

**Check Point Software Technologies LTD.ä**

***How To Configure Remote Link for  
Remote Deployment***

**Event: Partner Exchange Conference**

**Date: October 5, 1999**

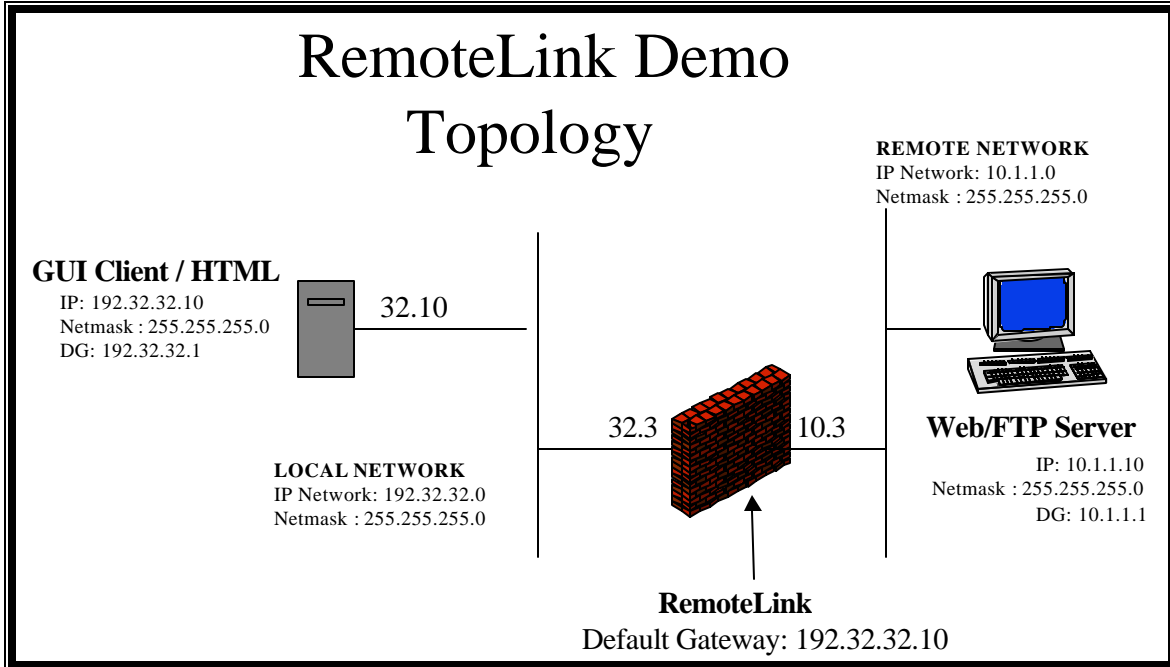
**Revision 1.2**

**Author: Lewis Colascione Jr., Regional Technical Manager, NE.**

# Remote Link VPN-1 Appliance

Check Point Remote Link VPN-1 Appliance is designed for remote deployment and management. It is designed to be configured at central site then shipped to a remote location to enable the locations to establish a VPN as well as providing Access Control and or Remote Access services for the remote location. The system's operating system characteristics would be managed by several utilities that we will have available from Nokia. The Check Point Software component would be managed in the standard fashion from the Check Point Enterprise Management console.

**Picture:**



Goal of the Demo:

- Show the ease of configuring and installing Remote Link.

**Picture:**



**- Required Equipment Needed For Demo:**

- Remote Link gateway.
- Operating System & Firewall Modules are Pre Installed
- The IPSO operating system is based on BSD but is hardened and tuned by Nokia for high performance routing
- ASCII terminal or serial cable to PC for Console.
- Network with Browser Client System for additional configuration options.
- Optional Internal system behind the Gateway.

**Configuration overview:**

1. Interconnect systems and hubs as per topology diagram.
2. Configure Network interfaces and routing. Insure you can ping from the Client system to the application server on the Remote Net.
3. Connect system or terminal to the console port of the Remote Link (9600, 8, None, 1)
4. Power up the Remote Link and follow the prompts for initial configuration options.

Remote link comes pre installed with all necessary software. Upon first power up the console will ask a series of questions for initial configuration. You will set the following settings;

- 1) Hostname
- 2) Select a Primary Interface
- 3) Define the IP Address & Netmask
- 4) Define the *admin* password.
- 5) The system will reboot and enable you to use other tools to administer the system option.

With the network enabled at this point you can use several tools to administer the Remote Link.

- 1) Command Line interface *iclid* . This has a Cisco look and feel for those users that need to have a Cisco like ability to manage the remote gateway. Type *iclid* at the command prompt.

```
Telnet - 192.32.32.3
Connect Edit Terminal Help

remotelink[admin]# iclid
remotelink> show
bgp      igmp      iphelper  mfc      rip      vrrp
bootpgw  igrp      krt       ospf     route
dvmrp    interface memory    resource  version
remotelink> show route
Codes: C - connected, S - static, I - IGRP, R - RIP, B - BGP, O - OSPF
       E - OSPF external, A - Aggregate, K - Kernel Remnant H - Hidden
       S - Suppressed

S  0.0.0.0/0      via 192.32.32.1, eth-s2p1c0, cost 0, age 4874
C  10.1.1/24     is directly connected, eth-s3p1c0
C  127.0.0.1/32  is directly connected, loop0c0
C  192.32.32/24  is directly connected, eth-s2p1c0

remotelink> show version

Ipsrd version 7.0 (obj.IPS0-3.1.1-FCS1-Ipsilon-rk - 1)
Built on Wed Feb 24 16:31:03 PST 1999
Started at Thu Oct 7 06:35:16 1999
Current time Thu Oct 7 15:08:14 1999
Up for 08:32:58

remotelink> █
```

- 2) Text based browser *lynx*. Type *lynx* at the command prompt.

```
Telnet - 192.32.32.3
Connect Edit Terminal Help

Nokia Network Voyager (p1 of 2)

Check Point Network Voyager

-----

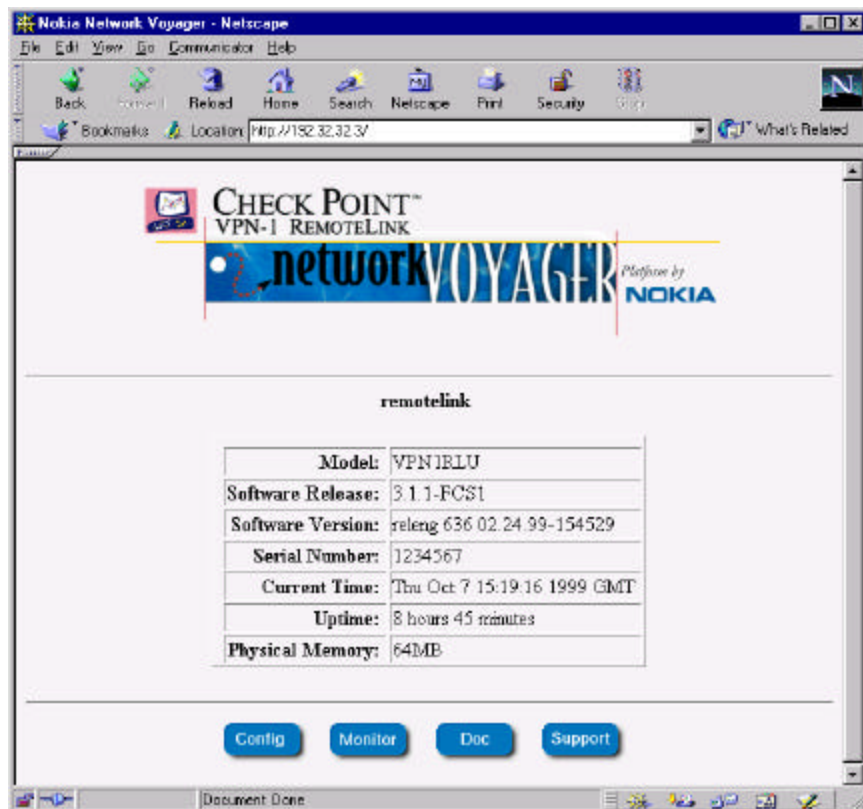
remotelink

Model: UPN1RLU
Software Release: 3.1.1-FCS1
Software Version: releng 636 02.24.99-154529
Serial Number: 1234567
Current Time: Thu Oct 7 15:05:59 1999 GMT
Uptime: 8 hours 31 minutes
Physical Memory: 64MB

-----

-- press space for next page --
Arrow keys: Up and Down to move. Right to follow a link; Left to go back.
H)elp O)ptions P)rint G)o M)ain screen Q)uit /=search [delete]=history list
```

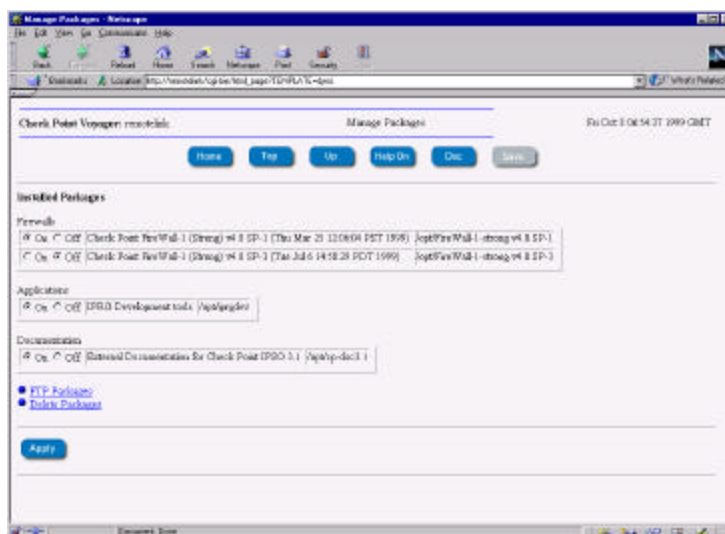
- 3) The HTML based interface using IE or Netscape; <http://192.32.32.3:80>



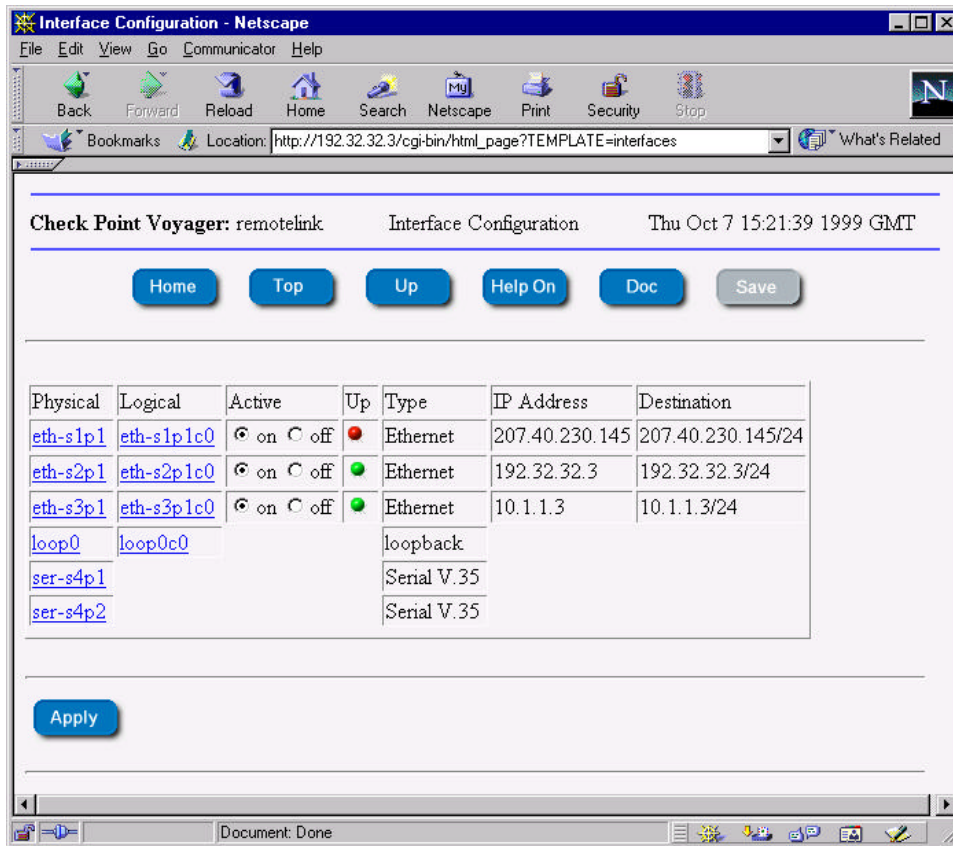
**Encrypted Remote Management:** There is also an ssh (Secure Shell) server component on Remote Link and you can ssh into the box or tunnel the HTTP traffic over the ssh port of 22. You can also configure Check Point SecuRemote to provide encrypted remote management.

You can perform the entire system configuration using this interface including rebooting and halting the Remote Link. Here are some screenshots of configuration options you will find using the HTML interface.

- 4) You can have multiple images of the operating system and the CheckPoint software loaded at the same time, and use the HTML GUI to switch between them. Click on the one to make active.

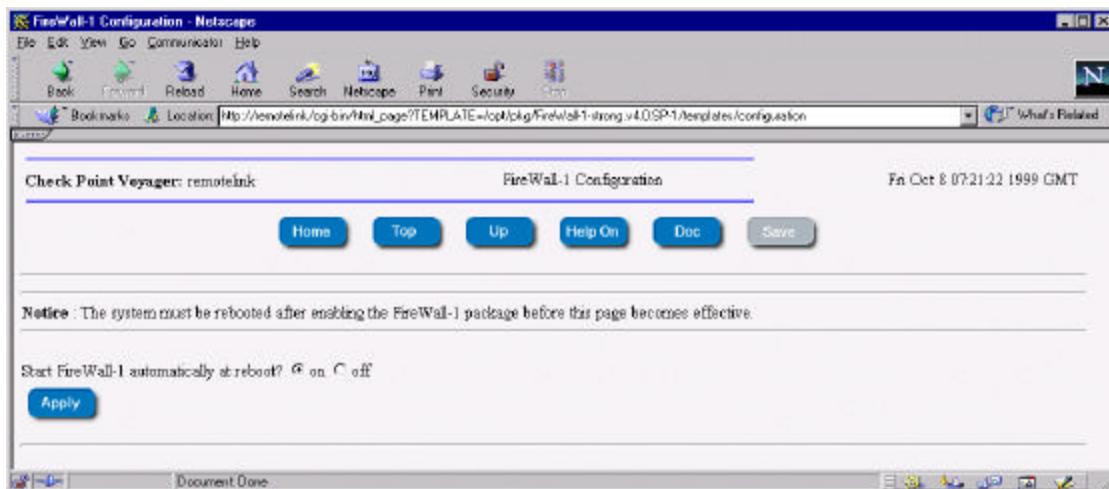


5) Configuring interface information with ease within Voyager.



**NOTE:** After making a change in Voyager when you *Apply* it this will be good for only this session. If you want this to be set after reboot then click *Save* to save it to the configuration database.

Once the system is configured and networked you will need to enable Firewall-1 in the Voyager GUI. Under *Security and Access Configuration* on the home page and select: **Check Point FireWall-1** and select to start Firewall-1 on boot up. Restart the Remote Link.



When the system comes back up login to the command line and perform the standard configuration functions that you would on a Firewall Module i.e.;

- 1) fwconfig
- 2) fw putlic
- 3) fw putkey ( To The Management Server)

Then install a security policy to the Remote Link from the Management Server.