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

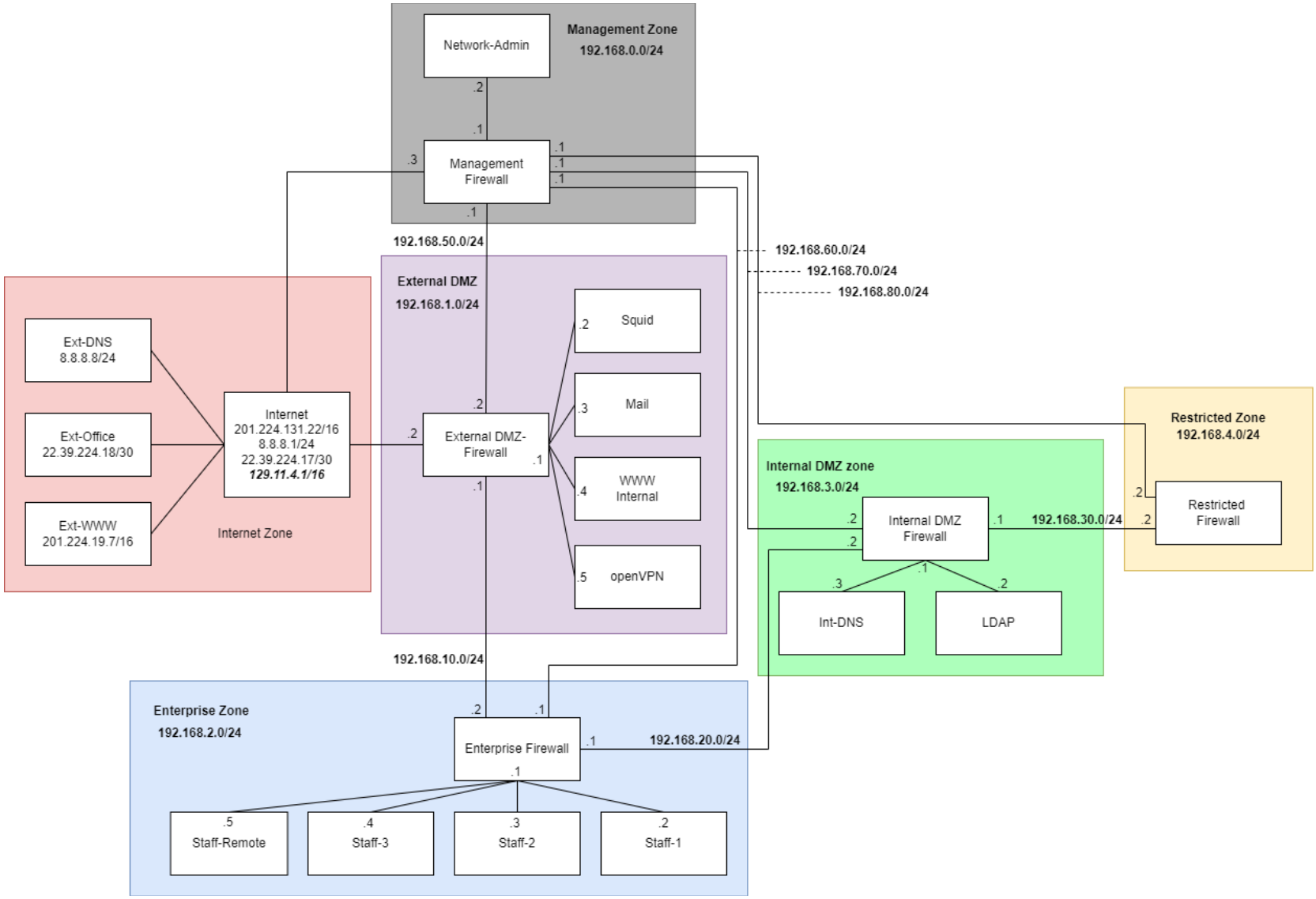


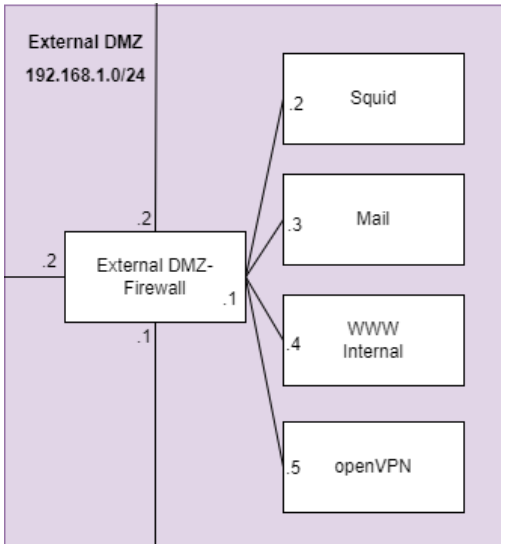
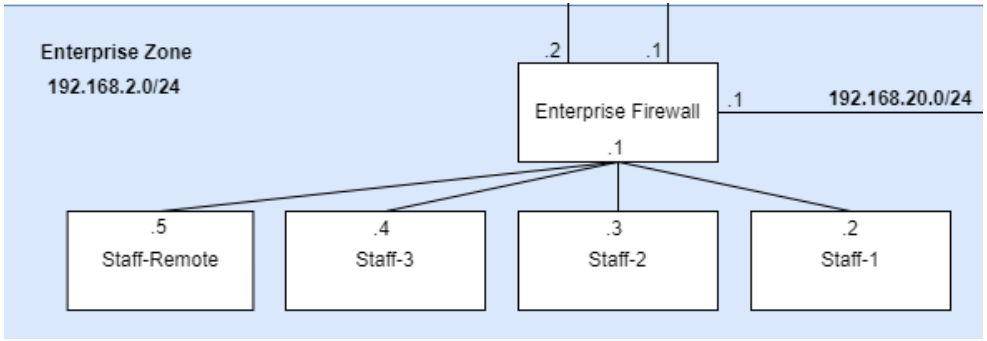
Figure 1 - Network Diagram

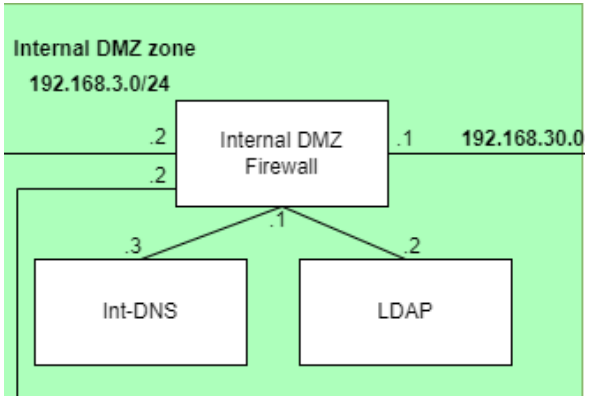
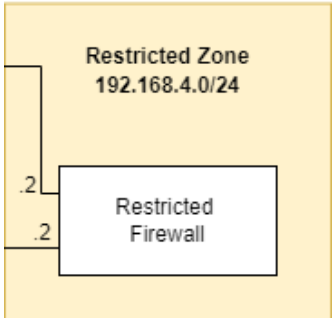
Key Points

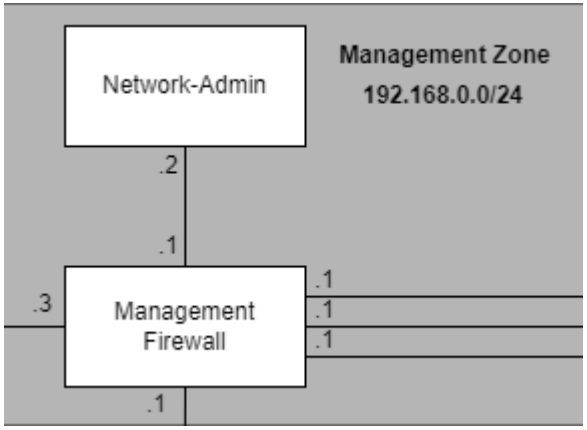
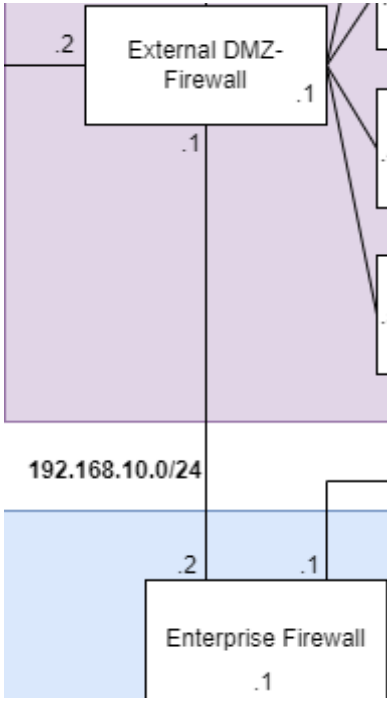
- Implemented a network topology according to the SANS Institute Infrastructure Security Architecture research paper (Obregon, 2015).
- Blocked all unnecessary traffic using firewall rules
- Ensured that DMZ machines cannot initiate connections
- Implemented Destination NAT for services exposed to the 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

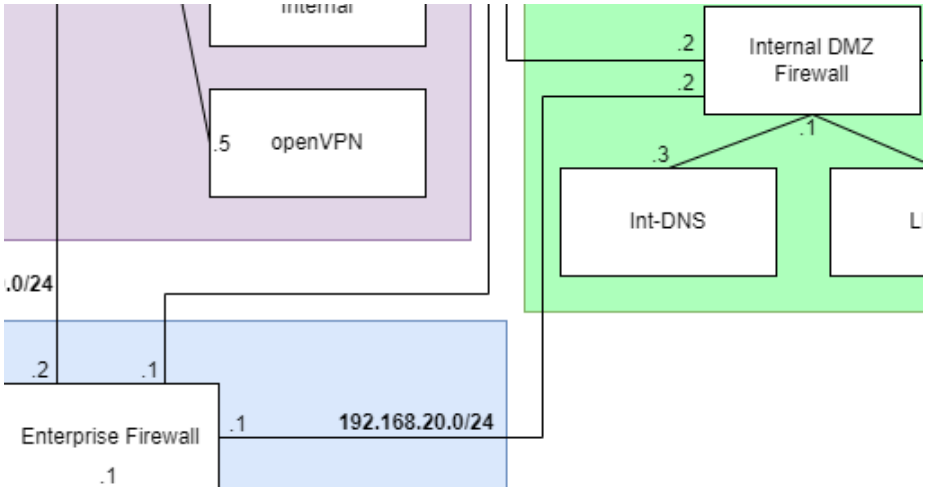
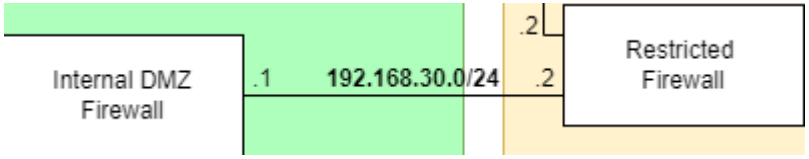
Phase 1

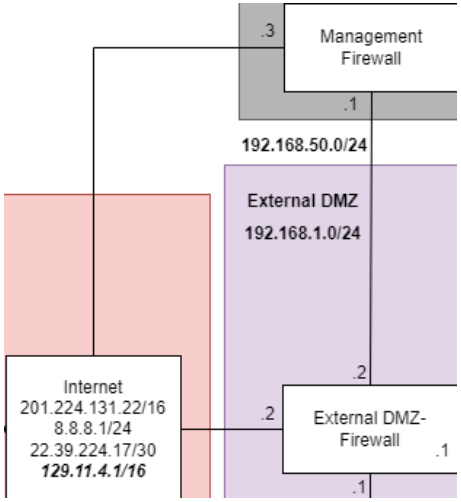
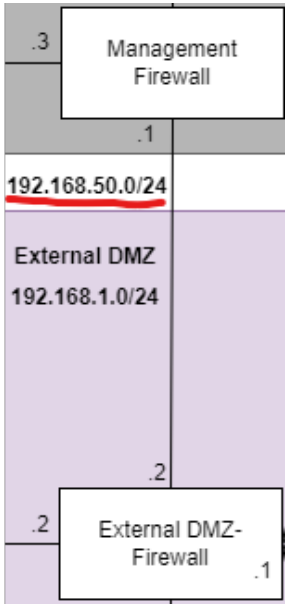
Reference	***Claim***	***Evidence***
Obregon, L. (2015)	We have a full network topology in place that makes use of zones and various different private subnets.	**Figure 1**

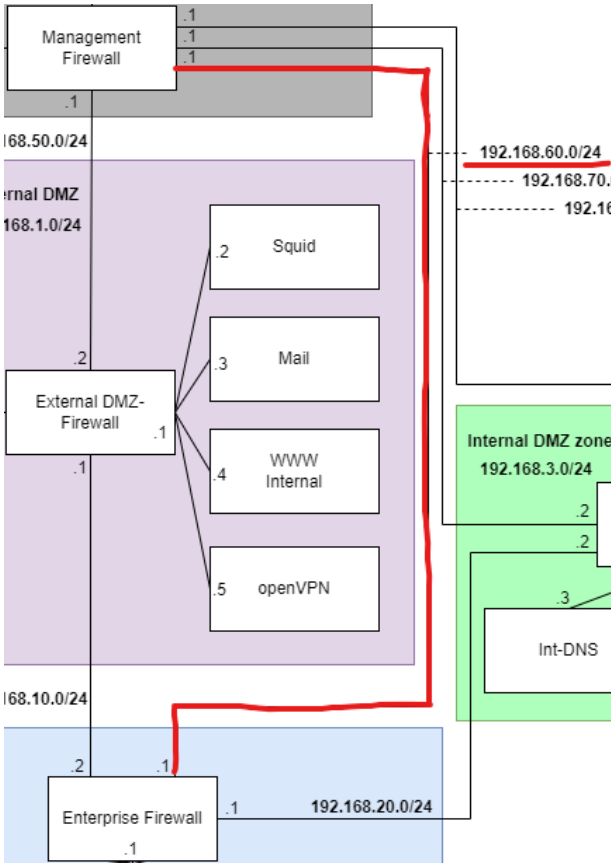
Obregon, L. (2015)	We have implemented an External DMZ zone of trust. We moved all of the services that would need to be exposed to the internet here, like the web server.	
Obregon, L. (2015)	We have implemented an Enterprise zone of trust where we have moved all of the staff machines in.	

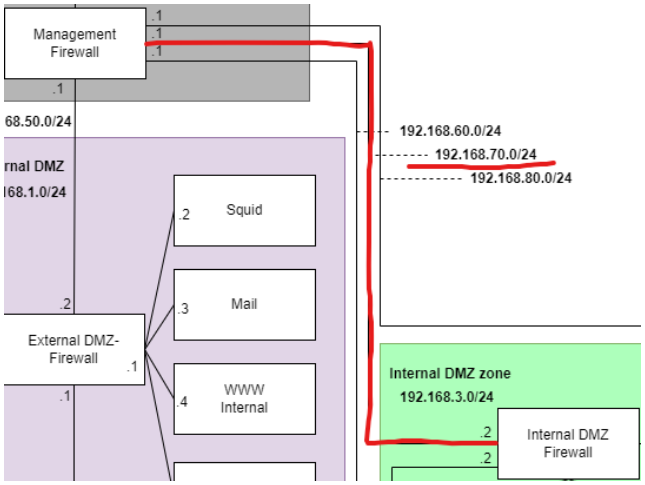
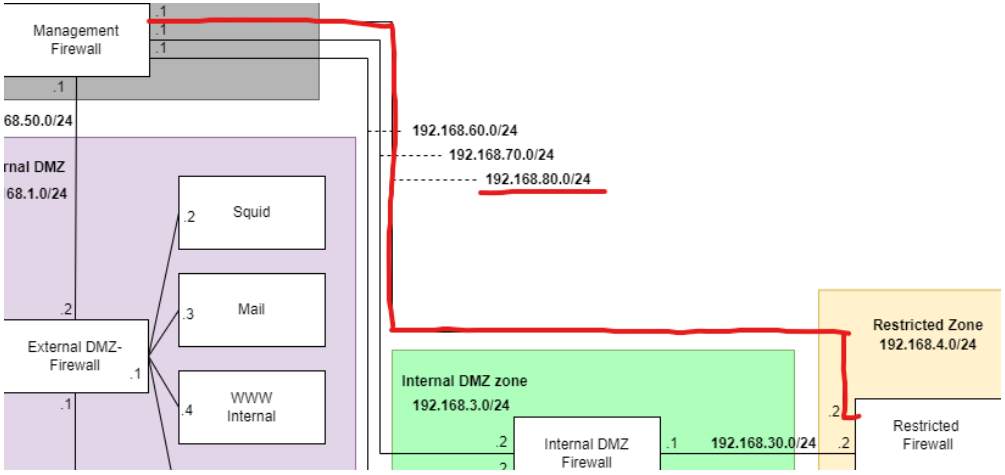
Obregon, L. (2015)	We have implemented an Internal DMZ zone of trust where we have moved all of the internal application services.	
Obregon, L. (2015)	We have implemented a Restricted zone of trust where we have implemented a firewall with a network card so that adding new machines would be easy.	

Obregon, L. (2015)	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	
N/A	We have implemented an "access subnet" to connect the External DMZ firewall to the Enterprise firewall on the 192.168.10.0/24 subnet	

N/A	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.	
N/A	We have implemented an “access subnet” to connect the Internal DMZ firewall to the Restricted Firewall on the 192.168.30.0/24 subnet	

N/A	We have implemented an “access subnet” to connect the Management firewall to the Internet, but it’s not in use.	
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.	

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	We have implemented an “access subnet” to connect the Management firewall to the Internal DMZ Firewall on the 192.168.70.0/24 subnet.	
N/A	We have implemented an “access subnet” to connect the Management firewall to the Restricted Firewall on the 192.168.80.0/24 subnet.	

Phase 2

Reference	***Claim***	***Evidence***

N/A	Users connecting to the internet are SNATed through the External DMZ Firewall	Line in .startup:
		iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
		
		Explanation
		1: Shows staff machine connect to external address via netcat
		`root@Staff-1:~# nc 201.224.19.7 1234`
		2: Shows external machine listen, and then accept a connection, from an external facing company address
		`root@Ext-WWW:~# nc -nlvp 1234`
		`Listening on 0.0.0.0 1234`
		`Connection received on 129.11.4.2 40050`
		The connection was received from the company's external address, not a private internal one, showing successful use of SNAT.

N/A	DNAT through External DMZ Firewall allows the internet to access port 80 on the internal web server	Line in .startup: *iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j DNAT --to-destination 192.168.1.4:80* Explanation The image below shows an external machine checking the headers of the companies external address using port 80, and receiving an OK response

| | | ```
root@Internet:~# curl -I 129.11.4.2
HTTP/1.1 200 OK
```<br>Line in .startup:<br>*iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 443 -j DNAT --to-destination 192.168.1.4:443*<br><br>Explanation<br>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.<br>```<br>root@Internet:~# curl -I 129.11.4.2:443<br>HTTP/1.1 400 Bad Request<br>```<br>Line in .startup:<br>*iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 25 -j DNAT --to-destination 192.168.1.3:25*<br><br>Explanation<br>1: Shows Mail machine set up listener on port 25, and receive a connection from an external machine<br>```<br>root@Mail:~# nc -nvlp 25<br>Listening on 0.0.0.0 25<br>Connection received on 129.11.4.1 41674<br>```<br>2: Shows external machine connect to listener through the companies external address<br>```<br>root@Internet:~# nc 129.11.4.2 25<br>```<br>N/A<br>DNAT through External DMZ Firewall allows the internet to access port 25 on the mail box |
```

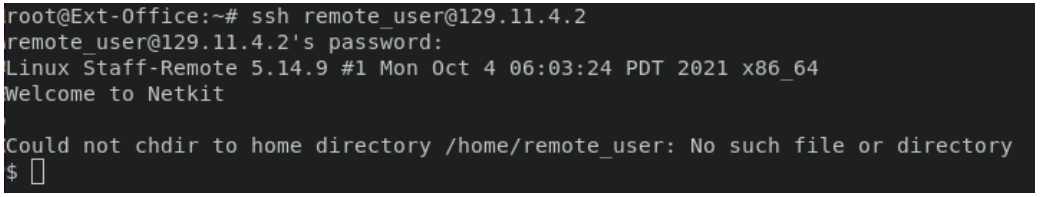
N/A	DNAT through External DMZ Firewall allows the internet to access port 587 on the mail box	Line in .startup:
		iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 587 -j DNAT --to-destination 192.168.1.3:587
		
		Explanation
		1: Shows Mail machine set up listener on port 587, and receive a connection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

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

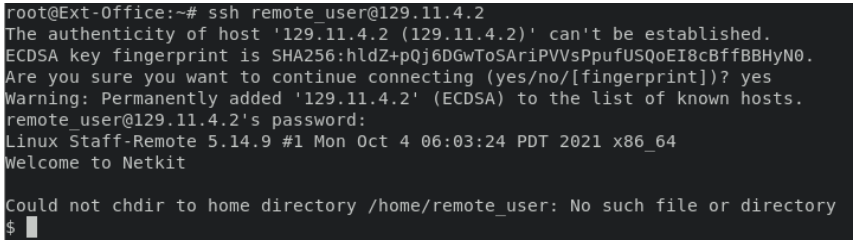
		2: Shows external machine connect to listener through the companies external address `root@Internet:~# nc 129.11.4.2 993`

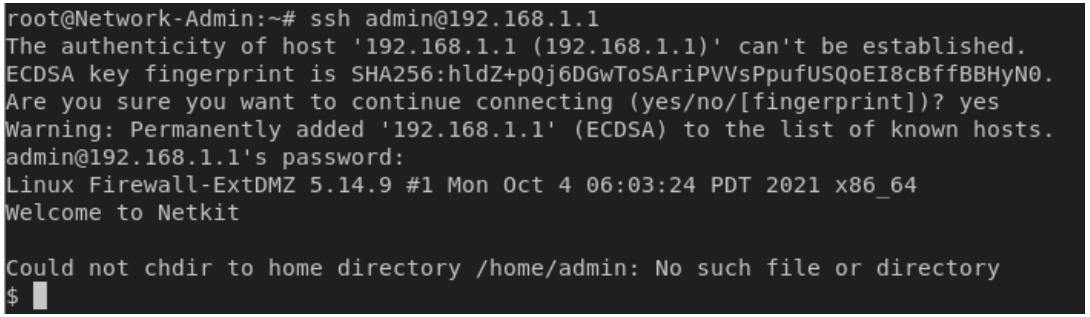
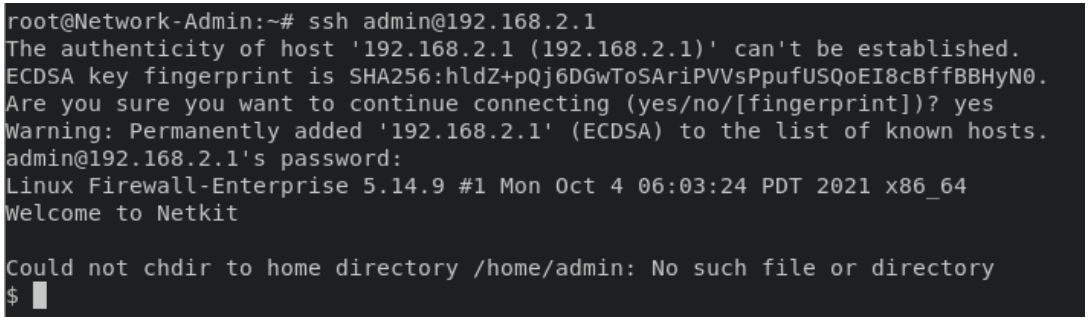
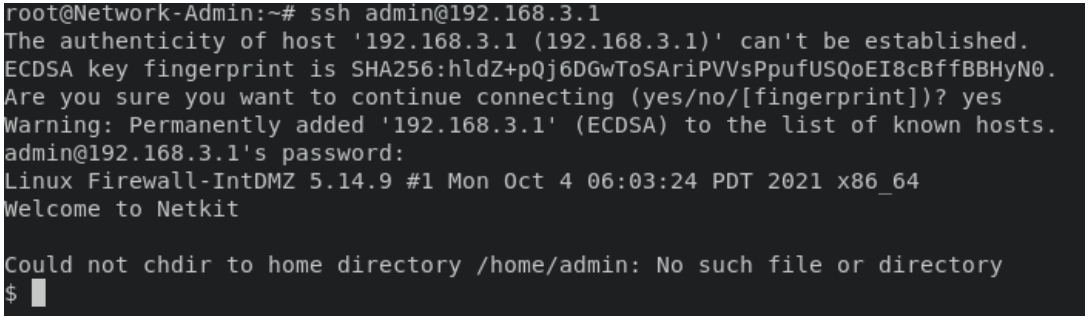
N/A	DNAT through External DMZ Firewall allows the internet to access port 1194 on the openVPN box	Line in .startup:
		iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 1194 -j DNAT --to-destination 192.168.1.5:1194
		
		Explanation
		1: Shows OpenVPN machine set up listener on port 1194, and receive a connection from an external machine
		`root@OpenVPN:~# nc -nlvp 1194`
		`Listening on 0.0.0.0 1194`
		`Connection received on 129.11.4.1 44086`
		2: Shows external machine connect to listener through the companies external address
		`root@Internet:~# nc 129.11.4.2 1194`

N/A	DNAT through External DMZ Firewall allows the remote office to access the SSH service (port 22) in the enterprise zone	Line in .startup: *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* Explanation 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:

Phase 3

Reference	***Claim***	***Evidence***
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.	Image below shows Ext-Office machine connecting via the external address of the company 
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

	machine.	 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 $ Firewall-Enterprise  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 $ Firewall-IntDMZ  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 $ Firewall-MGMT

```
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
$
```

Firewall-Restricted

```
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
$
```

Int-DNS

```
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
$
```

Int-WWW

```
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
$
```

OpenVPN

```
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
$
```

Squid

```
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
$
```

Mail

```
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
$
```

Staff-1

```
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
$
```

Staff-2

```
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
$
```

Staff-3

```
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
$
```

Staff-Remote

```
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
$
```

LDAP

```
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
$
```

(Reese, 2017)	Configured dnsmasq for the internal DNS and set the static hosts	`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`
		
		Static hosts:
		
		`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`

(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	Internal DMZ firewall rules, where the internal DNS is located:
		
		`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`
		
		Enterprise firewall rules, where the staff machines are located:
		
		`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`
		
		Pinging a host:

<table>
<tr>
<td></td>
<td></td>
<td>
<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>

The internal DMZ firewall iptables output shows that the forward table rule works:

<pre>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</pre>

The enterprise firewall iptables output shows that the forward table rule works:

<pre>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</pre>
</td>
</tr>
<tr>
<td>(Mockapetris, 1987; Reynolds and Postel, 1987)</td>
<td>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</td>
<td>
Internal DMZ firewall rules to allow communication between the DNSs:

<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>

And on the enterprise firewall:

<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>

Pinging a host on the internet:
</td>
</tr>
</table>

```
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
```

The internal DMZ firewall iptables output shows that the forward table rule works:

```
 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
```

Also for the enterprise firewall:

```
 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
```

To get out of the external DMZ to the Internet, the packets are sent with masquerade:

```
pkts bytes target     prot opt in     out     source               destinatior
  10   704 MASQUERADE  all  --  *      eth0    0.0.0.0/0            0.0.0.0/0
```

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/