

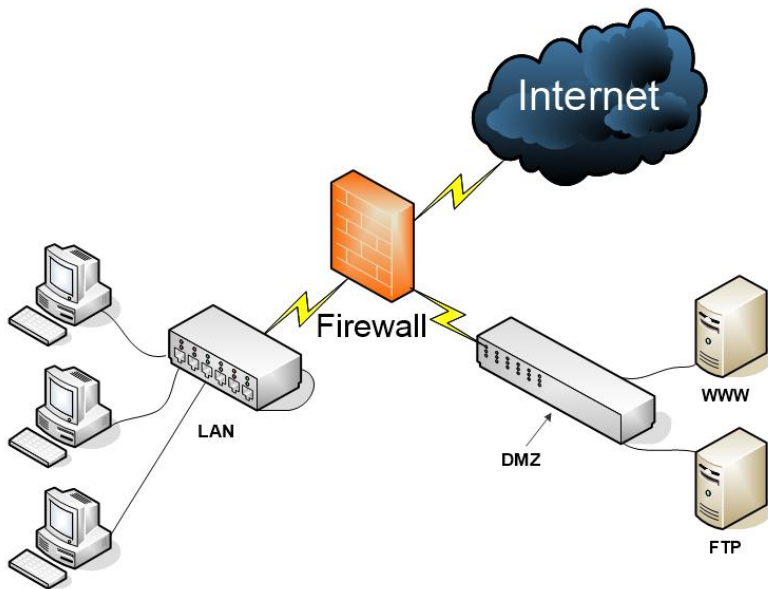
Real-World Scenario 6-1: Creating a DMZ

Scenario: Your organization's network has all of its servers running directly within the LAN. The new IT director knows this is quite insecure, and instructs you to develop a 3-leg firewall scheme.

Your task is to create a network diagram (either handwritten or with a program such as Microsoft Visio or ConceptDraw) that shows the LAN, Internet, firewall, and DMZ areas. Give examples of the IP addresses that might be used for all three connections to the firewall.

Real-World Scenario 6-1 Solution

As shown in the figure below, the 3-leg firewall scheme has a firewall in the center with three connections to the Internet, the LAN, and the DMZ. The LAN is using a Class B private IP network. The DMZ is on a separate Class C IP network, and the Internet connection uses a public IP address so that the firewall can connect directly to other systems and networks on the Internet.



This 3-leg solution is an excellent way (though not the only method) of separating web servers, FTP servers, and mail servers from the rest of the LAN. A separate set of rules (ACLs) can be configured for the DMZ connection and the LAN connection. In this way, the DMZ can be accessed by users on the Internet (and by users on the LAN), but the resources on the LAN are fully protected from users on the Internet. You can create a 3-leg firewall of this sort by using a hardware-based firewall with an Internet connection and two LAN connections (most common),

or a server with three network adapters running special firewalling software.

Simulation: Complete the simulation “6-1: Creating a DMZ.” See the following page for the solution.

Solution figure:

