# DMZ

av

Pål

IKT 207

Cybersikkerhet

Veiledet av

Sigurd Kristian Brinch

Fakultet for teknologi og realfag

Universitetet i Agder

Grimstad, September 2020

DMZ or Demilitarized Zone is an area in which treaties or agreements between two nations where a military presence is forbidden. But what is it in a computer setting, what does it do, and why do we use it?

In Computer security a DMZ or perimeter network is a sub-network that sits in between an external network and internal network. The point of having a DMZ is that connection from the internal and external network to the DMZ is allowed, but connection from the DMZ is only allowed to the external network(, meanwhile)A host in the DMZ can not connect to the internal network. This will allow the DMZ host to provide services to the external network while protecting the internal network in case a criminal is compromising a user in the DMZ. For someone that wants to access the internal network illegally, the DMZ is a dead end[1].

Commonly only systems which provide services to the internet are placed in this DMZ, such as web server, email services, DNS(Domain Name service), FTP(File Transport Protocol), and VoIP(Voice over IP). These system are generally most vulnerable to attacks[3].

The two most common architectures for a DMZ is either to have a single firewall or dual firewall.

- Single firewall: Creates a connection between the internet to the firewall, internal network to the firewall and then DMZ to the firewall. This makes the firewall the single point of failure and must be able to handle all the traffic going to the DMZ as well as the internal network[4].
- Dual firewall: The first wall which is the point of connection to the internet and is called ”Frontend Firewall”. The second firewall is the wall between DMZ and the internal network plus the Frontend Firewall and the second firewall, which is called ”Backend Firewall”. So even if they can bypass the Frontend Firewall there is still the Backend firewall they have to breach in order to access the internal network[4].

If you are using a Dual firewall it can be a solution to use two different firewall vendors, so if one of them have a security vulnerability, you still have one more that probably does not have this vulnerability.

The DMZ is intended as a buffer between the internal and external networks to prevent an ”easy” access for criminals on to your network. Even though it is supposed to protect user information, it has become common to store sensitive data on the DMZ. This has made a change in criminals focus, from the server to the actual DMZ since most, if not all, they need already is stored in here. This stems from workers having a home office or who are generally on the move with their work. Many corporations have settled with the risk, even though there is another alternative[2].

A DMZ is a must for all corporation servers that the customers need access to in order to use the corporate resource like Email services or web sites. This will let the users access what they need all within the DMZ without compromising the internal network. This is all on the basis that the DMZ is used correctly and all user information is not stored within the DMZ. On the other hand if used incorrectly it is the user that will suffer most of the consequences, loss of private information such as passwords. That can and will spill over to other sites or systems, for instance, the users social media accounts.

# References

[1] Department of Homeland Security. *Control System Security DMZ*. Read 21.9.2020. URL: https://us-cert.cisa.gov/ics/Control_System_Security_DMZ-Definition.html.

[2] Ben Rossi. *The DMZ as a corporate liability*. 5.12.2013. URL: https://www.information-age.com/the-dmz-as-a-corporate-liability-123457501/.

[3] Margaret Rouse. *DMZ (networking)*. November 2019. URL: https://searchsecurity.techtarget.com/definition/DMZ.

[4] SAP. *Understanding DMZ and Firewall*. Read 15.9.2020. URL: https://help.sap.com/viewer/843ee00512094cd68acca0323d67cfd7/6.6/en-US/7e0766306cbd1014a23cc679b0e91070.html.