Integration of Check Point VPN-1®/Firewall-1® and FreeBSD IPsec

Jon Orbeton

jono@securityreports.com

Matt Hite

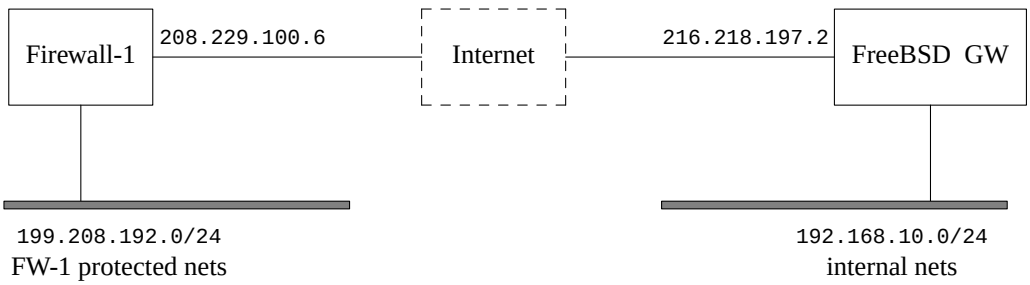
mhite@hotmail.com

$FreeBSD: doc/en_US.ISO8859-1/articles/checkpoint/article.sgml,v 1.23 2006/02/20 20:57:13 jcamou Exp $

This document explains how to configure a VPN tunnel between FreeBSD and Check Point's VPN-1®/ Firewall-1®. Other documents provide similar information, but do not contain instructions specific to VPN-1/Firewall-1 and its integration with FreeBSD. These documents are listed at the conclusion of this paper for further reference.

1 Prerequisites

The following is a diagram of the machines and networks referenced in this document.



The FreeBSD gateway GW serves as a firewall and NAT device for "internal nets."

The FreeBSD kernel must be compiled to support IPsec. Use the following kernel options to enable IPsec support in your kernel:

```
options         IPSEC
options         IPSEC_ESP
options         IPSEC_DEBUG
```

For instructions on building a custom kernel, refer to the FreeBSD handbook (http://www.FreeBSD.org/doc/en_US.ISO8859-1/books/handbook/kernelconfig.html). Please note that IP protocol 50 (ESP) and UDP port `500` must be open between the Firewall-1 host and the FreeBSD GW.

Also, **racoon** must be installed to support key exchange. **Racoon** is part of the FreeBSD ports collection in `security/racoon`. The **racoon** configuration file will be covered later in this document.

2 Firewall-1 Network Object Configuration

Begin by configuring the Firewall-1 Policy. Open the Policy Editor on the Firewall-1 Management server and create a new "Workstation" Network Object representing FreeBSD GW.

`General Tab:`

```
Set name and IP address

VPN Tab:
Encryption Schemes Defined:             IKE               ---> Edit

IKE Properties:
Key Negotiation Encryption Methods:     3DES

Authentication Method:
Pre-Shared Secret ---> Edit
```

Select the Firewall Object and set a pre-shared secret. (Do not use our example.)

```
Support Aggressive Mode:                 Checked
Supports Subnets:                       Checked
```

After setting the pre-shared secret in the Firewall-1 Network Object definition, place this secret in the `/usr/local/etc/racoon/psk.txt` file on FreeBSD GW. The format for `psk.txt` is:

```
208.229.100.6          rUac0wtoo?
```

3 Firewall-1 VPN Rule Configuration

Next, create a Firewall-1 rule enabling encryption between the FreeBSD GW and the Firewall-1 protected network. In this rule, the network services permitted through the VPN must be defined.

```
Source             | Destination         | Service      | Action  | Track
-------------------------------------------------------------------------
FreeBSD GW         | FW-1 Protected Net  | VPN services | Encrypt | Long
FW-1 Protected Net| FreeBSD GW          |              |         |
```

"VPN services" are any services (i.e. `telnet`, SSH, NTP, etc.) which remote hosts are permitted to access through the VPN. Use caution when permitting services; hosts connecting through a VPN still represent a potential security risk. Encrypting the traffic between the two networks offers little protection if a host on either side of the tunnel has been compromised.

Once the rule specifying data encryption between the FreeBSD GW and the Firewall-1 protected network has been configured, review the "Action Encrypt" settings.

```
Encryption Schemes Defined:     IKE ---> Edit
Transform:                      Encryption + Data Integrity (ESP)
Encryption Algorithm:           3DES
Data Integrity:                 MD5
Allowed Peer Gateway:           Any or Firewall Object
Use Perfect Forward Secrecy:    Checked
```

The use of Perfect Forward Secrecy (PFS) is optional. Enabling PFS will add another layer of encryption security, but does come at the cost of increased CPU overhead. If PFS is not used, uncheck the box above and comment out the `pfs_group 1` line in the `racoon.conf` file on FreeBSD GW. An example `racoon.conf` file is provided later in this document.

4 FreeBSD VPN Policy Configuration

At this point, the VPN policy on FreeBSD GW must be defined. The setkey(8) tool performs this function.

Below is an example shell script which will flush setkey(8) and add your VPN policy rules.

```
#
# /etc/vpn1-ipsec.sh
#
# IP addresses
#
#     External Interface                    External Interface
#       208.229.100.6                       216.218.197.2
#                     |                     |
#        +--> Firewall-1 <--> Internet <--> FreeBSD GW <--+
#        |                                                |
# FW-1 Protected Nets                                Internal Nets
#    199.208.192.0/24                                    192.168.10.0/24
#
# Flush the policy
#
setkey -FP
setkey -F
#
# Configure the Policy
#
setkey -c << END
spdadd 216.218.197.2/32 199.208.192.0/24 any -P out ipsec
esp/tunnel/216.218.197.2-208.229.100.6/require;
spdadd 199.208.192.0/24 216.218.197.2/32 any -P in ipsec
esp/tunnel/208.229.100.6-216.218.197.2/require;
END
#
```

Execute the setkey(8) commands:

```
# sh /etc/vpn1-ipsec.sh
```

5 FreeBSD Racoon Configuration

To facilitate the negotiation of IPsec keys on the FreeBSD GW, the `security/racoon` port must be installed and configured.

The following is a **racoon** configuration file suitable for use with the examples outlined in this document. Please make sure you fully understand this file before using it in a production environment.

```
# racoon.conf for use with Check Point VPN-1/Firewall-1
#
# search this file for pre_shared_key with various ID key.
#
        path pre_shared_key "/usr/local/etc/racoon/psk.txt" ;
        log debug;
```

```
#
# "padding" defines some parameter of padding.  You should not touch these.
#
        padding
      {
        maximum_length 20;      # maximum padding length.
        randomize off;          # enable randomize length.
        strict_check off;       # enable strict check.
        exclusive_tail off;     # extract last one octet.
      }

        listen
      {
        #isakmp ::1 [7000];
        #isakmp 0.0.0.0 [500];
        #admin [7002];          # administrative port by kmpstat.
        #strict_address;        # required all addresses must be bound.
      }
#
# Specification of default various timers.
#
        timer
      {
#
# These values can be changed per remote node.
#
        counter 5;              # maximum trying count to send.
        interval 20 sec;        # maximum interval to resend.
        persend 1;              # the number of packets per a send.
#
# timer for waiting to complete each phase.
#
        phase1 30 sec;
        phase2 15 sec;
      }

        remote anonymous
      {
        exchange_mode aggressive,main; # For Firewall-1 Aggressive mode

        #my_identifier address;
        #my_identifier user_fqdn "";
        #my_identifier address "";
        #peers_identifier address "";
        #certificate_type x509 "" "";

        nonce_size 16;
        lifetime time 10 min;   # sec,min,hour
        lifetime byte 5 MB;     # B,KB,GB
        initial_contact on;
        support_mip6 on;
        proposal_check obey;    # obey, strict or claim
```

```
  proposal {
          encryption_algorithm 3des;
          hash_algorithm md5;
          authentication_method pre_shared_key;
          dh_group 2 ;
  }
}

  sainfo anonymous
{
  pfs_group 1;
  lifetime time 10 min;
  lifetime byte 50000 KB;
  encryption_algorithm 3des;
  authentication_algorithm hmac_md5;
  compression_algorithm deflate ;
}
```

Ensure that the `/usr/local/etc/racoon/psk.txt` file contains the pre-shared secret configured in the "Firewall-1 Network Object Configuration" section of this document and has mode `600` permissions.

```
# chmod 600 /usr/local/etc/racoon/psk.txt
```

6 Starting the VPN

You are now ready to launch **racoon** and test the VPN tunnel. For debugging purposes, open the Firewall-1 Log Viewer and define a log filter to isolate entries pertaining to FreeBSD GW. You may also find it helpful to tail(1) the **racoon** log:

```
# tail -f /var/log/racoon.log
```

Start **racoon** using the following command:

```
# /usr/local/sbin/racoon -f /usr/local/etc/racoon/racoon.conf
```

Once **racoon** has been launched, telnet(1) to a host on the Firewall-1 protected network.

```
# telnet -s 192.168.10.3 199.208.192.66 22
```

This command attempts to connect to the ssh(1) port on `199.208.192.66`, a machine in the Firewall-1 protected network. The `-s` switch indicates the source interface of the outbound connection. This is particularly important when running NAT and IPFW on FreeBSD GW. Using `-s` and specifying an explicit source address prevents NAT from mangling the packet prior to tunneling.

A successful **racoon** key exchange will output the following to the `racoon.log` log file:

```
pfkey UPDATE succeeded: ESP/Tunnel 216.218.197.2->208.229.100.6
pk_recvupdate(): IPSec-SA established: ESP/Tunnel 216.218.197.2->208.229.100.6
get pfkey ADD message IPsec-SA established: ESP/Tunnel 208.229.100.6->216.218.197.2
```

Once key exchange completes (which takes a few seconds), an ssh(1) banner will appear. If all went well, two "Key Install" messages will be logged in the Firewall-1 Log Viewer.

```
Action      |  Source        |  Dest.            | Info.
Key Install |  216.218.197.2 |  208.229.100.6    | IKE Log: Phase 1 (aggressive) completion.
Key Install |  216.218.197.2 |  208.229.100.6    | scheme: IKE methods
```

Under the information column, the full log detail will read:

```
IKE Log: Phase 1 (aggressive) completion. 3DES/MD5/Pre shared secrets Negotiation Id:
scheme: IKE methods: Combined ESP: 3DES + MD5 + PFS (phase 2 completion) for host:
```

7 References

- The FreeBSD Handbook: VPN over IPsec. http://www.FreeBSD.org/doc/en_US.ISO8859-1/books/handbook/ipsec.html
- KAME Project. http://www.kame.net