



CHECK POINT™
Software Technologies Ltd.

Hybrid Mode IKE for SecuRemote Authentication

Authored By: Joe DiPietro
Date: September 6, 2000
Purpose: To describe and document how to configure Hybrid Mode IKE for SecuRemote Authentication
Credits:
Version: 1.4

This paper describes how to get Strong Encryption using Hybrid Mode IKE authentication. Check Point has proposed to the IETF a method to authenticate users while using IKE Encryption. These users can be authenticated by something other than Digital Certificates and Pre-shared Secrets (These are the only standards method for IKE authentication today). This means you can use your SecurID Cards, RADIUS, LDAP, or Firewall-1 Internal Password, etc. to be authenticated.

Steps to get Hybrid Mode Authentication Working:

1. Stop and close all firewall files by issuing an “fwstop”
2. Create the Internal CA on the Management Station
3. Create a Certificate for the VPN/Firewall Module
4. Start the firewall processes again by issuing an “fwstart”
5. Allow "Hybrid" Mode SecuRemote Authentication on the Firewall Object (IKE Tab)
6. Define a User with 3DES and Firewall-1 Password (Other Methods will also work)
7. Define a Rule and Push the policy to the VPN/Firewall Module
8. Update the SecuRemote Site
9. Test authentication

- =====
1. Issue an fwstop

The 'fw internalca' command line writes to the FW-1 files, so the best thing to do is close all of the files by issuing an fwstop.

```
trek# $FWDIR/bin/fwstop
trek#
```

2. Create the Internal CA on the Management Station

```
trek# cd $FWDIR/bin
trek# fw internalca create -dn "o=boston, c=us"
Internal CA created successfully
```

This creates an internal Certificate Authority to be used in the Hybrid Authentication Process. Select your own DN name (LDAP Format)

3. Create a Certificate for the VPN/Firewall Module

```
trek# cd $FWDIR/bin
trek# fw internalca certify -o trek "o=boston, c=us"
Certificate created successfully
trek#
```

Note: This certificate will show up in the "Certificate" tab of the firewall object after it has been created from the command line

4. Issue an fwstart

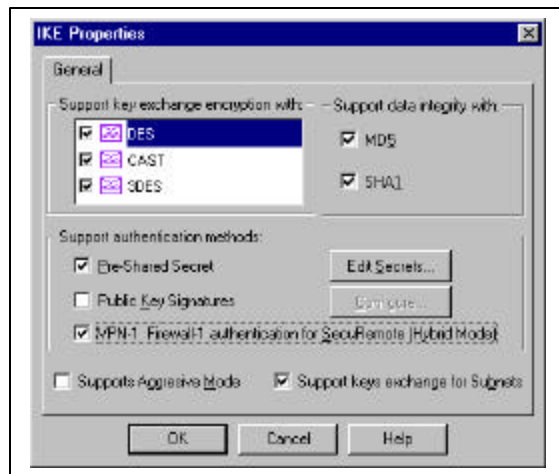
Start the firewall processes now.

```
trek# $FWDIR/bin/fwstart
```

5. Allow "Hybrid" Mode SecuRemote Authentication on the Firewall Object (IKE Tab)

Select
Manage → Network Objects → "firewall
object" → VPN tab
→ IKE Properties

- Make sure that "VPN-1 Firewall-1 Authentication for SecuRemote (Hybrid Mode) is Selected

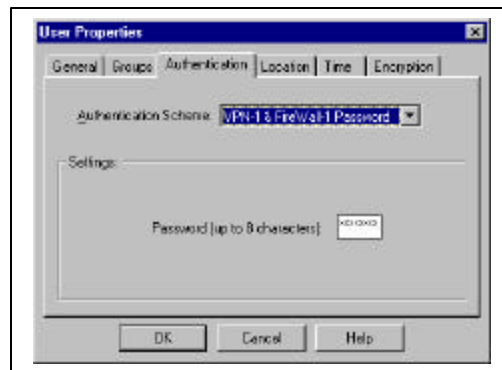


NOTE: If you don't see this option, you need at least 4.1 SP1 version of the GUI client

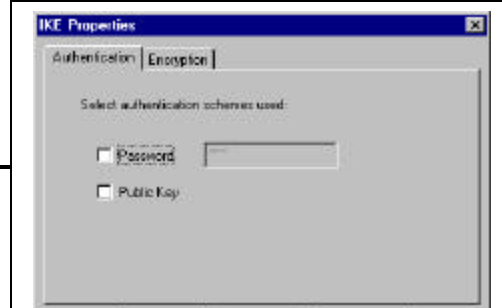
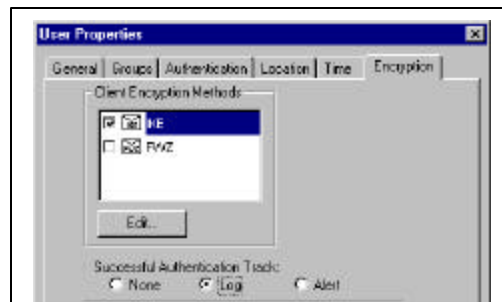
6. Define a User with 3DES and Firewall-1 Password

Make sure there is a User Defined
(Manage → Users)

- Select the Authentication Tab
- Select VPN-1 and Firewall-1 Password
- Other Methods of Authentication are also supported



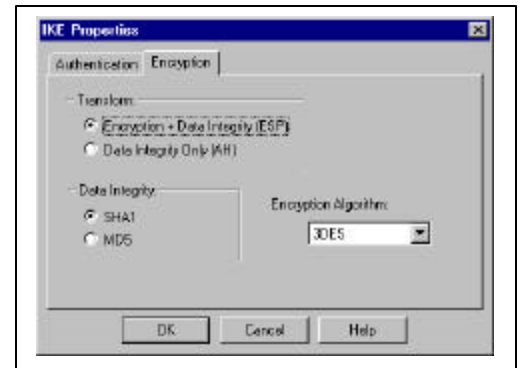
- Select Encryption
- Select IKE → "Edit"
- Select "Log" for Successful Authentication Track



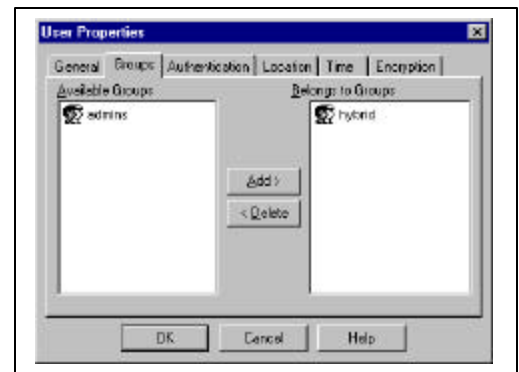
Note: If you want to download the topology from the Firewall Module using IKE, you could use this user with a IKE Password here, or you could use another user with an IKE Password (Shared Secret). For our purposes, you don't need to have Authentication Scheme Used here. However, the Encryption definition is very important.

- Select the "Encryption" Tab
- This is where the "strength" of the Encryption Algorithm for the Hybrid User will be used.
- We selected "3DES" (this is the Default with VPN + DES + STRONG)

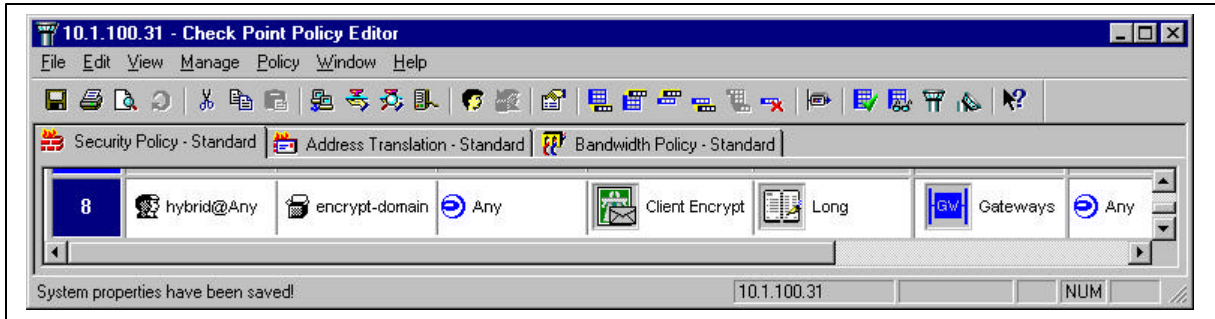
NOTE: To see what version the Firewall/VPN code is using, type in "fw ver" at the command line "\$FWDIR/bin/fw ver".



- Select the "Groups" tab
- Make sure the User is a member of a valid Group (Hybrid in our case)



7. Define a Rule and Push the policy to the VPN/Firewall Module



8. Update the SecuRemote Site

On the SecuRemote Client, define a new site, or "Update" the existing site.

You can validate that the new information has been received by looking into the "userc.c" file. Below is a Snapshot of this file, note the "cert" and the "dn" fields

```

      : (10.29.105.62
        :obj (
          :type (node)
          : (10.29.105.62)
        )
        :dnsinfo ( )
        :MgmtInternalCA (
          :public (
            :value (010001)
          )
          :modulus (
            :value (d4783f-TRUNCATED_VALUE-
5cdca066dfa4fc944f)
          )
          :cert (ffd3876-TRUNCATED_VALUE-----TRUNCATED_VALUE-
018230)
          :dn ("O=boston,C=us")
          :date (38a4590a)
        )
      )

```

You should also see ":ISAKMP_hybrid_support (true)" property on the site object with the userc.C file

9. Test authentication

Now try and get to the internal site with your web browser. You will see the authentication in the log files. You must look in the info field at the end of the Log View to see the following. You should see IKE phase I with 3DES/SHA/Internal Password. This is Hybrid Mode IKE with VPN-1/Firewall-1 Password using 3DES.



Troubleshooting

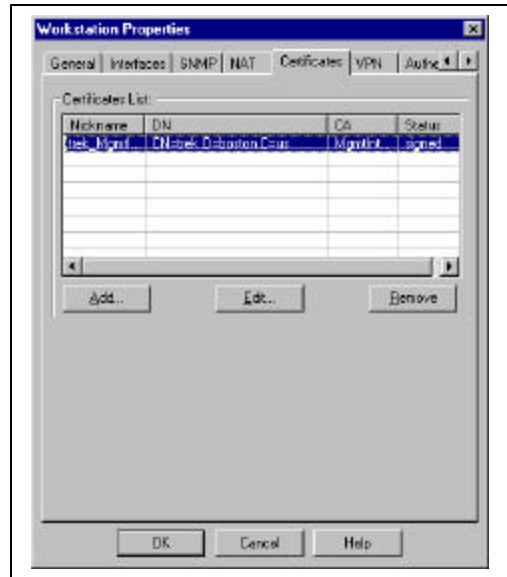
1. You should see the following under the Firewall Object in \$FWDIR/objects.C that will accept Hybrid Authentication:

```

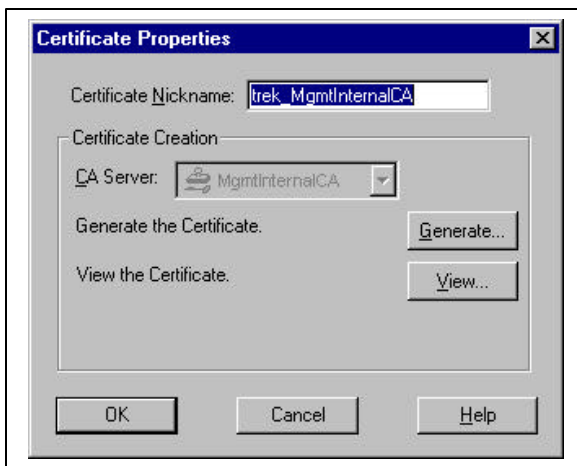
.....
:isakmp.authmethods (
: (pre-shared)
: (hybrid)
)
.....
    
```

This should be one of the methods "hybrid" ←

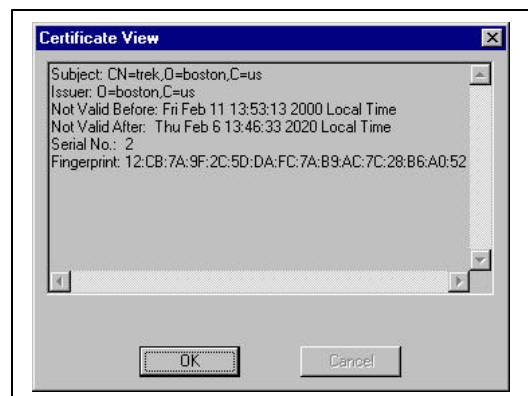
2. Make sure you can see the Certificate within the Firewall Object by click on the Certificate Tab as shown to the right →



3. To see the CA for this certificate click on Edit



4. Now Click on "View" to see the Certificate information that was generated and the time and date that this will be valid.
5. Also note, that you might run into Timing issues if the management station has a different time/date than the firewall module.



6. Please note that when you edit objects.C and/or run the internal ca command lines, the management station must not be running (fwstop), and you must remove backup copies of objects.C (.sav and .bak).

Provider-1 Environment

1. Before starting the configuration, shutdown the MDG and all GUI's.

On the MDS:

2. Start another terminal session on the MDS

3. Changed the shell to c-shell (It is easier running this script in csh)

```
csh
```

4. Set the environment variables using the setmdsenv script in \$FWDIR/bin

```
source setmdsenv
```

5. Run the alias command mdsenv. This command actually changes the FWDIR and MSP_SOMEIP_ADDR environment variables. This sets up your session so you can work in the CMA's environment (just like the FW-1/VPN-1 management station) within Provider-1.

```
mdsenv -v <cma-ip-address>  
mdsenv -v 10.0.100.50          ##### (For our Example) #####
```

6. Stopped the firewall

```
fwstop
```

7. Create an internal CA. (Example: Assume your CMA ip address is 10.0.100.50)

```
fw internalca create -dn "o=cphouston, c=US"
```

8. Create a certificate for the VPN-1/FW-1 module. (Example: Assume your gateway object is named "gw1a")

```
fw internalca certify -o gw1a "o=cphouston, c=US"
```

9. Restart the firewall

```
fwstart
```

10. Run the Policy Editor gui and edit your gateway network object.

11. Verify the policy has been created by clicking on the Certificate tab.