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 1 2019			
Proposed Change Start/End Time	4:00 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:	Beneficial:	Neutral:
No negative impact as this isn't production affecting.	Separate SSL VPN Server for G2 site.	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.

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

Physical Implementation Procedures / Advisory

1. Connect a cable from port of MKT-GL2- FW-1 to port 4 of Firewall 101e.
2. Connect a cable from Firewall 101e port 6 to DMZ-G2 switch.
3. Connect a cable from MKT-GL2-CSW-1 to port 4 of DMZ-G2 switch.
4. Connect a cable from Firewall 101e port 5 to VPN server.

Backup Procedures

I. Switches 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. Firewall 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:

   IP/Network: 10.2.0.1 255.255.255.0
   Hit Ok.

II. Firewall 101E Configuration

1. Configure the Firewall 101e **MGMT** port to 172.17.3.128 255.255.255.128
2. Configure the port 4 of Firewall 101e with the IP 10.2.0.102 255.255.255.0

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
 exit
 wr
```

3. Connect the systems team Duo server to the DMZ-G2 Switch.

Verification Procedures

I. Config Verification:

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

MKT-GL2-FW1
Port <#>: 10.2.0.1 255.255.255.0

MKT-GL2-CSW1
G1/0/11
Vlan 1000

ODYSSEUS2
Port 4: 10.20.1.102 /24 | MGT Port: 172.17.3.128 /25

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 10.2.0.1/24 **II. Core Switch Backout Procedure** 1. Unplug the cable connecting **MKT-GL2-CSW1** and **DMZ Switch**. 2. Config int g1/0/11, type *"no vlan 1000"* 3. Save config *"wr"**.***