Prevention: DMZ

DMZs and honeypots are security controls that can help an organization implement the "defense-in-depth" concept, using multiple layers of security to slow down an attacker, giving defenders a chance to detect and eliminate them. Both of these defenses are covered in more detail below.

WHAT IS A DMZ?

In computer networks, a DMZ (demilitarized zone) is a physical or logical subnet that separates an internet local area network (aka LAN) from other untrusted networks (usually the internet). External-facing servers, resources, and services that are located in the DMZ are directly accessible from the internet, however, this layer will keep the internal LAN unreachable, providing an additional layer of security to the LAN as it restricts a hacker's ability to directly access internal server and data via the internet.

So what are DMZs used for?

- Protect sensitive organizational systems and resources.
- Isolate and keep potential target systems separate from internal networks.
- Reduce and control access to those systems outside the organization.

DMZ SERVICES

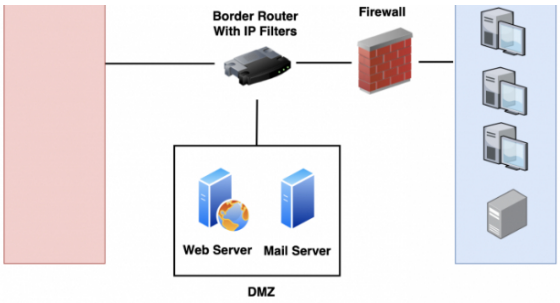
What services and systems are placed in a DMZ? Any service provided to users on the public internet should be placed in the DMZ network. Some of the most common of these services include web servers and proxy servers, as well as servers for email, domain name system (DNS), File Transfer Protocol (FTP) and voice over IP (VoIP).

DMZ ARCHITECTURE

There are numerous ways to construct a network with a DMZ. The two major methods are a single firewall (sometimes called a three-legged model), or dual firewalls. Each of these system can be expanded to create complex architectures built to satisfy network requirements.

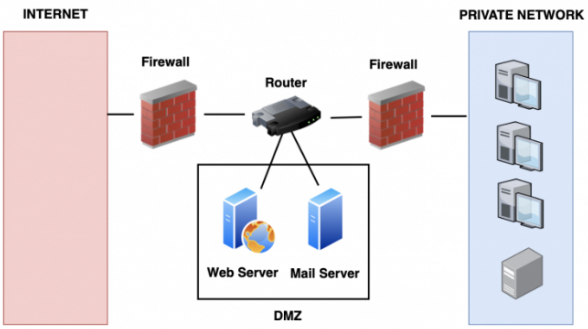
DMZ Architecture – Single Firewall

A modest approach to network architecture involves using a single firewall, with a minimum of 3 network interfaces. The DMZ will be placed inside of this firewall. The tier of operations is as follows: the external network device makes the connection from the ISP, the internal (private) network is connected by the second device, and connections within the DMZ is handled by the third network device.



DMZ Architecture – Dual Firewall

The more secure approach is to use two firewalls to create a DMZ. The first firewall (referred to as the "frontend" firewall) is configured to only allow traffic destined for the DMZ. The second firewall (referred to as the "backend" firewall) is only responsible for the traffic that travels from the DMZ to the internal (private) network. An effective way of further increasing protection is to use firewalls built by separate vendors because they are less likely to have the same security vulnerabilities. While more effective, this scheme can be more costly to implement across a large network.



BENEFITS OF A DMZ

The primary benefit of a DMZ is that it offers users from the public internet access to certain services offered by a private network, while still maintaining a buffer between those users and the private network. The security benefits of this buffer manifest in several ways, including:

Access Control for Organizations:

- The need for organizations to provide users with access to services situated outside of their network perimeters through the public internet is nearly ubiquitous in the modern organization. A DMZ network provides access to these necessary services while simultaneously introducing a level of network segmentation that increases the number of obstacles an unauthorized user must bypass before they can gain access to an organization's private network. In some cases, a DMZ includes a proxy server, which centralizes the flow of internal user — usually an employee — internet traffic and makes recording and monitoring that traffic simpler.

Prevent attackers from performing network reconnaissance:

- The accessible buffer the DMZ provides prevents an attacker from being able to scope out potential targets within the network. It makes internal reconnaissance more difficult because even if a system within the DMZ is compromised, the private network is still protected by the internal firewall separating it from the DMZ. It also makes external reconnaissance more difficult for the same reason.

Protection against IP spoofing:

- In some cases, attackers attempt to bypass access control restrictions by spoofing an authorized IP address to impersonate another device on the network. A DMZ can stall potential IP spoofers while another service on the network verifies the IP address's legitimacy by testing whether it is reachable.

Previous Topic
Mark Complete
Next Topic

Previous topic | Mark Complete | Next topic

Back to Lesson