TECHNICAL NOTE

EMC® NetWorker
Simplifying firewall port requirements with NSR tunnel
Release 8.0 and later

Technical Note

P/N 300-999-649
REV 03

February 6, 2014

This technical note describes how to configure and use NSR tunnel in a NetWorker environment. Topics include:

EMC²

Terminology

This section describes the terms used in this document.

- Secure network — An internal network protected from other networks by a firewall.
- Insecure network — A network external to a firewall.
- The tunnel — The connection established between the Proxy and Server.
- Server — The host at the end of the tunnel in the secure network. The Server uses the tunnel to provide services to the insecure network. The Server can be a NetWorker server or a NetWorker storage node in the data zone.
- Proxy — The host at the end of the tunnel in the insecure network. The Proxy forwards traffic to the Server. A non-dedicated Proxy forwards traffic between the insecure network and the Server. A dedicated Proxy only forwards its own traffic.
- NSR tunnel resource — An NSRLA database resource that defines the tunnel configuration. An NSR tunnel resource exists on the Server and the Proxy for each tunnel.
- nsrtund daemon — The tunnel daemon. This daemon runs on the Server and the Proxy after the NSR tunnel resource is created. The nsrexecd daemon manages the nsrtund process. All network traffic routes through the tunnel between the nsrtund daemon on the Server and nsrtund daemon on the Proxy.
- Server tunnel address — An unassigned IPv4 address allocated to the Server in the insecure network. The clients and storage nodes in the insecure network use this IP address to communicate with the Server in the secure network.
- Proxy tunnel address — An unassigned IPv4 address allocated to the Proxy host in the insecure network.
- Connection port — The port number used to establish the tunnel between the Server and the Proxy.
- Encapsulation — The process of adding a header containing the Server or Proxy IPv4 address to each block of data passed to the tunnel.

Overview of NSR tunnel

NSR tunnel is a configurable feature in the NetWorker 8.0 and later software that enables communications through a firewall by using a single TCP service port. You create an NSR tunnel resource on two separate hosts: the Server and the Proxy. The tunnel creates a connection between the Server in the secure network and the Proxy in the insecure network. NetWorker data passes between the secure and insecure network through the tunnel.

After you create an NSR tunnel resource on the Server and the Proxy, the following processing occurs:

1. The nsrexecd daemon on each host starts the nsrtund daemon.
2. The Proxy listens for incoming connections on the connection port.
3. The Server contacts the Proxy on the connection port.

4. Each nsrtund daemon creates a tunnel device interface.
5. NSR tunnel assigns:
   - The server tunnel address to the tunnel device interface on the Server
   - The proxy tunnel address to the tunnel device interface on the Proxy.
6. The Server creates a route to enable communication between the Server and the Proxy.
7. When the Proxy is non-dedicated:
   - The Server creates a route to enable communication between the Server and the insecure network.
   - NSR tunnel registers an entry in the arp table on the Proxy host. This entry maps the server tunnel address to a MAC address of a proxy network interface.
   - NetWorker clients and storage nodes in the insecure network use the server tunnel address to communicate with the NetWorker server.
8. After the tunnel forms, NSR tunnel encapsulates any data sent to the tunnel. This permits traffic through the firewall.

Note: The NSR tunnel feature does not provide data encryption natively.

NSR tunnel requirements

Before configuring NSR Tunnel, review the operating system requirements and network restrictions. When migrating to NSR Tunnel from the FTS NSR-FWX feature, review the NSR-FWX differences.

- "Operating system requirements" on page 3
- "Network restrictions" on page 4
- "FTS NSR-FWX differences" on page 4

Operating system requirements

NSR tunnel supports the following operating systems for the Server and Proxy hosts:

- Oracle Solaris on Sparc
- Oracle Solaris on AMD64
- Red Hat Enterprise on Linux (RHEL) on x86 and x64
- SUSE Linux Enterprise Server (SLES) on x86 and x64

The operating systems of the Server and Proxy can differ. For example, NSR tunnel supports a Solaris Server and a RHEL Proxy.

For a Solaris 11 Proxy host, you must apply the fix for issue CR 7169661 before configuring NSR tunnel. This fix,available in Solaris 11.1 SRU4.6 and later allows the creation of an arp entry for the Server on the Proxy. Contact Oracle for more information.

The *NetWorker Software Compatibility Guide* provides more information about the operating system versions the NetWorker client software supports.

Network restrictions

The NSR tunnel feature restricts traffic to the connection port and encapsulates the data. Encapsulation results in packet transmission delays and CPU overhead on the Proxy.

NSR tunnel does not support the following networking features:

- IPv6 protocol
- UDP traffic

Note: If a hop in a route contains the tunnel, you cannot trace the route with the **traceroute** command on UNIX or the **tracert** command on Windows because it uses the UDP protocol. Use an alternate program for example, **tcptraceroute** or if available use **traceroute** with the -T option.

FTS NSR-FWX differences

FTS NSR-FWX is the Fujitsu-Siemens implementation of a single port firewall solution.

Table 1 on page 4 describes the differences between the NSR tunnel and FTS NSR-FWX.

Table 1 The differences between NSR tunnel and FTS NSR-FWX

NSR tunnel	FTS NSR-FWX
The NetWorker client package includes the NSR tunnel software.	The FTS NetWorker client package does not include the FTS NSR-FWX feature. The FTS NSR-FWX feature is a separate package
Stores configuration information in the NSRLA database on the Server and Proxy host.	Stores configuration information in separate configuration files located in the /nsr/fwx folder.
The nsrtund daemon establishes a tunnel on the Server and Proxy at startup.	Start scripts establish the tunnel.
Does not require a license.	Requires a filter license.

Tunnel configurations

Before implementing NSR tunnel, review the following examples of common tunnel configurations:

Server and dedicated Proxy

Figure 1 on page 5 provides an example of a Server and dedicated Proxy configuration. In this example, the tunnel does not forward client and storage node traffic in the insecure network to the NetWorker server.

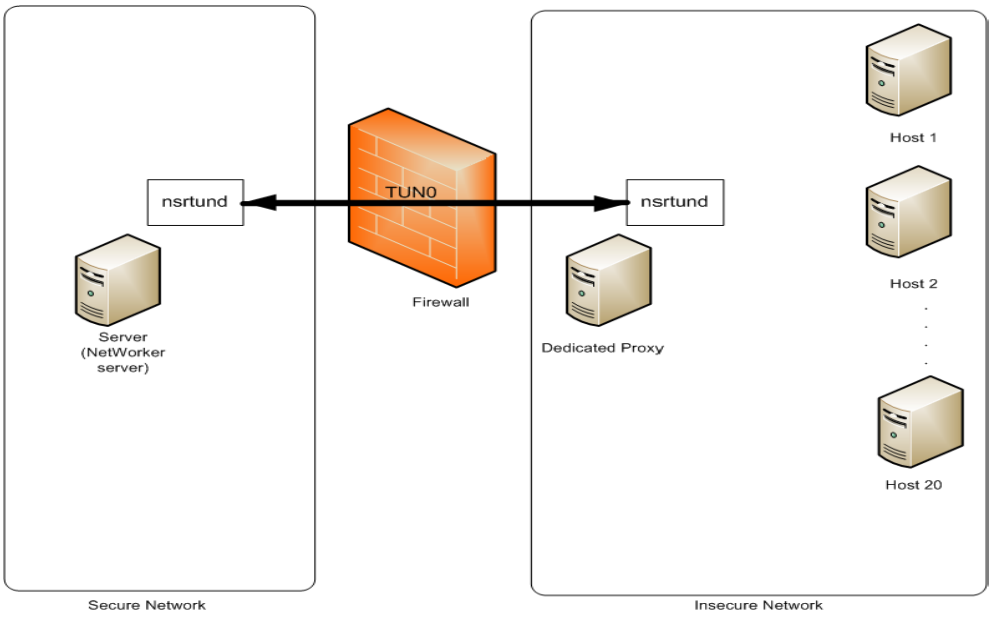

Figure 1 Server and dedicated Proxy configuration

Server and non-dedicated Proxy

Figure 2 on page 6 provides an example of a Sever and a non-dedicated Proxy serving multiple external NetWorker clients and one external storage node.

The configuration includes the following specifications:

- The Server is the NetWorker server in the secure network.
- NSR tunnel forwards client and storage node traffic in the insecure network to the NetWorker server through the tunnel, TUN0.
- All client metadata flows through the Proxy to the NetWorker server.
- All client backup data writes to the storage node in the insecure network.

This configuration results in faster backup performance because the tunnel forwards less traffic between the insecure and secure network.

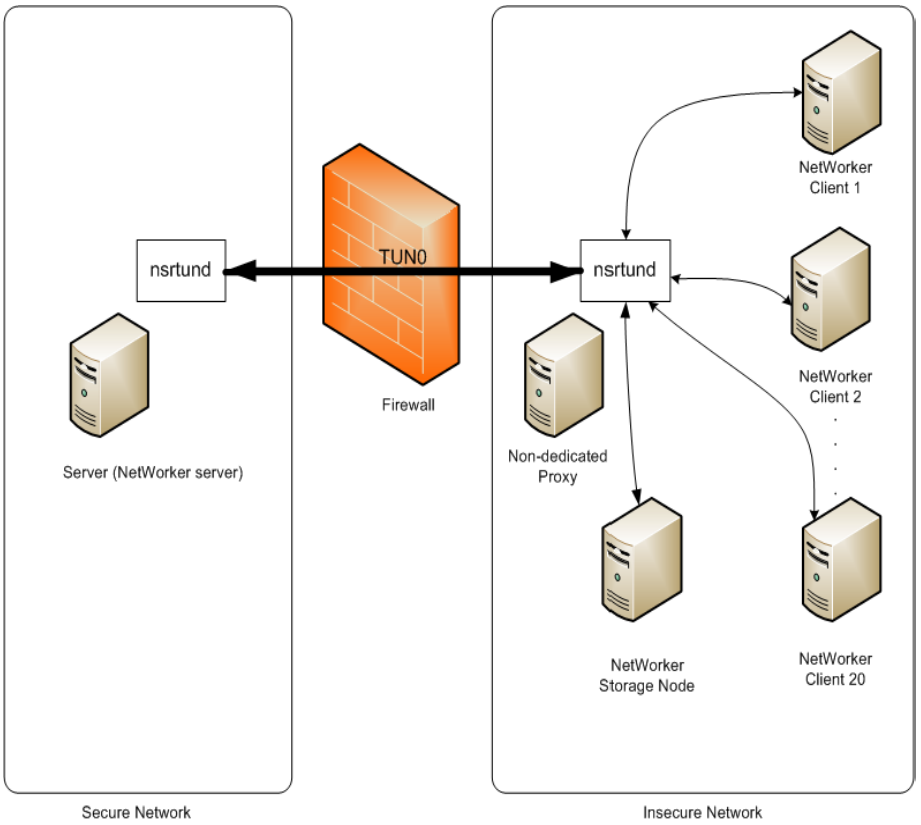

Figure 2 Sever and Proxy configuration with multiple external NetWorker clients

Multiple Servers with one Proxy and multiple clients

Figure 3 on page 7 provides an example of multiple Servers with one Proxy and multiple clients in the insecure network.

The configuration includes the following specifications:

- There are two tunnels on the same Proxy: Tun0 and Tun1.
- The secure network has two Servers: the NetWorker server and a storage node.
- A single host acts as the Proxy for the NetWorker server and the storage node in the secure network.
- All client backup data and metadata flow through the same Proxy.
- NSR tunnel forwards client metadata traffic to the NetWorker server through the tunnel, TUN0.
- NSR tunnel forwards client traffic in the insecure network to the NetWorker Storage Node through the tunnel, TUN1.
- This configuration may result in slower backup performance becaues the Proxy forwards all data between the secure and insecure network.

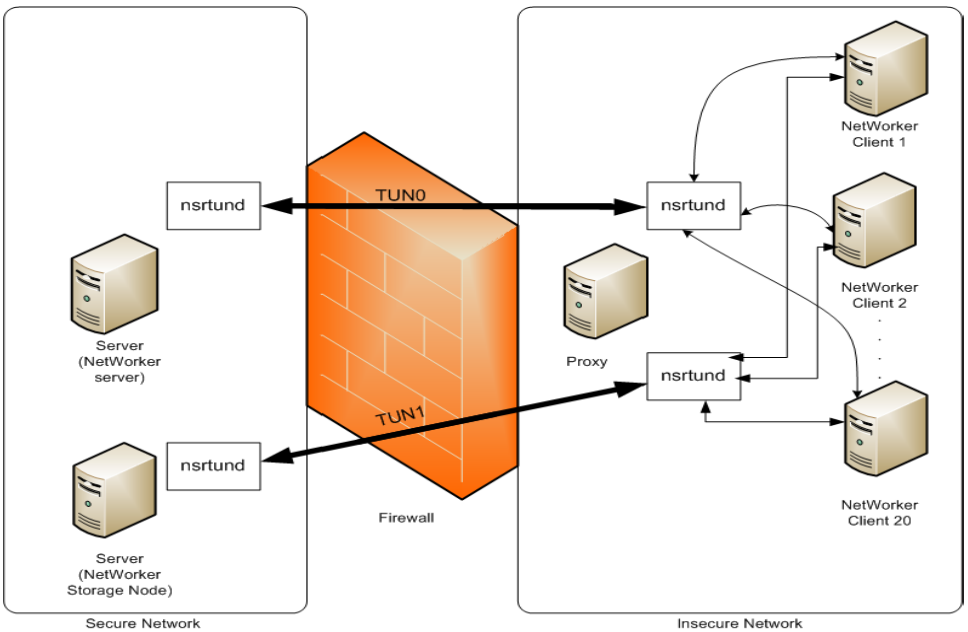

Figure 3 Multiple Servers with multiple Proxies and multiple NetWorker clients in the insecure network

Multiple Servers with multiple Proxies and multiple clients

Figure 4 on page 8 provides an example of multiple Servers with multiple Proxies and multiple NetWorker clients in the insecure network.

The configuration includes the following specifications:

- The secure network has two servers.
- One host acts as the Proxy for the NetWorker server (Proxy 1) and one host acts as the Proxy for the storage node (Proxy 2).
- NSR tunnel forwards client metadata traffic in the insecure network to the NetWorker server through the tunnel, TUNO.
- NSR tunnel forwards client data traffic in the insecure network to the NetWorker storage node through the tunnel, TUN1.

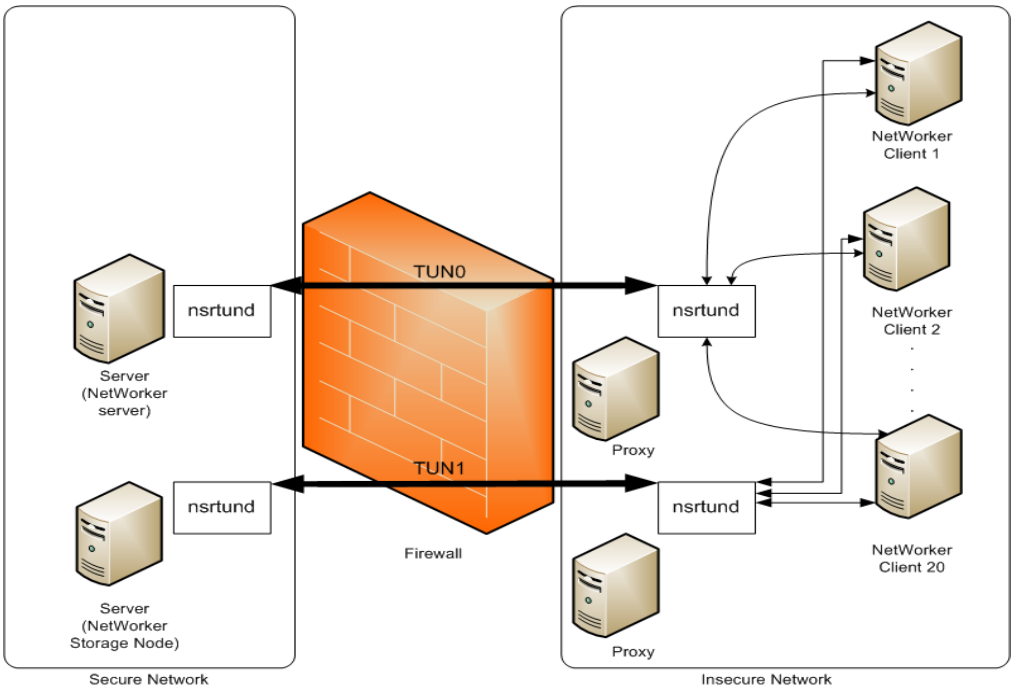

Figure 4 Multiple Servers with multiple Proxies and multiple NetWorker clients in the insecure network

Server with multiple Proxy hosts and storage node in the insecure network

Figure 5 on page 9 provides an example of multiple Servers with multiple Proxy hosts and multiple NetWorker clients in the insecure network.

The configuration includes the following specifications:

- The secure network has one Server.
- One host acts as the Proxy for the NetWorker server (Proxy 1) and a NetWorker storage node acts as the Proxy (Proxy 2).
- NSR tunnel forwards client metadata traffic in the insecure network to the NetWorker server through the tunnel, TUNO.
- NSR tunnel forwards backup metadata traffic from the NetWorker storage node to the NetWorker server through the tunnel, TUN1.

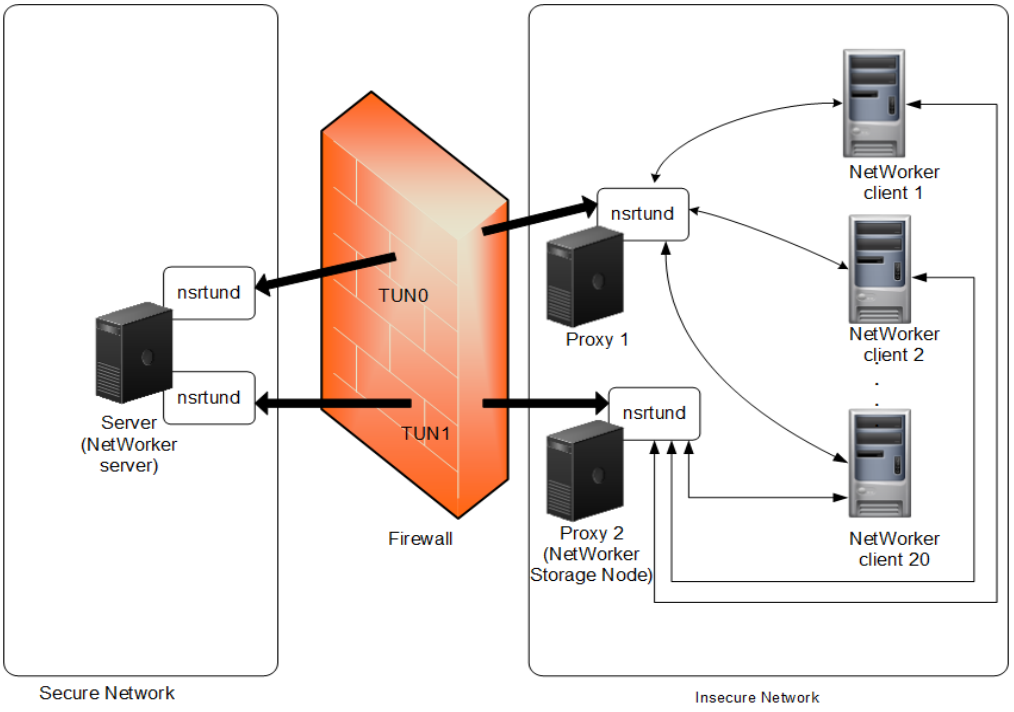

Figure 5 Single server with multiple Proxy hosts and and storage node in the insecure network

Preconfiguration checklists

Before you configure the NSR tunnel resources on the Server and Proxy hosts, review the following preconfiguration checklists.

- "FTS NSR-FWX migration checklist" on page 11 applies to FTS NSR-FWX migrations to NSR tunnel only.
- "Firewall checklist" on page 12 applies to all implementations of NSR tunnel.
- "Networking checklist" on page 13 applies to all implementations of NSR tunnel.

FTS NSR-FWX migration checklist

Before you migrate from FTS NSR-FWX to NSR tunnel resource, you must complete FTS NSR-FWX-related tasks. Table 2 on page 11 summarizes these tasks.

Table 2 FTS NSR-FWX migration checklist

Task	FTS NSR-FWX information
❑ Record the value for each variable in the FTS NSR-FWX configuration files. You will use this information when you configure the NSR tunnel resources.	From /nsr/fwx/vtun_xxx: ❑ tunnel= ❑ fwx_server= ❑ fwx_proxy= ❑ real_proxy= ❑ real_server= ❑ gateway_to_proxy= ❑ fwx_net_addr= ❑ fwx_proxy_interface= From vtun.conf: ❑ port= From nsrfwx.conf: ❑ ALLOW_ICMP= ❑ PERMANENT_TCP_PORTS=
❑ Uninstall the FTS NSR-FWX software.	On Linux, remove the nsr-fwx package on the Server and the nsr-vtun package on both the Server and the Proxy host. On Solaris, remove the SMAWnwfwx package on the Server and the SMAWnwvt and SMAWtun packages from both Server and Proxy.
❑ Remove the FTS NetWorker software from the Server and the Proxy hosts, and then install the EMC NetWorker software.	The *NetWorker Installation Guide* describes how to install the EMC NetWorker software.
❑ Remove the FTS NetWorker software from the FTS clients and storage nodes, and then install the EMC NetWorker software.	The *NetWorker Installation Guide* describes how to install the EMC NetWorker software.

Firewall checklist

Before you configure the NSR tunnel resource, you must complete firewall-related tasks. Table 3 on page 12 summarizes these tasks.

Table 3 Firewall configuration checklist

Task	Configuration information
❑ Select a TCP port that is available and unused by the Server and Proxy to establish communications between the secure and insecure network.	Specify the port number in **connection port** attribute in the NSR tunnel resource. Each tunnel connection uses one unique port. **connection port** value=
❑ For firewalls that use TCP Intercept, exclude the tunnel connection.	Firewall documentation describes how to add exclusions.
❑ Configure firewall rules to enable tunnel communications: Source = any Dest = *Server_host:connection_port* Permit all outbound traffic	Each tunnel between a secure and insecure network must communicate over a unique connection port. Add a destination rule on the firewall for each connection port.
❑ On Linux hosts only, update the local firewall to permit inbound traffic to reach the connection port.	The Linux kernel contains a built-in firewall which is always enabled. The default rule set on some Linux hosts, RHEL for example, blocks incoming traffic to unknown ports.
❑ Optionally on the Proxy host, configure a personal firewall.	A personal firewall prevents communication through the tunnel between unauthorized clients in the insecure network and the Server.
❑ Determine which host will initiate the connection and which host will listen on the connection.	When the Server initiates the connection, the tunnel direction attribute in the NSR tunnel resource is **server-to-proxy**. When the Proxy initiates the connection, the tunnel direction attribute in the NSR tunnel resource is **proxy-to-server.**

Networking checklist

Before you configure the NSR tunnel resource, you must complete networking-related tasks. Table 4 on page 13 summarizes these tasks.

Table 4 Networking checklist

Task	Configuration information
❑ Ensure that a route exists from the Server to the insecure network.	Use **netstat -rn.** Vendor documentation provides more information.
❑ Allocate one static IPv4 address in the insecure network for the Server: ❑ Associate one hostname with the IPv4 address. ❑ Ensure that the Server host, Proxy host, and each client and storage node in the insecure network can successfully perform forward and reverse lookups of the hostname and IPv4 address.	Specify the IP address in the **server tunnel address** attribute in the NSR tunnel resource. **server tunnel address** value=
❑ Allocate one IPv4 address in the insecure network for the Proxy: ❑ Associate one hostname with the IPv4 address. ❑ Ensure that the Server host and Proxy host can successfully perform forward and reverse lookups of the hostname and IPv4 address.	Specify the IP address in the **proxy tunnel address** attribute in the NSR tunnel resource. **proxy tunnel address** value=
❑ For non-dedicated Proxy configurations only: ❑ Choose a network interface on the Proxy host. The clients in the insecure network use this interface to connect to the tunnel. ❑ Ensure that you enable IPv4 forwarding on the Proxy host. The Operating System User Guide describes how to enable IPv4 forwarding.	Specify the name of the interface in the **proxy network interface** attribute in the NSR tunnel resource. For example, bge0 (Solaris) or eth0 (Linux). **proxy network interface** value= For a Solaris 11 Proxy, you must apply the fix for issue CR 7169661 before configuring NSR tunnel. This fix allows the creation of an arp entry for the Server on the Proxy. Contact Oracle for more information.

Table 4 Networking checklist

Task	Configuration information
❑ Record the real IPv4 address of the Server in the secure network.	Specify the IPv4 address in the **server address** attribute in the NSR tunnel resource. **server address** value:=
❑ Record the real IPv4 address of the Proxy in the insecure network.	Specify the IPv4 address in the **proxy address** attribute in the NSR tunnel resource. **proxy address** value=
❑ For non-dedicated Proxy configurations only, record the network and the subnet of the insecure network, to enable the Server to reply back to all clients in the insecure subnet.	Specify the network and the subnet in the **proxy network** attribute. For example, if the Proxy address is 199.123.123.123, the **proxy network** value is 199.123.123.0/24. **proxy network** value=

Configuring NSR tunnel

Perform the following tasks to configure NSR tunnel:

Task 1: Configure the Proxy

These steps describe how to configure the NSR tunnel resources and start the **nsrtund** daemon on the Proxy host.

1. Log in to the Proxy host as root.
1. Edit the **/nsr/res/servers** file.
2. In the first line of the file, specify the IP address of the **server tunnel address**.
3. Save the file.
4. Stop the NetWorker daemons:

   ```
   nsr_shutdown
   ```

5. Start the NetWorker daemons:

   ```
   /etc/init.d/networker start
   ```

6. Confirm that the nsrexecd daemon starts:

   ```
   ps -ef | grep nsrexecd
   ```

7. Type:

   ```
   /usr/sbin/nsr_install_tun
   ```

   On Solaris, this command installs and loads TUN drivers provided by the NetWorker software. Linux uses native tun drivers and the **nsr_install_tun** command loads the tun drivers.

8. Use **nsradmin** in visual mode to create the **NSR tunnel** resource in the NSRLA database:

   ```
   nsradmin -p nsrexec -c
   ```

9. Select **Create**.

10. Modify the NSR tunnel resource attributes. Table 5 on page 16 describes each NSR tunnel resource attribute and lists the equivalent NSR-FWX attribute name.

Table 5 **Proxy side** NSR tunnel resource attributes

NSR tunnel attribute	**Definition**	**NSR-FWX attribute name**
Name	The name of the tunnel resource. The name of each tunnel resource must be unique. Required.	n/a
autostart	The state of the **nsrtund** daemon. When creating a new resource, select **Enabled**. This starts the **nsrtund** daemon after you save the resource. This also enables the **nsrtund** daemon to start at startup. When modifying an existing resource, select **Restart now**. This restarts the nsrtund daemon after you save the resource. To disable the resource, select **Disabled.** This stops the **nsrtund** daemon after you save the resource. This also prevents the **nsrtund** daemon from starting at startup. Default: **Enabled**.	n/a
designated proxy	To define this host as a Proxy, select **Yes**. Default: **Yes**.	n/a
tunnel direction	Defines the initiating and listening hosts. When the Server is the initiating host and the Proxy is the listening host, use **server-to-proxy**. In this configuration, the Proxy and Server communicate on the connection port, bidirectionally. When the Proxy is the initiating host and the Server is the listening host, use **proxy-to-server**. In this configuration, the Proxy uses any source port to communicate with the Server. The Server listens on the connection port and responds to the source port of the Proxy by using the connection port of the Server. Default: **server-to-proxy** Required.	tunnel
server tunnel address	The IPv4 address in the insecure network assigned to the Server. Required.	fwx_server
proxy tunnel address	The IPv4 address in the insecure network assigned to the Proxy. Required.	fwx_proxy
server address	The real IPv4 address of the Server in the secure network. Required.	real_server
proxy address	The real IPv4 address of the Proxy in the insecure network. Required.	real_proxy

Table 5 **Proxy side** NSR tunnel resource attributes

NSR tunnel attribute	**Definition**	**NSR-FWX attribute name**
connection port	The port used to establish the tunnel connection between the Server and the Proxy. This value must be unique for each tunnel. Default: **7232** Required.	port
proxy network	Leave this value blank. This attribute is applicable to the Server only.	n/a
proxy network interface	The network interface on the Proxy that responds to requests against the server tunnel address. For example, bge0 (Solaris) or eth0 (Linux). A non-dedicated Proxy requires a value in this attribute.	fwx_proxy_interface
filter ICMP interface	This attribute is applicable to the Server only.	n/a
port exceptions	This attribute is applicable to the Server only.	n/a
gateway to proxy	This attribute is applicable to the Server only.	n/a
send buffer size	The size of the buffer, in bytes that NSR tunnel uses to send data between the Proxy and Server. Default: 0 (use operating system default value).	n/a
receive buffer size	The size of the buffer, in bytes that NSR tunnel uses to receive data between the Proxy and Server. Default: 0 (use operating system default value).	n/a
keepalive interval	This attribute is applicable to the Server only.	n/a
logging level	The amount of information logged to the log file. **Error**—Logs severe error messages and when packet filters occur. **Warning**—Logs when packet filters occur and tunnel errors. **Information**—Logs all filtered and unfiltered packets, tunnel errors, and diagnostic messages. Default: **Warning**.	n/a

11. Press **Esc**.
12. When prompted to create the new resource, select **Yes**.
13. Exit the **nsradmin** program.
14. Confirm that the nsrtund daemon starts:

```
ps -ef | grep nsrtund
```

Task 2: Configure a NSR tunnel resource on the Server

These steps describe how to configure the NSR tunnel resource and start the nsrtund daemon on the Server host.

1. Log in to the Server as root.
2. Confirm that the nsrd and nsrexecd daemons start:

   ```
   ps -ef | grep nsr
   ```

3. Type:

   ```
   /usr/sbin/nsr_install_tun
   ```

   On Solaris, this command installs and loads TUN drivers provided by the NetWorker software. Linux uses native tun drivers and the **nsr_install_tun** command loads the tun drivers.

4. Use **nsradmin** to create the **NSR tunnel** resource in the NSRLA database:

   ```
   nsradmin -p nsrexec -c
   ```

5. Select **Create**.
6. Select the **NSR tunnel** type.
7. In the NSR tunnel resource, modify the NSR tunnel attributes. Table 6 on page 18 describes each NSR tunnel resource attribute and the equivalent NSR-FWX attribute name.

Table 6 Server side NSR tunnel resource attributes

Attribute	Definition	NSR-FWX equivalent
Name	The name of the tunnel resource. Use the same value you defined in the Proxy NSR tunnel resource. Required.	n/a
autostart	The state of the **nsrtund** daemon. When creating a new resource, select **Enabled**. This starts the **nsrtund** daemon after you save the resource. This also enables the nsrtund daemon to start at startup. When modifying an existing resource, select **Restart now**. This restart the nsrtund daemon after you save the resource. To disable the resource, select **Disabled.** This stops the **nsrtund** daemon after you save the resource. This also prevents the **nsrtund** daemon from starting at startup. Default: **Enabled**.	n/a
designated proxy	To define this host as the Server, select **No**. Default: **Yes**. Required.	n/a

Table 6 Server side NSR tunnel resource attributes

Attribute	Definition	NSR-FWX equivalent
tunnel direction	Defines the initiating and listening hosts. When the Server is the initiating host and the Proxy is the listening host, use **server-to-proxy**. In this configuration, the Proxy and Server communicate on the connection port, bidirectionally. When the Proxy is the initiating host and the Server is the listening host, use **proxy-to-server**. In this configuration, the Proxy uses any source port to communicate with the Server. The Server listens on the connection port and responds to the source port of the Proxy by using the connection port of the Server. Default: **server-to-proxy** Required.	tunnel
server tunnel address	This value must match the **server tunnel address** attribute defined in the Proxy NSR tunnel resource. Required.	fwx_server
proxy tunnel address	This value must match the **proxy tunnel address** attribute defined in the Proxy NSR tunnel resource. Required.	fwx_proxy
server address	This value must match the **server address** attribute defined in the Proxy NSR tunnel resource. Required.	real_server
proxy address	This value must match the **proxy address** attribute defined in the Proxy NSR tunnel resource. Required.	real_proxy
connection port	This value must match the **connection port** attribute defined in the Proxy NSR tunnel resource. Default: **7232**.	port
proxy network	Specify the subnet of the Proxy to enable the Server to reply back to all external clients in the insecure subnet. For example, if the Proxy address is 199.123.123.123, the proxy network is 199.123.123.0/24. When this attribute is blank, the tunnel is dedicated to communication between the Server and the Proxy.	fwx_net_addr
proxy network interface	Leave this value blank. This attribute is applicable to the Proxy only.	n/a

Table 6 Server side NSR tunnel resource attributes

Attribute	Definition	NSR-FWX equivalent
filter ICMP interface	Defines how the tunnel handles ICMP traffic. To prevent ICMP traffic from traveling through the tunnel, set the ICMP messages attribute to **yes**. **Notice:** Network diagnostic tools that test connectivity between the secure and insecure network, for example ping fail when this value set to **Yes**. Default: **No**	ALLOW_ICMP
port exceptions	Enables NetWorker communication between the Server and Proxy through the tunnel. To enable traffic from additional port numbers to travel through the tunnel, specify additional ports. For example, to enable Console client connections and FTP, type the following: 111 9000 9001 22 Default: **111** Required.	PERMANENT_TCP_PORTS
gateway to proxy	The gateway address that the Server uses to forward traffic to the Proxy. Required.	gateway_to_proxy
send buffer size	The size of the buffer, in bytes that NSR tunnel uses to send data between the Proxy and Server. Default: **0** (use operating system value)	n/a
receive buffer size	The size of the buffer, in bytes that NSR tunnel uses to receive data between the Proxy and Server. Default: **0** (use operating system value)	n/a
keepalive interval	How frequently to send a keepalive packet from the Server to the Proxy. A value of **0** disables the transmission of keepalive packet. Default: **60** seconds	n/a
logging level	The amount of information logged to the log file **Error**—Logs severe error messages and when packet filters occur. **Warning**—Logs when packet filters occur and tunnel errors. **Information**—Logs all filtered packets, unfiltered packets, tunnel errors, and diagnostic messages. Default: **Warning**.	n/a

8. Press **Esc**.
9. When prompted to create the new resource, select **Yes**.
10. Exit the **nsradmin** program.
11. Confirm that the **nsrtund** daemon starts:

    ```
    ps -ef | grep nsrtund
    ```

12. To confirm that NSR tunnel establishes an active connection, review the **daemon.raw** file on the Server or Proxy.

    For example, on the Proxy host, messages similar to the following appear:

    ```
    nsrtund NSR Accepted connection from real_proxy_ip_address for NSR
    tunnel instance 'TUN_name'.
    nsrtund NSR tunnel instance 'TUN_name' via server_tunnel_address is
    now active.
    ```

Task 3: Configure the client resources to use the tunnel

Configure each client in the insecure network to communicate with the NetWorker server by using the server tunnel address.

1. Connect to the NetWorker server by using NMC.
2. Click **Configuration** and select **Clients**.
3. Right click the client resource and select **Properties**.
4. Select **Globals (1 of 2)**.
5. In the **Server network interface** attribute, type the **server tunnel address**.
6. Log in to each NetWorker client and update the **/nsr/res/servers** file to include the **server tunnel address**, shortname, and FQDN of the NetWorker server.
7. Stop and start the NetWorker daemons or services on each client.

Task 4: Update the client resources to use the storage node in the secure network

Note: In addition to the tunnel between the NetWorker server and a Proxy host, a secure storage node requires its own tunnel to a Proxy host. Figure 4 on page 8 provides more information.

Modify the client resource for each client in the insecure network that uses a storage node in the secure network.

1. Connect to the NetWorker server by using NMC.
2. Right click the NetWorker client and select **Edit**.
3. Select **Globals (2 of 2)**.

4. In the **Storage Node** attribute, update the affinity list:
   - For clients that back up to devices that are local to the NetWorker server, replace **nsrserverhost** with the server tunnel address.
   - For clients that back up to devices that are on a storage node in the secure network, type the server tunnel address of the tunnel for the storage node.
5. Click **Ok**.

Task 5: Configure the storage node resource for each storage node in the insecure network

If your storage node is a Proxy host, ensure the storage node communicates with the NetWorker server by using the tunnel interface. Figure 5 on page 9 depicts this configuration.

Specify the server tunnel address in the Server network interface attribute of the storage node resource:

1. Connect to the NetWorker server by using NMC.
2. From the **View** menu, select **Diagnostic mode**.
3. Click **Devices** and select **Storage node**.
4. Right-click the storage node resource and select **Properties**.
5. On **Globals (1 of 2)** in the **Server network interface** attribute, type the server tunnel address.
6. Click **Ok**.
7. Log in to the storage node.
8. Update the **/nsr/res/servers** file to include the server tunnel address, shortname, and FQDN of the NetWorker server.
9. Stop and start the NetWorker daemons.

Task 6: Configure the client resource for each storage node in the secure network

When the Server host is a storage node in the secure network, you must add the server tunnel address to the Alias attribute of the client resource for the storage node.

1. Connect to the NetWorker server by using NMC.
2. Click **Configuration** and select **Clients**.
3. Right-click the client resource for the storage node and select **Properties**.

   Note: If the client resource for the storage node does not exist, create a new resource.
4. Select **Globals (1 of 2)**.
5. In the **Alias** attribute, type the server tunnel address.
6. Click **Ok**.

Task 7: Create the client resource for Proxy backups

Create a client resource for the Proxy that communicates with the NetWorker server by using the server tunnel address.

1. Connect to the NetWorker server by using NMC.
2. Click **Configuration** and select **Clients**.
3. Right-click in the **Clients** window and select **New**.
4. In the **Name** attribute, type the proxy tunnel address.
5. Click **Globals (1 of 2)**.
6. In the **Server network interface** attribute, type the server tunnel address.
7. Click **Globals (2 of 2)**.
8. In the **Aliases** attribute, type the real IP address of the Proxy.
9. Click **Ok**.

Monitoring NSR tunnel

Use **nsrwatch** to monitor active connections within the tunnel.

1. Log in to the NetWorker server as root.
2. From a system prompt, type **nsrwatch**.
3. To display the **Active TUNNEL connection** window, type **t**. Close existing sub windows, as required. For example to close the sessions window, type **s**. To close the message window, type **m**.

   Output similar to the following appears in the Active TUNNEL connection window on a Server:

TUNNEL	LOCAL ADDRESS	REMOTE ADDRESS
TUN1	192.168.2.2:53657	192.168.2.3:9060
TUN1	192.168.2.2:53714	192.168.2.3:8714
TUN1	192.168.2.2:9371	192.168.2.3:33312
TUN1	192.168.2.2:9371	192.168.2.3:35614
TUN1	192.168.2.2:9371	192.168.2.3:49908
TUN1	192.168.2.2:9371	192.168.2.3:54093

   where:

   - The name of the tunnel is TUN1.
   - The Server tunnel address is 192.168.2.2.
   - The Proxy tunnel address is 192.168.2.3.

Reporting NSR tunnel messages

NSR tunnel messages appear on both the Server and Proxy hosts. Two log files contain NSR tunnel messages:

- /nsr/logs/daemon.raw—This file contains messages about the stop and start of the tunnel connection. Use the **nsr_render_log** command to review the tunnel log file.

  When NSR tunnel successfully establishes an active tunnel connection, messages similar to the following appear in the /nsr/logs/daemon.raw file:

  - On the Server:

    ```
    nwserver.emc.com nsrtund NSR notice Successfully connected to
    192.168.2.75 for NSR tunnel instance 'TUN0'
    nwserver.emc.com nsrtund NSR notice NSR tunnel instance 'TUN0' via
    192.168.2.2 is now active.
    ```

  - On the Proxy:

    ```
    nwproxy.emc.com nsrtund NSR notice Waiting for connection from
    10.5.162.106 on port 7232 to complete NSR tunnel instance
    'TUN0'...
    nwproxy.emc.com nsrtund NSR notice Accepted connection from
    10.5.162.106 for NSR tunnel instance 'TUN0'.
    nwproxy.emc.com nsrtund NSR notice Published ARP entry 192.168.2.2
    -> eth0 (00:0c:29:d0:ab:54) for NSR tunnel instance 'TUNO'.
    nwproxy.emc.com nsrtund NSR notice NSR tunnel instance 'TUN0' via
    192.168.2.2 is now active.
    ```

- /nsr/logs/*tunnel_name*.raw file—This file contains messages related to tunnel activities. The logging level attribute in the NSR tunnel resource defines the amount and type of information logged to this file.

  Use the **nsr_render_log** command to review the tunnel log file.

  For example:

  - The tunnel name is TUN1.
  - The logging level for the Server is warning.

  Messages similar to the following appear in the *tunnel_name*.raw file:

  ```
  # nsr_render_log -pathyem TUN1.raw
  07/11/12 10:39:01  1 nsrtund SYSTEM DENY IN=tun1 OUT= PROTO=UDP
  SRC=[192.163.123.3]:46847 DST=[192.168.2.3]:7938
  07/11/12 10:39:01  1 nsrtund SYSTEM DENY IN=tun1 OUT= PROTO=UDP
  SRC=[192.163.123.3]:46847 DST=[192.168.2.3]:111
  07/11/12 10:39:52  1 nsrtund SYSTEM DENY IN=tun1 OUT= PROTO=UDP
  SRC=[192.163.123.3]:33324 DST=[192.168.2.3]:7938
  ```

Troubleshooting NSR tunnel

This section lists NSR Tunnel error messages that appear in the /nsr/logs/daemon.raw file and provides resolutions.

SYSTEM warning: A NSR tunnel end was closed unexpectedly

This message appears on the Proxy and Server hosts when the tunnel connection closes unexpectedly. For example when the autostart attribute in the NSRLA database is Restart now or a host reboot occurs.

If the tunnel connection does not reestablish after this message appears, an inactivity timeout on the firewall can cause the tunnel connection to close unexpectedly.

Resolve this issue in one of the following ways:

- Ensure that the **keepalive interval** attribute value in the Server and Proxy NSRLA database is less than the firewall timeout value.

  NOTICE

  If you change the **keepalive interval** value, set the **autostart** attribute to **Restart Now**.

- Increase the firewall timeout to a value greater than the value specified in the **keepalive interval** attribute.

NSR warning Accepted connection from remote address *ip_address* does not match entry for the NSR tunnel attribute 'server address' of tunnel instance '*TUN_name*'; closing connection

This messages appears on the Proxy host when the real IP address of the Server does not match the value specified in the server address attribute in the NSRLA database.

To resolve this issue, ensure that the server address attribute in the NSRLA database is:

- The real IP address of the Server host.
- The same value on the Proxy and Server hosts.

SYSTEM warning Unable to connect to [*ip_address*]:7232 for NSR tunnel instance '*TUN_name*': Connection refused

This message appears on the initiating host when the nsrtund daemon is not running on the listening host.

To resolve this issue:

- Ensure that the autostart attribute value in the NSRLA database is not disabled.
- Try to start the nsrtund daemon in one of the following ways:
  - Stop and start the nsrexecd daemon on the listening host.
  - Set the value in the **autostart** attribute value in the NSRLA database on the listening host to **Restart Now**.

SYSTEM severe Unable to open /dev/net/tun driver for NSR tunnel instance '*TUN_name*': No such file or directory

This message appears on the Proxy or Server host if you did not install or load the tunnel driver.

To resolve this issue:

1. Log in as root.
2. Type:

   /usr/sbin/nsr_install_tun

3. Start the nsrtund daemon in one of the following ways:
   - Stop the nsrexecd daemon on the host and restart it.
   - Set the autostart attribute in the NSRLA database to Restart Now.

SYSTEM warning An error was encountered while reading from *ip_address* for NSR tunnel instance '*TUN_name*': Connection reset by peer

This message appears on the Proxy or Server host when the firewall uses TCP Intercept in Intercept mode and intercepts requests from the initiating host. When the intercept occurs, the tunnel connection closes and NSR tunnel establishes another connection which the firewall intercepts.

You will see messages similar to the following repeated in the daemon.raw file:

```
SYSTEM warning An error was encountered while reading from the network
interface for NSR tunnel instance 'TUN_name': Connection reset by peer
NSR warning NSR tunnel instance 'TUN_name' is now closed.
NSR notice Successfully connected to ip_address for NSR tunnel
instance 'TUN_name'
NSR notice NSR tunnel instance 'TUN_name' via ip_address is now active.
SYSTEM warning An error was encountered while reading from the network
interface for NSR tunnel instance 'TUN_name': Connection reset by
peer.
```

To resolve this issue, exclude the tunnel connection from the TCP Intercept configuration.

Tunnel process starts but the tunnel connection does not establish

When the nsrtund process starts but fails to establish the tunnel connection, review the attribute values in the NSRLA database on the Proxy and Server hosts. For all required fields, ensure the values are the same on the Server and Proxy hosts.