

Check Point Bridge Mode Support on Linux

April 2002

<http://www.checkpoint.com>

Introduction

Thank you for using Check Point Bridge Mode Support.

Check Point Bridge Mode Support is based on Check Point VPN-1/FireWall-1 NG FP1. This document describes the Bridge Mode Support features added to VPN-1/FireWall-1 NG FP1.

Please review this information before installing Check Point Bridge Mode Support.

Configuring VPN-1/FireWall-1 on Linux for Bridge-Mode Operation

FIGURE 1 shows a sample configuration for Bridge Mode.

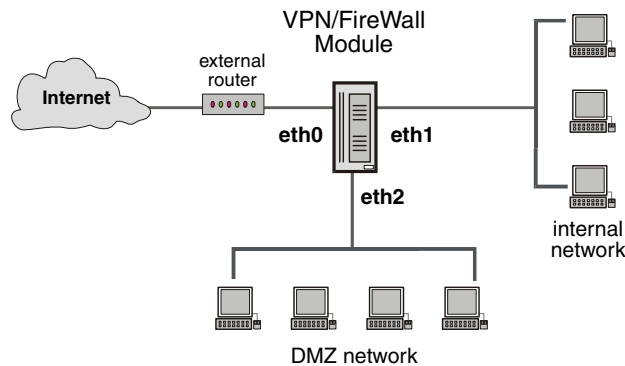


FIGURE 1 Sample Configuration

To configure VPN-1/FireWall-1 for bridge support, proceed as follows:

- 1 Assign the VPN/FireWall Module machine an available IP address of the internal network. Configure all three interfaces with the same IP address and network mask.
The external router and servers in the DMZ network should all have IP addresses from the internal network range.
- 2 Execute the following commands:

```
echo 1 > /proc/sys/net/ipv4/conf/eth0/proxy_arp
echo 1 > /proc/sys/net/ipv4/conf/eth1/proxy_arp
echo 1 > /proc/sys/net/ipv4/conf/eth2/proxy_arp
```

- 3 Configure the VPN/FireWall Module machine's routing table as follows:

```
ip route del x.x.x.x/y dev eth0
ip route del x.x.x.x/y dev eth1
ip route del x.x.x.x/y dev eth2
    (where x.x.x.x is the network address and y is the network mask bits; for example
    192.168.14.0/24)
ip route add x.x.x.a dev eth0
ip route add x.x.x.b dev eth2
ip route add x.x.x.x/y dev eth1
    (where x.x.x.a is the IP address of the external router and x.x.x.b should be repeated for
    each of the servers in the DMZ network).
```

- 4 Use **Get interfaces** and configure the topology as follows:
 - For eth2, define a group containing the IP addresses of all the servers in the DMZ and assign it as "specific".

- For eth1, define a group with exclusion containing the network of the internal network and excluding the IP address of the external router and the IP addresses of all the servers in the DMZ, and assign it as “specific”.
- For eth0, define “external”.

More Information

More information on the Linux Proxy ARP feature can be found at:

<http://www.sjdjweis.com/linux/proxyarp/>