

Tech Note

Redundant Internet Connections in Remote Offices

Chris Prince
Sr. Systems Engineer



Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
408 745 2000 or 888 JUNIPER
www.juniper.net

Part Number: 552022-001

Contents

Introduction.....	3
Configuring the Serial Port for Automatic Failover.....	3
Configure VPN Settings	5
Configure Routing and Policies for Traffic Flow	6
Configuring the Second Untrust Ethernet Port for Automatic Failover	7
Configure VPN Settings	8
Configure Routing and Policies for Traffic Flow	9

Introduction

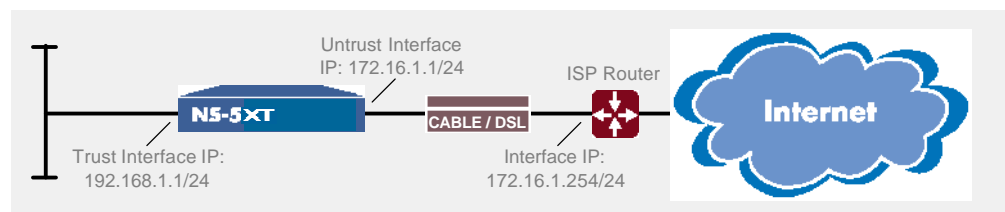
Today's business-critical applications require redundant network connectivity to avoid downtime. Often with small remote offices or home offices, it is not cost effective to deploy redundant hardware to provide a backup Internet connection. The Juniper Networks ScreenOS in the NetScreen-5XT and NetScreen-5GT security appliances offers the ability to configure a backup Ethernet or dialup interface for Internet connectivity, should the default connection become unavailable. This paper explains how to configure the Juniper Networks NetScreen 5XT appliance to redirect firewall and VPN traffic to either a dial backup or Ethernet backup interface in the event of a failure on the primary interface.

Configuring the Serial Port for Automatic Failover

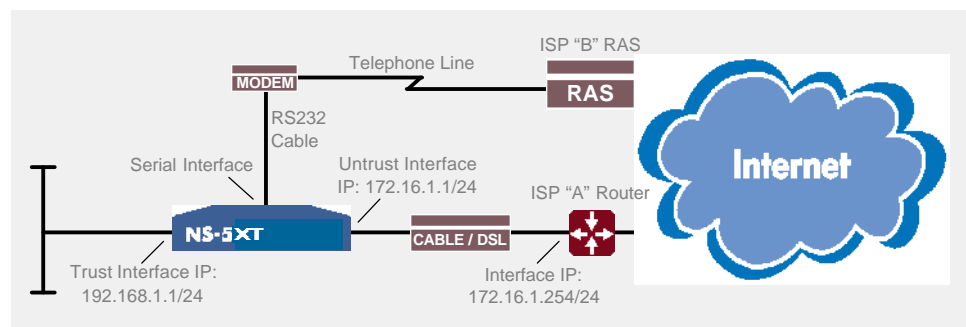
The Juniper Networks NetScreen-5XT or NetScreen-5GT devices offer a 9-Pin serial port labeled Modem. Through this serial interface, ScreenOS can use the Point-to-Point Protocol (PPP) to authenticate and obtain an IP address from an Internet Service Provider (ISP).

Configuring the NetScreen-5XT to utilize the serial interface as a dial backup interface requires several steps. Please note that the examples provided below represent a standard implementation for the dial backup feature.

- Configure the Juniper Networks NetScreen-5XT for normal firewall operation using an Ethernet connection with a static IP as the primary Internet connection. Validate Internet connectivity by performing a ping and/or a DNS lookup from a workstation in the Trust zone.



- Connect a modem or terminal adapter to the port labeled "Modem" on the Juniper Networks NetScreen-5XT appliance using a straight-through RS-232 cable. You can verify serial connectivity by observing the Terminal Ready light on the modem.



- Bind the serial interface to the Untrust zone

```
set interface serial zone Untrust
```

NOTE When binding the serial interface from the WebUI, a backup default route is added to allow traffic to be routed over the serial interface during a failover state.

- Configure a default route for the serial interface. This will enable the routing of Internet-bound traffic during failover operation.

```
set route 0.0.0.0/0 interface serial
```
- Configure the global failover mode for auto mode and the holddown timer for 10 seconds. This will force an automatic failover to take place 10 seconds after link status goes down on the primary Untrust interface.

```
set failover auto
set failover holddown 10
```
- Configure modem and connection behavior. In the command below, we add a new modem type with an initialization string for a US Robotics 5686 model. Also, we configure the connect speed for a maximum of 57.6Kbps and configure the modem to retry an ISP connection attempt two times, waiting 20 seconds between each retry. Lastly, we configure an inactivity timeout of 20 minutes before dropping the dialup link.

```
set modem settings "USR5686" active
set modem settings "USR5686" init "AT&F1"
set modem speed 57600
set modem retry 2
set modem interval 20
set modem idle-time 20
```
- Configure primary dialup ISP connection with the highest priority, 1. Configure primary/alternative phone numbers and a login username and password for this account.

```
set modem isp PrimaryDialupISP priority 1
set modem isp PrimaryDialupISP primary-number 5551212 alternative-
number 5551213
set modem isp PrimaryDialupISP account login username password xxx
```
- Configure optional secondary dialup ISP connection with the second highest priority, 2. Configure primary/alternative phone numbers and login username and password for this account.

```
set modem isp AltDialupISP priority 2
set modem isp AltDialupISP primary-number 5551222 alternative-
number 5551223
set modem isp AltDialupISP account login username password yyy
```

Configure VPN Settings

For VPN configuration, we only cover the configuration steps required for a local gateway device. It will be necessary to configure the remote gateway device VPN settings to match the local phase 1 and phase 2 settings outlined below.

- Configure two unnumbered tunnel interfaces to be used by the primary and backup VPN connection. The tunnel interfaces will reside in the trust zone and is associated with the untrust interface for addressing since this is an unnumbered interface.

```
set interface tunnel.1 zone Trust
set interface tunnel.1 ip unnumbered interface untrust
set interface tunnel.2 zone Trust
set interface tunnel.2 ip unnumbered interface untrust
```

- Configure an AutoKey IKE VPN to a gateway device with a static IP address of 172.16.2.1, which will serve as the primary VPN using the default Untrust Ethernet interface. In this example, the remote network is 192.168.2.0/24.

```
set ike gateway PrimaryToCorp ip 172.16.2.1 Main outgoing-
interface untrust preshare netscreen sec-level standard

set vpn PrimaryToCorp gateway PrimaryToCorp no-replay tunnel
idletime 0 sec-level standard

set vpn PrimaryToCorp bind interface tunnel.1

set vpn PrimaryToCorp proxy-id local-ip 192.168.1.0/24 remote-ip
192.168.2.0/24 ANY
```

- Configure a second AutoKey IKE VPN to a gateway with a static IP address of 172.16.2.1 which will serve as the backup VPN which will use the serial interface. In this example, the remote network is 192.168.2.0/24.

```
set ike gateway BackupToCorp ip 172.16.2.1 aggressive local-id
dialbackup outgoing-interface serial preshare netscreen sec-level
standard

set vpn BackupToCorp gateway BackupToCorp no-replay tunnel
idletime 0 sec-level standard

set vpn BackupToCorp bind interface tunnel.2

set vpn BackupToCorp proxy-id local-ip 192.168.1.0/24 remote-ip
192.168.2.0/24 ANY
```

NOTE Since the serial interface receives its IP address dynamically (using PPP), the following configuration differences should be noted:

- IKE gateway configuration must always be to a device with a static IP.
 - You must configure a Peer ID on this device since the remote gateway device will be configured to use a dynamic IP address for its gateway settings.
 - The Peer ID configured in this step should be identical to the Peer ID configured on the remote gateway device.
 - Aggressive mode must be selected for the IKE gateway configuration.
-

Configure Routing and Policies for Traffic Flow

- Configure routes to direct traffic through the appropriate tunnel interface/VPN. In this example, the remote network is 192.168.2.0/24. Note that the second route will only be used when the serial interface is active.

```
set route 192.168.2.0/24 interface tunnel.1
```

```
set route 192.168.2.0/24 interface tunnel.2
```

- Configure address-book entries and policies to allow traffic to pass between zones. Note, since we configured the tunnel interfaces to reside in the trust zone, traffic will not be checked against a policy before traversing the VPN, because the source and destination both reside in the Trust zone. To enable policy checking for this scenario, you will need to turn on intra-zone blocking for the trust zone and create a policy to allow traffic to pass. To enable intra-zone blocking for policy control of traffic through the tunnel, perform the following step.

```
set zone trust block
```

Configuring the Second Untrust Ethernet Port for Automatic Failover

The Juniper Networks ScreenOS also offers a backup Ethernet interface in the Juniper Networks NetScreen-5XT and NetScreen-5GT. This second interface can be configured with a static IP address or it can obtain an IP address dynamically through DHCP or PPPoE. Also note that the backup Ethernet interface can never be active at the same time as the default Untrust interface.

NOTE In ScreenOS 4.0.0-DIAL, two instances of PPPoE are supported but only a single instance of DHCP client is supported.

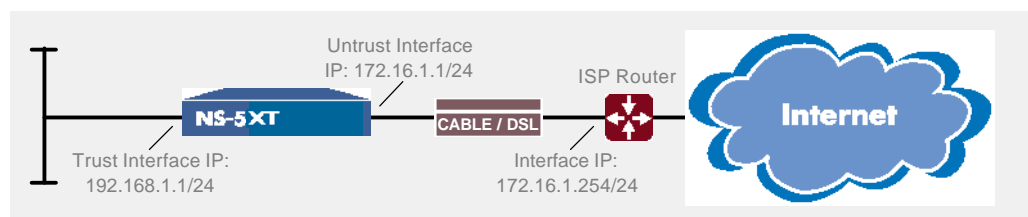
The following steps must be completed to configure a Juniper Networks NetScreen-5XT with dual untrust for a network redundancy via a secondary Ethernet port.

- Configure the NetScreen-5XT for Dual Untrust mode.

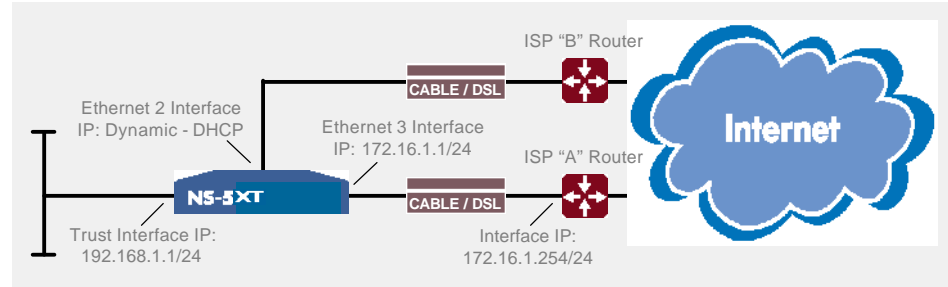
```
exec port-mode dual-untrust
```

NOTE Operational mode change will erase current configuration. Once the device reboots, it will be at a factory default configuration in Dual Untrust mode.

- Configure the NetScreen-5XT for normal firewall operation using an Ethernet connection with a static IP as the primary Internet connection. Validate Internet connectivity by performing a ping and/or a DNS lookup from a workstation in the Trust zone.



- Connect an Ethernet cable to the port labeled “Trusted 4” on the Juniper Networks NetScreen-5XT chassis. The other end of the Ethernet cable will connect to a hub or directly to the backup CPE device provided by your ISP (i.e. cable modem).



- Configure the global failover mode for auto mode and the holddown timer for ten seconds. This will force an automatic failover to take place ten seconds after link status goes down on the primary Untrust interface.

```
set failover auto
set failover holddown 10
```

NOTE Since the backup Ethernet interface obtains its IP address dynamically using DHCP, a backup default route does not need to be configured.

Configure VPN Settings

For VPN configuration this paper will only cover the configuration steps required for the local gateway device. It will be necessary to configure the remote gateway device VPN settings to match the local phase 1 and phase 2 settings outlined in the steps below.

- Configure two unnumbered tunnel interfaces to be used by the primary and backup VPN connection. The tunnel interfaces will reside in the trust zone but will be associated with the untrust interface for addressing since this is an unnumbered interface.

```
set interface "tunnel.1" zone "Trust"
set interface tunnel.1 ip unnumbered interface untrust
set interface "tunnel.2" zone "Trust"
set interface tunnel.2 ip unnumbered interface untrust
```

- Configure an AutoKey IKE VPN to a gateway device with a static IP address of 172.16.2.1 which will serve as the primary VPN using the default Untrust Ethernet interface (ethernet3). In this example, the remote network is 192.168.2.0/24

```
set ike gateway PrimaryToCorp ip 172.16.2.1 Main outgoing-
interface ethernet3 preshare netscreen sec-level standard
set vpn PrimaryToCorp gateway PrimaryToCorp no-replay tunnel
idletime 0 sec-level standard
set vpn PrimaryToCorp bind interface tunnel.1
```

```
set vpn PrimaryToCorp proxy-id local-ip 192.168.1.0/24 remote-ip
192.168.2.0/24 ANY
```

- Configure a second AutoKey IKE VPN to a gateway with a static IP address of 172.16.2.1 which will serve as the backup VPN which will use the backup Ethernet interface (ethernet2). In this example, the remote network is 192.168.2.0/24.

```
set ike gateway BackupToCorp ip 172.16.2.1 Aggr local-id ethbackup
outgoing-interface ethernet2 preshare netscreen sec-level standard
```

```
set vpn BackupToCorp gateway BackupToCorp no-replay tunnel
idletime 0 sec-level standard
```

```
set vpn BackupToCorp bind interface tunnel.2
```

```
set vpn BackupToCorp proxy-id local-ip 192.168.1.0/24 remote-ip
192.168.2.0/24 ANY
```

Configure Routing and Policies for Traffic Flow

- Configure routes to direct traffic through the appropriate tunnel interface/VPN. In this example, the remote network is 192.168.2.0/24. Note that the second route will only be used when the backup Ethernet interface is active

```
set route 192.168.2.0/24 interface tunnel.1
```

```
set route 192.168.2.0/24 interface tunnel.2
```

- Configure address-book entries and policies to allow traffic to pass between zones. Note, since we configured the tunnel interfaces to reside in the trust zone, traffic will not be checked against a policy before traversing the VPN, because the source and destination both reside in the Trust zone. To enable policy checking for this scenario, you will need to turn on intra-zone blocking for the trust zone and create a policy to allow traffic to pass. To enable intra-zone blocking for policy control of traffic through the tunnel, perform the following step

```
set zone trust block
```

Copyright © 2004, Juniper Networks, Inc. All rights reserved. Juniper Networks is registered in the U.S. Patent and Trademark Office and in other countries as a trademark of Juniper Networks, Inc. Broadband Cable Processor, ERX, ESP, G10, Internet Processor, Internet Processor II, JUNOS, JUNOScript, M5, M10, M20, M40, M40e, M160, M-series, NMC-RX, SDX, ServiceGuard, T320, T640, T-series, UMC, and Unison are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners. All specifications are subject to change without notice.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.