Network Demilitarized Zone (DMZ)

Jack Webb

ICTN 6870

Network Demilitarized Zone

1. Abstract

In today's information security, it is necessary to take advantage of all possible security options available to IT professionals. One of these options is network demilitarized zone or DMZ. A DMZ is the process of setting up a semi-secure network segment that houses all publicly accessible resource. This paper will cover the purpose of DMZ and its benefits in relation to security. It will cover the types and levels of DMS and security measure used within. This paper will also cover the differences between hardware and virtual DMZs as well as any commercial or vendor support for the creation of a DMZ.

2. Introduction

The key aspect of information security is to ensure that the collected data is protected. This is accomplished through confidentiality, availability and integrity. This is the goal of every IT professional. Make sure the data or resource is only accessible to those that have need. Make sure the data is available to those with access and make sure the data is protected to the point one can ensure the data hasn't been changed. This can all be compromised if an attacker can penetrate the trusted network. That is why the trusted networks are as secure as possible. The problem lies with publicly accessible resources such as web servers. If public resources are housed within the trusted network, an organization is just inviting an attacker inside. Most businesses rely on public interaction to survive. So, what is the solution to this problem? The answer is to setup a separate network segment that has enough security to ensure security but

not too much to hinder the accessibility of public interaction. This network segment is called a Demilitarized Zone or DMZ.

3. DMZ Purpose

A typical DMZ is a designated area just outside of the trusted network that houses public accessible resources. This keeps the trusted network secure by keeping non-trusted users out. DMZs can be setup to enhance security, used for testing or lab environments or for guest networks. As for security, a DMZ is considered a semi-trusted network because it isn't entirely open as there will be network and resource security. Leaving a DMZ wide open is just asking for trouble. A DMZ can house various different resources that both public users and trusted network user will have access to. These can include web, e-mail, FTP, DNS, VoIP, VPN and Proxy servers. Really, it comes down to what services an organization wants to place in this area based on security. That being said, a DMZ can also be used to separate specific resources or systems within the trusted network. So, why does one need a DMZ? A DMZ becomes the frontline barrier between the outside world and your vital resources. This is one of the components is the setup of a defense-in-depth principle by separating the external from the internal. Of course, one also needs to understand that separation comes at a risk in performance. Traffic now has to move through multiple components such as firewalls. The level of degradation depends on the design of the DMZ.

4. DMZ Levels

In today's world of information security, it isn't whether one should implement a DMZ but how it should be designed. When it comes to the design of a DMZ, there really isn't just one way. If one polled a group of 10 IT professionals, one would probably find 10 different ways to

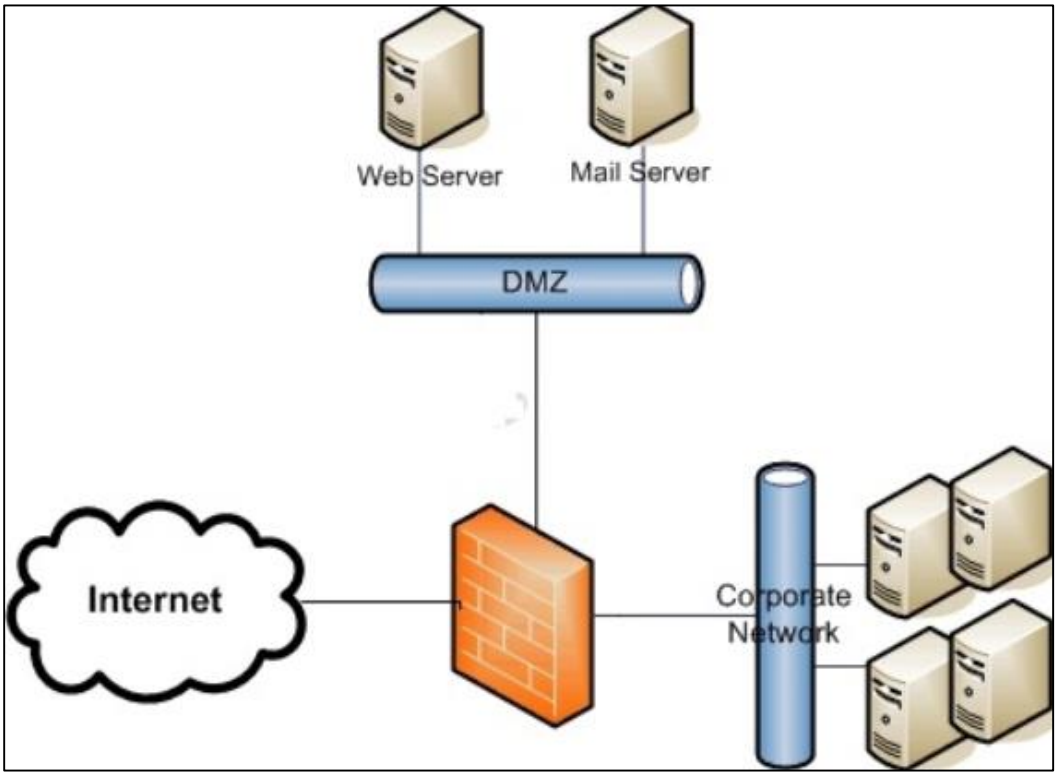
design a DMZ. A DMZ is comprised of either a separate IP address segment or using a segment from the current network using VLAN. The zone is separated from the internet and the trusted network utilizing firewalls, routers and/or switches. The IP address scheme can either be public or private addressing. Network Address Translation or NAT is also used to mask the DMZ addresses. This is especially necessary when using private IP addressing as it is necessary to translate the private addresses to public and vice versa as traffic moves in and out of the zone. It is also necessary to decide on the makeup of the zone. Will the design incorporate all hardware, be all virtualization or parts of each.

Considering DMZ designs can vary, there are four levels of DMZ designs. These design levels are nothing more than just basic designs to build from. The design that is used depends on the type of assets that need to be secured. With each level of design, comes an increase in security but also comes at a cost of complication and cost. Therefore, one needs to go through a decision process when deciding on a design level. One needs to ask the following questions:

- What are the assets that need to be available to the public and at what level of security?
- At what level of cost, can the organization incur?
- Can the organization live with the decrease in performance? If so, what design level and degradation can the organization live with?
- With each design level, the design becomes more complicated. Therefore, one needs to decide how much down time an organization can afford because with each increase in design complexity down time is also increased.

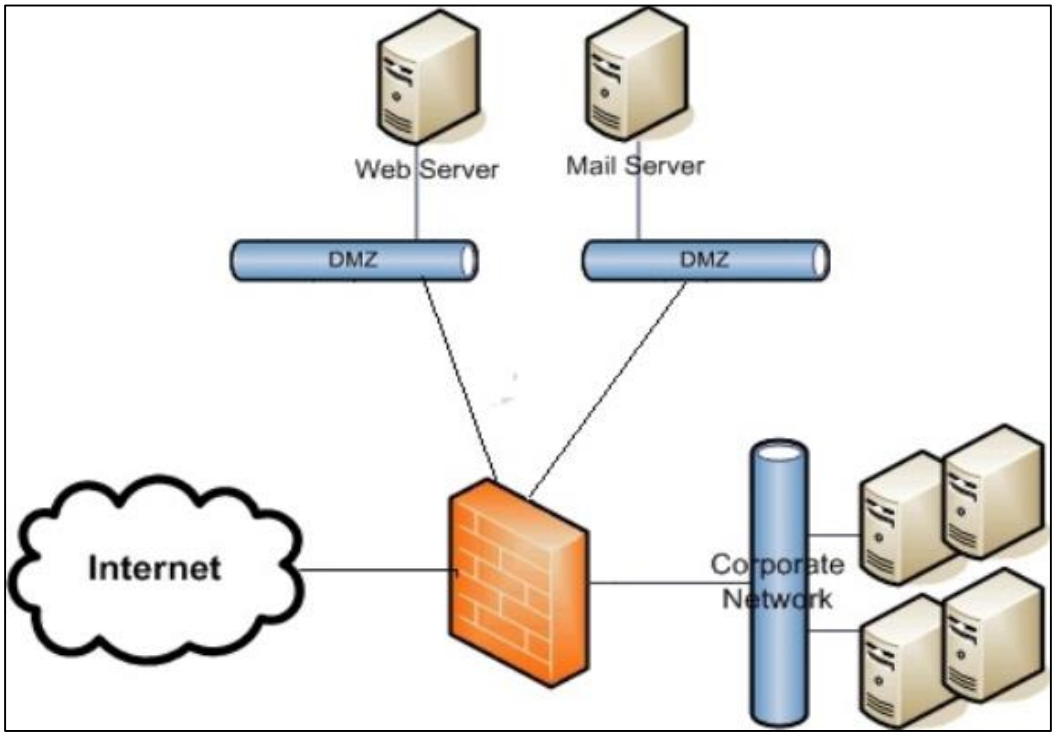
The first design level is the least complicated in design of the four with the lowest level of security. Figure 1 is the basic design of a Level 1 DMZ. In the Level 1 Design, the DMZ is a separate segment that is accessible off a port from the boundary firewall. This creates a single point of both protection and filtering. This design would work for those that have few public accessible resources such as a web or application server. Because it is not acceptable to locate a database in this type of DMZ design, the database would be located within the trusted network. This possess a problem if the database is attacked through the DMZ resources. Years ago this type of design with databases would have been acceptable but not today considering how susceptible databases are to attack, which places the trusted network in jeopardy. Because e-commerce relies on multiple server systems and databases, a Level 1 Design is nowhere close to being adequate in support and security.

Figure 1. Level 1 DMZ Design



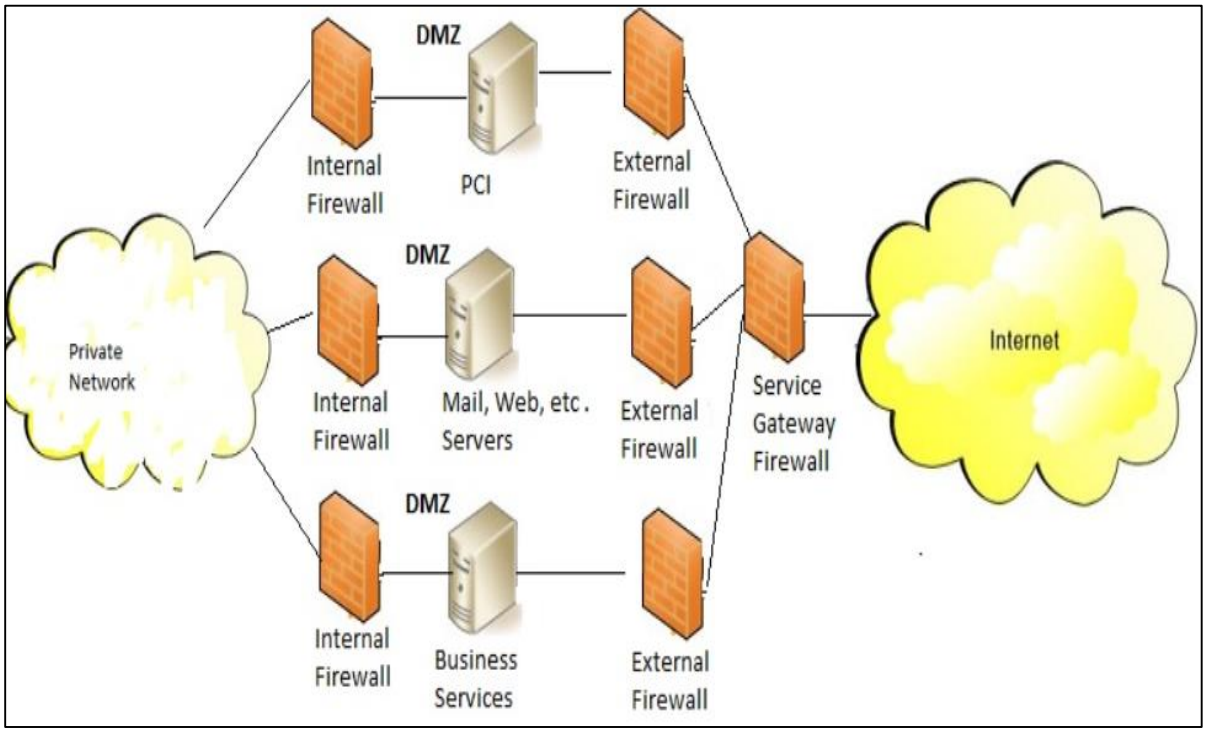
With a Level 2 Design, there is still one point of filtering and security. However, in this design, there are multiple DMZs utilizing multiple ports off the firewall. Now, there is a requirement for multiple network segments or VLANs where traffic rules must be written to pass the right resource traffic to the right segment. This design allows for resource separation providing increase security. As one can see, an increase in design level means an increase in complexity. This is the first DMZ design that will house a database or databases outside the trusted network. Because this design uses multiple firewall ports, it is much easier to secure these databases using filtering and traffic rules. Of course, this doesn't mean that these databases aren't still subjected to attacks such as injections but the trusted network is not safer. One problem utilizing a single firewall with a multi-port DMZ design is that overly permissive traffic rules can grant internet access to resources that may not need it. The basic Level 2 DMZ Design is shown in figure 2.

Figure 2. Level 2 DMZ Design



With increased security and complication, we move to the Level 3 DMZ Design. With this design, we are now using multiple firewalls that create an external and internal boundary within each DMZ. This allows for increased security as firewall rules or access from the internet can be granted through the external firewall but blocked at the internal firewall. This keeps public traffic between the firewalls while allowing external access by users on the trusted network. Figure 3 shows a basic design of a Level 3 MZ Design with a service gateway firewall.

Figure 3. Level 3 DMZ Design

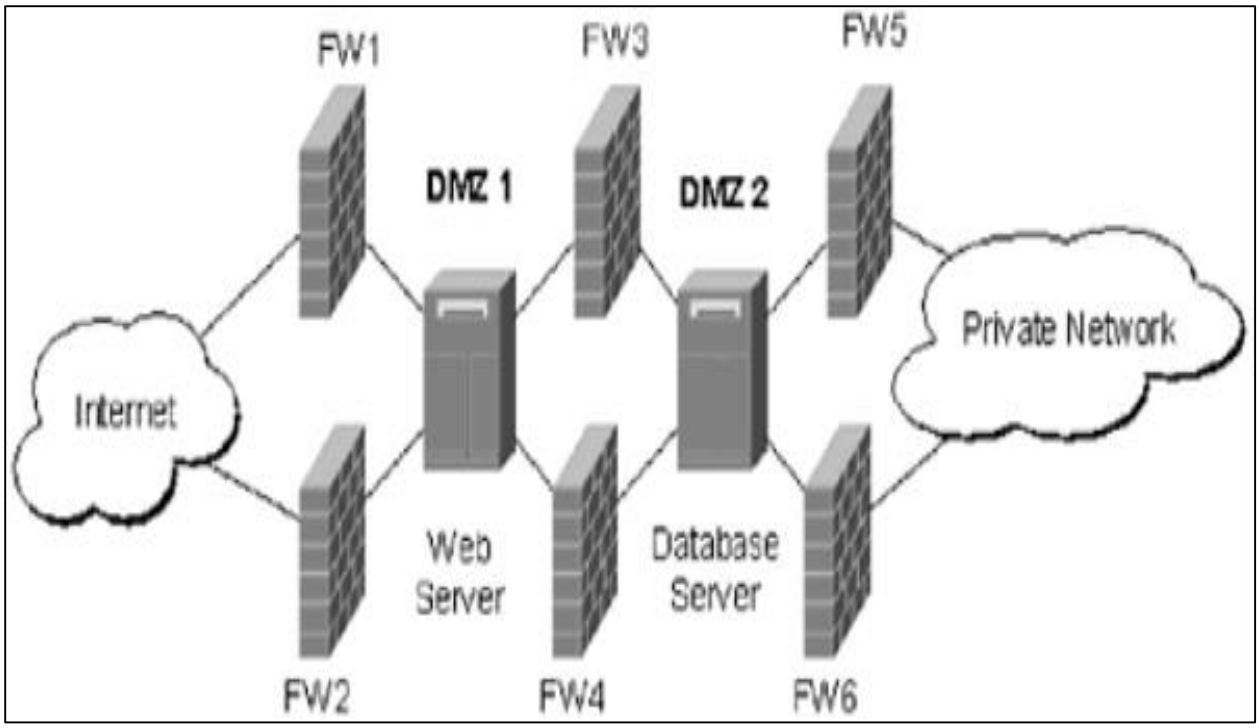


The service gateway firewall is the entry point for initial internet traffic before being routed to the necessary external firewall that controls traffic to the different resources. This double boundary design further protects the trusted network. So, moving all services into the DMZs further removes the exposer of the trusted network. Resources and databases are also further protected in the double boundary design. Only traffic designated for these resources will pass through the appropriate firewall based on either IP addressing or port numbers. Databases can

be reasonably secure using filters and access controls while keeping the trusted network safe from database attacks. Internet can be accessed from the trusted network using access controls and filters through the internal and external firewalls. Web traffic from the trusted network can be routed through a DMZ placed proxy server. The down sides of this design is the possibility on lack of coordination and communication with IT personnel during configuration, which could lead to restriction violation. These violation can happen if new resources or software are rushed into deployment without measures into place on the firewalls. Because of the complexity of this design, the other problem is the amount of delay that may incur.

The last design is the Level 4 DMZ Design. This is the most complicated and expensive design to create; however, it is the most secure. This design like level 3 utilizes a double boundary design. The difference is that level 4 utilizes a multiple firewall pairing to create the boundaries between DMZs. This allows an organization to spread t's resources between each boundary firewall pairs. This also allows an organization to separate its DMZ areas into functional or business areas. Another option is to set them up into trust level zones. The easiest way to create the separate firewall stacks is to build them based on Service Level Agreements or SLAs to include data classification. This allows for the separation of the various resources in the firewall stacks. The basic Level 3 Design is depicted in figure 4. The down side to this design level is the same as that of level 3. There is an increase in delay as traffic moves across the various firewalls and the possibility of configuration error if there is a loss of communication and coordination between IT groups.

Figure 4. Level 4 DMZ Design



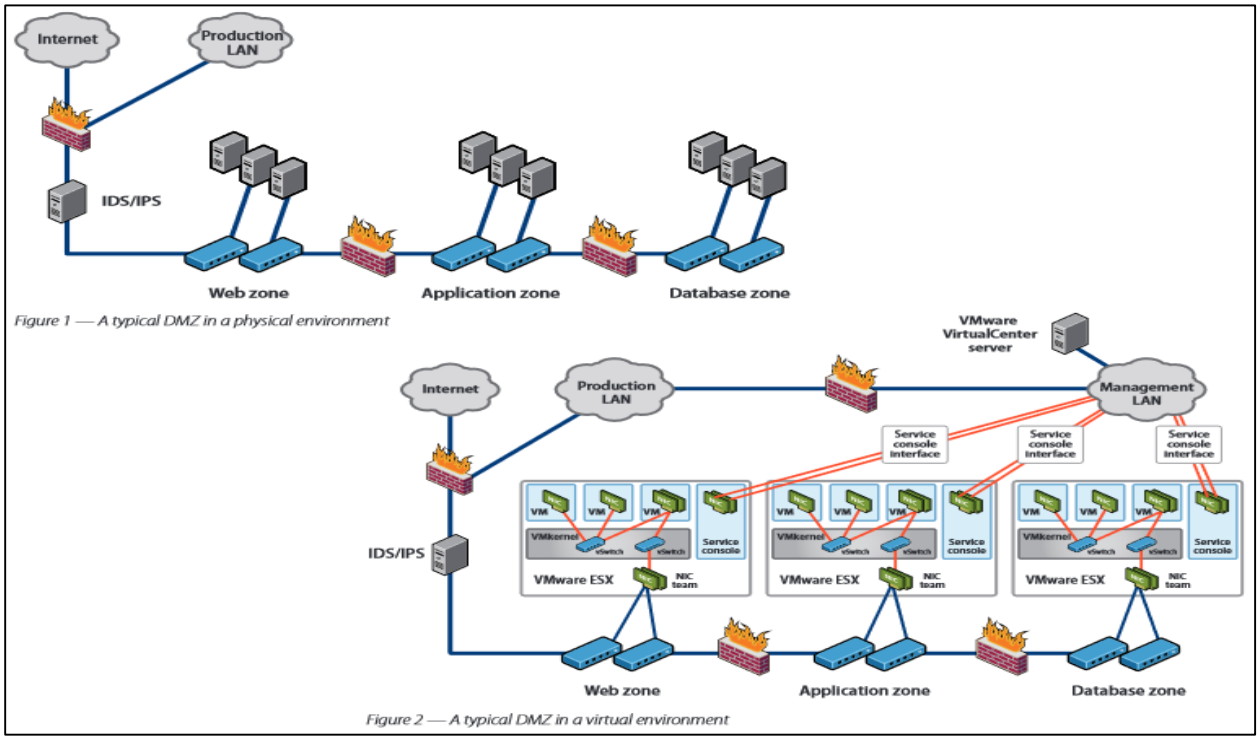
As these are just basic design level, there are many different configurations that DMZ user implement that are outside the norm. Aside from the design and configuration that IT professionals should use, the next question to ask is what type of components should be use in the design.

5. Physical vs Virtualization

When deciding on a DMZ design or configuration a decision needs to be made as to what components to use. Will the design be created using all hardware components, virtualization or a mixture of both? With any DMZ design, cost becomes a factor in the decision. An all hardware design comes at a premium cost and increases as the design level increases. Some organizations decrease the level of design to stay within budget but at the sacrifice of security. Utilizing a certain degree of virtualization cuts into the cost of the design and

implementation. The same level of DMZ designs can also be created within a virtual environment. Figure 5 shows both a hardware DMZ design and a hardware/virtual equivalent.

Figure 5. Hardware vs Virtual

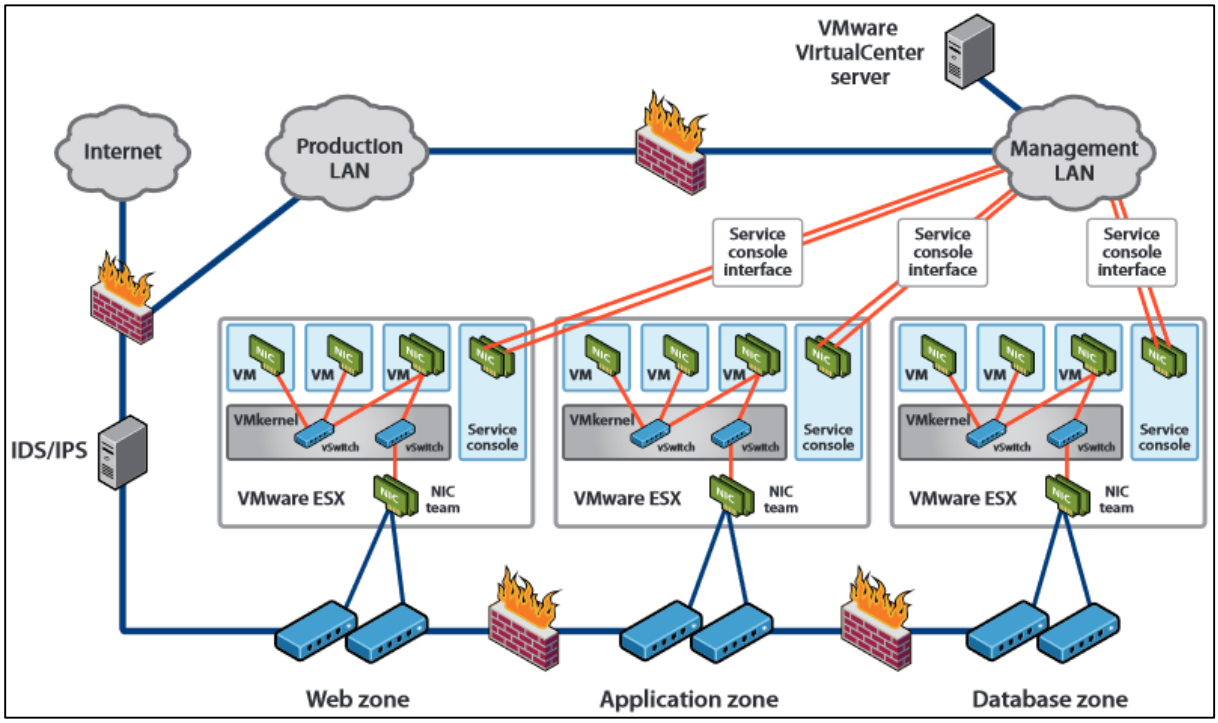


As with the basic DMZ level designs covered earlier, there are also basic DMZ configurations within virtual DMZs. These designs utilize a hardware/virtual mix and straight visualization. Each of these designs come with the same security concerns as the basic design levels previously covered. Of course, as the complexity increases so does the security.

The first configuration utilizes both hardware and virtualization to create the DMZ. This configuration is referred to as a Partially Collapsed DMZ with a Separate Physical Trust Zone. This configuration keeps each of the DMZ zones separate by utilizing separate ESX servers to create each zone. The physical hardware is used as an isolation means. There isn't much in the way of a configuration difference between this virtual configuration and a straight hardware

design. The odds of misconfiguration is low. Figure 6 is the partially collapsed DMZ with separate physical trust zones. With this design, we gain the advantage of less complexity with the same configuration requirements as a full hardware design. The physical environment stays the same as one would find in a typical DMZ design. Of course, there are disadvantages to this design. One such disadvantage is the consolidation of the DMZ resources. They spread across different isolated virtual systems. Because the design uses both hardware and virtual resources, the design fails to utilize all advantages of virtualization. The last downside of this configuration is the cost. Because this design uses both hardware and virtual components, the cost is higher. Each zone requires its own ESX server cluster, which increases cost. This is also true with necessity of power requirements and cooling.

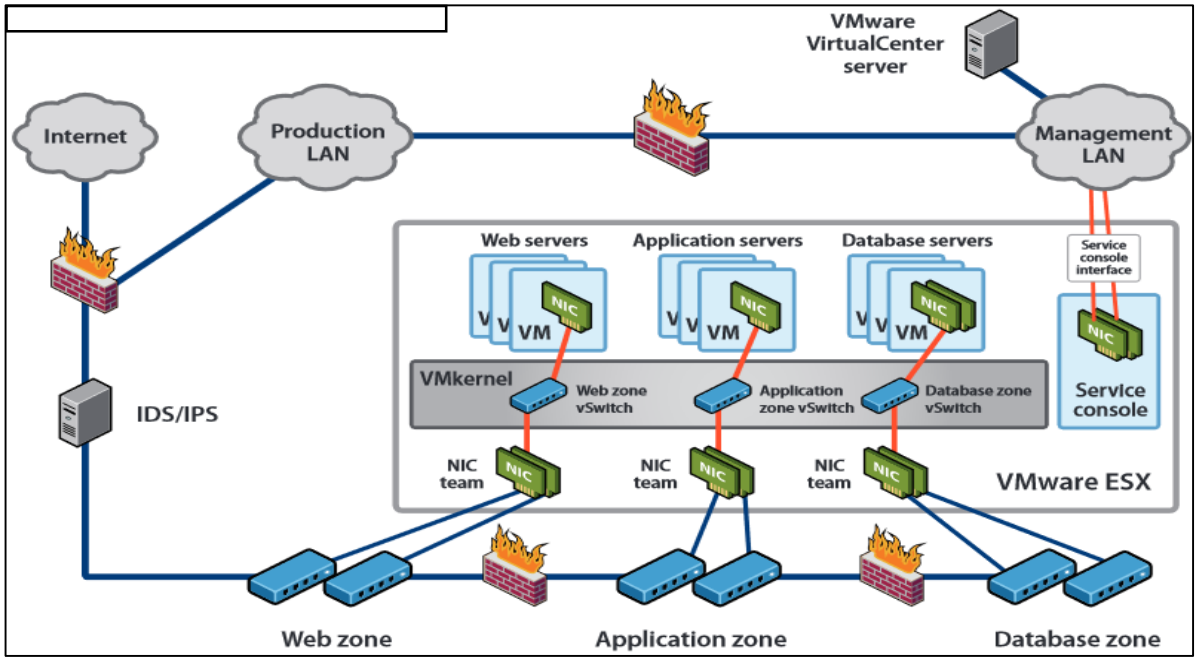
Figure 6. Partial Collapsed DMZ w/ Separate Physical Trust Zones



The second virtual level design is called Partially Collapsed with Virtual Separation of Trust Zones. This configuration is a step up from the previous. Where all of the DMZ zone

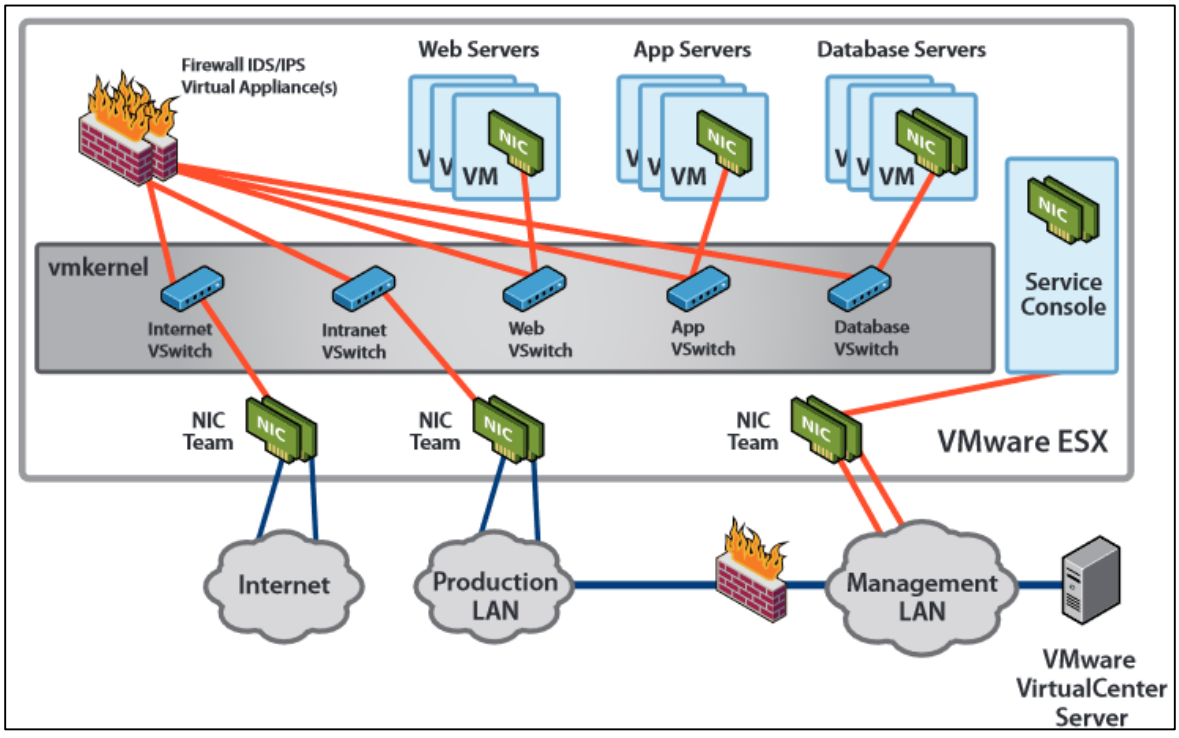
security took place at the physical level in configuration 1, the zone security now takes place in both the physical and virtual environments with configuration 2. The reason is that in configuration 2, all resource DMZ zones are located on the same ESX server. This allows for setting up different DMZ trust levels. Software security it increased and all physical zone security remains at the firewall/switch hardware level. The benefits of this configuration is that it take the next step towards full virtualization utilization and decreases the costs. This design also consolidates all of the resources under one roof. As with any advancement, there are downsides. In this case, the configuration becomes more complicated and requires more specialized IT personnel. This creates an increase in misconfiguration possibilities. Figure 7 is a Partially Collapsed DMZ with Virtual Separation of Trust Zones.

Figure 7. Partially Collapsed DMZ w/ Virtual Separation of Trust Zones



The last configuration is the Fully Collapsed configuration. This configuration is the most complicated of the three. This configuration utilizes the full advantages of the virtual environment consolidation all DMZ resources on one ESX server. This greatly decreases costs. All devices used in the security of each zone both networking and security reside on this server making management easier from a consolidated service console. This console assists in the management across all zones and provides a single point of notifications or alerts. This configuration also fully isolates each zone allowing the configuration of different trust levels, which enhances security. Because of the complexity of this infrastructure, the possibilities of misconfigurations is greatly increased. Because this infrastructure is fully virtual, it requires IT professionals with specialized talents in virtualization as all configurations at both the network and server level will be different than one configuring standard hardware. Figure 8 is a Fully Collapsed design.

Figure 8. Fully Collapsed



6. Vendor Support

As the need for DMZs have increased over the years, so has technology support from the various vendors. There are now vendors that have adapted current components to support DMZ configurations at both the hardware and software levels. When it comes to hardware, firewalls are being designed that come with multiple ports that are specialized to support DMZs. Therefore, an organization can purchase a firewall that comes with designated DMZ ports. These are preconfigured ports that assist in configuration of these ports for DMZ support.

At the software level, there has been an increased support for DMZs within the components operating system. These operating systems now assist in the configuration of traffic to the appropriate servers utilizing PAT. The configurations can support both IP addressing or the utilization of port numbers to distinguish between the different DMZ resources.

7. DMZ Security

As discussed, the amount of security is based on the complexity of the design of the DMZ. Granted all designs utilize a firewall scheme and require the same basic filters and access controls, the design complexity determines whether there is a basic scheme without a separation or one with resource separation. Isolation the various DMZ resources assists in security. It one DMZ resource is attacked, the other DMZs can be assumed safe.

The problem with security is that it can't be implemented at full strength because there is a huge possibility that it would impede access from those that are in need. That being said, it is necessary to create the rules that are needed to isolate each resource to contain possible attacks. It is also necessary to implement an application layer defense to root out any malicious

activities such as SQL injections before they find their marks. At the resource level, it is necessary to disable any unneeded service. This removes any possible access to these resources through other services. It is also necessary to limit access and run services at the lowest privilege. When in doubt, keep them out. As with any type of account, it is only as secure as the password or passphrase. Security always begins with password and passphrase security. If there are unneeded accounts, then they must either be removed, disguised or change. This also limits a possible avenue for an attacker to access the resource. The last two necessary security measures that need to be setup and implemented are security updates/patches and security logs for monitoring. Security updates and patches with fix vulnerabilities in not only operating systems but software alike. This is necessary in fixing vulnerabilities that attackers can use to gain access. As for logging, this provides an IT professional with the ability to monitor resources and track possible attacks.

8. Honeynet/Pot

The last security measure to cover is a honeynet or honeypots. These are configured resources that reside in a DMZ zone. They are essentially fake resources that are meant to attract attackers and divert them way from real resources. A honeypot/net DMZ should be on the menu when considering a DMZ design for actual resources. It assists with delaying actions that allow IT professionals' time to take corrective measures to stop the attack at a minimum. Several honeypots makeup a honeynet. Another purpose of these systems is to capture an attacker to gain knowledge of their actions and the tools they are using so that rules can be created to combat future attacks. IT professionals can also use these systems to also track the attackers for possible prosecution. The design of this DMZ as with other DMZ designs can be

either hardware or virtual. It can also incorporate IDS resources that are used for intrusion detection that assists IT professionals in their never ending endeavor of combating attackers.

9. Conclusion

In today's business environment, it totally necessary to protect that one asset that just about every business lives by and that is data and resources. As attacker have become increasingly more sophisticated and technologically savvy, one needs to pull out all the stop to secure protected areas. Years ago allowing public access to public accessible resource that may have been placed inside of the trusted network may have not been that much of a concern. However, decade later this is not acceptable practice. Placing publicly accessible resources inside of the trusted network is nothing more than asking for a death warrant for the business. DMZs are no longer a possibility but a necessity. This really is the only security measure that can be utilized to separate publicly accessible resources from the trusted network. The degree of design will determine how secure these resources can be. End the end it comes down to how protected does an organization want to be and how much of a loss can they take till these types of security measures need to be implemented.

Work Cited

Bauer, Mick. *Designing and Using DMZ Networks to Protect Internet Servers*. 01 May 2001. Linux Journal. 11 Apr. 2014. <http://www.linuxjournal.com/article/4415>.

Chapple, Mike. *Four Tips for Securing a Network DMZ*. 18 May 2012. 11 Apr. 2014. <http://www.fedtechmagazine.com/article/2012/05/four-tips-securing-network-dmz>.

DMZ Virtualization with VMware Infrastructure. n.d. 11 Apr. 2014. <http://www.vmware.com/files/pdf/dmz_virtualization_vmware_infra_wp.pdf>.

Hamelin, Michael. *How to Design a Secure DMZ*. 1 Sep. 2010. Quinstreet Eneterprise. 11 Apr. 2014. <http://www.eweek.com/c/a/Security/How-to-Design-a-Secure-DMZ/>.

Murphy, Jack. *The Demilitarized Zone as an Information Protection Network*. 2006. Idea Group Publishing. 11 Apr. 2014. <http://www.irma-international.org/viewtitle/18389/>.

Rodriguez, Erik. *HOWTO- Design and Configure a DMZ Network*. 16 Oct. 2010. SKULLBOX.NET. 11 Apr. 2014. <http://www.skullbox.net/configureDMZnetwork.php>.

Salimi, Ali and Peyman Kabiri. *Avoiding Cyber-attacks to DMZ and Capturing Forensics from Intruders Using Honeypots*. 1 Feb. 2012. Journal of Advances in Computer Research. 11 Apr. 2014. <http://www.sid.ir/en/VEWSSID/J_pdf/1035220120106.pdf>.

Science DMZ Security - Firewalls vs. Router ACLs. n.d. US Department of Energy. 11 Apr. 2014. <http://fasterdata.es.net/science-dmz/science-dmz-security/>.

Shinder, Deb. *SolutionBase: Strength network defense by using a DMZ*. 29 Jun. 2005. CBS Interactive. 11 Apr. 2014. <http://www.techrepublic.com/article/solutionbase-strengthen-network-defenses-by-using-a-dmz/>.

Thurman, Mathias. *Security Manager's Journal: Keeping the DMZ safe*. 22 Aug. 2011. ComputerWorld Inc. 11 Apr. 2014. <http://www.computerworld.com/s/article/358142/Keeping_the_DMZ_Safe>.

Yadav, Ajay. *Network Design Part 2: Demilitarized Zone/Honeypots*. n.d. INFOSEC Institute. 11 Apr. 2014. <http://resources.infosecinstitute.com/network-design-part-2-demilitarized-zonehoneypots/>.

Young, Scott. *Designing a DMZ*. 26 MAr. 2001. SANS Institute. 11 Apr. 20014. <http://www.sans.org/reading-room/whitepapers/firewalls/designing-dmz-950>.