Take into consideration the following when you're preparing your network to connect to Transfer Appliance:

- **Security:** Many networks implement strict security policies. These policies can prevent Transfer Appliance from functioning properly because they block certain network ports or filter certain types of network traffic. Review the information in this section to ensure that your network is set up to work properly with the Transfer Appliance.
- **Performance:** The configuration and capabilities of the network environment have a significant impact on the speed and success of the capture process. For better capture performance, use as few network hops between the data source and Transfer Appliance as possible. For an appliance capture scenario, place Transfer Appliance on the same subnet as the data source, if possible. Similarly, for a workstation capture scenario, place both the workstation and the data source on the same subnet as Transfer Appliance.
- **Network and port address translation:** Transfer Appliance doesn't support Network Address Translation (NAT) or Port Address Translation (PAT), so it won't work in network configurations where Transfer Appliance and a workstation are separated by a network device performing NAT or PAT.
- **Network connectivity:** Before running a capture job, test network connectivity between Transfer Appliance and either the workstation for a workstation capture or the network share containing the data for an appliance capture. See Testing Network Connectivity (/transfer-appliance/docs/2.0/testing-network-connectivity).
- **Link aggregation:** If you plan to use link aggregation, ensure that the network switch ports serving Transfer Appliance are set to their default configurations, with LACP/LAG disabled. Both Transfer Appliance and the data source must be in the same subnet to use link aggregation. Transfer Appliance uses NIC bonding mode 6 for link aggregation, which provides adaptive load balancing.

You may need to open ports in the firewall so that Transfer Appliance can communicate with computers on the network. The following tables describe the ports that are open on Transfer Appliance and the ports that need to be open on computers that communicate with the appliance.

Transfer Appliance uses a non-standard SCP port.

Transfer Appliance ports that are open

Service	Port	Protocol	Type
HTTP	80	TCP	ingress
SCP	6422	TCP	ingress
HTTPS	443	TCP	ingress
Transfer Appliance Control	25025	TCP	ingress
Transfer Appliance Data	25026	TCP	ingress
NFS mountd	25027	TCP, UDP	ingress
NFS statd	25028	TCP, UDP	ingress
NFS lockd/lockmgr	25029	TCP, UDP	ingress
NFS	2049	TCP, UDP	ingress
RPC	111	TCP, UDP	ingress

Linux workstation ports that must be open

Your Linux workstations may be configured to use custom ports for the various NFS processes. To get a list of ports l be open, run the following command on the Linux system containing the data you need to capture: **`rpcinfo -p host`**.

Service	Port	Protocol	Type
SCP for Transfer Appliance	6422	TCP	egress
HTTP	80	TCP	egress
HTTPS	443	TCP	egress
Transfer Appliance Control	25025	TCP	egress
Transfer Appliance Data	25026	TCP	egress

Windows workstation ports that must be open

Service	Port	Protocol	Type

SCP for Transfer Appliance	6422	TCP	egress
HTTP	80	TCP	egress
HTTPS	443	TCP	egress
Transfer Appliance Control	25025	TCP	egress
Transfer Appliance Data	25026	TCP	egress

Server ports that must be open for Transfer Appliance capture

- NFS capture: NFS server mountd and statd ports

To use Transfer Appliance Capture Utility, verify that ICMP is not blocked or filtered on your network. Otherwise, the Capture Utility will fail to contact Transfer Appliance.

Once you have prepared your network for data transfer, prepare to receive the Appliance (/transfer-appliance/docs/2.0/receiving-appliance).