Request Information				
Requestor	Network Operations			
Implementing Team	Network Operations			
Ticket Number/s	201915972			
Change Classification	X	Major		Minor
After the fact		Yes	X	No
Emergency		Yes	X	No
Proposed Change Date	June 8 2019			
Proposed Change Start/End Time	5:00 pm – 9:00 pm			
Proposed Change Verification Time	10:00 pm			

Objective of the change
To create a separate SSL VPN server for G2 site. Network 172.17.3.127.0/25 will be assigned for G2 Management and creation of 10.2.0.0/24 for DMZ.

Technical/Operational Impact of the change		
Negative: No negative impact as this isn't production affecting.	Beneficial: Separate SSL VPN Server for G2 site.	Neutral: Network Device management

Affected IT Infrastructure components			
Site	Hostname	IP Address	Function
G2	MKT-GL2-CSW-1	172.17.3.130	Network Access Switch
G2	MKT-GL2-FW-1	172.17.3.102	Network Firewall
G2	ODYSSEUS-2	172.17.3.128	Network Firewall

Affected Departments and corresponding contact persons		
Department	Contact Name	Contact Info
All	Rynel Ryson Yanes	09178535630
Network Operations	Mau Mendoza	09176328103

Test Environment implementation and Verification Summary
No testing needed since it is already implemented in Jaka site. Reference: http://172.22.9.5/result3.php?id=5cdd2640a2eca

Test Environment Results Summary
New management IP are going to use for the affected devices and separate VPN server will be created for G2 site.

Configuration Change Template

Baseline File	3.1.10.1, 3.1.11.3
Baseline Version	April 30,2019, March 29, 2019

Baseline File Changes:

Existing Configuration	Proposed Change	Impact	Section
MKT-GL2-FW1: No interface and IPv4 Policy configured for DMZ Interface. **MKT-GL2-CSW1:** No Management IP configured (VLAN 1000).	**MKT-GL2-FW1:** Interface and IPv4 Policy will be configured for DMZ 10.20.0.1 /24 **MKT-GL2-CSW1:** Separate VLAN (1000) will be created for Management of DMZ.	Creation of DMZ network for G2 site. Data and Management traffic will be separated for G2 Core Switch,	3.1.10.1 3.1.11.3

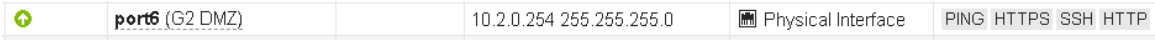
Physical Implementation Procedures / Advisory
1. Connect a cable from port 6 of MKT-GL2- FW-1 to port 5 of Firewall 101e. 2. Connect a cable from G1/0/11 MKT-GL2-CSW-1 to MGMT of Firewall 101e. 3. Connect a cable from Firewall 101e port 6 to Radius server.

Backup Procedures
I. Devices Backup 1. Access **MKT-GL2-CSW1** and **MKT-GL2-FW1.** Save the backup config to: \\172.17.0.124\it\Backup\Network Backup Logs With the following naming convention: BACKUP_HOSTNAME_2019XXXX

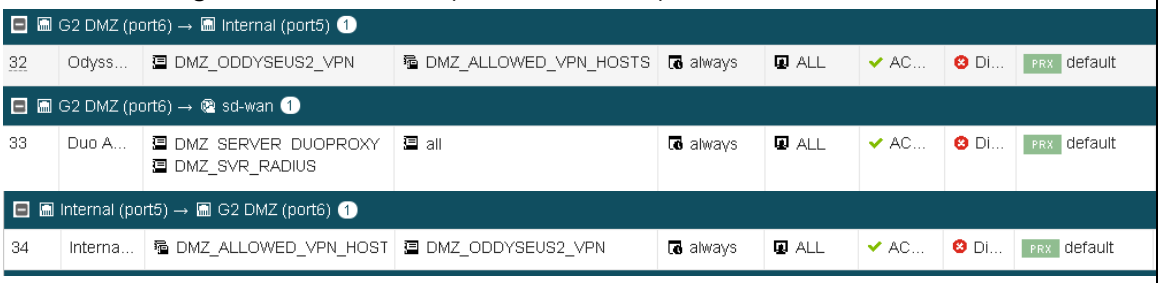
Technical Configuration Procedures

I. MKT-GL2-FW1 Configuration

1. Login to MKT-GL2-FW-1.
2. Go to **Network** > **Interface** and select the **port 6** then **Edit**.
3. Configure the IP/Network Mask: (screenshot below)

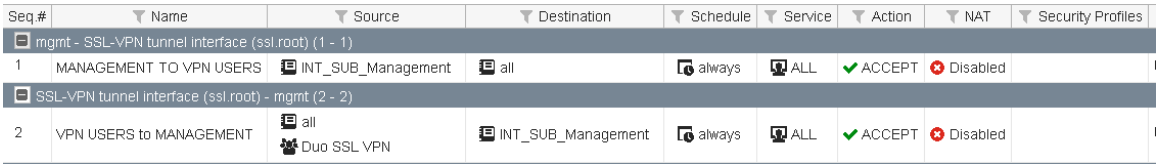


4. Configure the IPv4 Policies: (screenshot below)

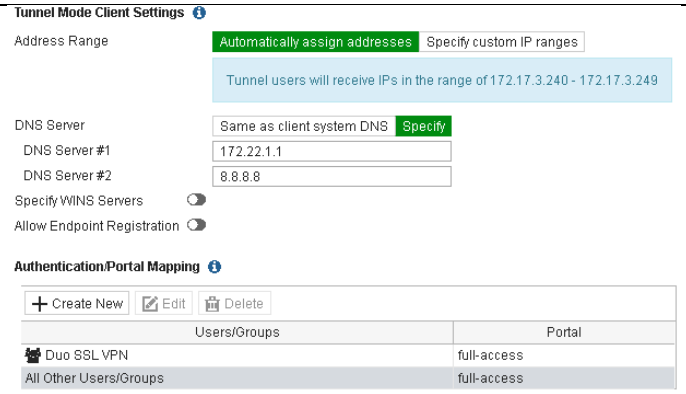


II. Firewall 101E Configuration

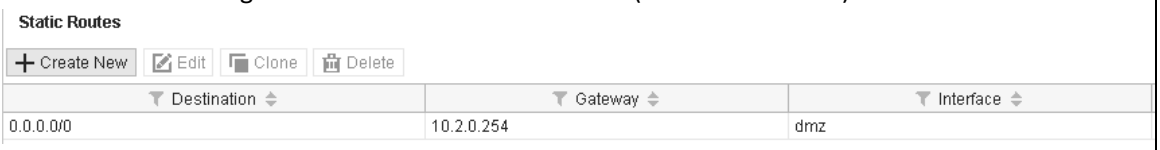
1. Configure the Firewall 101e MGMT to 172.17.3.129 255.255.255.128
2. Configure the port 5 and 6 of Firewall 101e with the IP 10.2.0.100 255.255.255.0
3. Configure the port MGMT of FW101e: 172.17.3.129 255.255.255.128
4. Configure the following IPv4 policies: (screenshot below)



5. SSL VPN Settings:
   Listen on Interface: G2-DMZ (dmz)
   Listen on Port: 443
   Restrict Access: Allow access from any host
   Idle Logout: Enable
   Inactive For: 300 seconds
   Server Certificate: Fortinet_Factory
   Require Client Certificate: Disable



6. Configure Default Route to **ODYSSEUS2** (screenshot below):



7. Create Virtual Interface (Software Switch) where Radius server will be connected.
8. Go to **NETWORK** > **INTERFACES. CREATE** > **INTERFACES.** Copy the details below:

Interface name: ***DMZ-G2***
Type: ***Software Switch***
Physical Interface Member: ***port 5*** *(for MKT-GL2-FW-1) and* ***port 6*** *(for Radius Server)*
Addressing Mode: ***Manual***
IP/Network Mask: ***10.2.0.100/255.255.255.0***
Administrative Access: Select ***SNMP, PING, RADIUS ACCOUNTING***
DHCP SERVER: ***Disable***
Detect Device: ***Disable***
Admission Control: ***None***
Scan Outgoing Connection to Botnet Site: ***Disable***
Secondary IP address: ***Disable***
Comment: ***VPN***

Hit ***OK.***

III. Core Switch Configuration

1. Access the **MKT-GL2-CSW-1** via ssh.
2. Configure the port 11 with following command line by line:

```
configure terminal
 int gi1/0/11
 vlan 1000
 ip address 172.17.3.130 255.255.255.128
 exit
 wr
```

3. Configure static route on G2 Core Switch going to DMZ segment (10.2.0.0/24)

   conf t
   ip route 10.2.0.0 255.255.255.0 172.22.0.75
   wr

4. Configure the management IP address for the following switches:

Switch5_1	172.17.3.90
Switch5_2	172.17.3.91
Switch5_3	172.17.3.92
Switch5_4	172.17.3.93
Switch5_5	172.17.3.94
Switch5_6	172.17.3.95
Switch5_7	172.17.3.96
Switch3_1	172.17.3.97
Switch3_2	172.17.3.98
Switch3_3	172.17.3.99
MKT-GL2-CSW-1	172.17.3.130
MKT-GL2-SW-A1	172.17.3.131
MKT-GL2-SW-A2	172.17.3.132
MKT-GL2-SW-A3	172.17.3.133
MKT-GL2-SW-A4	172.17.3.134
MKT-GL2-SW-A5	172.17.3.135
MKT-GL2-SW-B1	172.17.3.136
MKT-GL2-SW-B2	172.17.3.137

Verification Procedures

I. Config Verification:

1. Access **MKT-GL2-FW1, ODYSSEUS2**.
2. Navigate to **Network > Interfaces,** the config should be:
   MKT-GL2-FW1
   Port <#>: 10.2.0.254 255.255.255.0

   MKT-GL2-CSW1
   G1/0/11

Vlan 1000
Ip address 172.17.3.129 255.255.255.128

ODYSSEUS2
Port 5: 10.2.0.100 /24 | **MGT Port**: 172.17.3.129 /25

3. Connect to **Fortigate SSL VPN (ODYSSEUS2)** 10.2.1.100.
4. Open **Putty** and remote connect **G2 servers** and **network** devices on **172.17.3.128/25** segment.

Back-out Procedures

I. Firewall Backout Procedure

1. Unplug the cable from **MKT-GL2-FW1 port** connecting to **ODYSSEUS2**.
2. Remove the IP from interface 10.2.0.254/24

II. Core Switch Backout Procedure

1. Unplug the cable connecting **MKT-GL2-CSW-1** and **DMZ Switch**.
2. Config int g1/0/11, type "*no vlan 1000*"
3. Save config "***wr*".**