

# FiDo Secure Architecture Report

## ***Table of Contents***

Key Points	4
Phase 1	4
Phase 2	12
Phase 3	16
Further Work	24
References	24

## ***Table of Figures***

Figure 1 - Network Diagram	3
----------------------------	---

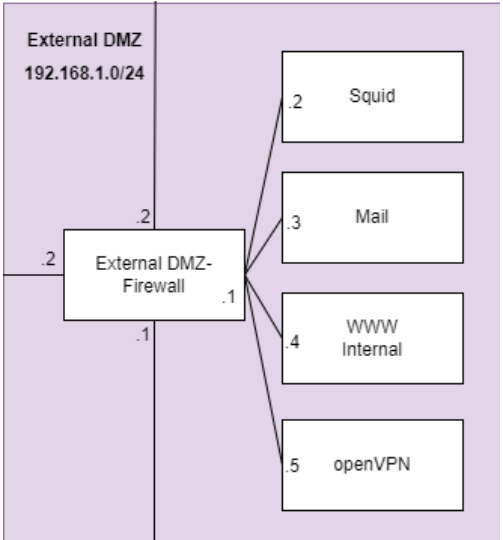
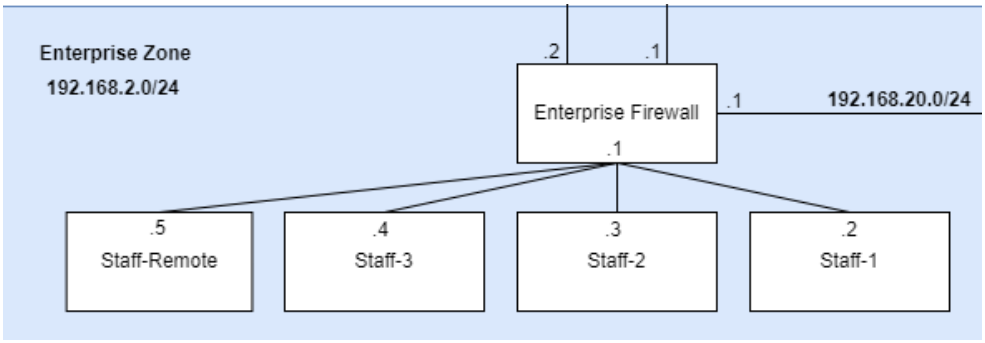


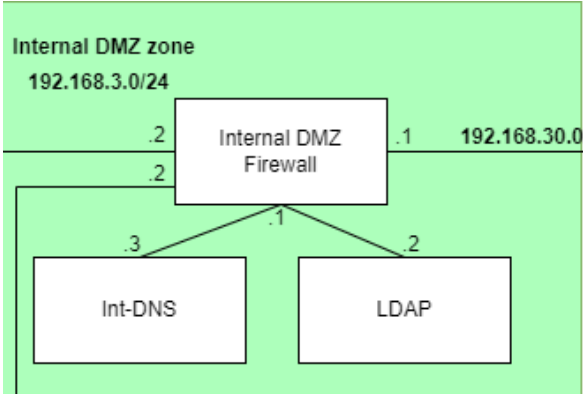
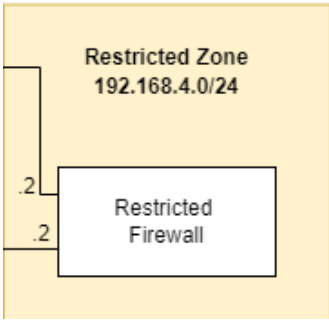
## Key Points

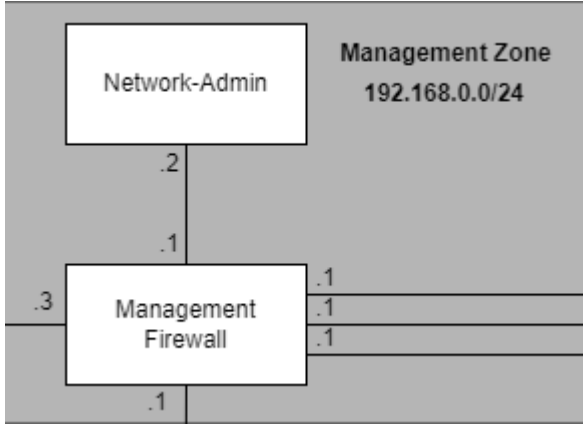
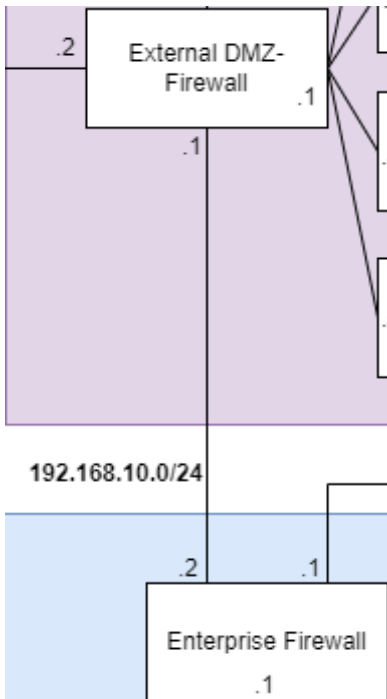
- Implemented a network topology according to the SANS Institute Infrastructure Security Architecture research paper (Obregon, 2015).
- Blocked all unnecessary traffic using firewall rules
- Ensured that DMZ machines cannot initiate connections
- Implemented Destination NAT for services exposed to the Internet
- Implemented Source NAT for anything going out to the Internet, eth0, on the External DMZ Firewall machine using masquerade
- Implemented DNS internally using dnsmasq with the local address being *fido.cyber.test*
- Configured the internal DNS to access the external DNS if it doesn't have the static hosts in its file
- Disabled IPv6 on all firewalls
- Enabled SSH for remote office users to connect into the enterprise zone

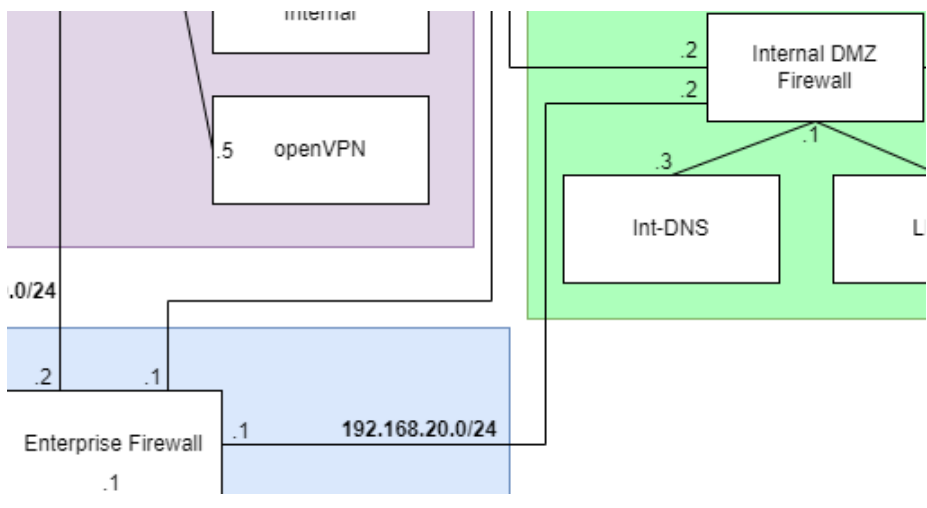
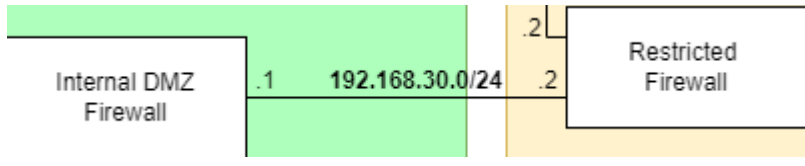
## Phase 1

<i>Reference</i>	<i>Claim</i>	<i>Evidence</i>
Obregon, L. (2015)	We have a full network topology in place that makes use of zones and various different private subnets.	<b>Figure 1</b>

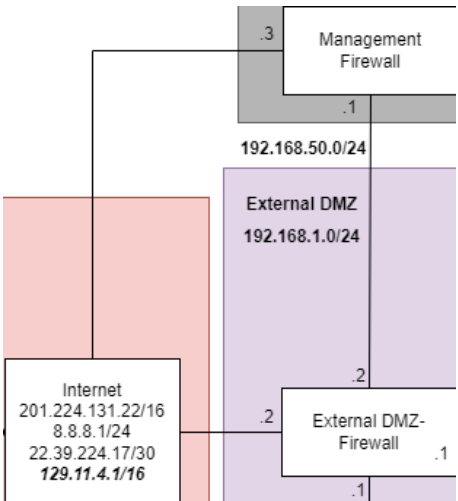
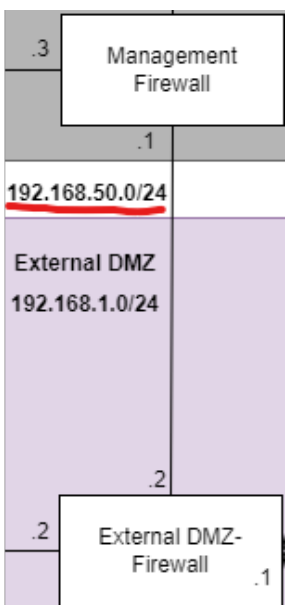
<p>Obregon, L. (2015)</p>	<p>We have implemented an External DMZ zone of trust. We moved all of the services that would need to be exposed to the internet here, like the web server.</p>	
<p>Obregon, L. (2015)</p>	<p>We have implemented an Enterprise zone of trust where we have moved all of the staff machines in.</p>	

<p>Obregon, L. (2015)</p>	<p>We have implemented an Internal DMZ zone of trust where we have moved all of the internal application services.</p>	 <p>The diagram shows a green-shaded area representing the 'Internal DMZ zone' with IP range 192.168.3.0/24. At the top, a box labeled 'Internal DMZ Firewall' is connected to the left edge of the zone with a line labeled '.2'. A line labeled '.1' connects the firewall to the right edge of the zone, which is labeled '192.168.30.0'. Below the firewall, two boxes labeled 'Int-DNS' and 'LDAP' are connected to the firewall with lines labeled '.3' and '.2' respectively. A line labeled '.1' also connects the firewall to the top of the 'Int-DNS' box.</p>
<p>Obregon, L. (2015)</p>	<p>We have implemented a Restricted zone of trust where we have implemented a firewall with a network card so that adding new machines would be easy.</p>	 <p>The diagram shows a yellow-shaded area representing the 'Restricted Zone' with IP range 192.168.4.0/24. A box labeled 'Restricted Firewall' is connected to the left edge of the zone with a line labeled '.2'. Another line labeled '.2' connects the firewall to the right edge of the zone.</p>

<p>Obregon, L. (2015)</p>	<p>We have implemented a Management zone of trust where we created a “Network-Admin” machine that can manage every machine on the network but it cannot be accessed by the machines</p>	 <p>The diagram shows a Management Zone with the IP range 192.168.0.0/24. It contains a 'Network-Admin' machine and a 'Management Firewall'. The Network-Admin machine has an interface with IP .2 connected to the firewall's .1 interface. The firewall has three other interfaces: .3 on the left, and two .1 interfaces on the right connected to external networks.</p>
<p>N/A</p>	<p>We have implemented an “access subnet” to connect the External DMZ firewall to the Enterprise firewall on the 192.168.10.0/24 subnet</p>	 <p>The diagram shows two firewalls connected via an access subnet. The 'External DMZ-Firewall' is in a purple-shaded area and has an interface with IP .1 connected to the 'Enterprise Firewall's .1 interface. The Enterprise Firewall is in a blue-shaded area and has an interface with IP .2 connected to the access subnet. The access subnet is labeled 192.168.10.0/24. There are also other interfaces shown on both firewalls.</p>

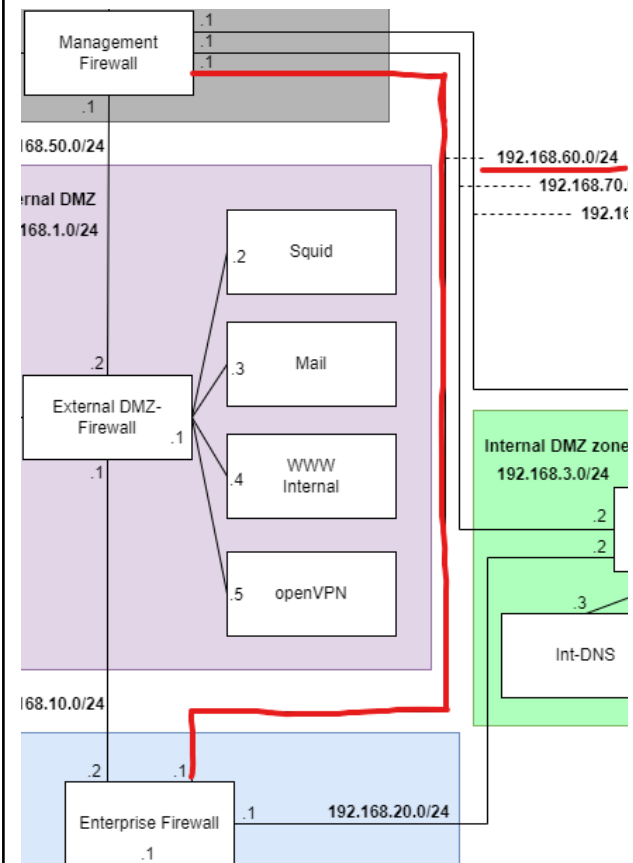
N/A	<p>We have implemented an “access subnet” to connect the Enterprise firewall to the Internal DMZ firewall on the 192.168.20.0/24 subnet. An access subnet was required as we didn’t want the firewalls/gateways to overlap with zones they were not supposed to be in.</p>	 <p>The diagram illustrates a network topology. On the left, a purple box labeled 'internal' contains an 'openVPN' box with IP .5. Below this is a blue box labeled 'Enterprise Firewall' with IP .1. To the right of the Enterprise Firewall is a light blue box labeled '192.168.20.0/24'. On the right side, a green box labeled 'Internal DMZ Firewall' has IP .1. It is connected to a green box labeled 'Int-DNS' with IP .3. Above the Internal DMZ Firewall are two green boxes with IP .2. A line connects the Enterprise Firewall to the Internal DMZ Firewall through the 192.168.20.0/24 subnet.</p>
N/A	<p>We have implemented an “access subnet” to connect the Internal DMZ firewall to the Restricted Firewall on the 192.168.30.0/24 subnet</p>	 <p>The diagram shows a green box labeled 'Internal DMZ Firewall' with IP .1. To its right is a yellow box labeled 'Restricted Firewall' with IP .2. A line connects them through a green box labeled '192.168.30.0/24'. Above the Restricted Firewall is another yellow box with IP .2.</p>

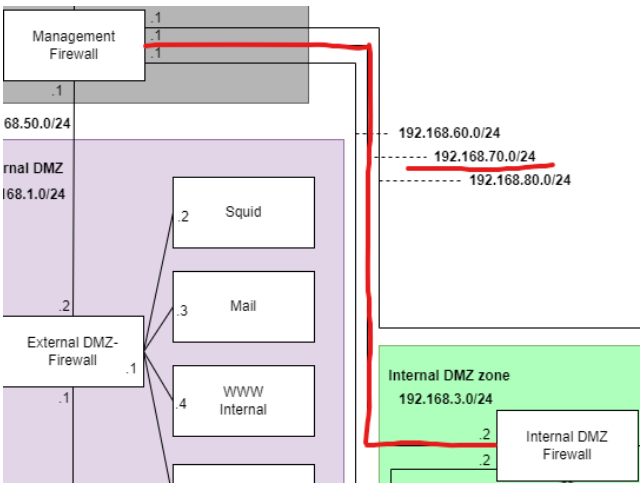
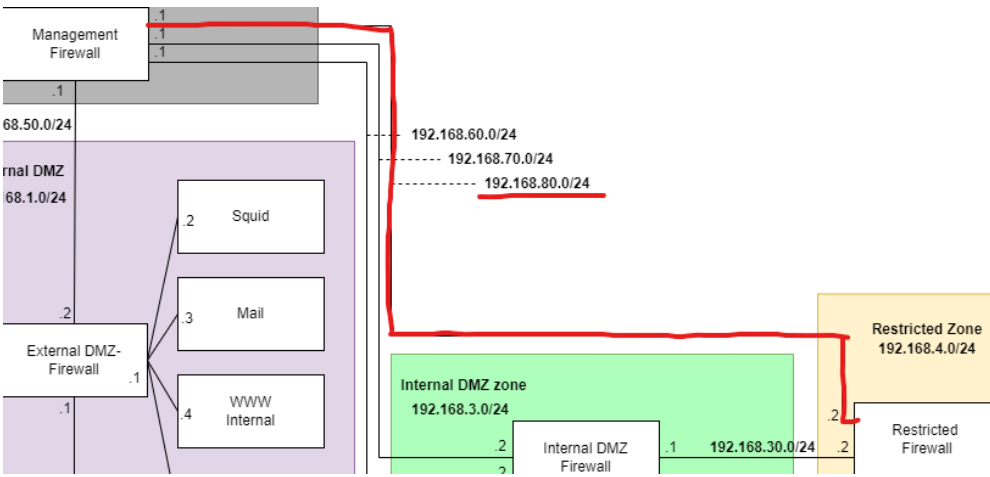


N/A	We have implemented an “access subnet” to connect the Management firewall to the Internet, but it’s not in use.	 <p>The diagram illustrates a network configuration. At the top, a grey box labeled 'Management Firewall' has an interface labeled '.3' connected to a grey box labeled '.1'. Below this, a purple box labeled 'External DMZ' with IP '192.168.1.0/24' has an interface labeled '.2' connected to a white box labeled 'External DMZ-Firewall' with interface '.1'. The 'External DMZ-Firewall' also has an interface labeled '.2' connected to a white box labeled 'Internet' with IP ranges '201.224.131.22/16', '8.8.8.1/24', '22.39.224.17/30', and '129.11.4.1/16'. A red box is positioned between the Internet and the External DMZ.</p>
N/A	We have implemented an “access subnet” to connect the Management firewall to the External DMZ Firewall on the 192.168.50.0/24 subnet.	 <p>The diagram shows a network configuration. A grey box labeled 'Management Firewall' has an interface labeled '.3' connected to a grey box labeled '.1'. Below this, a purple box labeled 'External DMZ' with IP '192.168.1.0/24' has an interface labeled '.2' connected to a white box labeled 'External DMZ-Firewall' with interface '.1'. The 'External DMZ-Firewall' also has an interface labeled '.2' connected to a grey box labeled '192.168.50.0/24'.</p>


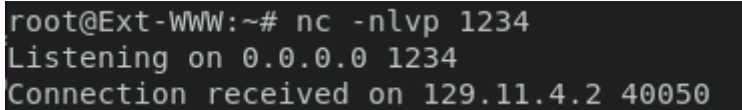
N/A

We have implemented an “access subnet” to connect the Management firewall to the Enterprise Firewall on the 192.168.60.0/24 subnet.



N/A	<p>We have implemented an “access subnet” to connect the Management firewall to the Internal DMZ Firewall on the 192.168.70.0/24 subnet.</p>	 <p>The diagram illustrates a network topology. On the left, a 'Management Firewall' is connected to a '68.50.0/24' subnet. Below it, an 'External DMZ-Firewall' is connected to a '68.1.0/24' subnet. This subnet contains three services: 'Squid' (IP .2), 'Mail' (IP .3), and 'WWW Internal' (IP .4). To the right, there is an 'Internal DMZ zone' with IP '192.168.3.0/24' and an 'Internal DMZ Firewall'. A red line represents the 'access subnet' connecting the Management Firewall to the Internal DMZ Firewall. The subnets 192.168.60.0/24, 192.168.70.0/24, and 192.168.80.0/24 are shown at the top right.</p>
N/A	<p>We have implemented an “access subnet” to connect the Management firewall to the Restricted Firewall on the 192.168.80.0/24 subnet.</p>	 <p>This diagram is similar to the one above but includes an additional 'Restricted Zone' with IP '192.168.4.0/24' and a 'Restricted Firewall'. The 'Internal DMZ zone' (192.168.3.0/24) and 'Internal DMZ Firewall' are also present. A red line represents the 'access subnet' connecting the Management Firewall to the Restricted Firewall. The subnets 192.168.60.0/24, 192.168.70.0/24, and 192.168.80.0/24 are shown at the top right. The 'Restricted Firewall' is connected to the 'Restricted Zone'.</p>

## Phase 2

<i>Reference</i>	<i>Claim</i>	<i>Evidence</i>
N/A	Users connecting to the internet are SNATed through the External DMZ Firewall	<p>Line in .startup:  <code>iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE</code></p> <p>Explanation            1: Shows staff machine connect to external address via netcat              2: Shows external machine listen, and then accept a connection, from an external facing company address              The connection was received from the company's external address, not a private internal one, showing successful use of SNAT.</p>
N/A	DNAT through External DMZ Firewall allows the internet to access port 80 on the internal web server	<p>Line in .startup:  <code>iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j DNAT --to-destination 192.168.1.4:80</code></p> <p>Explanation            The image below shows an external machine checking the headers of the companies external address using port 80, and receiving an OK response</p>

		<pre>root@Internet:~# curl -I 129.11.4.2 HTTP/1.1 200 OK</pre>
N/A	DNAT through External DMZ Firewall Allows the internet to access port 443 on the internal web server	<p>Line in .startup:</p> <pre>iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 443 -j DNAT --to-destination 192.168.1.4:443</pre> <p>Explanation</p> <p>The image below shows an external machine checking the headers of the companies external address using port 443, and receiving an Bad request response; this shows the server received the request and can't process it.</p> <pre>root@Internet:~# curl -I 129.11.4.2:443 HTTP/1.1 400 Bad Request</pre>
N/A	DNAT through External DMZ Firewall allows the internet to access port 25 on the mail box	<p>Line in .startup:</p> <pre>iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 25 -j DNAT --to-destination 192.168.1.3:25</pre> <p>Explanation</p> <p>1: Shows Mail machine set up listener on port 25, and receive a connection from an external machine</p> <pre>root@Mail:~# nc -nvlp 25 Listening on 0.0.0.0 25 Connection received on 129.11.4.1 41674</pre> <p>2: Shows external machine connect to listener through the companies external address</p> <pre>root@Internet:~# nc 129.11.4.2 25</pre>

N/A	DNAT through External DMZ Firewall allows the internet to access port 587 on the mail box	<p>Line in .startup:</p> <pre>iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 587 -j DNAT --to-destination 192.168.1.3:587</pre> <p>Explanation</p> <p>1: Shows Mail machine set up listener on port 587, and receive a connection from an external machine</p> <pre>root@Mail:~# nc -nvlp 587 Listening on 0.0.0.0 587 Connection received on 129.11.4.1 35492</pre> <p>2: Shows external machine connect to listener through the companies external address</p> <pre>root@Internet:~# nc 129.11.4.2 587</pre>
N/A	DNAT through External DMZ Firewall allows the internet to access port 993 on the Mail box	<p>Line in .startup:</p> <pre>iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 993 -j DNAT --to-destination 192.168.1.3:993</pre> <p>Explanation</p> <p>1: Shows Mail machine set up listener on port 993, and receive a connection from an external machine</p> <pre>root@Mail:~# nc -nvlp 993 Listening on 0.0.0.0 993 Connection received on 129.11.4.1 52328</pre>

		<p>2: Shows external machine connect to listener through the companies external address</p> <pre>root@Internet:~# nc 129.11.4.2 993</pre>
N/A	DNAT through External DMZ Firewall allows the internet to access port 1194 on the openVPN box	<p>Line in .startup:</p> <pre>iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 1194 -j DNAT --to-destination 192.168.1.5:1194</pre> <p>Explanation</p> <p>1: Shows OpenVPN machine set up listener on port 1194, and receive a connection from an external machine</p> <pre>root@OpenVPN:~# nc -nlvp 1194 Listening on 0.0.0.0 1194 Connection received on 129.11.4.1 44086</pre> <p>2: Shows external machine connect to listener through the companies external address</p> <pre>root@Internet:~# nc 129.11.4.2 1194</pre>
N/A	DNAT through External DMZ Firewall allows the remote office to access the SSH service (port 22) in the enterprise zone	<p>Line in .startup:</p> <pre>iptables -t nat -A PREROUTING -i eth0 -s 22.39.224.16/30 -p tcp --dport 22 -j DNAT --to-destination 192.168.2.5:22</pre> <p>Explanation</p> <p>Image below shows external office machine connecting to the remote staff machine via ssh through the companies external facing address as opposed to the machines private address:</p>

		<pre> root@Ext-Office:~# ssh remote_user@129.11.4.2 remote_user@129.11.4.2's password: Linux Staff-Remote 5.14.9 #1 Mon Oct 4 06:03:24 PDT 2021 x86_64 Welcome to Netkit  Could not chdir to home directory /home/remote_user: No such file or directory \$  </pre>
--	--	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

## Phase 3

<i>Reference</i>	<i>Claim</i>	<i>Evidence</i>
Damien (2010), Christian (2020)	SSH service on the Staff-Remote machine alongside specific firewall rules allows only external office to connect to the Enterprise Zone via the “remote_user” user.	<p>Image below shows Ext-Office machine connecting via the external address of the company</p> <pre> root@Ext-Office:~# ssh remote_user@129.11.4.2 The authenticity of host '129.11.4.2 (129.11.4.2)' can't be established. ECDSA key fingerprint is SHA256:hldZ+pQj6DGwToSAriPVVsPpufUSQoEI8cBffBBHyN0. Are you sure you want to continue connecting (yes/no/[fingerprint])? yes Warning: Permanently added '129.11.4.2' (ECDSA) to the list of known hosts. remote_user@129.11.4.2's password: Linux Staff-Remote 5.14.9 #1 Mon Oct 4 06:03:24 PDT 2021 x86_64 Welcome to Netkit  Could not chdir to home directory /home/remote_user: No such file or directory \$  </pre>
Damien (2010), Christian (2020)	SSH service on any internal machine allows the Network-Admin machine to connect to the “admin” user on each	Firewall-ExtDMZ



	<p>machine.</p>	<pre> root@Network-Admin:~# ssh admin@192.168.1.1 The authenticity of host '192.168.1.1 (192.168.1.1)' can't be established. ECDSA key fingerprint is SHA256:hldZ+pQj6DGwToSAriPVVsPpufUSQoEI8cBffBBHyN0. Are you sure you want to continue connecting (yes/no/[fingerprint])? yes Warning: Permanently added '192.168.1.1' (ECDSA) to the list of known hosts. admin@192.168.1.1's password: Linux Firewall-ExtDMZ 5.14.9 #1 Mon Oct 4 06:03:24 PDT 2021 x86_64 Welcome to Netkit  Could not chdir to home directory /home/admin: No such file or directory \$ █ </pre> <p>Firewall-Enterprise</p> <pre> root@Network-Admin:~# ssh admin@192.168.2.1 The authenticity of host '192.168.2.1 (192.168.2.1)' can't be established. ECDSA key fingerprint is SHA256:hldZ+pQj6DGwToSAriPVVsPpufUSQoEI8cBffBBHyN0. Are you sure you want to continue connecting (yes/no/[fingerprint])? yes Warning: Permanently added '192.168.2.1' (ECDSA) to the list of known hosts. admin@192.168.2.1's password: Linux Firewall-Enterprise 5.14.9 #1 Mon Oct 4 06:03:24 PDT 2021 x86_64 Welcome to Netkit  Could not chdir to home directory /home/admin: No such file or directory \$ █ </pre> <p>Firewall-IntDMZ</p> <pre> root@Network-Admin:~# ssh admin@192.168.3.1 The authenticity of host '192.168.3.1 (192.168.3.1)' can't be established. ECDSA key fingerprint is SHA256:hldZ+pQj6DGwToSAriPVVsPpufUSQoEI8cBffBBHyN0. Are you sure you want to continue connecting (yes/no/[fingerprint])? yes Warning: Permanently added '192.168.3.1' (ECDSA) to the list of known hosts. admin@192.168.3.1's password: Linux Firewall-IntDMZ 5.14.9 #1 Mon Oct 4 06:03:24 PDT 2021 x86_64 Welcome to Netkit  Could not chdir to home directory /home/admin: No such file or directory \$ █ </pre> <p>Firewall-MGMT</p>
--	-----------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

		<pre> root@Network-Admin:~# ssh admin@192.168.0.1 The authenticity of host '192.168.0.1 (192.168.0.1)' can't be established. ECDSA key fingerprint is SHA256:hldZ+pQj6DGwToSAriPVVsPpufUSQoEI8cBffBBHyN0. Are you sure you want to continue connecting (yes/no/[fingerprint])? yes Warning: Permanently added '192.168.0.1' (ECDSA) to the list of known hosts. admin@192.168.0.1's password: Linux Firewall-MGMT 5.14.9 #1 Mon Oct 4 06:03:24 PDT 2021 x86_64 Welcome to Netkit  Could not chdir to home directory /home/admin: No such file or directory \$ █ </pre> <p>Firewall-Restricted</p> <pre> root@Network-Admin:~# ssh admin@192.168.4.1 The authenticity of host '192.168.4.1 (192.168.4.1)' can't be established. ECDSA key fingerprint is SHA256:hldZ+pQj6DGwToSAriPVVsPpufUSQoEI8cBffBBHyN0. Are you sure you want to continue connecting (yes/no/[fingerprint])? yes Warning: Permanently added '192.168.4.1' (ECDSA) to the list of known hosts. admin@192.168.4.1's password: Linux Firewall-Restricted 5.14.9 #1 Mon Oct 4 06:03:24 PDT 2021 x86_64 Welcome to Netkit  Could not chdir to home directory /home/admin: No such file or directory \$ █ </pre> <p>Int-DNS</p> <pre> root@Network-Admin:~# ssh admin@192.168.3.3 The authenticity of host '192.168.3.3 (192.168.3.3)' can't be established. ECDSA key fingerprint is SHA256:hldZ+pQj6DGwToSAriPVVsPpufUSQoEI8cBffBBHyN0. Are you sure you want to continue connecting (yes/no/[fingerprint])? yes Warning: Permanently added '192.168.3.3' (ECDSA) to the list of known hosts. admin@192.168.3.3's password: Linux Int-DNS 5.14.9 #1 Mon Oct 4 06:03:24 PDT 2021 x86_64 Welcome to Netkit  Could not chdir to home directory /home/admin: No such file or directory \$ █ </pre>
--	--	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

		<p>Int-WWW</p> <pre> root@Network-Admin:~# ssh admin@192.168.1.4 The authenticity of host '192.168.1.4 (192.168.1.4)' can't be established. ECDSA key fingerprint is SHA256:hldZ+pQj6DGwToSAriPVVsPpufUSQoEI8cBffBBHyN0. Are you sure you want to continue connecting (yes/no/[fingerprint])? yes Warning: Permanently added '192.168.1.4' (ECDSA) to the list of known hosts. admin@192.168.1.4's password: Linux Int-WWW 5.14.9 #1 Mon Oct 4 06:03:24 PDT 2021 x86_64 Welcome to Netkit  Could not chdir to home directory /home/admin: No such file or directory \$ █ </pre> <p>OpenVPN</p> <pre> root@Network-Admin:~# ssh admin@192.168.1.5 The authenticity of host '192.168.1.5 (192.168.1.5)' can't be established. ECDSA key fingerprint is SHA256:hldZ+pQj6DGwToSAriPVVsPpufUSQoEI8cBffBBHyN0. Are you sure you want to continue connecting (yes/no/[fingerprint])? yes Warning: Permanently added '192.168.1.5' (ECDSA) to the list of known hosts. admin@192.168.1.5's password: Linux OpenVPN 5.14.9 #1 Mon Oct 4 06:03:24 PDT 2021 x86_64 Welcome to Netkit  Could not chdir to home directory /home/admin: No such file or directory \$ █ </pre> <p>Squid</p> <pre> root@Network-Admin:~# ssh admin@192.168.1.2 The authenticity of host '192.168.1.2 (192.168.1.2)' can't be established. ECDSA key fingerprint is SHA256:hldZ+pQj6DGwToSAriPVVsPpufUSQoEI8cBffBBHyN0. Are you sure you want to continue connecting (yes/no/[fingerprint])? yes Warning: Permanently added '192.168.1.2' (ECDSA) to the list of known hosts. admin@192.168.1.2's password: Linux Squid 5.14.9 #1 Mon Oct 4 06:03:24 PDT 2021 x86_64 Welcome to Netkit  Could not chdir to home directory /home/admin: No such file or directory \$ █ </pre>
--	--	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

		<p>Mail</p> <pre> root@Network-Admin:~# ssh admin@192.168.1.3 The authenticity of host '192.168.1.3 (192.168.1.3)' can't be established. ECDSA key fingerprint is SHA256:hldZ+pQj6DGwToSAriPVVsPpufUSQoEI8cBffBBHyN0. Are you sure you want to continue connecting (yes/no/[fingerprint])? yes Warning: Permanently added '192.168.1.3' (ECDSA) to the list of known hosts. admin@192.168.1.3's password: Linux Mail 5.14.9 #1 Mon Oct 4 06:03:24 PDT 2021 x86_64 Welcome to Netkit  Could not chdir to home directory /home/admin: No such file or directory \$ █ </pre> <p>Staff-1</p> <pre> root@Network-Admin:~# ssh admin@192.168.2.2 The authenticity of host '192.168.2.2 (192.168.2.2)' can't be established. ECDSA key fingerprint is SHA256:hldZ+pQj6DGwToSAriPVVsPpufUSQoEI8cBffBBHyN0. Are you sure you want to continue connecting (yes/no/[fingerprint])? yes Warning: Permanently added '192.168.2.2' (ECDSA) to the list of known hosts. admin@192.168.2.2's password: Linux Staff-1 5.14.9 #1 Mon Oct 4 06:03:24 PDT 2021 x86_64 Welcome to Netkit  Could not chdir to home directory /home/admin: No such file or directory \$ █ </pre> <p>Staff-2</p> <pre> root@Network-Admin:~# ssh admin@192.168.2.3 The authenticity of host '192.168.2.3 (192.168.2.3)' can't be established. ECDSA key fingerprint is SHA256:hldZ+pQj6DGwToSAriPVVsPpufUSQoEI8cBffBBHyN0. Are you sure you want to continue connecting (yes/no/[fingerprint])? yes Warning: Permanently added '192.168.2.3' (ECDSA) to the list of known hosts. admin@192.168.2.3's password: Linux Staff-2 5.14.9 #1 Mon Oct 4 06:03:24 PDT 2021 x86_64 Welcome to Netkit  Could not chdir to home directory /home/admin: No such file or directory \$ █ </pre>
--	--	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

		<p>Staff-3</p> <pre> root@Network-Admin:~# ssh admin@192.168.2.4 The authenticity of host '192.168.2.4 (192.168.2.4)' can't be established. ECDSA key fingerprint is SHA256:hldZ+pQj6DGwToSAriPVVsPpufUSQoEI8cBffBBHyN0. Are you sure you want to continue connecting (yes/no/[fingerprint])? yes Warning: Permanently added '192.168.2.4' (ECDSA) to the list of known hosts. admin@192.168.2.4's password: Linux Staff-3 5.14.9 #1 Mon Oct 4 06:03:24 PDT 2021 x86_64 Welcome to Netkit  Could not chdir to home directory /home/admin: No such file or directory \$ █ </pre> <p>Staff-Remote</p> <pre> root@Network-Admin:~# ssh admin@192.168.2.5 The authenticity of host '192.168.2.5 (192.168.2.5)' can't be established. ECDSA key fingerprint is SHA256:hldZ+pQj6DGwToSAriPVVsPpufUSQoEI8cBffBBHyN0. Are you sure you want to continue connecting (yes/no/[fingerprint])? yes Warning: Permanently added '192.168.2.5' (ECDSA) to the list of known hosts. admin@192.168.2.5's password: Linux Staff-Remote 5.14.9 #1 Mon Oct 4 06:03:24 PDT 2021 x86_64 Welcome to Netkit  Could not chdir to home directory /home/admin: No such file or directory \$ █ </pre> <p>LDAP</p> <pre> root@Network-Admin:~# ssh admin@192.168.3.2 The authenticity of host '192.168.3.2 (192.168.3.2)' can't be established. ECDSA key fingerprint is SHA256:hldZ+pQj6DGwToSAriPVVsPpufUSQoEI8cBffBBHyN0. Are you sure you want to continue connecting (yes/no/[fingerprint])? yes Warning: Permanently added '192.168.3.2' (ECDSA) to the list of known hosts. admin@192.168.3.2's password: Linux LDAP 5.14.9 #1 Mon Oct 4 06:03:24 PDT 2021 x86_64 Welcome to Netkit  Could not chdir to home directory /home/admin: No such file or directory \$ █ </pre>
--	--	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

(Reese, 2017)	Configured dnsmasq for the internal DNS and set the static hosts	<pre> interface=eth0 domain-needed bogus-priv no-resolv no-poll server=8.8.8.8 local=/fido.cyber.test/ no-hosts addn-hosts=/etc/dnsmasq_static_hosts.conf expand-hosts domain=fido.cyber.test </pre> <p>Static hosts:</p> <pre> 127.0.0.1    localhost  192.168.1.2  squid.fido.cyber.test 192.168.3.3  dns.fido.cyber.test 192.168.1.3  mail.fido.cyber.test 192.168.1.4  www.fido.cyber.test 192.168.1.5  vpn.fido.cyber.test 192.168.2.2  staff1.fido.cyber.test 192.168.2.3  staff2.fido.cyber.test 192.168.2.4  staff3.fido.cyber.test 192.168.3.2  ldap.fido.cyber.test </pre>
(Mockapetris, 1987; Reynolds and Postel, 1987)	Allowed the internal DNS TCP and UDP packets to flow through the network to the staff machines in the enterprise zone through port 53	<p>Internal DMZ firewall rules, where the internal DNS is located:</p> <pre> iptables -A FORWARD -p tcp --dport 53 -i eth2 -o eth3 -s 192.168.2.0/24 -d 192.168.3.3 -j ACCEPT iptables -A FORWARD -p udp --dport 53 -i eth2 -o eth3 -s 192.168.2.0/24 -d 192.168.3.3 -j ACCEPT iptables -A FORWARD -p tcp --sport 53 -i eth3 -o eth2 -s 192.168.3.3 -d 192.168.2.0/24 -j ACCEPT iptables -A FORWARD -p udp --sport 53 -i eth3 -o eth2 -s 192.168.3.3 -d 192.168.2.0/24 -j ACCEPT </pre> <p>Enterprise firewall rules, where the staff machines are located:</p> <pre> iptables -A FORWARD -p tcp --dport 53 -i eth3 -o eth2 -s 192.168.2.0/24 -d 192.168.3.3 -j ACCEPT iptables -A FORWARD -p udp --dport 53 -i eth3 -o eth2 -s 192.168.2.0/24 -d 192.168.3.3 -j ACCEPT iptables -A FORWARD -p tcp --sport 53 -i eth2 -o eth3 -s 192.168.3.3 -d 192.168.2.0/24 -j ACCEPT iptables -A FORWARD -p udp --sport 53 -i eth2 -o eth3 -s 192.168.3.3 -d 192.168.2.0/24 -j ACCEPT </pre> <p>Pinging a host:</p>

		<pre>root@Staff-1:~# ping -c 1 www.fido.cyber.test PING www.fido.cyber.test (192.168.1.4) 56(84) bytes of data. 64 bytes from www.fido.cyber.test (192.168.1.4): icmp_seq=1 ttl=62 time=0.542 ms  --- www.fido.cyber.test ping statistics --- 1 packets transmitted, 1 received, 0% packet loss, time 0ms rtt min/avg/max/mdev = 0.542/0.542/0.542/0.000 ms</pre> <p>The internal DMZ firewall iptables output shows that the forward table rule works:</p> <table><thead><tr><th>pkts</th><th>bytes</th><th>target</th><th>prot</th><th>opt</th><th>in</th><th>out</th><th>source</th><th>destination</th><th></th></tr></thead><tbody><tr><td>0</td><td>0</td><td>ACCEPT</td><td>tcp</td><td>--</td><td>eth2</td><td>eth3</td><td>192.168.2.0/24</td><td>192.168.3.3</td><td>tcp dpt:53</td></tr><tr><td>9</td><td>600</td><td>ACCEPT</td><td>udp</td><td>--</td><td>eth2</td><td>eth3</td><td>192.168.2.0/24</td><td>192.168.3.3</td><td>udp dpt:53</td></tr><tr><td>0</td><td>0</td><td>ACCEPT</td><td>tcp</td><td>--</td><td>eth3</td><td>eth2</td><td>192.168.3.3</td><td>192.168.2.0/24</td><td>tcp spt:53</td></tr><tr><td>9</td><td>747</td><td>ACCEPT</td><td>udp</td><td>--</td><td>eth3</td><td>eth2</td><td>192.168.3.3</td><td>192.168.2.0/24</td><td>udp spt:53</td></tr></tbody></table> <p>The enterprise firewall iptables output shows that the forward table rule works:</p> <table><thead><tr><th>pkts</th><th>bytes</th><th>target</th><th>prot</th><th>opt</th><th>in</th><th>out</th><th>source</th><th>destination</th><th></th></tr></thead><tbody><tr><td>0</td><td>0</td><td>ACCEPT</td><td>tcp</td><td>--</td><td>eth3</td><td>eth2</td><td>192.168.2.0/24</td><td>192.168.3.3</td><td>tcp dpt:53</td></tr><tr><td>9</td><td>600</td><td>ACCEPT</td><td>udp</td><td>--</td><td>eth3</td><td>eth2</td><td>192.168.2.0/24</td><td>192.168.3.3</td><td>udp dpt:53</td></tr><tr><td>0</td><td>0</td><td>ACCEPT</td><td>tcp</td><td>--</td><td>eth2</td><td>eth3</td><td>192.168.3.3</td><td>192.168.2.0/24</td><td>tcp spt:53</td></tr><tr><td>9</td><td>747</td><td>ACCEPT</td><td>udp</td><td>--</td><td>eth2</td><td>eth3</td><td>192.168.3.3</td><td>192.168.2.0/24</td><td>udp spt:53</td></tr></tbody></table>	pkts	bytes	target	prot	opt	in	out	source	destination		0	0	ACCEPT	tcp	--	eth2	eth3	192.168.2.0/24	192.168.3.3	tcp dpt:53	9	600	ACCEPT	udp	--	eth2	eth3	192.168.2.0/24	192.168.3.3	udp dpt:53	0	0	ACCEPT	tcp	--	eth3	eth2	192.168.3.3	192.168.2.0/24	tcp spt:53	9	747	ACCEPT	udp	--	eth3	eth2	192.168.3.3	192.168.2.0/24	udp spt:53	pkts	bytes	target	prot	opt	in	out	source	destination		0	0	ACCEPT	tcp	--	eth3	eth2	192.168.2.0/24	192.168.3.3	tcp dpt:53	9	600	ACCEPT	udp	--	eth3	eth2	192.168.2.0/24	192.168.3.3	udp dpt:53	0	0	ACCEPT	tcp	--	eth2	eth3	192.168.3.3	192.168.2.0/24	tcp spt:53	9	747	ACCEPT	udp	--	eth2	eth3	192.168.3.3	192.168.2.0/24	udp spt:53
pkts	bytes	target	prot	opt	in	out	source	destination																																																																																														
0	0	ACCEPT	tcp	--	eth2	eth3	192.168.2.0/24	192.168.3.3	tcp dpt:53																																																																																													
9	600	ACCEPT	udp	--	eth2	eth3	192.168.2.0/24	192.168.3.3	udp dpt:53																																																																																													
0	0	ACCEPT	tcp	--	eth3	eth2	192.168.3.3	192.168.2.0/24	tcp spt:53																																																																																													
9	747	ACCEPT	udp	--	eth3	eth2	192.168.3.3	192.168.2.0/24	udp spt:53																																																																																													
pkts	bytes	target	prot	opt	in	out	source	destination																																																																																														
0	0	ACCEPT	tcp	--	eth3	eth2	192.168.2.0/24	192.168.3.3	tcp dpt:53																																																																																													
9	600	ACCEPT	udp	--	eth3	eth2	192.168.2.0/24	192.168.3.3	udp dpt:53																																																																																													
0	0	ACCEPT	tcp	--	eth2	eth3	192.168.3.3	192.168.2.0/24	tcp spt:53																																																																																													
9	747	ACCEPT	udp	--	eth2	eth3	192.168.3.3	192.168.2.0/24	udp spt:53																																																																																													
(Mockapetris, 1987; Reynolds and Postel, 1987)	Allowed the internal DNS to communicate with the external DNS in the firewalls if the static hosts are not found on the internal DNS dnsmasq file	<p>Internal DMZ firewall rules to allow communication between the DNSs:</p> <pre>iptables -A FORWARD -p tcp --dport 53 -s 192.168.3.3 -d 8.8.8.8 -j ACCEPT iptables -A FORWARD -p udp --dport 53 -s 192.168.3.3 -d 8.8.8.8 -j ACCEPT iptables -A FORWARD -p tcp --sport 53 -d 192.168.3.3 -s 8.8.8.8 -j ACCEPT iptables -A FORWARD -p udp --sport 53 -d 192.168.3.3 -s 8.8.8.8 -j ACCEPT</pre> <p>And on the enterprise firewall:</p> <pre>iptables -A FORWARD -p tcp --dport 53 -s 192.168.3.3 -d 8.8.8.8 -j ACCEPT iptables -A FORWARD -p udp --dport 53 -s 192.168.3.3 -d 8.8.8.8 -j ACCEPT iptables -A FORWARD -p tcp --sport 53 -d 192.168.3.3 -s 8.8.8.8 -j ACCEPT iptables -A FORWARD -p udp --sport 53 -d 192.168.3.3 -s 8.8.8.8 -j ACCEPT</pre> <p>Pinging a host on the internet:</p>																																																																																																				

		<pre> root@Staff-1:~# ping -c 1 webserver.googly.com PING webserver.googly.com (201.224.19.7) 56(84) bytes of data. 64 bytes from webserver.googly.com (201.224.19.7): icmp_seq=1 ttl=61 time=0.747 ms  --- webserver.googly.com ping statistics --- 1 packets transmitted, 1 received, 0% packet loss, time 0ms rtt min/avg/max/mdev = 0.747/0.747/0.747/0.000 ms </pre> <p>The internal DMZ firewall iptables output shows that the forward table rule works:</p> <pre> 0      0 ACCEPT    tcp  --  *    *    8.8.8.8          192.168.3.3      tcp spt:53 5     383 ACCEPT    udp  --  *    *    8.8.8.8          192.168.3.3      udp spt:53 </pre> <p>Also for the enterprise firewall:</p> <pre> 0      0 ACCEPT    tcp  --  *    *    8.8.8.8          192.168.3.3      tcp spt:53 5     383 ACCEPT    udp  --  *    *    8.8.8.8          192.168.3.3      udp spt:53 </pre> <p>To get out of the external DMZ to the Internet, the packets are sent with masquerade:</p> <pre> pkts bytes target    prot opt in     out     source        destination  10   704 MASQUERADE all  --  *      eth0    0.0.0.0/0     0.0.0.0/0 </pre>
--	--	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

## Further Work

- Implement logging machines for every connection to store event logs to record security incidents, policy violations and to track network performance
- Implement alternative routes in the case that a crucial gateway fails, to ensure that there is no single point of failure
- Switch to ssh using keys and not only passwords
- Implement OpenVPN for the external office
- Implement Squid
- Implement the web server proxy



## References

Mockapetris, P. (1987). *RFC 1035 - DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION*. [online] ietf.org. Available at: <https://datatracker.ietf.org/doc/html/rfc1035>.

Obregon, L. (2015). *Infrastructure Security Architecture for Effective Security Monitoring*. [online] Egnyte. Available at: <https://sansorg.egnyte.com/dl/YfjJGOOfnH>.

Reese, K. (2017). *Implementing DNS via dnsmasq*. [online] YouTube. Available at: <https://www.youtube.com/watch?v=P2kiinwg00c>.

Reynolds, J. and Postel, J. (1987). *RFC 1010 - Assigned numbers*. [online] ietf.org. Available at: <https://datatracker.ietf.org/doc/html/rfc1010>.

Damien (2010), *How to automatically add user account AND password with a Bash script?*. [online] Stack Overflow. Available at: <https://stackoverflow.com/questions/2150882/how-to-automatically-add-user-account-and-password-with-a-bash-script>

Christian Crawley (2020), *How to Set Up SSH on Linux and Test Your Setup: A Beginner's Guide*, [online] MUD, Available at: <https://www.makeuseof.com/tag/beginners-guide-setting-ssh-linux-testing-setup/>