Common network ports

Typical destination ports and transports used in everyday administration.

Core network services

22 TCP - SSH; also SFTP over SSH.
53 UDP/TCP - DNS; TCP is also used for normal DNS queries when needed.
67/68 UDP - DHCPv4 server/client.
80 TCP - HTTP.
123 UDP - NTP time service.
161 UDP - common SNMP queries.
162 UDP - common SNMP traps.
443 TCP - HTTPS over TCP.
443 UDP - commonly HTTP/3 over QUIC.

Mail services

25 TCP - SMTP transport / server relay.
465 TCP - submission with implicit TLS.
587 TCP - message submission, commonly with STARTTLS.
143 / 993 TCP - IMAP / IMAP over implicit TLS.
110 / 995 TCP - POP3 / POP3 over implicit TLS.
Port 25 is not interchangeable with authenticated client submission.

Web and file access

445 TCP - SMB.
3389 TCP/UDP - RDP.
2049 TCP - commonly NFSv4; other NFS versions and setups can need additional ports.
A service can be configured to use a different port.

Active Directory-related services

88 TCP/UDP - Kerberos.
389 TCP/UDP - LDAP / CLDAP.
636 TCP - LDAP over TLS.
3268 / 3269 TCP - Global Catalog / TLS.
135 TCP - RPC endpoint mapper.
49152-65535 TCP - default modern Windows dynamic RPC server range; configuration and workload matter.
AD also relies on DNS, time and SMB. This is not a complete firewall rule set.

Management and databases

5985 / 5986 TCP - WinRM HTTP / HTTPS.
1433 TCP - common SQL Server listener.
3306 TCP - MySQL / MariaDB.
5432 TCP - PostgreSQL.
514 UDP / 6514 TCP - syslog / syslog over TLS.

Test the correct transport

```
Test-NetConnection host.example -Port 443
```

Windows TCP check. Replace the target with your host.

```
ss -lntup
```

Linux local listeners; process details can require privileges.

A TCP test cannot prove that a UDP service works. For DNS, make a DNS query. For HTTPS, also test the TLS connection and application response.

Before changing a firewall

Confirm source, destination, traffic direction, transport, destination port and actual listener. Limit access to the intended systems. An open port does not prove a service is healthy or encrypted; a timeout alone does not identify which device dropped the traffic.

References (click to open): IANA service and port registry | Microsoft: AD ports and firewall requirements | Microsoft Test-NetConnection