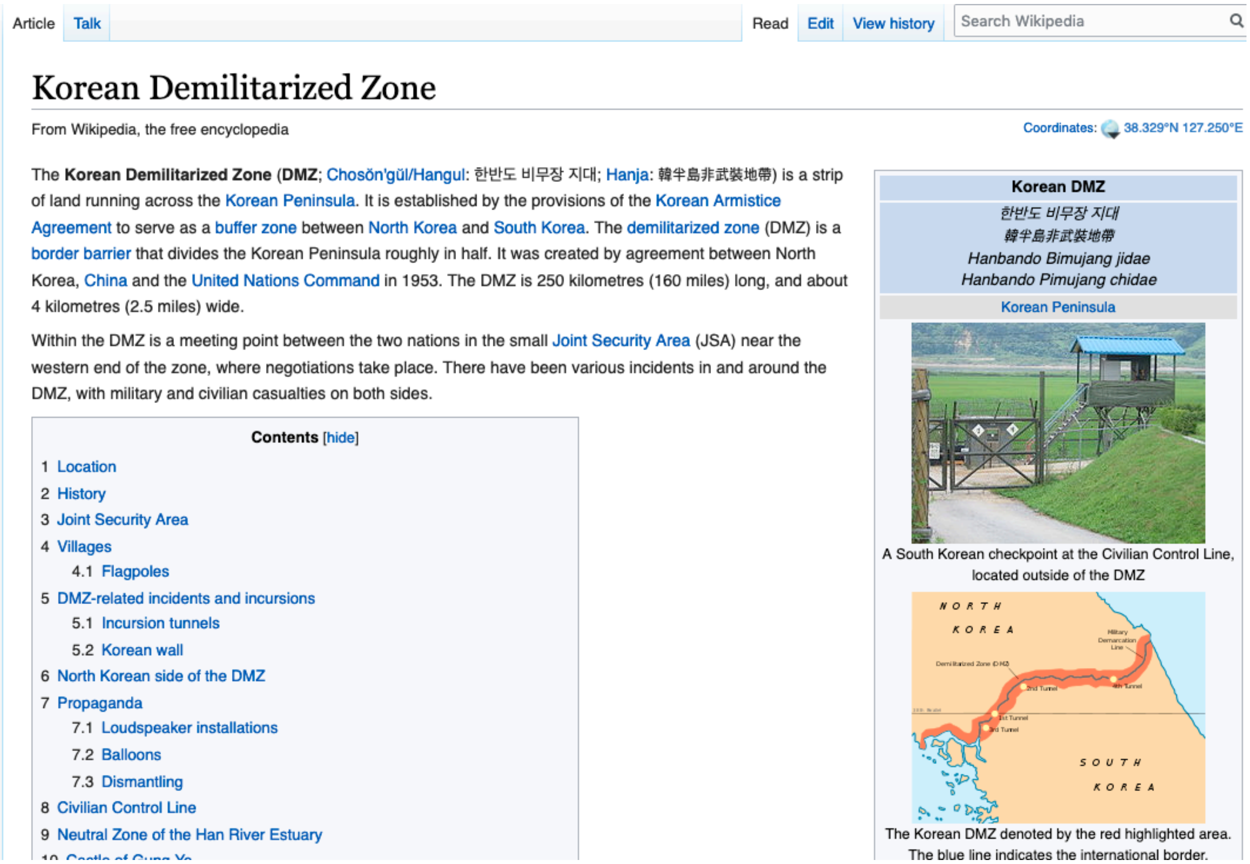
pfSense Fundamentals

Configuring a DMZ - What is a DMZ?

Welcome back!

As mentioned in the last lesson, DMZ stands for Demilitarized Zone. It is a term borrowed from the military.

Think of the boundary between North and South Korea. This is perhaps the most famous DMZ.



Korean Demilitarized Zone

From Wikipedia, the free encyclopedia

Coordinates: 38.329°N 127.250°E

The **Korean Demilitarized Zone** (**DMZ**; Chosŏn'gŭl/Hangul: 한반도 비무장 지대; Hanja: 韓半島非武裝地帶) is a strip of land running across the Korean Peninsula. It is established by the provisions of the Korean Armistice Agreement to serve as a buffer zone between North Korea and South Korea. The demilitarized zone (DMZ) is a border barrier that divides the Korean Peninsula roughly in half. It was created by agreement between North Korea, China and the United Nations Command in 1953. The DMZ is 250 kilometres (160 miles) long, and about 4 kilometres (2.5 miles) wide.

Within the DMZ is a meeting point between the two nations in the small Joint Security Area (JSA) near the western end of the zone, where negotiations take place. There have been various incidents in and around the DMZ, with military and civilian casualties on both sides.

Korean DMZ

한반도 비무장 지대
韓半島非武裝地帶
Hanbando Bimujang jidae
Hanbando Pimujang chidae

Korean Peninsula

A South Korean checkpoint at the Civilian Control Line, located outside of the DMZ

The Korean DMZ denoted by the red highlighted area. The blue line indicates the international border.

Contents [hide]

https://en.wikipedia.org/wiki/Korean_Demilitarized_Zone

The fenced-off and heavily guarded and patrolled border is a no-man's-land. Anyone in there is suspect. Anyone having to enter must be authorized and will be very closely monitored by both sides.

It would be very nice if we could trust people to behave well when we expose a server to the Internet, like a web server, or email server. As you'll see from your logs on any server exposed to the Internet, this just isn't the case. Hostile forces are constantly looking for weaknesses in our servers, and if they find any, they'll try to exploit them to take over or abuse our server.

The next logical step for an attacker is to see what else she could get to after breaking into the exposed server.

If someone breaks into your web server, and your web server is on your internal network, the attacker would be able to go after any system on your corporate local area network or LAN!

If you configure your environment as I recommend and show you here, damage from such an attack will be limited.

You should put any service you have to expose to the Internet or to people outside your network in a DMZ.

This server should be hardened and monitored closely for any sign of compromise.

Network traffic to and from the server should be tightly restricted.

For a web server, only web traffic from the Internet should be allowed to access it.

Management traffic such as SSH for Linux or Remote Desktop Protocol (RDP) for Windows should only be allowed from the internal network.

The DMZ server should not be allowed to communicate with the LAN except in very controlled circumstances like allowing logs to be sent to a log server.

To summarize, a DMZ is a network location where you can put things you want to share with outside consumers. Traffic flow into and out of the DMZ should be closely monitored.

See you in the next lesson!