Request Information				
Requestor	Maurice Mendoza			
Implementing Team	Network Operations			
Ticket Number/s	201914770			
Change Classification	X	Major		Minor
After the fact		Yes		No
Emergency		Yes		No
Proposed Change Date	April 27, 2019			
Proposed Change Start/End Time	6:00 PM to 9:00 PM			
Proposed Change Verification Time	8:00 PM			

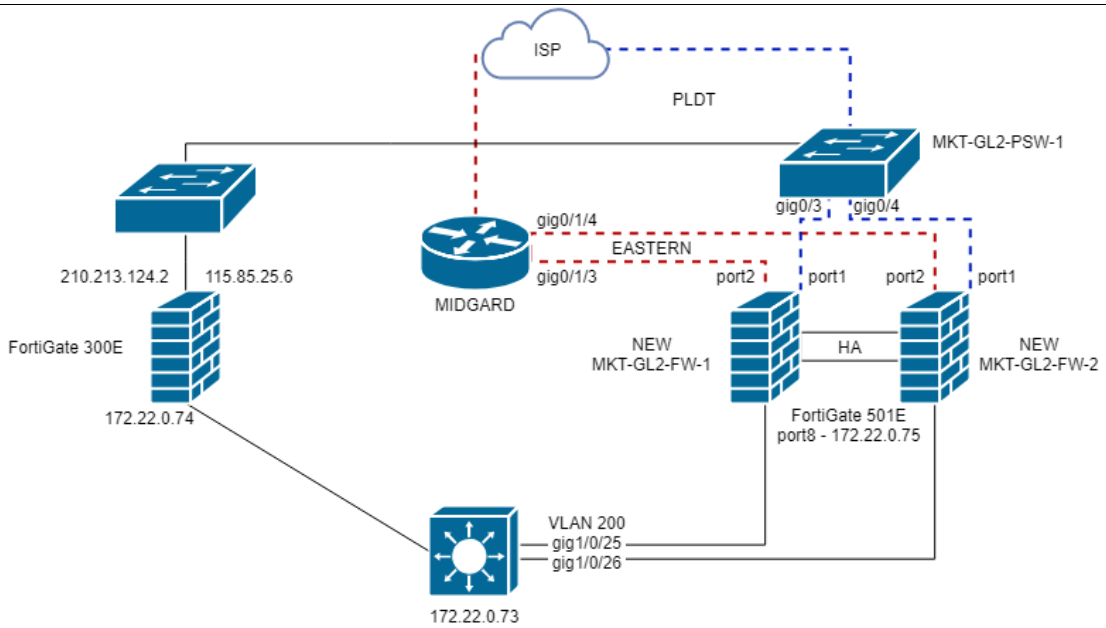
Objective of the change
To replace the FortiGate 300E in G2 with FortiGate 501E.

Technical/Operational Impact of the change		
Negative: Utilization of Metro-E 60Mbps due to rerouting of G2 traffic to JAKA.	Beneficial: Better software and hardware specifications. Pullout of FortiGate 300E for deployment in Davao.	Neutral: Mounting of FortiGate 501E to Rack C.

Affected IT Infrastructure components			
Site	Hostname	IP Address	Function
G2	Midas	172.22.0.74	Network Firewall

Affected Departments and corresponding contact persons		
Department	Contact Name	Contact Info
Quora	Myka Florendo	mflorendo@openaccessbpo.com
World Ventures	Clint Ortiz	cortiz@openaccessbpo.com
UI Path	Nate Martinez	nmartinez@openaccessbpo.com
Ava Women	Crissy Tuazon	ctuazon2@openaccessbpo.com
IT	Rynel Yanes	09178535630
Network Operations	Maurice Mendoza	09176328103

Test Environment implementation and Verification Summary
Since there's no test environment, the procedures below will serve as the test before implementation. Before the test, the configuration of FortiGate 300E has been replicated to FortiGate 501E. Logical Topology:



1. Mount the 2 FortiGate 501E to Rack C below the Globe Router.
2. Access MKT-GL2-CSW-1 via SSH
3. Copy and paste the commands below:

   enable
   configure terminal
   interface gigabitEthernet1/0/25
   no switchport mode trunk
   description TO MKT-GL2-FW-1
   switchport access vlan 200
   switchport mode access
   interface gigabitEthernet1/0/26
   no switchport mode trunk
   description TO MKT-GL2-FW-2
   switchport access vlan 200
   switchport mode access

4. For PLDT, connect a cable from **MKT-GL2-PSW-1**'s port **gig0/3** to **port1** of the new MKT-GL2-FW-1.
5. For PLDT, connect a cable from **MKT-GL2-PSW-1**'s port **gig0/4** to **port1** of the new MKT-GL2-FW-2.
6. Access old FortiGate G2 > Network > Interfaces and disable port2(Eastern). Since there's only 1 IP address remaining in the Eastern's IP Block.
7. For Eastern, connect a cable from **MIDGARD**'s port **gig0/1/3** to **port2** of the new MKT-GL2-FW-1.
8. For Eastern, connect a cable from **MIDGARD**'s port **gig0/1/4** to **port2** of the new MKT-GL2-FW-2.
9. Connect a cable from MKT-GL2-CSW-1 port **gig1/0/25** to **port8** of new MKT-GL2-FW-1.

10. Connect a cable from MKT-GL2-CSW-1 port **gig1/0/26** to **port8** of the new MKT-GL2-FW-2.
11. Do the tests below by batch per campaign. Access MKT-GL2-CSW-1 again and paste the commands below:

    access-list 50 permit ip 172.22.11.0 0.0.0.255
    route-map WV permit 10
    match ip address 50
    set ip next-hop 172.22.0.75
    int vlan 211
    ip policy route-map WV

12. Coordinate with World Ventures agents and check their internet connection and tools. Once verified, remove the configurations.

    int vlan 211
    no ip policy route-map WV
    exit
    no route-map WV permit 10
    no access-list 50 permit ip 172.22.11.0 0.0.0.255

13. Copy and paste the commands below for Quora testing.

    access-list 60 permit ip 172.22.12.0 0.0.0.255
    route-map QUORA permit 10
    match ip address 60
    set ip next-hop 172.22.0.75
    int vlan 212
    ip policy route-map QUORA

14. Coordinate with Quora agents and check their internet connection and tools. Once verified, remove the configurations.

    int vlan 212
    no ip policy route-map QUORA
    exit
    no route-map QUORA permit 10
    no access-list 60 permit ip 172.22.12.0 0.0.0.255

15. Copy and paste the commands below for Ava Women testing.

    access-list 70 permit ip 172.22.13.0 0.0.0.255
    route-map AVA permit 10
    match ip address 70
    set ip next-hop 172.22.0.75
    int vlan 213
    ip policy route-map AVA

16. Coordinate with AVA agents and check their internet connection and tools. Once verified, remove the configurations.

    int vlan 213
    no ip policy route-map AVA
    exit
    no route-map AVA permit 10
    no access-list 70 permit ip 172.22.13.0 0.0.0.255

Test Environment Results Summary
This is the Pilot testing. If successful, the implementation will be done.

Configuration Change Template

Baseline File	3.1.10.1 – 4
Baseline Version	April 3, 2019

Baseline File Changes:

Existing Configuration	Proposed Change	Impact	Section
Current existing equipment, FortiGate 300E.	To replace the current existing equipment with FortiGate 501E.	N/A, baseline for the new equipment will be the same as the old one.	N/A, baseline for the new equipment will be the same as the old one.

Physical Implementation Procedures / Advisory

Send an email to all the GTLs and Campaign Managers that will be affected during the implementation.

"Everyone,

We will be a having Network Maintenance and testing in G2 this coming Saturday, April 27 between 6 pm - 9 pm. There will be 2-4 minutes downtime. The IT team will be on standby for support.

For any concerns please call us at 4038 or email us at itgroup@openaccessmarketing.com

Thank you.

Regards,"

1. Mount the other FortiGate 501E to RACK C below the first FortiGate 501E.
2. Connect the port7 and port8 of the first FortiGate 501E to port7 and port8 of the second FortiGate 501E. This is for the HA configuration.

Backup Procedures

Access FortiGate G2 and MKT-GL2-CSW-1
Backup the configurations files using the naming conventions:

BACKUP_DEVICENAME_DATE.cfg
Example: BACKUP_MIDAS_4272019.cfg, BACKUP_G2CORE_4272019.cfg

Technical Configuration Procedures
1. Access MKT-GL2-CSW-1 via SSH 2. Copy and Paste the commands below: ***enable*** ***configure terminal*** ***no ip route 0.0.0.0 0.0.0.0 172.22.0.74*** ***ip route 0.0.0.0 0.0.0.0 172.22.0.75*** Commands above will force the traffic to go to the newly deployed FortiGate 501E.

Verification Procedures
1. Check all the stations in G2 and verify if there's an internet connection. 2. Access FortiGate 501E and check if the LDAP server is up and connected. 3. Access FortiGate 501E navigate to Log & Report > Forward Traffic. Check the logs of each campaign using their IPv4 Policy as source. 4. Access FortiGate 501E navigate to System > HA. Check and verify the HA Settings of both FortiGate unit. The first unit should be the master and the second should be the slave. 5. Coordinate with Agents on shift and advise them to login and logout. They should still have internet connection and must be passing thru their campaigns IPv4 policy along with their username. Also, their tools should be accessible.

Back-out Procedures
1. Access MKT-GL2-CSW-1 and paste the commands below: ***enable*** ***configure terminal*** ***no ip route 0.0.0.0 0.0.0.0 172.22.0.75*** ***ip route 0.0.0.0 0.0.0.0 172.22.0.74***