave Bousfield**

**Diagram of network:**



**Action:** Demonstrate the MEP functionality of FW-1 4.1. SecuRemote will prefer encrypting with Gateway A. When Gateway A is not responding, it will encrypt with Gateway B.

**Note:** Gateway A and Gateway B are not synchronized.

## Configuration overview:

1. Install FireWall-1 4.1 on Gateways A & B
2. Ensure proper routing on network
3. Enable backup gateway for SecuRemote connections
4. Enable IP pool NAT if needed & create IP pool
5. Ensure gateways will not respond to unauthenticated cleartext topology requests
6. Create objects for Gateways A & B and configure workstation properties
7. Configure SecuRemote

## Configurations details:

1. Install FireWall-1 4.1 on Gateways A & B

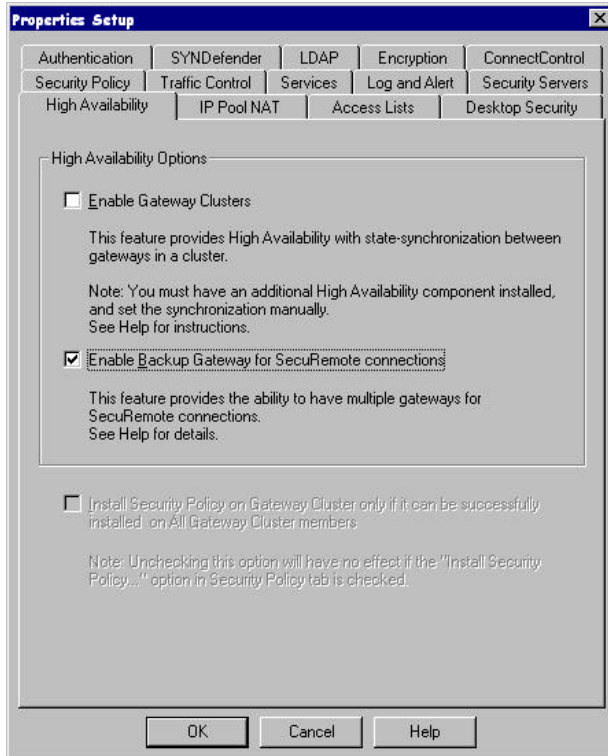
Install FireWall-1 4.1 on Gateways A & B. Configure encryption settings.

2. Ensure proper routing on network

In the network diagram provided, the routing must be configured to properly route packets around either Gateway A or B in the event of a failure.

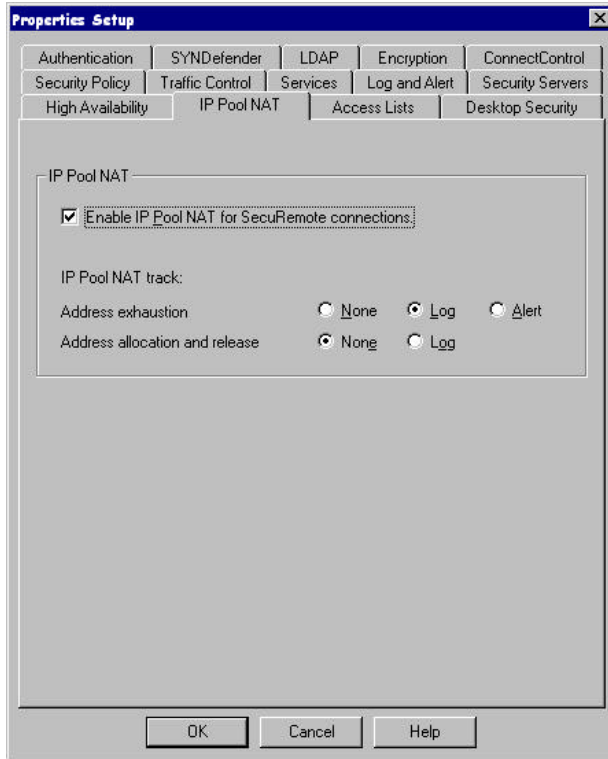
3. Enable backup gateway for SecuRemote connections

From the Policy Editor, select the 'Policy', 'Properties...' menu. Now select the 'High Availability' tab and check the box next to 'Enable Backup Gateway for SecuRemote Connections'.



#### 4. Enable IP pool NAT if needed

To do this, access the 'Policy', 'Properties...' menu. Select the 'IP Pool NAT' tab. Check the box next to 'Enable IP Pool NAT for SecuRemote connections'.



In an Asymmetric routing environment, there is a chance that after a SecuRemote connection enters the network through Gateway A it will be routed back out to the Internet through Gateway B. Since Gateway B is not aware of the SecuRemote session, the connection will not be accepted. As a solution IP pool Network Address Translation (NAT) is used. On each of the gateways, an IP pool is assigned for SecuRemote connections. This IP pool is created in the network objects manager by selecting 'New', 'Network...'. The pool can also be created as an 'address range'. If you select an "address range" or a network that is local to the firewall's internal Interface, then you will have to "Proxy -ARP" for the addresses that are define in the range. This is why we don't suggest a local network, but another IP network not on the Firewall's local interface. The network or address range should probably be chosen from RFC 1918, which details private network address space. The pools should not conflict with existing addresses from anywhere else on the Internal Network and can not overlap at all. To get this to work I had to use the same subnet mask throughout the network.

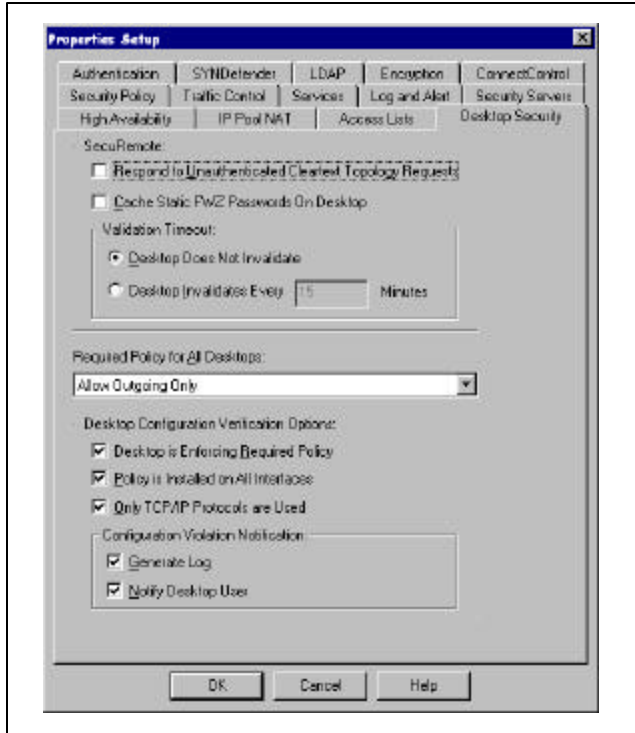
As a SecuRemote connection goes through a gateway to the internal network, the gateway assigns the client an address from the IP pool. The packet is then translated such that the source address of the packet becomes the address assigned from the SecuRemote IP pool. By translating the source address of SecuRemote connections as they enter the internal network, we can use routing to force SecuRemote packets to go out through the proper gateway.

Example: a connection originates at a remote laptop, IP 199.1.1.1. A SecuRemote connection is initially established with Gateway A. As the connection passes through Gateway A to the internal network, the source address of the packet is translated to an address from the SecuRemote IP NAT pool of Gateway A. For this example we'll assume that Gateway A's IP NAT pool is the network 10.1.0.0, mask 255.255.0.0, and Gateway B's IP NAT pool is network 10.2.0.0, mask 255.255.0.0. For this laptop, all SecuRemote packets will have the source address translated from 199.1.1.1 to 10.1.0.1 as they pass through Gateway A onto the internal network. With routing properly configured, all packets destined for network 10.1.0.0 will be routed back through Gateway A, thereby eliminating the chance that packets will be misdirected to Gateway B. If SecuRemote is no longer able to communicate with Gateway A, it will establish a new VPN connection with Gateway B. Now as packets from this connection are passed through Gateway B, the source address will be translated to an address from Gateway B's IP NAT pool, say 10.2.0.1. Again, using routing we can force all packets destined for network 10.2.0.0 back through Gateway B, which will know what to do with them. **To set up this routing scheme just make sure the "next hop" routers on the internal side of the gateways know to send packets destined for addresses in the SecuRemote IP NAT pool to the proper gateway. Say Gateway A's internal interface is 10.10.10.10 and Gateway B's internal interface is 10.10.11.11. On NT the commands would be 'route -p add 10.1.0.0 mask 255.255.0.0 10.10.10.10' on Gateway A's downstream/"next hop"/internal router, and 'route -p add 10.2.0.0 mask 255.255.0.0 10.10.11.11' on Gateway B's downstream/"next hop"/internal router.**

\* Note: when the SecuRemote IP NAT pool is a 'network', say 10.1.0.0 (mask 255.255.0.0), the first SecuRemote connection will be assigned the address 10.1.0.0, which may not be routable. In this case a dial-in user would have to disconnect and reconnect to the Internet in order to get a new IP address, this next connection will be assigned the next address in the pool, say 10.1.0.1, which should work. This will be fixed shortly.

5. For our configuration, Insure firewall will not respond to unauthenticated cleartext topology requests; this is necessary when using IKE encryption scheme

From the Policy Editor, select the 'Policy', 'Properties...' menu. Now select the 'Desktop Security' tab and make sure box next to 'Respond to Unauthenticated Cleartext Topology Request' is not checked.



**NOTE:**

You can configure this to work with unauthenticated cleartext topology requests. If you do this, you can only receive the topology from the management station. You will also need to configure the RSA keys in the FWZ/CA key property of the FW object.

6. Create objects for Gateways A & B and configure workstation properties

Create Gateways A & B as new workstations. Fill in all the information in the 'General', 'Interfaces', 'Certificates' & 'Authentication' tabs.

\*Note: if your screen shots don't look like the ones that follow, go back and make sure steps 3 & 4 were done correctly.

On the 'NAT' tab select 'Use IP Pool NAT for SecuRemote Connections' if necessary and select the 'network' or 'address range' you created in step 4.

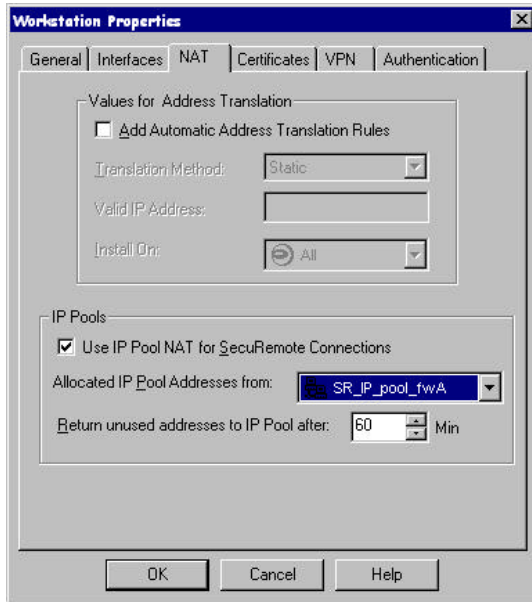
On the 'VPN' tab, fill in the encryption domain of the gateway. Select IKE as an encryption scheme. With 'IKE' highlighted, click on the 'Edit...' button and fill in the info on 'General' tab. Next on 'VPN' tab, check

the box next to 'Exportable for SecuRemote' on both firewalls; if you don't check this box on both firewalls MEP won't work. On the bottom of the 'VPN' tab, check the box next to 'Use Backup Gateways for SecuRemote Connections:' on the primary gateway, and select backup gateway\* from the pull-down menu below. Leave the box unchecked on the 'VPN' tab of the backup gateway's workstation properties.

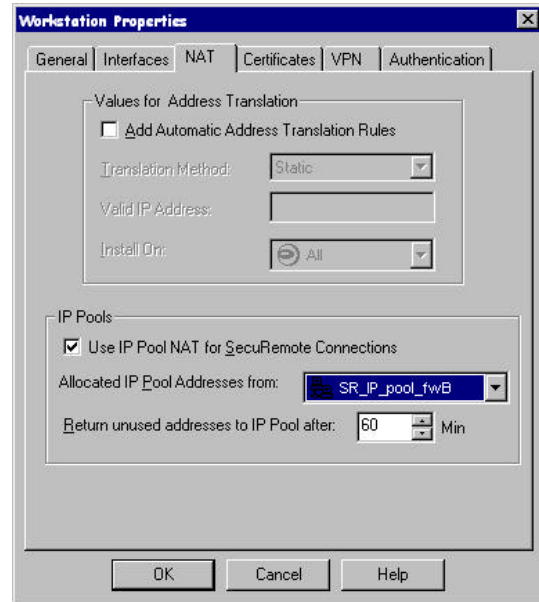
---

\* It is possible to define a 'group' of firewalls, created in Network Objects Manager, as a backup gateway. All firewalls in this group should be configured the same as the backup gateway above. In the event of a failure, SecuRemote will query all backup gateways; the first to respond becomes the backup gateway used.

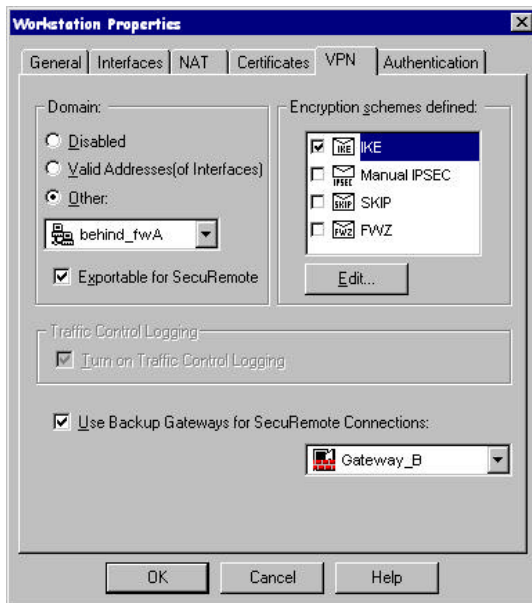
Primary Gateway, 'NAT' tab:



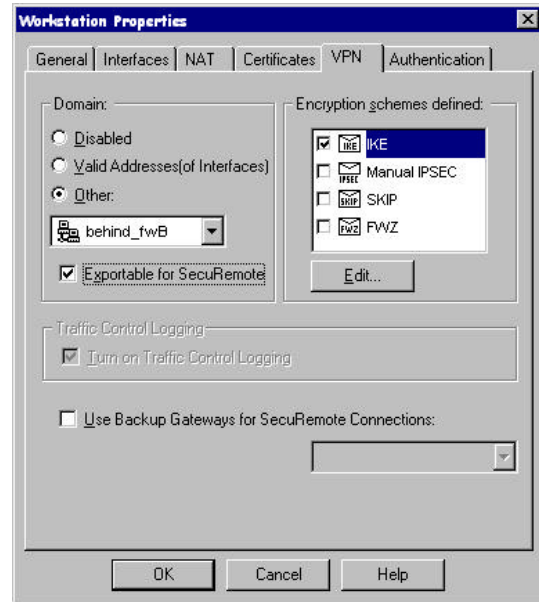
Backup Gateway, 'NAT' tab:



Primary Gateway, 'VPN' tab:



Backup Gateway, 'VPN' tab:



## 7. Configure SecuRemote

Click on the SecuRemote icon in the icon tray to bring up the interface. Create a site for the primary gateway. It is not necessary to create the backup gateway site. Select the 'Tools', 'Key Scheme...' pull-down menu and for our configuration make sure IKE is the selected key scheme.

Note: You could have also selected FWZ Encapsulation as the key scheme as well.

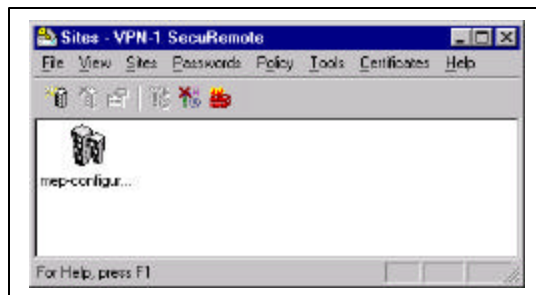
SecuRemote will query the gateway every 60 seconds. On average it will take SecuRemote about 40 seconds to discover that a gateway is down.

The parameter that controls the SecuRemote query of the gateway is the property "resolver\_session\_interval". This property allows SecuRemote to configure the interval between two RDP status queries. Its default value is 60 seconds. You can modify this value in the file `userc.C` located in the `$SRDIR/database` directory. Please reference 4.1 VPN book, page 165.

### userc.c parameters

Note The following parameters apply to overlapping encryption domains and MEP (see "Multiple Entry Point (MEP) Example Configuration" on 4.1 VPN Book page 239).

<code>active_resolver(true)</code>	If true, the SecuRemote Client will automatically initiate an RDP status query with a gateway to check if it is still alive. If false, the SecuRemote Client will postpone sending the query until that information is actually needed (in which case the user may experience some delay).
<code>resolver_session_interval(60)</code>	The interval (in seconds) between RDP status queries.
<code>resolver_ttl(10)</code>	The number of seconds the SecuRemote Client will wait for a reply on an RDP status query before concluding that the gateway is unavailable.



**Limitations and Unsupported Configurations:**

- Overlapping of modules belonging to different sites is prohibited
- Partial overlap of encryption domains is not allowed
- Existing connections will not survive rollover
- VPN (gateway to gateway) configurations are not supported
- All participating modules need to be version 4.1
- All clients need to be version 4.1 to allow for a proper subnet or fully overlapping configurations
- IPSEC/IKE encryption only