

Check Point Software Technologies Inc.

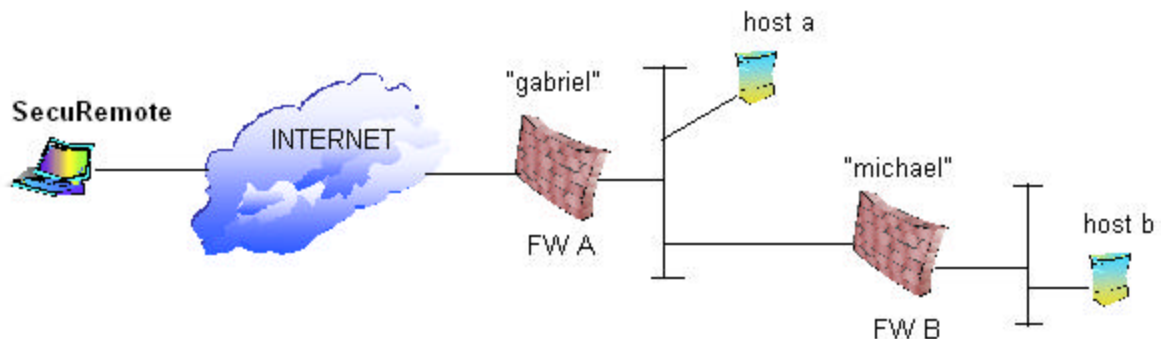
FireWall-1 Version 4.1
SecuRemote Version 4.1
Client Authentication Used To Provide
Out Of Band (OOB) Authentication
For IPSEC tunnels on FW –1 / VPN –1

Author: Brad Molles
Credits: Kupi, Roy
Date: Revision 1.1 – April, 2000
Purpose: To describe how to set up OOB authentication on a primary VPN Gateway in order to gain network access and create an IPSEC VPN tunnel to a secondary VPN Gateway.

This document describes how to setup a VPN tunnel through a primary Gateway to a secondary Gateway using OOB (Out-of-Band) authentication on the primary firewall to authenticate and pass IPSEC traffic. Additionally this setup allows the primary gateway to handle the encryption / decryption process for hosts in the encryption domain using the normal IB (in band) authentication of the IKE process.

This configuration requires at least version 4.1 of FW-1 / VPN -1 and SecuRemote. The concept was tested and proven on version 4.1 SP 1.

Using the following diagram as a reference we can explain the different scenarios involved.



1 Authentication needs to take place at **FW A** to gain access to the network, plus encryption needs to take place from the SR client to the secondary gateway (**FW B**) in order to communicate securely with host b.

- a. The SecuRemote user will authenticate to **FW A** by using client authentication methods, telnet to **FW A** port 259 or HTTP to port 900.
- b. After authentication takes place the IP address of the SR client is allowed to pass IPSEC protocols through **FW A** to **FW B**.
- c. The SecuRemote client sends IKE negotiation and encrypted packets to **FW B**.
- d. **FW B** handles the encryption process for host b. Host b is defined in **FW B's** encryption domain.

This is called Out-of-Band authentication by some because authentication takes place before the VPN is set up to **FW B**.

*Note: If set up as described below, then OOB authentication is also done via VPN to **FW A**.

2 In cases where the SecuRemote client wants to communicate with host a, authentication takes place on **FW A** as part of the IKE negotiation and therefore the Client Authentication rule on **FW A** is not used.

- a. The SecuRemote client tries to connect to host a.
- b. If a previous IKE negotiation has not timed out the traffic is immediately encrypted between the SR client and **FW A**.
- c. If there was no previous IKE session or a previous IKE session has timed out, then an IKE negotiation takes place between the SR client and **FW A**.

- d. After the IKE negotiation a VPN is set up, meaning, encryption is taking place between the SR client and **FW A**. **FW A** handles the encryption process for hosts or networks defined within it's encryption domain.

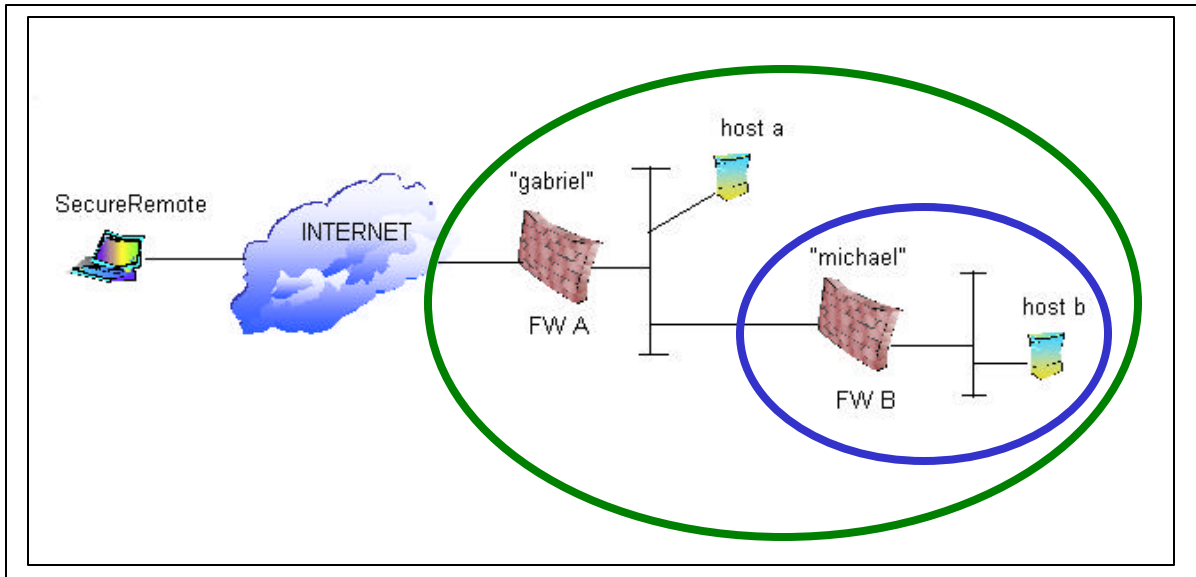
The following configuration is needed to set this up:

The encryption domain for **FW A** must be **larger** than **FW B** and include all that **FW B's** encryption domain includes. This creates a **“proper subset”** overlapping encryption domain.

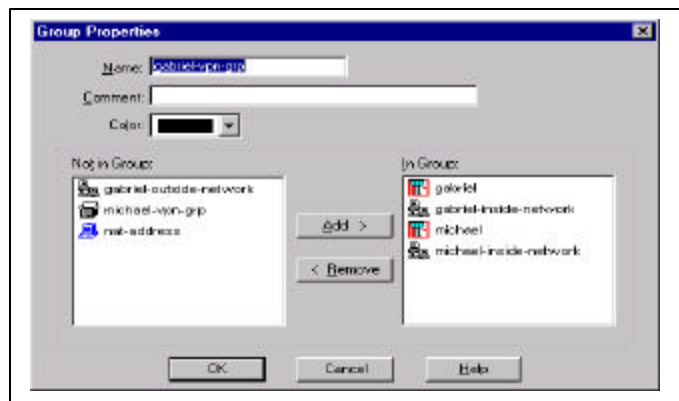
Here is an example of how to set up the encryption domains:

FW A_vpn_grp = FW A, FW A_inside_network, FW B, FW B_hostb_network

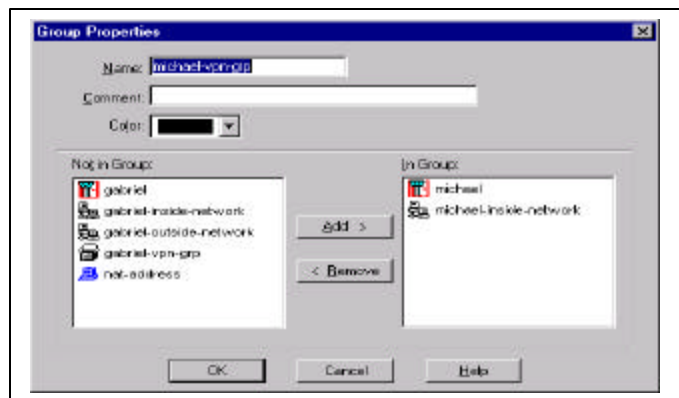
FW B_vpn_grp = FW B, FW B_hostb_network



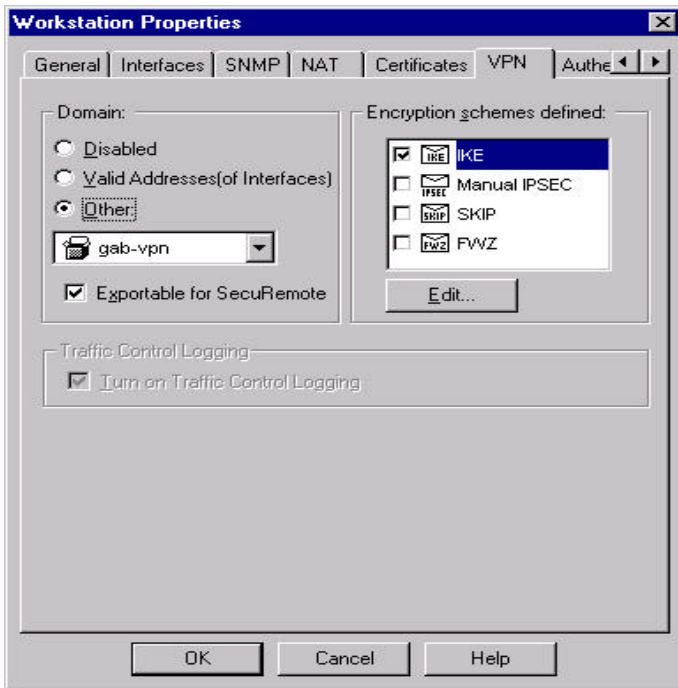
FW A_vpn_grp →



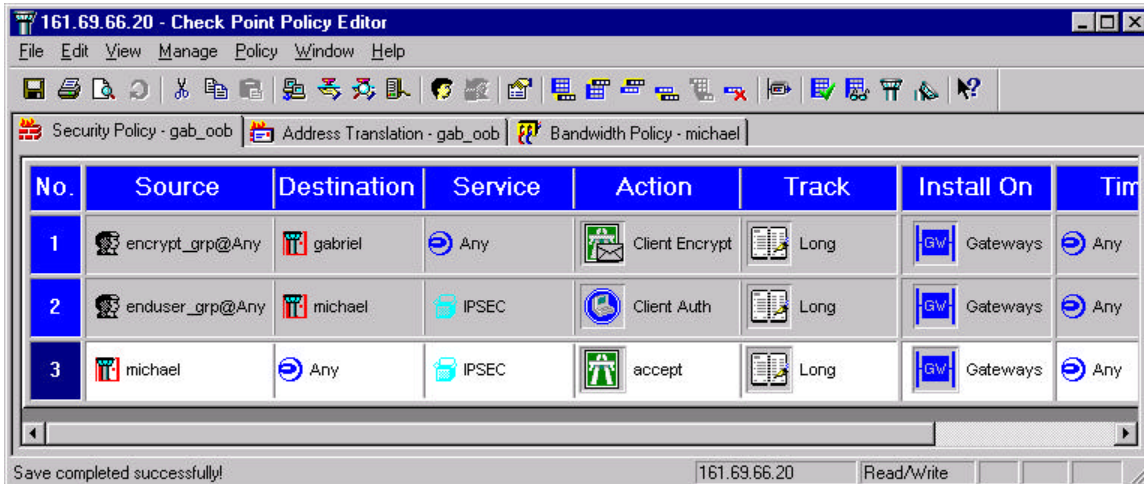
FW B_vpn_grp →



The firewall objects need to have IKE encryption turned on and have “exportable for Secure Remote” checked.



FW A Policy:

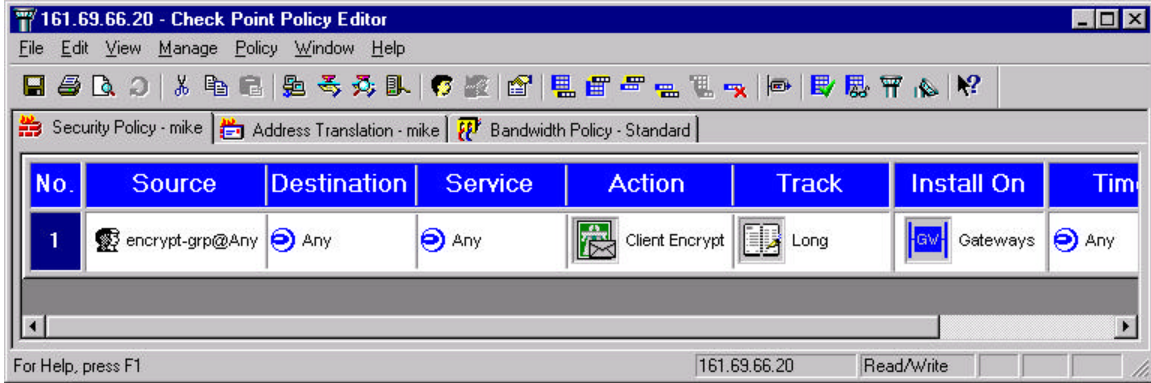


*Note: Rule 3 is in place to allow IPSEC packets returning from **FW B** to pass through the Gateway (**FW A**) to the SecuRemote client. Specifically, this rule allows ESP traffic to pass back through the Gateway. Rule 2 is sufficient to authenticate the client and pass IKE in both directions. IKE is not affected by the absence or existence of rule 3 since IKE uses UDP port 500 and Stateful Inspection tracks UDP. ESP is a different case, since only the encrypting / decrypting gateway (**FW B**) has a view inside the original packet. The tunneling gateway (**FW A**) does not keep state information on ESP, therefore rule 3 is needed to allow the returning ESP packets to pass **FW A**. In essence the service in rule 3 could be ESP and the affect would be the same. The IPSEC service includes AH, ESP, IKE, ISAKMP and SKIP.

Text View of FW A policy:

encrypt_grp@any	FW A	any	Client Encrypt	long
enduser_grp@any	FW B	IPSEC	Client Authentication	long
FW B	any	IPSEC	Accept	long

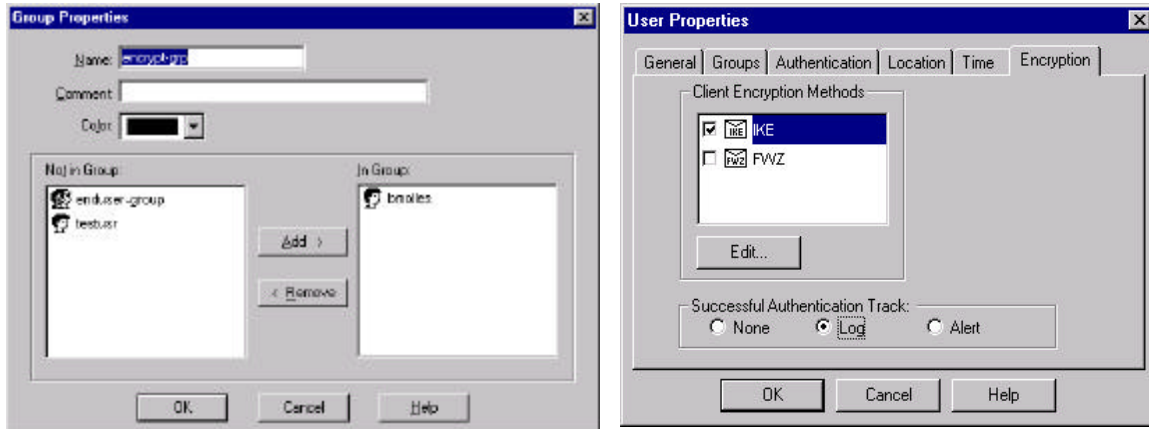
FW B policy:



Text View of FW B Policy:

encrypt_grp@any	any	any	Client Encrypt	long
---------------------------------	-----	-----	----------------	------

The encrypt_grp has a user set up with IKE encryption and password:



The enduser_grp has a user set up with a FW-1 / VPN-1 password. This could be RADIUS or any other authentication method. **Make sure that the authentication method is checked on the firewall objects authentication tab.**

On SecuRemote:

Add a new site, use IKE encryption.

The new site should be the management server (which has all the objects and groups defined above), or the firewall module. If you define the topology to be downloaded from the firewall module, please look for additional configuration papers regarding "topology downloads from a firewall module".

To connect to host a, just telnet, ftp, http, etc. to hosta. SecuRemote may prompt you for user name and password if any previous session has timed out. This will be the SR username and password.

To connect to host b, you will have to authenticate to FW A first, (unless a previous authentication has not timed out). To authenticate to FW A either telnet to FW A:port 259 or HTTP to FW A:port 900, put in the user name, you will be prompted for a password, (put in the password), you will be given the choice to sign on or sign off, choose sign on. This connection will immediately drop but the username and IP address have been mapped and you will now be able to pass IPSEC traffic to FW B. You can now connect to host b via SecuRemote

With this configuration ALL traffic is 3DES encrypted. Even the Client Auth rule is encrypted fully.

We can use the following log view to illustrate what happens:

No.	Origin	Type	Action	Service	Source	Destination	Proto.	Rule	S_Port	Us
278	gabriel	log	key install			161.69.66.30				
279	gabriel	log	key install		161.69.66.30	gabriel	ip	0		
280	gabriel	log	decrypt	FW1_clntauth_http	161.69.66.30	gabriel	tcp	1	1261	de
281	gabriel	log	decrypt	FW1_clntauth_http	161.69.66.30	gabriel	tcp	1	1262	de
282	gabriel	log	decrypt	FW1_clntauth_http	161.69.66.30	gabriel	tcp	1	1263	de
283	gabriel	log	decrypt	FW1_clntauth_http	161.69.66.30	gabriel	tcp	1	1264	de
284	gabriel	log	authorize	Std Sign On	161.69.66.30		ip	2	1261	en
285	gabriel	log	accept	FW1_log	michael	gabriel	tcp	0	1029	
286	michael	log	deauthorize		161.69.66.30					des
287	michael	log	key install			161.69.66.30				
288	michael	log	key install		161.69.66.30	michael	ip	0		
289	gabriel	log	accept	16251	161.69.66.30	michael	esp	2	4870	enc
290	michael	log	decrypt	http	161.69.66.30	192.168.5.10	tcp	1	1265	des
291	gabriel	log	accept	18962	michael	161.69.66.30	esp	3	11668	
292	gabriel	log	accept	16251	161.69.66.30	michael	esp	2	4870	enc

Lines 278 & 279 (circled in blue) are the key exchange between SecuRemote and **FW A**.

Lines 280 to 284 (red) are the client authentication, these packets are encrypted.

Lines 287 & 288 (black) is the key exchange with **FW B** that takes place after authentication with **FW A** allows IPSEC to tunnel through **FW A**.

Lines 289 to 292 show **FW A** accepting ESP to pass to **FW B**, **FW B** decrypts, and ESP passing back through **FW A**. Notice that line 291 show rule 3 passing ESP.