Process Owner: **IT Operations**	**FORM** *Configuration Change Request*	**F-CMG-3.1**

Request Information

Requestor	Network Operations			
Implementing Team	Network Operations			
Ticket Number/s	201915290			
Change Classification	X	Major		Minor
After the fact		Yes	X	No
Emergency	X	Yes		No
Proposed Change Date	May 6, 2019			
Proposed Change Start/End Time	19:30 MNL			
Proposed Change Verification Time	19:45 MNL			

Objective of the change

To allow the Internal VA activity of GTI Team via VPN

Technical/Operational Impact of the change

Negative: Disabling of VLAN ACL; reduces network security.	Beneficial: GTI Team will be able to proceed with the Internal VA activity.	Neutral: GTI Team will be able to see the affected host.

Affected IT Infrastructure components

Site	Hostname	IP Address	Function
JAKA	ZEUS	172.31.1.1	Network Core Switch
G2	MKT-GL2-FW1	172.22.2.1	Network Core Switch

Affected Departments and corresponding contact persons

Department	Contact Name	Contact Info
IT	Rynel Yanes	09178535630
Network Operations	Mau Mendoza	09176328103

Test Environment implementation and Verification Summary

There is no test environment for this change, verification will be checked after the configuration.

Test Environment Results Summary

The expected result of the change is GTI Team will be able to scan the affected IPs.

Configuration Change Template

Baseline File	3.1.101, 3.1.102
Baseline Version	April 23, 2019

Baseline File Changes:

Existing Configuration	Proposed Change	Impact	Section
VLAN ACL is applied to Zenefits and Postmates VLAN.	Deletion of vlan access-map 132, 137	No network restriction will be applied to their respective VLANs	

Physical Implementation Procedures / Advisory
No Advisory is needed for this change request.

Backup Procedures
Copy the configuration of **Zeus** and **Jupiter** and save it to: \\172.17.0.124\it\Backup\Network Backup Logs\May 6, 2019

Physical Implementation Procedures
No Physical Implementation is needed for this request.

Technical Configuration Procedures

1. Access **ZEUS** 172.31.1.1 and **Jupiter** 172.31.1.252 via **SSH**.
2. Type the following command to negate the VLAN segmentation for Postmates and Zenefits:

   no ip access-list standard ALLOWED_NETWORKS_132
   no vlan access-map ACL_132 10
   no vlan filter ACL_132 vlan-list 132

   no ip access-list standard ALLOWED_NETWORKS_137
   no vlan access-map ACL_137 10
   no vlan filter ACL_137 vlan-list 137

Verification Procedures

1. Access a workstation from **Zenefits**.
2. Open **cmd** and ping a random IP from **Postmates** segment, the result should be pingable.
3. Access a workstation from **Postmates**.
4. Open **cmd** and ping a random IP from **Zenefits** segment, the result should be pingable.
5. Access **ZEUS** and **Jupiter** via **ssh**.
6. Type the command on **user** mode:

   Show vlan access-map

   Once entered, there should be no **ACL_137** and **ACL_132** listed.

Back-out Procedures

Reapplying of the **VLAN Segmentation** below:

ip access-list standard ALLOWED_NETWORKS_132
10 permit 172.17.0.0 0.0.0.255
20 permit 172.17.1.0 0.0.0.255
30 permit 172.18.133.0 0.0.0.255
40 permit 172.18.132.0 0.0.0.255
deny any
vlan access-map ACL_132 10
match ip address ALLOWED_NETWORKS_132
match ip address ANTISPOOFING
action forward
vlan filter ACL_132 vlan-list 132

ip access-list standard ALLOWED_NETWORKS_137
10 permit 172.17.0.0 0.0.0.255

```
20 permit 172.17.1.0 0.0.0.255
30 permit 172.18.133.0 0.0.0.255
40 permit 172.18.137.0 0.0.0.255
deny any
vlan access-map ACL_137 10
match ip address ALLOWED_NETWORKS_137
match ip address ANTISPOOFING
action forward
vlan filter ACL_137 vlan-list 137
```