National College of Ireland

Configuration Manual

MSc Research Project
MSc in Cybersecurity

Lorenzo Lombardi
Student ID: x22198024

School of Computing
National College of Ireland

Supervisor: Dr. Ross Spelman

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: Lorenzo Lombardi

Student ID: X22198024

Programme: MSc in Cybersecurity **Year:** 2023-2024

Module: Msc Research Project

Lecturer: Dr.Ross Spelman

Submission Due Date: 2024/08/12

Project Title: Design advantages of the ZTNA model: Architectural Evolution for More Secure and Efficient Remote Access

Word Count: **Page Count:**

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature:

Date:

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Configuration Manual

Lorenzo Lombardi
Student ID: x22198024

Rome Firewall – Fortinet FGT60E 7.0.14

----------**FW POLICY**----------

```
config firewall policy
    edit 75
        set name "REVERSE PROXY ROME"
        set srcintf "wan1"
        set dstintf "DMZ"
        set action accept
        set srcaddr "remoteuser-tester99"
        set dstaddr "DS215_EXT"
        set schedule "always"
        set service "ALL"
        set logtraffic all
    next

    edit 79
        set name "TESTER RA"
        set srcintf "ssl.root"
        set dstintf "any"
        set action accept
        set srcaddr "SSLVPN_TUNNEL_ADDR1"
        set dstaddr "SSL_SPLIT_RM"
        set schedule "always"
        set service "ALL"
        set ssl-ssh-profile "certificate-inspection"
        set logtraffic all
        set users "vpn_tester99"
    next

    edit 78
        set name "REVERSE PROXY ADMIN"
        set srcintf "wan1"
        set dstintf "wan2"
        set action accept
        set srcaddr "remoteuser-tester99"
        set dstaddr "ESXI_EXT"
        set schedule "always"
        set service "ALL"
        set logtraffic all
    next
```

```
    edit 55
        set name "IPSEC From DUBLIN to ROME"
        set srcintf "L2L_DUBLIN"
        set dstintf "DMZ" "esxi_128" "esxi_130" "internal" "wan2"
        set action accept
        set srcaddr "LAN_DUBLIN" "SSLVPN_DUBLIN-10.212.135.200-210"
        set dstaddr "LAN_RM"
        set schedule "always"
        set service "ALL"
        set logtraffic all
    next

    edit 57
        set name "IPSEC From ROME to DUBLIN"
        set srcintf "DMZ" "esxi_128" "esxi_130" "internal" "wan2"
        set dstintf "L2L_DUBLIN"
        set action accept
        set srcaddr "LAN_RM"
        set dstaddr "LAN_DUBLIN"
        set schedule "always"
        set service "ALL"
        set logtraffic all
    next
```

----------**ALLOWED SRC FQDN**----------

```
config firewall address
    edit "remoteuser-tester99"
        set type fqdn
        set fqdn "remoteuser-tester99.float-zone.com"
    next
end
```

----------**REVERSE PROXY ROME (NAS and ESXI)**---

```
config firewall vip
    edit "DS215_EXT"
        set extip 192.168.1.99
        set mappedip "192.168.25.101"
        set extintf "any"
        set portforward enable
        set extport 1155
        set mappedport 5001
    next


config firewall vip
    edit "ESXI_EXT"
        set extip 192.168.1.99
        set mappedip "192.168.12.101"
        set extintf "any"
        set portforward enable
        set extport 5511
        set mappedport 443
    next
end
```

----------**SSL VPN RA**----------

```
config vpn ssl web portal
   edit "tunnel-access"
      set tunnel-mode enable
      set ipv6-tunnel-mode enable
      set ip-pools "SSLVPN_TUNNEL_ADDR1"
      set split-tunneling-routing-address "172.31.128.0/24" "DS213J" "DS215J"
      set ipv6-pools "SSLVPN_TUNNEL_IPv6_ADDR1"
   next
end

config vpn ssl settings
   set ciphersuite TLS-AES-256-GCM-SHA384
   set servercert "romeoffice.dscloud.me"
   set idle-timeout 28800
   set tunnel-ip-pools "SSLVPN_TUNNEL_ADDR1"
   set tunnel-ipv6-pools "SSLVPN_TUNNEL_IPv6_ADDR1"
   set dns-server1 8.8.8.8
   set dns-server2 1.1.1.1
   set port 443
   set source-interface "wan1"
   set source-address "all"
   set source-address6 "all"
   set default-portal "web-access"
   config authentication-rule
      edit 2
         set users "vpn_tester99"
         set portal "tunnel-access"
      next
   end
end
```

----------**IPSEC ROME DUBLIN**----------

```
config vpn ipsec phase1-interface
   edit "L2L_DUBLIN"
      set type ddns
      set interface "wan1"
      set ike-version 2
      set keylife 28800
      set peertype any
      set net-device disable
      set proposal aes256-sha256
      set dhgrp 27 21 19
      set remotegw-ddns "dublinoffice.dscloud.me"
      set psksecret ENC XXXXXXXXXXXXXX
   next
end

config vpn ipsec phase2-interface
   edit "L2L_DUBLIN"
      set phase1name "L2L_DUBLIN"
      set proposal aes256-sha256
      set dhgrp 21 19 14
      set keepalive enable
      set keylifeseconds 7200
   next
end
```

----------**NETWORKS ROUTES**----------

```
config router static
   edit 1
      set gateway 192.168.1.1
      set device "wan1"
   next
   edit 4
      set dst 192.168.32.0 255.255.255.0
      set device "L2L_DUBLIN"
   next
   edit 3
      set dst 192.168.23.0 255.255.255.0
      set device "L2L_DUBLIN"
   next
   edit 8
      set dst 10.212.135.0 255.255.255.0
      set device "L2L_DUBLIN"
   next
end
```

----------**NETWORKS INTERFACES**----------

```
config system interface
   edit "wan1"
      set vdom "root"
      set ip 192.168.1.99 255.255.255.0
      set allowaccess ping
      set type physical
      set alias "UNTRUST_internet"
      set lldp-reception disable
      set lldp-transmission disable
      set estimated-upstream-bandwidth 20000
      set estimated-downstream-bandwidth 200000
      set monitor-bandwidth enable
      set role wan
      set snmp-index 1
   next
   edit "wan2"
      set vdom "root"
      set ip 192.168.12.99 255.255.255.0
      set type physical
      set alias "ESXI"
      set lldp-reception disable
      set lldp-transmission disable
      set snmp-index 2
      set secondary-IP enable
   next
   edit "ssl.root"
      set vdom "root"
      set type tunnel
      set alias "SSL VPN interface"
      set snmp-index 7
   next
```

```
    edit "internal"
        set vdom "root"
        set ip 192.168.21.99 255.255.255.0
        set allowaccess ping https ssh http
        set type hard-switch
        set device-identification enable
        set lldp-reception disable
        set lldp-transmission disable
        set role lan
        set snmp-index 5
    next
    edit "esxi_128"
        set vdom "root"
        set ip 172.31.128.99 255.255.255.0
        set allowaccess ping snmp
        set device-identification enable
        set role lan
        set snmp-index 9
        set interface "wan2"
        set vlanid 128
    next
    edit "DMZ"
        set vdom "root"
        set ip 192.168.25.99 255.255.255.0
        set allowaccess ping
        set type hard-switch
        set alias "DS215j"
        set lldp-reception disable
        set lldp-transmission disable
        set snmp-index 8
    next
    edit "L2L_DUBLIN"
        set vdom "root"
        set ip 0.0.0.0 255.255.255.255
        set allowaccess ping fabric
        set type tunnel
        set monitor-bandwidth enable
        set snmp-index 21
        set interface "wan1"
    next

end
```

Dulbin Firewall - Fortinet FGT60E 7.0.14

----------**FW POLICY**----------

```
config firewall policy
   edit 19
      set name "REVERSE PROXY DUBLIN"
      set srcintf "wan1"
      set dstintf "dmz"
      set action accept
      set srcaddr "remoteuser-tester99"
      set dstaddr "DS213_EXT"
      set schedule "always"
      set service "ALL"
      set logtraffic all
   next

   edit 3
      set name "IPSEC From ROME to DUBLIN"
      set srcintf "L2L_RM"
      set dstintf "dmz"
      set action accept
      set srcaddr "DS215j" "192.168.21.0-24" "SSL_RM_10.212.134.0-24"
      set dstaddr "DS213j"
      set schedule "always"
      set service "ALL"
      set logtraffic all
   next

   edit 4
      set name "IPSEC From DUBLIN to ROME"
      set srcintf "dmz"
      set dstintf "L2L_RM"
      set action accept
      set srcaddr "DS213j"
      set dstaddr "DS215j"
      set schedule "always"
      set service "ALL"
      set logtraffic all
   next
end
```

----------**ALLOWED SRC FQDN**----------

```
config firewall address
   edit "remoteuser-tester99"
      set type fqdn
      set fqdn "remoteuser-tester99.float-zone.com"
   next
end
```

```
----------------------------------------------REVERSE PROXY NAS DUBLIN----------
config firewall vip
   edit "DS213_EXT"
      set extip 192.168.1.99
      set mappedip "192.168.23.101"
      set extintf "any"
      set portforward enable
      set extport 1155
      set mappedport 5001
   next
end
----------------------------------------------RM SSL VPN RA----------------------------

config vpn ssl web portal
   edit "tunnel-access"
      set tunnel-mode enable
      set ipv6-tunnel-mode enable
      set ip-pools "SSLVPN_TUNNEL_ADDR1"
      set split-tunneling-routing-address "172.31.128.0/24" "DS213J" "DS215J"
      set ipv6-pools "SSLVPN_TUNNEL_IPv6_ADDR1"
   next
end

config vpn ssl settings
   set ciphersuite TLS-AES-256-GCM-SHA384
   set servercert "dublinoffice.dscloud.me"
   set idle-timeout 28800
   set tunnel-ip-pools "SSLVPN_TUNNEL_ADDR1"
   set tunnel-ipv6-pools "SSLVPN_TUNNEL_IPv6_ADDR1"
   set dns-server1 8.8.8.8
   set dns-server2 1.1.1.1
   set port 443
   set source-interface "wan1"
   set source-address "all"
   set source-address6 "all"
   set default-portal "web-access"
   config authentication-rule
      edit 2
         set users "vpn_tester99"
         set portal "tunnel-access"
      next
   end
end

------------------------------------------------IPSEC DUBLIN ROME-------------------------------

config vpn ipsec phase1-interface
   edit "L2L_RM"
      set type ddns
      set interface "wan1"
      set ike-version 2
      set keylife 28800
      set peertype any
      set net-device disable
      set proposal aes256-sha256
      set dhgrp 27 21 19
      set remotegw-ddns "romeoffice.dscloud.me"
```

```
        set psksecret ENC XXXXXXX
    next
end


config vpn ipsec phase2-interface
    edit "L2L_RM"
        set phase1name "L2L_RM"
        set proposal aes256-sha256
        set dhgrp 21 19 14
        set keepalive enable
        set keylifeseconds 7200
    next
end
```

----------**NETWORKS ROUTES**----------

```
config router static
    edit 1
        set gateway 192.168.1.1
        set device "wan1"
    next
    edit 2
        set dst 192.168.25.0 255.255.255.0
        set device "L2L_RM"
    next
    edit 3
        set dst 192.168.21.0 255.255.255.0
        set device "L2L_RM"
    next
    edit 4
        set dst 10.212.134.0 255.255.255.0
        set device "L2L_RM"
    next
    edit 5
        set dst 192.168.12.0 255.255.255.0
        set device "L2L_RM"
    next
    edit 6
        set dst 172.31.128.0 255.255.255.0
        set device "L2L_RM"
    next
    edit 7
        set dst 172.31.255.0 255.255.255.0
        set device "L2L_RM"
    next
end
```

----------**NETWORKS INTERFACES**----------

```
config system interface
    edit "wan1"
        set vdom "root"
        set ip 192.168.1.99 255.255.255.0
        set type physical
        set monitor-bandwidth enable
        set role wan
```

```
        set snmp-index 1
    next
    edit "dmz"
        set vdom "root"
        set ip 192.168.23.99 255.255.255.0
        set allowaccess ping
        set type physical
        set device-identification enable
        set snmp-index 3
    next
    edit "ssl.root"
        set vdom "root"
        set type tunnel
        set alias "SSL VPN interface"
        set snmp-index 12
    next
    edit "internal"
        set vdom "root"
        set ip 192.168.32.99 255.255.255.0
        set allowaccess ping https ssh fgfm
        set type hard-switch
        set stp enable
        set role lan
        set snmp-index 13
    next
    edit "L2L_RM"
        set vdom "root"
        set ip 0.0.0.0 255.255.255.255
        set type tunnel
        set snmp-index 15
        set interface "wan1"
    next
end
```

References

Fortigate Administration Guid / Fortios RSS.
Available at: https://docs.fortinet.com/product/fortigate/7.0