The Strengths and Limitations of DMZs in Network Security

By

Cameron Meyer

Submitted to the Department of Technology Systems

In partial fulfillment of the requirements for the degree of

Master of Science in Networking Technology

At

EAST CAROLINA UNIVERSITY

November 2017

This page intentionally left blank.

Abstract

A demilitarized zone (DMZ) in terms of a network is a segmented area in the network that is available to the public but is segmented in order to stay separated from a network's internal private network. In other words, it separates the untrusted public Internet from the trusted network of an organization. This is done through the act of subnetting and is a useful network security design feature within the network architecture. A DMZ can have a completely different IP addressing scheme from the internal network, or it can reside on the same network broken up logically through the use of VLANs. Typically, an organization will place assets that house information, resources or servers that the public needs access to; such as its public web servers in the DMZ. This allows the public can have open access to them and their data or services they provide but integral organizational data is stored on the private network not directly accessible from the public Internet or the assets that are placed within the DMZ. Firewalls play an important role is the security architecture of a network especially in setting up a DMZ. Due to the idea of opening up this segment of the network to the public, the assets here can become compromised. These firewalls will help to contain and even prevent malicious entities from affecting the DMZ and especially the internal network. There are two simple DMZ architectures: a single firewall implementation and a double firewall implementation. The most common network architecture for a DMZ is to set up a firewall between the external network and a public facing server such as a web server in the DMZ and then another firewall set up in between the server in the DMZ and an organization's internal trusted network. This helps to control access coming into the server in the DMZ. If the server is maliciously attacked, then this server is isolated in the DMZ without access to the internal network, thus protecting an organization's vital data. With this in mind, more advanced DMZs will include an intrusion detection or

intrusion prevention system to accompany firewalls and servers in order to alert an organization to malicious or suspicious activity and attempt to root it out within the DMZ. DMZs are useful and can improve the network security posture of an organization by preventing malicious attacks by keeping them from reaching the internally trusted network of an organization.

Introduction

A demilitarized zone or DMZ for short, in terms of a computer network is a physical or even a logical subnetwork within an organization that is purposely designed to sit outside of the internal network of that organization. This adds an advantageous layer of security to the network's security posture. By having this design feature utilized in a network, an organization can make selected services available for public access such as hypertext transfer protocol (HTTP-web servers) and file transfer protocol (FTP) or even domain name system (DNS) while still protecting the computer assets on the internal land area network (LAN) (Weaver et al, 2014). Essentially, an organization is separating its private trusted network from that of the untrusted public network which is granted access on some level to the resources that are housed within the DMZ. This segmented network essentially becomes a semi-secure area of the network. This means that the DMZ is designed to be used on the edge or the perimeter of an internal network with a firewall separating it from the Internet facing router on the network.

The most basic purpose of a DMZ is to provide an additional level of network security for the internal network. The key to the design of a DMZ is the firewalls and their placement. There are different designs for the DMZ utilizing firewalls, but the two most common designs in implementing a DMZ utilize either a single or dual firewalls. The architecture of the of the DMZ mainly depends on the type of organization that is implementing it and what it is trying to accomplish.

DMZs can be a very beneficial design feature to bolster network security for an organization but they are not perfect. They have their strengths and their weaknesses just as every network security component does and these must be evaluated in order to determine if implementing a DMZ is worth the risk/reward. Not every organization will have the need to implement a DMZ into their network architecture. When is a DMZ necessary and if/when is it beneficial for an organization to utilize one?

Design Features of DMZs

DMZs can vary in their complexity and can provide more security to the network than just the design/architecture facet. The DMZ can be set up with its own separate IP addressing scheme to subnet it differently than the internal network or it can be set up on the same IP addressing scheme with the use of VLANs. They can house tools such as Intrusion Detection or Intrusion Prevention systems, honeypots, and proxy servers but the most important feature in the implementation of a DMZ is the firewall. This firewall is key because with a DMZ, you are inviting unknown, untrusted users from the public network in to access the resources that your organization provides. Although there are several different levels of DMZs and how to construct them, the two most prevalent are the single and dual firewall setup. The more secure DMZ network architecture of these two common designs is that of a dual firewall and thus will be the subject discussed most prominently. The way that this is set up is with a firewall between the border or public side of the network and the DMZ. The other firewall is placed on the other side of the DMZ between the DMZ and the internal, trusted network. This firewall placed between the DMZ and the internal network will be set up with stricter rules and configurations than the first firewall between the public network and the DMZ is. The responsibilities of the firewall

between the DMZ and internal network can even be split between two firewalls in order to provide load balancing and redundancy for traffic bound for the internal network (Cisco).

Although the purpose of a DMZ is to have a portion of the network exposed to the public internet or border network, this perimeter portion of your network cannot be left out and exposed completely. Rather, the DMZ needs to be treated just as another part of an organization's network although it is considered to be more of a buffer between the internal network and public network. However, the two should not store information on the workings of their individual network functions. Internal network hosts should view and interact with the assets in the DMZ as if they are external assets and assets in the DMZ should handle traffic from internal assets just the same as it would external assets. This means that the assets housed in the DMZ should have no working knowledge of the internal network. If an asset in the DMZ were to be completely compromised, then it will not compromise the internal network by giving attackers vital information on the internal network (Danen, 2001).

Installing a firewall between the border network and DMZ is important. This firewall will perform stateful inspections of the network traffic coming into the DMZ and deny IP packets that it believes are malicious (Microsoft). This stateful inspection is important because it can filter out and deny access based on the source and destination IP addresses. This is important because attackers may be using IP spoofing techniques. An attacker may spoof an IP address such as using a trusted IP address from the internal trusted network but it will originate from the border network there. This attack is attempting to gain access to the network by pretending to be a trusted source when it is in fact untrusted. Or in another case of spoofing, the firewall needs to deny packets that are leaving the network with a source address that doesn't match an IP address from your network (Microsoft).

Beyond just denying suspected malicious packets, the firewall must be configured with the appropriate rules to protect the DMZ. Since the DMZ often houses important functions that numerous public users or customers are accessing, they need to have a high level of availability and cannot sacrifice downtime due to a security event such as a denial of service attack. Setting up rules on the firewall such as denying ICMP requests can help protect against attacks like denial of service which aim to take down network assets such as servers.

Within the DMZ, an organization may decide to deploy additional security elements. A common security element to include in the design of a DMZ is a honeypot. Cole and Northcutt define a honeypot as "an information system resource whose value lies in unauthorized or illicit use of that resource" (Cole and Northcutt). This is essentially saying, that a honeypot is an excellent way to gather information about attack attempts on the network. Contrary to popular belief, you always want to keep attackers away from your network and not draw them in. Once an attacker is in however, the honeypot is set up to look like it has valuable information to lure attackers to deploy their methods and that is where the honeypot becomes useful. The information gathered on these attack vectors used by attackers can be used by the security administrators to better defend the network. In other words, the security team is deceiving attackers to show their strategy giving the security team the necessary information to stop similar attacks in the future. As stated by White and Donohue in *The Art of Network Architecture,* network security is like a game of chess. However, honeypots aren't perfect and in some cases the security team may get exactly what it was asking for by deploying a honeypot as it is often more attractive to attackers. The security team may not actually be able to contain the damage done to a honeypot. For instance, an attacker could deploy a worm with the honeypot being the platform to launch this attack from. This is exactly what Chapple warns against in his article as a

mismanaged honeypot or poorly configured honeypot can quickly turn a valuable and informative network security tool into a compromised weak point in the network's security (Chapple). This also highlights one of the more important reasons to deploy the dual firewall network design with a firewall placed between the DMZ and the internal network. This second, more stringent firewall can help to protect the internal network from malicious entities in the DMZ. Likewise, this firewall can (in more unlikely circumstances), serve to protect the DMZ assets from an attack that originates from the internal network. These attacks are generated from malicious entities that have made it through the network security into the internal network.

Allowing the public to access the resources within the DMZ leaves it vulnerable, that is why it is a good option for the network security team to consider including intrusion detection and/or intrusion prevention systems in this segment of the network. There are two variations each of intrusion detection and intrusion prevention systems. The host based and network based options are available to the network security team and have different capabilities. A network based intrusion detection and prevention system would be best served to be installed with a sensor between the firewall and the DMZ and another one placed between the second firewall and the internal network. This allows the sensor to monitor and collect data on all traffic that is coming onto the network and analyze this data to catch anomalies and suspicious activities and handle it accordingly. These network based intrusion detection and prevention systems can operate as high as the application layer of incoming traffic (Weaver et al, 2014). These systems use a combination of anomaly detection, signature detection and stateful protocol analysis in order to determine if there are malicious entities attempting to penetrate the network (Yadav, 2013). On the other hand, host based intrusion detection and prevention systems are software that is installed on individual assets or can be a dedicated appliance that monitors all traffic on a

selected host. These are not going to be placed on every asset on the network due to cost considerations, rather these would be deployed on high value assets that are in the DMZ such as web servers, database servers or mail servers. These host based intrusion detection and prevention systems can analyze system logs, system process, operating systems and even central processing unit anomalies (Weaver et al, 2014). With intrusion detection and prevention systems, the best practice would be to use a hybrid plan where both are utilized as each system has shortfalls but when used together these two systems can help to overcome these shortfalls. Some examples of this are a host based intrusion detection and prevention system can inform whether an attack was successful and a network based systems cannot. A network based intrusion detection system can detect attacks that target the network as a whole and a host based systems can only detect attacks that target individual assets that are on the network and chosen to be monitored (Weaver et al, 2014). An intrusion detection or intrusion prevention system may be one of the most important tools to incorporate in conjunction with the DMZ due to the complexity and abilities of newer malicious entities. Guri discusses some of these in his article and points to the creation of polymorphic viruses that have the ability to change themselves and actively avoid being detected (Guri, 2016). In addition, some malicious entities use "anti-forensic" techniques to avoid detection and can remain dormant for long periods of time (Guri, 2014).

An important factor in regards to the DMZ is that network performance should not suffer by adding this wrinkle into the network architecture. There are various ways to accomplish implementing a DMZ without negatively impacting network performance in a significant manner. Packet filtering and inspection will typically cause a bottleneck in network traffic as discussed by Wu et al. This research group uses the example of Kansas State University's

network where the bandwidth of their links is ten Gbps but when Deep Pack Inspection is performed, this speed drops seventy percent to just three Gbps (Wu et al, 2015). In order to achieve faster, more reliable network speeds, the research team implemented a technology known as OpenFlow. This OpenFlow is a tool born out of Software Defined Networking and used as a routing tool and implemented through the use of a controller and switches throughout their experiments. In the experiment, the OpenFlow controller runs statistics on the amount of traffic that is coming through the network and the size and actively makes routing choices and packet inspection choices accordingly and then sends commands to the switch. With a term the researchers coin as "elephant flow" (a threshold established by comparing the network link capability, current traffic flow and deep packet inspection processing rate), the team established a rule that anything exceeding this level of flow would be directly routed and skip the deep packet inspection stage in order to boost network performance. With all other traffic flows under the level of elephant flow, a sample of packets would go through deep packet inspection but not just a random sample of packets, rather the first several would be inspected and then the rest of the flow would be routed accordingly (Wu et al, 2015). Although this method will bolster network performance by limiting the number of packets that go through the process of deep packet inspection, there is a tradeoff in terms of network security. By not inspecting packets in a large flow of traffic, an attacker could ultimately hide a malicious payload in the transmission that would not get detected and thus dropped. The packet filtering that is performed by the firewalls plays another role in the DMZ architecture. The packet filtering will allow public internet users to access the DMZ and block their access to the internal network and meanwhile it will not allow internal network users to directly access the public internet but will allow them to access the DMZ. The reason behind this is if there is a device known as a proxy server placed in

the DMZ. The proxy server acts similar to a firewall by adding additional packet filtering and forwarding authorized packets on path to their destination. This is important because the proxy server will also change the packet leaving the network to a different source ip address and thus shielding the original ip address of the original host that is on the internal network adding some additional security (Weaver et al, 2014). The proxy server can also benefit the network by increasing performance because it works to cache website data that is requested in order to make it quicker for users to get the requested data. This can also be beneficial from a security standpoint because the requested data is now stored on a more trusted source than retrieving it from the public internet.

Strengths of DMZs

In today's world with the ever expanding internet and computing capabilities, security is paramount. Hackers and their techniques are becoming increasingly more sophisticated and network security professionals must keep pace and need to incorporate as many tools as necessary to thwart potential attacks. Implementing a DMZ into the network architecture can be a useful tool to increase network security and an important part of a comprehensive security approach. This promotes a philosophy of defense in depth which deploys multiple levels of security across multiple layers of the network in order to ensure the confidentiality, integrity and availability of data on the network.

One of the greatest strengths that a DMZ offers an organization is access control. By segregating the network into these zones of DMZ and internal network, the network administrators break the network up into zones that are based on trust. Depending on the level of

trust associated with each zone is what determines the level of access the administrators allow to both internal trusted users and untrusted public users alike. The public untrusted users are granted some level of access to the DMZ in order to access the resources that are housed within it such as web servers but these users are denied access to the trusted network. Trusted users although trusted, must still be monitored as they are permitted to access the resources of the DMZ and may access the public internet. The trusted users must be monitored in case of a potential infection that originates from inside the trusted network that may impact the DMZ. The DMZ is not simply left unprotected or unmanaged, the resources that are housed there are still valuable and must be protected. High availability is a requirement for resources such as web servers, imagine if Google's servers went offline. The impact of this on their customers would be detrimental.

DMZs are a good network tool to prevent attackers from performing network reconnaissance. Network administrators want to hide the ip addressing scheme that is used on the network from attackers, especially the addresses that are associated with the assets in the trusted network. Many attackers will seek to perform some level of reconnaissance on a network to learn not only the ip addresses in use but also the ports that are used and open which gives them information on how to better form an attack (Microsoft). When an attacker learns what sort of services are being provided by an asset and what ports are open, the attacker can exploit these vulnerabilities.

Another advantage provided by a DMZ is protection against ip spoofing. The firewall in conjunction with the DMZ will mask the ip addressing scheme of the interior network. This is important because if an attacker can learn the ip address of the internal trusted network, the attacker can then alter their packets to appear as though packets coming into the network are

from the trusted network. The firewall will catch this anomaly and block the packets accordingly. Ip spoofing in itself is not a dangerous activity on the network, but the traffic being permitted means that an attacker can effectively deliver a malicious payload into the network (Microsoft). In addition to the firewall, a DMZ can house a proxy server within it which will also mask the source ip address of packets which originate from the internal trusted network and are destined for the public internet (Chapple, 2008).

One of the most common attacks that face large organizations is a denial of service attack. This attack seeks to deteriorate the throughput of the network's links to a very low level or in some cases to even shut down assets completely. This is done through the use of ICMP or ping messages flooding the network and being targeted at a single device. The firewalls around the DMZ can be configured with rules so as to deny or block these ping messages as they are not a necessary function of the network. Another benefit in denying ICMP messages is related to network reconnaissance as it doesn't allow attackers to know that a device is where they think or expect it to be in terms of ip addressing (Microsoft).

The firewalls that are around the DMZ also need to be configured so that they provide protection against certain application layer attacks. Application layer exploits can cripple valuable assets such as servers. SQL injections are an example of an application layer exploit but Microsoft SQL servers are not the only vulnerable high value target, web and database servers need to be protected as well. The firewalls are not foolproof to stop these exploits however, it is necessary to perform routine maintenance and keep these devices up to date with the latest patches and fixes that are provided by the manufacturer (Microsoft).

Limitations of DMZs

Every network security tool, device or architecture is imperfect and will not be able to stop every possible way that attackers try to penetrate the network. Especially in today's modern world where attackers have numerous tools and techniques to accomplish their goals. A DMZ is not perfect and it is not the be all end all in an organizations network security posture. The DMZ is meant to be a part (a valuable part but just one piece of the puzzle) of a comprehensive network security posture where there are numerous other facets involved to make the network as secure as possible.

One example of how a DMZ falls short in protecting the network is packet sniffing. Packet sniffing may not always be dangerous, but it is something that is not desired on the network either. If an attacker is able to use a packet sniffer and capture packets from the network, then they will have access to all sorts of information regarding the network and even the individual devices that are communicating. This is especially dangerous if there is not some sort of encryption protocol being used on the packets that are being sent. If there is no encryption protocol used on the transmission of data from one point to the other and an attacker captures these packets, then everything from usernames, passwords, personal data, transaction information, etc. can all be captured and read as plain text (Microsoft).

A DMZ also falls short in another important area. A DMZ itself cannot do anything once the network has been penetrated (aside from keeping it quarantined in he DMZ). If a malicious entity gains access to the resources that are housed within the DMZ such as a virus, Trojan horse or a worm then the DMZ will not be able to do anything to quarantine or root out the malicious entity. Although this is one of the basic reasons for having a DMZ (so this area gets infected and not the internal network), as discussed earlier the resources that are housed here are still

valuable. For an enterprise these resources are client facing and any downtime that they experience means potential lost revenue or business for the organization. Beyond this, the firewalls that are installed around the DMZ typically cannot detect these types of malicious entities and thus will not be able to handle them accordingly (Microsoft). This is why it is important to incorporate security tools within the DMZ itself to help root out issues such as these. Good examples of these other security tools to implement inside of the DMZ are honeypots and intrusion detection and intrusion prevention systems. These additional tools can not only help protect and prevent attacks from happening or being successful on the network but also can be informative to teach the network security team about tactics that are commonly deployed against the network. This will help the team better prepare for and handle future potential attacks.

DMZs an impact the network in another way that is often times overlooked as it is considered and implemented into the architecture. These can negatively impact the performance of the network especially for users that are on the internal network by adding extra hops that these users must go through before being able to access the external, public network. However, the OpenFlow controller technology discussed earlier in this paper addresses this issue and potentially solves this issue. Not only does this technology seem to solve the issue of network performance of a DMZ but it potentially accomplishes this without sacrificing security by actively gauging and managing flow control of network traffic.

Conclusion

In the modern Internet landscape of today cyber security threats are an ever growing presence to organizations. Appropriate measures must be taken in order to safeguard the assets, information and resources that these organizations have. The confidentiality, integrity and

availability of these systems and the information that they house is paramount. Organizations need to employ as many security tools, devices and measures as possible in order to attain a comprehensive network security stance that is capable of handling attacks and incidents on the network. Each security measure that is implemented is not foolproof against every attack and is only one piece of the puzzle. One measure that can be taken is for an organization to incorporate a DMZ into the network architecture. DMZs are a way to put one more level of defense on the network, especially to protect valuable assets that are on the internal network as public facing assets and services are placed inside the DMZ.

Adding a DMZ provides many advantages such as a "quarantined" area of the network in case of an intrusion/incident that affects a publicly available resource such as a web server. Access control can be organized based upon trust levels associated with various zones of the network. Network reconnaissance can be mitigated keeping attackers from knowing what ports and protocols are used by devices. The firewalls work with the proxy server in the DMZ to protect against ip spoofing attacks and to hide the ip addresses of devices on the network. The firewalls associated with the DMZ also work to shut down attacks such as denial of service and SQL injections. DMZs can also be used with a honeypot as trap to lure attackers in and attack a fake resource which can be an informative experience to help the security team better protect the network against similar attacks in the future.

Every network security tool and device has its limitations and weaknesses and DMZs are no different. This is more of an architectural wrinkle that is added in which in and of itself cannot take action to handle malicious entities aside from keeping them quarantined in this area. A common approach attackers use to get valuable information is packet sniffing, this is a

vulnerability that DMZs are unable to properly address and handle. Finally, the performance of the network can suffer with the implementation.

Ultimately each organization must determine whether or not using a DMZ is going to add some value to the network security and whether it is the right choice. Implementing a DMZ takes careful thought and planning and must be configured appropriately in order to handle the demands of the network and the challenges that it will face. The strengths and limitations should always be considered when deciding whether or not to include something new in the network but one limitation that should not have much weight is the network performance dip. The more levels of security (defense in depth) there are the more protected the network and its information is. Security should come first and foremost in today's cyber security world.

References

Cole, E, and Northcutt, S. “Security Laboratory.” *Honeypots: A Security Manager's Guide to Honeypots*, SANS Institute, www.sans.edu/cyber-research/security-laboratory/article/honeypots-guide.

“Converged Plantwide Ethernet (CPwE) Design and Implementation Guide.” *Cisco*, Cisco, 31 Oct. 2013, www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/CPwE_DIG/CPwE_chapter6.html.

Danen, V. “Lock IT Down: Implementing a DMZ.” TechRepublic, TechRepublic, 29 Mar. 2001, www.techrepublic.com/article/lock-it-down-implementing-a-dmz/.

Mordechai G, Chief Science Officer at MorphisecJune 10, 2016. “The Future of Intrusion Detection.” *Help Net Security*, HelpNet Security, 10 June 2016, www.helpnetsecurity.com/2016/06/10/future-intrusion-detection/.

“Perimeter Firewall Design.” *Microsoft TechNet*, Microsoft, 2017, technet.microsoft.com/en-us/library/cc700828.aspx.

Stallings, W, and Brown, L. “ISBN 9780133773927Computer Security: Principles, and Practice with Access 3rd.” *Direct Textbook*, Pearson.

Weaver, R, et al. “Intrusion Detection and Prevention Systems.” *Guide to Network Defense and Countermeasures*, Course Technology, Cengage Learning, 2014, pp. 275–284.

White, R, and Donohue, D. *The Art of Network Architecture: Business-Driven Design*. Cisco Press, 2014.

Wu, H, et al. “Size-Based Flow Management Prototype for Dynamic DMZ.” *11th Conference on the Design of Reliable Communication Networks*, 2015.

Yadav, A. “Network Design: Firewall, IDS/IPS.” *InfoSec Resources*, Infosec Institute, 18 Feb. 2015, resources.infosecinstitute.com/network-design-firewall-idsips/#gref.