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

Request Information				
Requestor	Ian John Lastimoso			
Implementing Team	Network Operations			
Ticket Number/s	201915887			
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	6:00 PM			
Proposed Change Verification Time	7:00 PM			

Objective of the change

Implementation of VLAN /25 on VLAN 215 on switch and Web Filter, Application Control & IPv4 policies for Firewall

Technical/Operational Impact of the change

Negative:	Beneficial:	Neutral:
High Utilization of RAM and CPU usage on the Firewall during the Implementation	Segment Implementation for Wireless Segment of Recruitment Area	Access Switches connected to Core switch

Affected IT Infrastructure components

Site	Hostname	IP Address	Function
G2	MKT-GL2-FW-1	172.17.3.102:10443	Firewall
G2	MKT-GL2-SW-B2	172.17.3.132	Access Switch

Affected Departments and corresponding contact persons

Department	Contact Name	Contact Info
IT	Rynel Yanes	09178535630
Network Operations	Maurice Mendoza	09176881085

Test Environment implementation and Verification Summary

No Test Environment needed as this was implemented before this is for Ipv4 policy, Web Filter and Application control. *Please refer on this ticket #201914195*

No Testing Environment available to configure an Access Point, to Test on a Live Production, Follow the steps below

I. Access Point Configuration

1. Connect the Wireless Access Point to a POE Switch.

2. Connect the WAP to a port on a POE Switch and configure the port to Trunk mode

3. Access WAP by its default IP *192.168.1.254 via Web browser* to change the management IP of the WAP. Navigate to **LAN > VLAN and IPv4 Address**

Untagged VLAN: Enable
Untagged VLAN ID: 1
Management VLAN ID: 1

Connection Type: Static IP
Static IP Address: **Assigned IP address**
Subnet: 255.255.255.0
Default Gateway: **Assigned Gateway Address**

4. Use **cisco** as its username and **cisco** as its password

5. Navigate to **Wireless** > **Networks >** Click on **Add**

Name: OAMRecruitment
VLAN ID: 215
SSID Broadcast: *Check the box*
Security: WPA Personal **Password to be set is:** *#0@mr3cruitm3nt*
Mac Filter: Disable

Click on **Save.**

6. Navigate to **Administration** > **Copy/Save Configuration**

7. To verify, SSID *OAMRecruitment* should be seen on your available wireless network

8. Credential set to the SSID should be work and you should be able to connect to the network

NOTE: If creation and testing of WAP is a success, Proceed with the change request (document should be approved) using the configurations above. If the creation and testing is a fail, Then proceed with the configurations below.

Test Environment Results Summary
Implementation was a success based on the previous Implementations. *Please refer on this ticket #201914195*

Configuration Change Template

Baseline File	3.1.101, 3.1.401, 3.1.402, 3.1.403, 3.1.404
Baseline Version	As of March 01, 2019

Baseline File Changes:

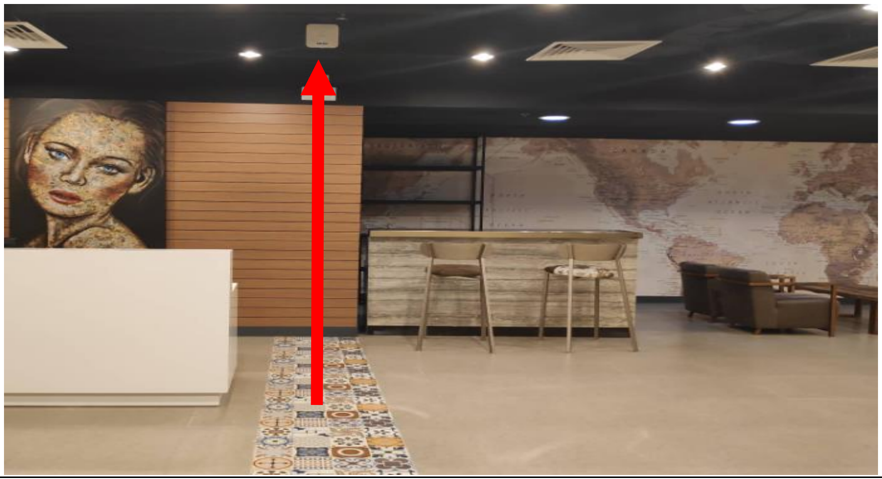
Existing Configuration	Proposed Change	Impact	Section
Existing VLAN for Recruitment PCs	Subnet Existing VLAN for Recruitment into two (Wireless and Recruitment PCs) , Create address group, ipv4 policy for Wireless Recruitment Area	VLAN Database, Address Object, Ipv4 Policies, Address Group Web Filter	3.1.101, 3.1.102, 3.1.402, 3.1.403, 3.1.404, 3.1.405

Physical Implementation Procedures / Advisory

I. Part A (Access Point Implementation)

1. Connect Access Point to Switch B2 Port 47

2. Access Point now will be deployed on **New Recruitment Area** above the **Emergency light** behind the **Front desk**. Since this is where the installed cable is the nearest. *Please refer on the image below*



Backup Procedures

I. Part A (Firewall Configuration)

1. Connect to OAM-VPN via Forti Client

2. Enter your given credential / Accept Notification from Duo App

3. Access G2 Firewall (https://172.17.0.102:10443)

4. Backup Configuration with the following naming convention and then save it inside \\172.17.0.124 \IT\Back up\G2_FW

5. BACKUP;Device;Date;Time,.Extension e.g. BACKUP_G2_07152017_17:45.cfg

II. **PART B (Switch Configuration)**

1. Access Switch via SSH (172.17.3.132)

2. Run the command "*Show run*".

3. Highlight all the text and paste it to notepad with the naming convention and save it inside \\172.17.0.124\it \Back Up\Network Backup Logs

Technical Configuration Procedures

I. PART A (Firewall Configuration)

A. Login to Fortigate G2 (https://172.17.3.102:10443)

B. **Policy & Object > Addresses >** Click on **Create new** and select **Addresses**

Name: INT_SUB_IMAC_RECRUITMENT
Subnet/IPRange: 172.22.15.128/25

C. Go to **Security Profile > Web Filter**

Click the + button at the upper right corner to create new web filter.

Name: WF_ IMAC_RECRUITMENT

Follow the Category Filter

Category	Name	Action
Local Categories	OAM_Blocked	Block
Potentially Liable	Child Abuse	Block
	Discrimination	Block
	Drug Abuse	Block
	Explicit Violence	Block
	Extremist Groups	Block
	Hacking	Block
	Illegal or Unethical	Block
	Plagiarism	Block
	Proxy Avoidance	Block
Adult / Mature Content	Abortion	Block
	Advocacy Organizations	Block
	Alcohol	Block
	Alternative Beliefs	Block
	Dating	Block
	Gambling	Block
	Lingerie and Swimsuit	Block
	Marijuana	Block
	Nudity and Risque	Block
	Other Adult Materials	Block
	Pornography	Block
	Sex Education	Block
	Sports Hunting and War Games	Block
	Tobacco	Block
	Weapons (Sales)	Block
Bandwidth Consuming	File Sharing and Storage	Block

		Freeware and Software Downloads	Block
		Internet Radio and TV	Block
		Internet Telephony	Block
		Peer-to-peer File Sharing	Block
		Streaming Media and Download	Block
	Security Risk	Dynamic DNS	Block
		Malicious Websites	Block
		Phishing	Block
		Spam URLs	Block
	General Interest - Personal	Advertising	Allow
		Arts and Culture	Allow
		Auction	Block
		Brokerage and Trading	Block
		Child Education	Allow
		Content Servers	Block
		Digital Postcards	Block
		Domain Parking	Block
		Dynamic Content	Block
		Education	Allow
		Entertainment	Block
		Folklore	Allow
		Games	Block
		Global Religion	Allow
		Health and Wellness	Allow
		Instant Messaging	Block
		Job Search	Block
		Meaningless Content	Block
		Medicine	Block
		News and Media	Block
		Newsgroups and Message Boards	Allow
		Personal Privacy	Block

	Personal Vehicles	Block
	Personal Websites and Blogs	Allow
	Political Organizations	Block
	Real Estate	Block
	Reference	Allow
	Restaurant and Dining	Block
	Shopping	Block
	Social Networking	Block
	Society and Lifestyles	Allow
	Sports	Allow
	Travel	Block
	Web Chat	Block
	Web-based Email	Block
General Interest - Business	Armed Forces	Block
	Business	Block
	Finance and Banking	Block
	General Organizations	Allow
	Government and Legal Organizations	Block
	Information Technology	Allow
	Information and Computer Security	Block
	Search Engines and Portals	Allow
	Secure Websites	Allow
	Web Hosting	Block
	Web-based Applications	Block
Unrated	Unrated	Block

D. Create new URL Filter and copy the lists of websites below.

typingtest.com
quora.com
avawomen.com
dictionary.com
grammar websites

uipath.com
skype.com

E. Go to **Security Profile** > **Application Control.** Click the + to add new application sensor.

Name: **AC_ IMAC_RECRUITMENT**

Copy the following Categories

Categories	Action
Botnet	Block
Business	Allow
Cloud.IT	Block
Collaboration	Allow
Email	Allow
Game	Block
General.Interest	Allow
Mobile	Allow
Network.Service	Block
P2P	Block
Proxy	Block
Remote.Access	Block
Social.Media	Block
Storage.Backup	Block
Update	Block
Video/Audio	Block
VoIP	Block
Web.Client	Block
Unknown Applications	Block

F. On Application Overrides, click **add signatures** and copy the following configuration:

Application Signature	Category	Action
Adobe.Flash.Media.Playback	Video/Audio	Block
Adobe.Update	Update	Block
Arctic.Torrent	P2P	Block
AVI.Media.Player	Video/Audio	Block
Baidu.Player	Video/Audio	Block
BBC.iPlayer	Video/Audio	Block
BitTorrent	P2P	Block
Chrome.Update	Update	Block
CTorrent	P2P	Block
ExtraTorrent	P2P	Block
Facebook	Social.Media	Block
Facebook_AppNameParameters Required	Social.Media	Block
Facebook_Apps	Social.Media	Block
Facebook_Like.Button	Social.Media	Block
Facebook_Personal	Social.Media	Block
Facebook_Plugins	Social.Media	Block
Facebook_Search	Social.Media	Block
Facebook_Video.Play	Social.Media	Block
Firefox.Update	Update	Allow
Flowplayer	Video/Audio	Block
G3.Torrent	P2P	Block
GOM.Player	Video/Audio	Block
Google.Play	General.Interest	Block
HTTP.Download.Accelerator	General.Interest	Block
HTTP.Segmented.Download	Network.Service	Block
Instagram	Social.Media	Block
Instagram_Video	Social.Media	Block
iTunes	Video/Audio	Block
iTunes_App.Download	Video/Audio	Block
iTunes_BroadCast	Video/Audio	Block

iTunes_Mobile	Video/Audio	Block
iTunes_Podcast	Video/Audio	Block
iTunes_Select.Play	Video/Audio	Block
iTunes_Store	Video/Audio	Block
LinkedIn	Social.Media	Block
LinkedIn_Message	Social.Media	Block
Microsoft.Authentication	Collaboration	Allow
Microsoft.Office.365	Collaboration	Allow
Microsoft.Outlook.Web.App	Collaboration	Allow
One Drive	Collaboration	Block
Pipi.Player	P2P	Block
Playstation.Network	Game	Block
Skype	Collaboration	Allow
Skype.Portals	Collaboration	Allow
Skype.For.Business	Collaboration	Block
Spotify	Video/Audio	Block
SVT.Play	Video/Audio	Block
TorrentLocker.Botnet	Botnet	Block
TorrentSpy	P2P	Block
Torrentz	P2P	Block
Twitter	Social.Media	Block
Twitter_Message	Social.Media	Block
Veoh.Player	Video/Audio	Block
Viber	VoIP	Block
Windows.Media.Player	Video/Audio	Block
YouTube	Video/Audio	Block
YouTube.Downloader.YTD	Video/Audio	Block
YouTube_Comment.Posting	Video/Audio	Block
YouTube_HD.Streaming	Video/Audio	Block
YouTube_Search.Safety.Mode.Off	Video/Audio	Block
YouTube_Search.Video	Video/Audio	Block

YouTube_Video.Embedded	Video/Audio	Block

G. Create WRECRUITMENT IPv4 Policy.

Go to **Policy & Objects** > **IPv4 Policy > Create New**

Name: *CatchAll Policy* IMAC_RECRUITMENT
Incoming Interface: Internal(port16)
Outgoing Interface: wan-load-balance
Source: INT_SUB_ IMAC_RECRUITMENT
Destination Address: ***ALL***
Schedule: *Always*
Service: *HTTPS , DNS , 5228 / TCP , ICMP , TRACEROUTE*
Action: *ACCEPT*
NAT: *Enable*
Fixed Port: *Disable*
IP Pool Configuration: *Use Outgoing Interface*
AntiVirus: *Disable*
Web Filter: *WF_* IMAC_RECRUITMENT
Application Control: *AC_* IMAC_RECRUITMENT
IPS: *Disable*
SSL/SSH Inspection: *Disable*
Log Allowed Traffic: *Enable – Security Events*
Enable this policy: *Enable*

Click ***OK***

H. Go to **Network** > **WAN LLB RULES** > **Create New**

Name: PR_ IMAC_RECRUITMENT
Source Address: INT_SUB_ IMAC_RECRUITMENT
User Group: None
Destination: *Address*
Destination Address: *all*
Interface Members: Specify
port2(Gateway: 210.213.124.2)

I. Get the MAC Address of the IMAC of Recruitment and reserve it to their right segment with the help of Systems team.

J. Navigate to Address > Search: **INT_SUB_RECRUITMENT** > Click on **INT_SUB_RECRUITMENT** > **Edit**

Name: INT_SUB_RECRUITMENT
Subnet: 172.22.15.0/25

NOTE: The Web Filter and Application Control of the new subnet of Recruitment will be reused *WF_RECRUITMENT & AC_RECRUITMENT*

Click on **OK**

II. Part B (AP Configuration)

1. Access the AP deployed on Recruitment Area, Open your web browser and key in *172.22.2.36*

2. Login using the credential given

3. Once logged in, Navigate to **Wireless** > **Networks** > Click on **Add**

4. Click on the box on the new SSID created and then click on > **Edit**

Name: OAMRecruitment
VLAN ID: 215
SSID Broadcast: *Check the box*
Security: WPA Personal **Password to be set is:** *#0@mr3cruitm3nt*
Mac Filter: Disable

5. Then click on > **Save**

III. Part C (Switch Configuration)

1. Access switch via Putty (*172.17.3.132)*

2. Login by using the given credentials. Input the following commands below

```
En
Conf t
Int gi1/0/47
Switchport mode trunk
End
Wr
```

Verification Procedures

- Do an “ipconfig” command in all IMAC Recruitment Area workstations to verify the network segment.

- Test access the internet using Chrome or Firefox. Listed websites on WF_ IMAC_RECRUITMENT should be the only websites that is accessible.

- IP address should be on 15 segment and 4th octet should be 129 above. Ex. 172.22.15.129 – 172.22.15.253

Back-out Procedures

I. Firewall Configuration

a. Go to **Policy & Objects** > **IPv4 Policy** > Right click on *CatchAll Policy WRECRUITMENT and* select **delete**.

b. Go to **Security Profile** > **Application Control** select *AC_ WRECRUITMENT* and then click the trash bin located at the upper right corner to delete. Click OK to confirm.

c. Go to **Security Profile** > **Web Filter,** click this icon select *WF_WRECRUITMENT* and then click **delete**.

d. Go to **Network** > **WAN LLB RULES** then select **PR_INT_SUB_** *WRECRUITMENT* delete.

e. Delete address object named **INT_SUB_** *WRECRUITMENT*.

II. Firewall Configuration

a. Access Switch via Putty *172.17.3.132*

b. Input the given credentials and enter the following command below

```
En
Conf t
Int gi1/0/47
Shut
End
Wr
```