

Check Point Software Technologies LTD.

FireWall-1 Version 4.0 SecuRemote Split/Encrypted DNS Quick Reference Guide Revision 1.4

Authored By: David Goodman
Date: Revision 1.5 - November, 1999
Purpose: To describe and Document how to configure encrypted/split DNS within Checkpoint SecuRemote & Firewall-1 Version 4.0

Check Point Software Technologies LTD.

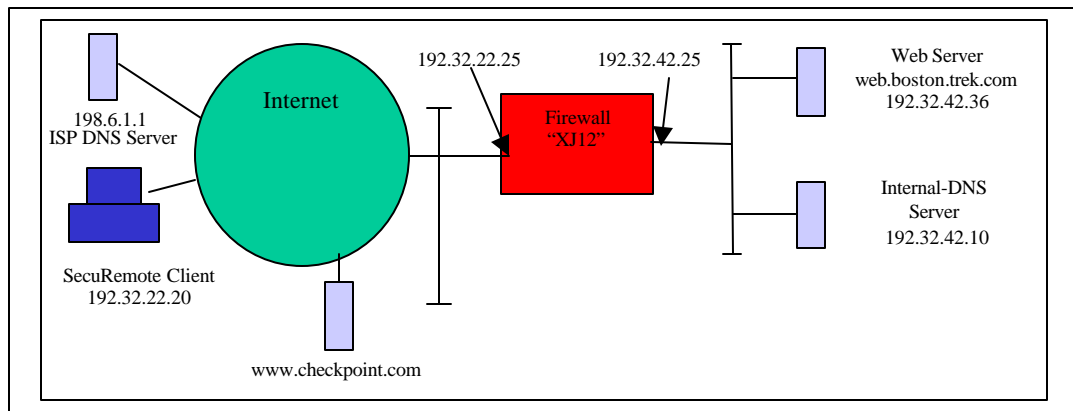
FireWall-1 4.0 SecuRemote Split/Encrypted DNS Quick Reference Revision 1.3

This document describes how to setup “Redirected DNS” for a SecuRemote user so that DNS queries to the Internal Domain may be encrypted and resolved by the Internal DNS server. All other DNS queries are resolved by an external (ISP) public DNS server. The security aspect of this feature is clearly to hide internal domain information from the outside world. This feature can also prove valuable for non routable internal address schemes such as 10.x.x.x or 172.x.x.x .

The primary focus of this document is to highlight the combination of split and encrypted DNS functionality. While this combination will be the preferred design in most cases, design flexibility also allows encrypted DNS configuration to a single internal DNS server. A design summary will be given at the end of this document highlighting the encrypted DNS only configuration steps.

This document assumes a knowledge of Client Encryption with SecuRemote and that a functional implementation of this feature has been previously configured. In addition, the information contained herein refers to software functionality present in SecuRemote version 4.0 (Build 4003 and beyond) and Firewall-1 version 4.0 SP-1 and beyond. For more information on how to configure Client Encryption and SecuRemote, please see the associated documentation in the VPN-1 User’s Guide version 4.0 SP1 (9/98 Edition) and www.checkpoint.com/~joe

Consider the following diagram. A DNS Server (192.32.42.10) is employed on the internal network that resolves all names within the domain of boston.trek.com. For security reasons, the administrator does not wish to publish this information to the public network. A remote user in this case must connect securely to the internal DNS server for names within boston.trek.com, while also being able to connect to a public DNS (198.6.1.1) server for all other DNS inquires (i.e. www.checkpoint.com).



In order to accomplish this goal, we will perform the following steps:

1. Create/Modify \$FWDIR/conf/dnsinfo.C file on the Management Station. This info will be downloaded to the SecuRemote client during a topology update process. You must specify the information below:
 - The Internal DNS Server hostname, in our case this will be "trek-pc"
 - The Internal DNS Server IP address, in our case this will be 192.32.42.10
 - The Network Addresses for which it resolves the boston.trek.com domain.. In our case this is a single subnet, 192.32.42.x
 - The Network Mask for this subnet is 255.255.255.0
 - The maximum number of labels to resolve. In our case 4 for xxx.boston.trek.com
 - The domain for which it resolves names. In our case .boston.trek.com

- Set :encrypt_dns (true) at the end of the dnsinfo.C file. This tells the SecuRemote client to encrypt DNS requests to the boston.trek.com domain.

NOTE: If you have one FW-1 Module and one FW-1 Management on two different computers, and you want to get the topology from your FW Module (version 4.0 feature), then you will not receive the dns information.

Reason : you also need to manually copy the file dnsinfo.C in the \$FWDIR/conf directory of your FW-1 Module to make it work.

2. Tell the firewall to encrypt SecuRemote DNS by adding #define ENCDNS above the line "define USERC_DECRYPT_SRC" in the crypt.def file. These files are located on the management station at:

on NT: \winnt\fw\lib\crypt.def
on UNIX: /etc/fw/lib/crypt.def

3. Reinstall a policy on the firewall gateway so the proper updates are compiled into the kernel.
4. Kill the SecuRemote application

Double Click the Envelope with the key in the lower right hand toolbar. Then select File → kill

5. Modify the userc.C file on the SecuRemote Client by adding the following lines under the ":options" line.

```
:dns_xlate (true)
:dns_encrypt (true)
```

These files are located:

On Win95 \Program Files\CheckPoint\secureremote\database\userc.C file
On Win NT \winnt\fw\database\userc.C file

6. Restart the SecuRemote Client

Start → Programs → Firewall-1 → SecuRemote (Win 95)
Start → Programs → SecuRemote → SecuRemote (Win NT)

7. On the SecuRemote client, update the new topology information from the Management Station.
8. Test the configuration

Step 1 Create a file called dnsinfo.C in the \$FWDIR/conf directory on the Management Station. This file will redirect local DNS queries for anything like xxx.boston.trek.com to the internal DNS server.

The contents of this file should have the following syntax:

===== \$FWDIR/conf/dnsinfo.C should look like this for our example =====

```
(
  :dns_servers (
    : ( trek-pc.xj12
      :obj (
        : ( 192.32.42.10
          )
        :topology (
          : (
            :ipaddr ( 192.32.42.0 )
            :ipmask ( 255.255.255.0 )
          )
        )
      :domain (
        : (
          :dns_label_count ( 4 )
          :domain ( .boston.trek.com )
        )
      )
    )
  )
  :encrypt_dns (true)
)
```

=====

NOTE: Please make sure that the syntax of this file is very particular. If you misspell "**encrypt**" for "**encript**", you might be looking for this typo for quite a long time!

=====

Substitute your network structure for the above **boldface** information in the following places:

- yourDNS.yourfirewallobject *for* **trek-pc.xj12**
In our example trek-pc is the DNS server and our firewall object is XJ12
- your DNS server IP Address (xxx.xxx.xxx.xxx) *for* **192.32.42.10**
In our example the DNS server IP address 192.32.42.10
- The network addresses for which your DNS server resolves(xxx.xxx.xxx.xxx) *for* **192.32.42.0**.
In our example the IP Network is 192.32.42.0. It is likely that your environment contains multiple IP Networks. In this case simply include the IP Network and Subnet mask for each network that is within your internal DNS domain.
- The network mask associated with your IP Network (xxx.xxx.xxx.xxx) *for* **255.255.255.0**.
In our example, the subnet mask is 255.255.255.0

- The maximum number of labels to resolve (X) *for 4*
In our example the maximum number of labels to resolve is 4 for xxx.boston.trek.com
- The domain which the internal DNS server resolves .xxx.xxx.xxx *for .boston.trek.com*
In our example the domain which our DNS server resolves is .boston.trek.com.

Note The example of the dnsinfo.C file on Page 97 of the VPN-1 User's Guide version 4.0 SP1 (9/98 Edition) contains a syntax error. As documented in the above example, the file requires an additional open parenthesis at the beginning of the file and an additional close parenthesis at the end of the file.

Step 2 Tell the firewall to encrypt SecuRemote DNS requests by adding #define ENCDNS above "define USERC_DECRYPT_SRC" in crypt.def file. This file can be found:

On NT: \winnt\fw\lib\crypt.def
On UNIX: /etc/fw/lib/crypt.def

Add the line #define ENCDNS above "define USERC_DECRYPT_SRC"

```

===== crypt.def BEFORE =====

define USERC_DECRYPT_SRC {
(
#ifdef ENCDNS
    not(dport = SERV_domain, (udp or tcp)),
#endif
    not(dport = FWD_SVC_PORT, tcp),
    not(dport = FWM_SVC_PORT, tcp),
    not(dport = ISAKMPD_DPORT, sport = ISAKMPD_SPORT, udp)
)
};

deffunc ACCEPT_CLIENT_ENCRYPTION(rule) {
(
    USERC_DECRYPT_SRC,
    (direction = 0, <src,0> in userc_rules,
    USER_DECRYPTPTION(rule,0))
    or
    (direction = 1, <dst,0> in userc_rules, USER_ENCRYPTION(rule))
)
};

===== crypt.def AFTER =====

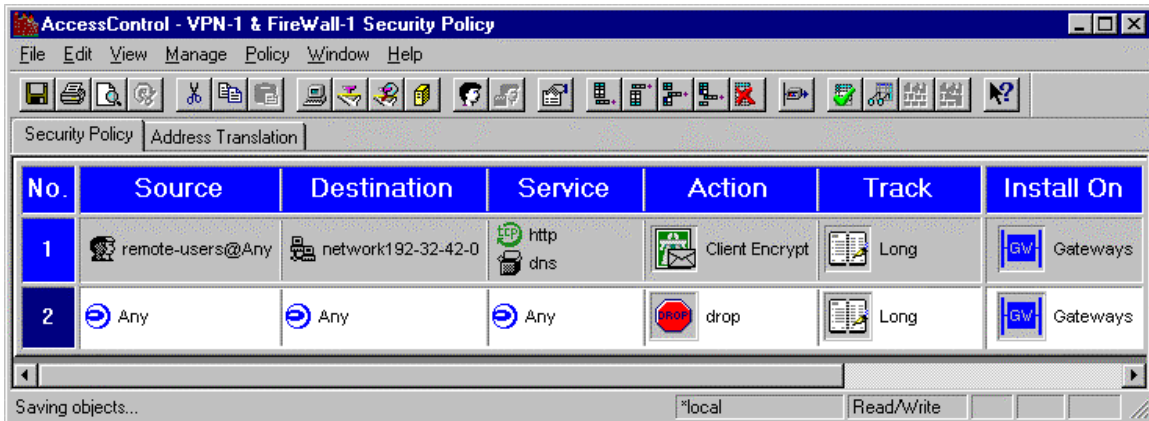
#define ENCDNS
define USERC_DECRYPT_SRC {
(
#ifdef ENCDNS
    not(dport = SERV_domain, (udp or tcp)),
#endif
    not(dport = FWD_SVC_PORT, tcp),
    not(dport = FWM_SVC_PORT, tcp),
    not(dport = ISAKMPD_DPORT, sport = ISAKMPD_SPORT, udp)
)
};

deffunc ACCEPT_CLIENT_ENCRYPTION(rule) {
(
    USERC_DECRYPT_SRC,
    (direction = 0, <src,0> in userc_rules,
    USER_DECRYPTPTION(rule,0))
    or
    (direction = 1, <dst,0> in userc_rules, USER_ENCRYPTION(rule))
)
};

```

};

Step 3 Reinstall the client encryption policy on the gateway.



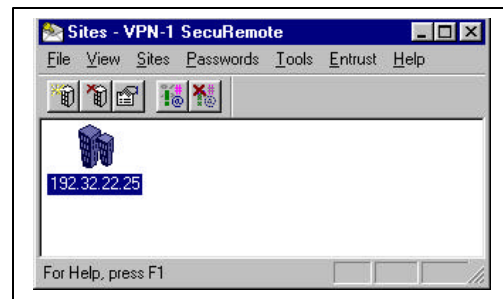
Note A Policy must be recompiled and sent to the firewall gateway for the proper updates to take place when the SecuRemote client updates its policy information.

Step 4 Kill the SecuRemote application

Double Click the Envelope with the key in the lower right hand toolbar.



Then select File → kill



Step 5 On the SecuRemote Client, add the following lines under the “:options(” line in the userc.C file

```
:dns_xlate (true)
:dns_encrypt (true)
```

These files are located:

On Win95/98 = \Program Files\CheckPoint\secureremote\database\userc.C file
On Win NT = \winnt\fw\database\userc.C file

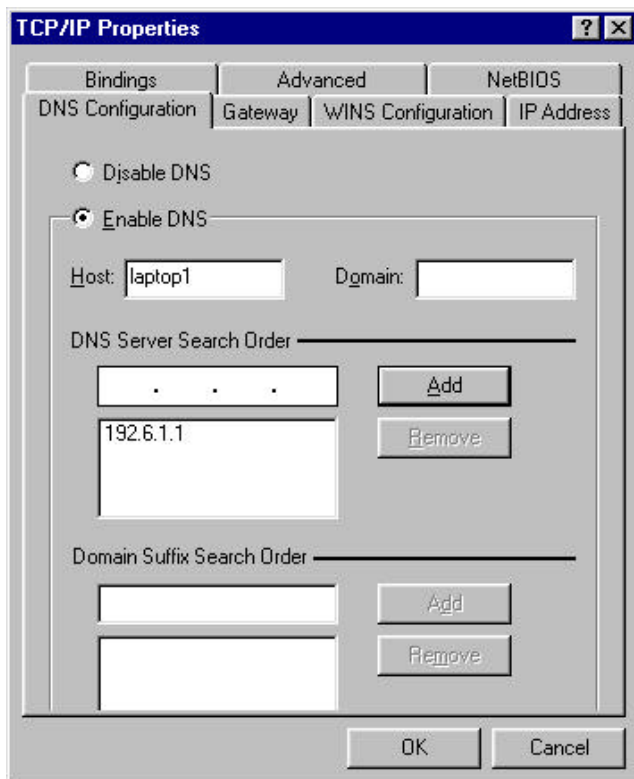
Usenc.C options section BEFORE modification:

```
+++++
)
:options (
    :expire (15)
    :use_cert (false)
)
+++++
```

Usenc.C AFTER Modification:

```
+++++
)
:options (
    :expire (15)
    :use_cert (false)
    :dns_xlate (true)
    :dns_encrypt (true)
)
+++++
```

Note The DNS configuration must contain at least one DNS server entry as shown below.



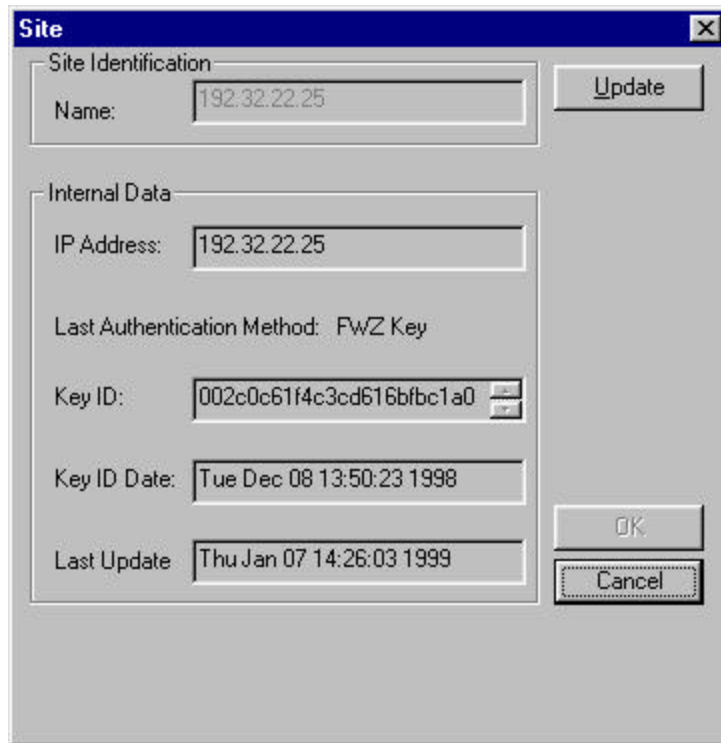
Step 6 Restart the SecuRemote Client.

Select **Start → Programs → Firewall-1 → SecuRemote** (Win 95)

Select **Start → Programs → SecuRemote → SecuRemote** (Win NT)

Step 7 On the SecuRemote Client, update the site information so the new topology information is downloaded to the userc.C file.

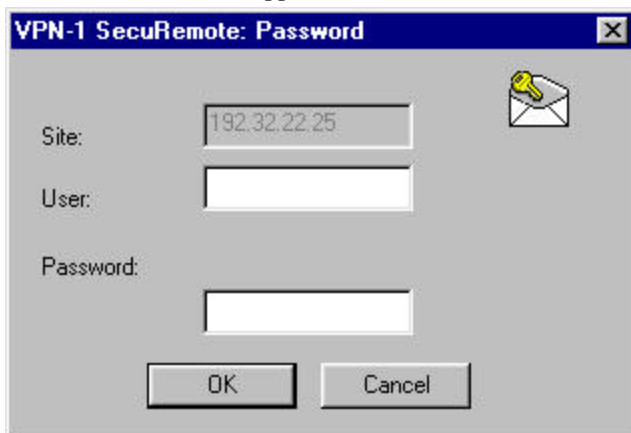
From the Sites – VPN-1 SecuRemote window Select **Site → Properties → Update**



- Note**
1. As always, an updated userc.C file can also be distributed out of band and placed in the correct directory on the client.
 2. Verify that the previous settings are still accurate under the :options section

Step 8 Testing your new configuration should be fairly straight forward. On your client machine, dial up your ISP as usual. Open a web browser and enter the URL of your internal web server.

The SecuRemote challenge should appear. Enter your username and password and the authenticated confirmation should appear.

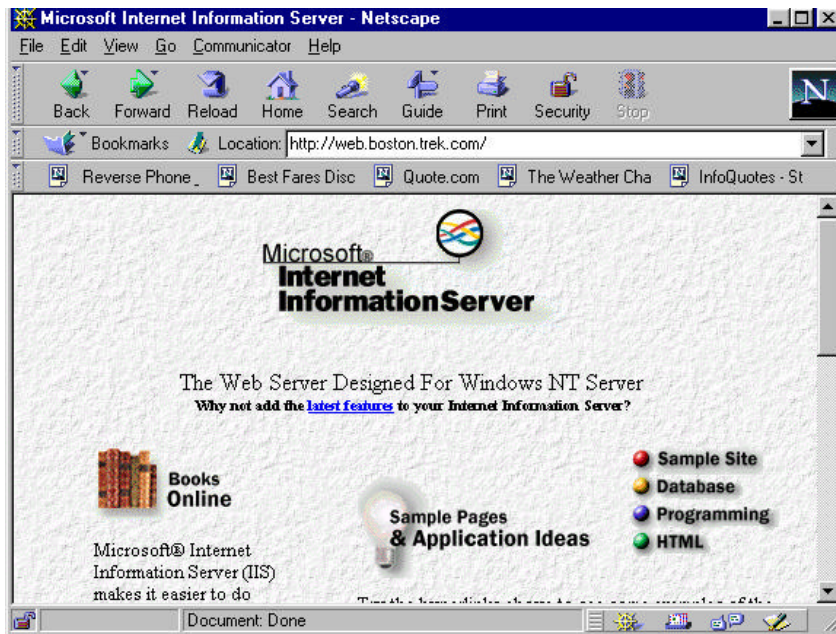


Enter your user name and password as usual.

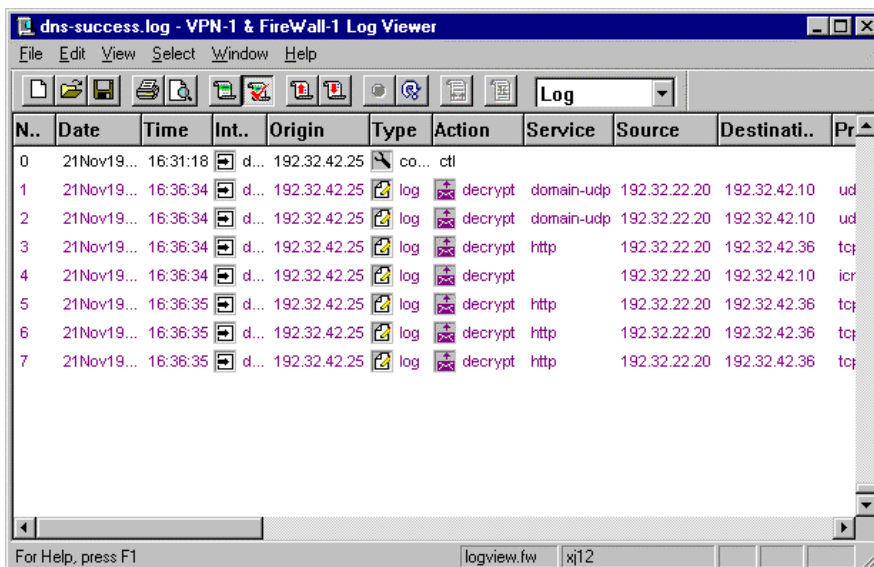


If SecuRemote is configured properly and the password is correct, you should be authenticated and a response will be launched stating that you have been authenticated.

Successful operation is indicated by a properly loaded web page,



and the following log file that shows the encrypted DNS to the Internal DNS Server (192.32.42.10) and HTTP requests to the Internal Web Server (192.32.42.36).



Configuration Summary for Encrypted (and not Split) DNS

Configuring Encrypted DNS only will resemble the above configuration except in the following areas:

Step1 Create/modify the dnsinfo.C file on the management console.

The contents of this file should have the following syntax:

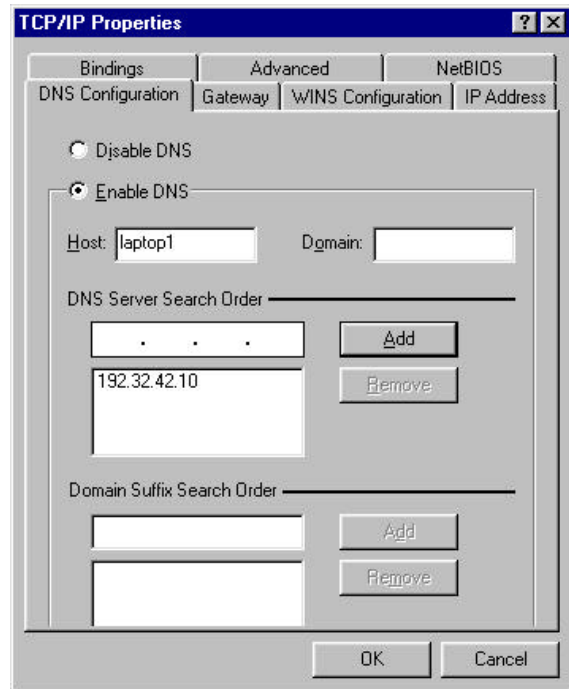
===== \$FWDIR/conf/dnsinfo.C should look like this for encrypted DNS =====

```
(  
  :encrypt_dns (true)  
)
```

=====

Step5 In the userc.C file on the client, **Omit** the line **:dns_xlate (true)**

Note The DNS configuration in the TCP/IP Properties window on the client must contain the IP address of the internal DNS server.



Appendix A - Known Issues with SecuRemote version 4003 and 4005

With SecuRemote 4003 (or 4005), you can send encrypted DNS requests from your SecuRemote to a computer in the Encryption Domain of the FireWall. When using this you must be aware of two different known issues :

1. If you define multiple suffixes for DNS redirection.

Example:

You can define to have the SecuRemote redirect all DNS queries of the form:

..aaa.com or *.*.yyy.com

to a certain DNS server. The problem is that SecuRemote will redirect only DNS queries of the form *.*.yyy.com. This is because the last entry runs over the previous entry. However, if you define the following two suffixes

*.aaa.com or *.*.yyy.com

then the last entry won't run over the previous one because it has a different label count (the first has 3 labels and the latter has 4).

A workaround is therefore to define different label counts to each suffix.

2. Second problem.

Suppose you define SecuRemote to redirect all queries of the form: *.aaa.com to a certain DNS server. Now suppose you try to resolve the name

www2.aaa.com

SecuRemote will wrongly think that the name www2.aaa.com consists of 4 labels instead of 3 and will not redirect it. The problem is with the presence of a numeric character (the 2) inside the name. A workaround is to define longer label counts to each such suffix.