

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

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 235 on Core 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-CSW-1	172.17.3.125	Core Switch
G2	MKT-GL2-FW-1	172.17.3.102:10443	Firewall

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. <i>Please refer on this ticket #201914195</i>

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

Configuration Change Template

 OPEN ACCESS <small>WE SPEAK YOUR LANGUAGE</small>	Proprietary and Confidential	Effectivity: April 1, 2019	Page 1
			Template Version : 02

Process Owner: IT Operations	FORM	F-CMG-3.1
	<i>Configuration Change Request</i>	

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
N/A

Backup Procedures
<p>I. Part A (Firewall Configuration)</p> <ol style="list-style-type: none"> 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

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

Technical Configuration Procedures																																										
<p>I. PART A (Firewall Configuration)</p> <p>A. Login to Fortigate G2 (https://172.17.3.102:10443)</p> <p>B. Policy & Object > Addresses > Click on Create new and select Addresses</p> <p>Name: INT_SUB_WRECRUITMENT Subnet/IPRange: 172.22.15.128/25</p> <p>C. Go to Security Profile > Web Filter Click the + button at the upper right corner to create new web filter.</p> <p>Name: WF_WRECRUITMENT</p> <p>Follow the Category Filter</p> <table> <tr> <th>Category</th><th>Name</th><th>Action</th></tr> <tr> <td>Local Categories</td><td>OAM_Blocked</td><td>Block</td></tr> <tr> <td rowspan="9">Potentially Liable</td><td>Child Abuse</td><td>Allow</td></tr> <tr> <td>Discrimination</td><td>Allow</td></tr> <tr> <td>Drug Abuse</td><td>Allow</td></tr> <tr> <td>Explicit Violence</td><td>Allow</td></tr> <tr> <td>Extremist Groups</td><td>Block</td></tr> <tr> <td>Hacking</td><td>Allow</td></tr> <tr> <td>Illegal or Unethical</td><td>Allow</td></tr> <tr> <td>Plagiarism</td><td>Allow</td></tr> <tr> <td>Proxy Avoidance</td><td>Block</td></tr> <tr> <td rowspan="7">Adult / Mature Content</td><td>Abortion</td><td>Block</td></tr> <tr> <td>Advocacy Organizations</td><td>Block</td></tr> <tr> <td>Alcohol</td><td>Block</td></tr> <tr> <td>Alternative Beliefs</td><td>Block</td></tr> <tr> <td>Dating</td><td>Block</td></tr> <tr> <td>Gambling</td><td>Block</td></tr> <tr> <td>Lingerie and Swimsuit</td><td>Block</td></tr> </table>			Category	Name	Action	Local Categories	OAM_Blocked	Block	Potentially Liable	Child Abuse	Allow	Discrimination	Allow	Drug Abuse	Allow	Explicit Violence	Allow	Extremist Groups	Block	Hacking	Allow	Illegal or Unethical	Allow	Plagiarism	Allow	Proxy Avoidance	Block	Adult / Mature Content	Abortion	Block	Advocacy Organizations	Block	Alcohol	Block	Alternative Beliefs	Block	Dating	Block	Gambling	Block	Lingerie and Swimsuit	Block
Category	Name	Action																																								
Local Categories	OAM_Blocked	Block																																								
Potentially Liable	Child Abuse	Allow																																								
	Discrimination	Allow																																								
	Drug Abuse	Allow																																								
	Explicit Violence	Allow																																								
	Extremist Groups	Block																																								
	Hacking	Allow																																								
	Illegal or Unethical	Allow																																								
	Plagiarism	Allow																																								
	Proxy Avoidance	Block																																								
Adult / Mature Content	Abortion	Block																																								
	Advocacy Organizations	Block																																								
	Alcohol	Block																																								
	Alternative Beliefs	Block																																								
	Dating	Block																																								
	Gambling	Block																																								
	Lingerie and Swimsuit	Block																																								

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

		Marijuana	Block	
		Nudity and Risque	Block	
		Other Adult Materials	Block	
		Pornography	Block	
		Sex Education	Block	
		Sports Hunting and War Games	Allow	
		Tobacco	Block	
		Weapons (Sales)	Block	
	Bandwidth Consuming	File Sharing and Storage	Allow	
		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	Allow	
		Brokerage and Trading	Allow	
		Child Education	Allow	
		Content Servers	Allow	
		Digital Postcards	Allow	
		Domain Parking	Allow	
		Dynamic Content	Allow	
		Education	Allow	
		Entertainment	Allow	
		Folklore	Allow	
		Games	Block	

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

		Global Religion	Allow	
		Health and Wellness	Allow	
		Instant Messaging	Allow	
		Job Search	Allow	
		Meaningless Content	Allow	
		Medicine	Allow	
		News and Media	Allow	
		Newsgroups and Message Boards	Allow	
		Personal Privacy	Allow	
		Personal Vehicles	Allow	
		Personal Websites and Blogs	Allow	
		Political Organizations	Allow	
		Real Estate	Allow	
		Reference	Allow	
		Restaurant and Dining	Allow	
		Shopping	Allow	
		Social Networking	Block	
		Society and Lifestyles	Allow	
		Sports	Allow	
		Travel	Block	
		Web Chat	Block	
		Web-based Email	Block	
	General Interest - Business	Armed Forces	Allow	
		Business	Allow	
		Finance and Banking	Allow	
		General Organizations	Allow	
		Government and Legal Organizations	Allow	
		Information Technology	Allow	
		Information and Computer Security	Allow	
		Search Engines and Portals	Allow	
		Secure Websites	Allow	

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

	Web Hosting	Allow
	Web-based Applications	Allow
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_WRECRUITMENT**

Copy the following Categories

Categories	Action
Botnet	Block
Business	Allow
Cloud.IT	Allow
Collaboration	Allow
Email	Allow
Game	Block
General.Interest	Allow
Mobile	Allow
Network.Service	Allow
P2P	Block
Proxy	Block
Remote.Access	Allow
Social.Media	Block
Storage.Backup	Allow

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

Update	Block
Video/Audio	Block
VoIP	Allow
Web.Client	Allow
Unknown Applications	Allow

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

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

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	Allow
Pipi.Player	P2P	Block
Playstation.Network	Game	Block
Skype	Collaboration	Allow
Skype.Portals	Collaboration	Allow
Skype.For.Business	Collaboration	Allow
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

Process Owner: IT Operations	FORM	F-CMG-3.1
	<i>Configuration Change Request</i>	

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 WRECRUITMENT*
Incoming Interface: *Internal(port16)*
Outgoing Interface: *wan-load-balance*
Source: *INT_SUB_WRECRUITMENT*
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_WRECRUITMENT*
Application Control: *AC_WRECRUITMENT*
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_INT_SUB_WRECRUITMENT*
Source Address: *INT_SUB_WRECRUITMENT*

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

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/TV Displays 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

Click on **OK**

III. 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**

Verification Procedures

Process Owner: IT Operations	FORM	F-CMG-3.1
	<i>Configuration Change Request</i>	

- Do an “ipconfig” command in all WRECRUITMENT Recruitment Area workstations and Appliances , to verify the network segment.
- Test access the internet using Chrome or Firefox.
- 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

- Go to **Policy & Objects > IPv4 Policy** > Right click on *CatchAll Policy WRECRUITMENT* and select **delete**.
- 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.
- Go to **Security Profile > Web Filter**, click this icon select *WF_ WRECRUITMENT* and then click **delete**.
- Go to **Network > WAN LLB RULES** then select **PR_INT_SUB_ WRECRUITMENT** delete.
- Delete address object named **INT_SUB_ WRECRUITMENT**.