Windows Firewall

Windows Firewall is a built-in, host-based, stateful firewall that is included in Windows Vista, Windows Server 2008, Windows XP with Service Pack 2 and later, and Windows Server 2003 with Service Pack 1 and later. Windows Firewall drops incoming traffic that does not correspond to either traffic sent in response to a request of the computer (solicited traffic) or unsolicited traffic that has been specified as allowed (excepted traffic). Windows Firewall helps provide protection from malicious users and programs that rely on unsolicited incoming traffic to attack computers. In Windows Vista and Windows Server 2008, Windows Firewall can also drop outgoing traffic and is configured using the Windows Firewall with Advanced Security snap-in, which integrates rules for both firewall behavior and traffic protection with Internet Protocol security (IPsec).

Windows Firewall Defaults

The following table is a list of default Windows Firewall settings and the variances between various Microsoft Windows Operating Systems:

Enabled/On	WinXP SP2	Win2k3	Vista	Win 7
Windows Firewall	**Yes**	**Yes**	**Yes**	**Yes**
Outbound Traffic Protection	**N/A**	**N/A**	**No**	**Yes**
Inbound Traffic Protection	**Yes**	**Yes**	**Yes**	**Yes**
Allow ICMP echo requests	**No**	**No**	**Yes**	**No**
Windows Firewall Logging	**No**	**No**	**No**	**No**

Recommended Internet Sites

- Windows Firewall: https://web.archive.org/web/20160804161634/https://technet.microsoft.com/en-us/network/bb545423.aspx
- File and Printer Sharing: https://web.archive.org/web/20160804161942/https://social.technet.microsoft.com/Forums/windows/en-US/b1b806be-d655-498d-a587-ed3cb5630d92/file-and-printer-sharing-only-for-domain-profile?%20forum=w7itpronetworking

Please contact the Course Coordinators if you are unable to access any of the Recommended Internet Sites.