

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

Request Information				
Requestor	Network Operations			
Implementing Team	Network Operations			
Ticket Number/s	201913359			
Change Classification	X	Major		Minor
After the fact		Yes	X	No
Emergency		Yes	X	No
Proposed Change Date	July 20, 2019			
Proposed Change Start/End Time	16:00			
Proposed Change Verification Time	16:30			

Objective of the change
For Advent campaign implementation of separate broadcast domain (VLAN) on our core switch, IPv4 Policy, Web Filter and Application Control profile on our network firewall.

Technical/Operational Impact of the change		
<b>Negative:</b> Firewall – Additional IPv4 Policy; more resources consumed  Core Switch – Additional VLAN; more resources consumed	<b>Beneficial:</b> Advent campaign will have their separate broadcast domain, IPv4 Policy, Web and Application Control.	<b>Neutral:</b> Workstations

Affected IT Infrastructure components			
Site	Hostname	IP Address	Function
G2	MKT-GL2-CSW-1	172.17.3.130	Network Core Switch
G2	MKT-GL2-FW-1	172.17.3.102	Network Firewall

Affected Departments and corresponding contact persons		
Department	Contact Name	Contact Info
All	Rynel Yanes	09178535630
Network Operations	Maurice Mendoza	09176328103

Test Environment implementation and Verification Summary
No test environment is needed for this change as this change was previously implemented by the Network Ops before.

Test Environment Results Summary
Expected result of the change is Advent campaign will be able to access their tools and applications.

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

### Configuration Change Template

Baseline File	3.1.10.2, 3.1.11.3
Baseline Version	April 18, 2019

#### Baseline File Changes:

Existing Configuration	Proposed Change	Impact	Section
<b>MKT-GL2-CSW-1:</b> No existing VLAN for Advent (225)  <b>MKT-GL2-FW-1:</b> No existing IPv4 policy for Advent	<b>MKT-GL2-CSW-1:</b> Create VLAN 225 and SVI with an IP address of 172.22.25.254.  <b>MKT-GL2-FW-1:</b> Create new IPv4 policy for Advent that is aligned to their requirements.	Core Switch, Firewall	3.1.10.2, 3.1.11.3

#### Physical Implementation Procedures / Advisory

No physical implementation or advisory is needed for the change.

#### Backup Procedures

1. Access **MKT-GL2-CSW-1** via **SSH** (172.17.3.130)
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\NetworkOps\Backup](#)
4. Access **MKT-GL2-FW1** via **HTTPS** (172.17.3.130)
5. Backup the files to: [\\172.17.0.124\it\NetworkOps\Backup](#)

#### Technical Configuration Procedures

1. Connect to the Fortigate **SSL VPN 10.1.0.100**.
2. Access **MKT-GL2-CSW1 172.22.2.1** via **SSH**.
3. Create the VLAN, SVI, segmentation by typing the following commands:

```
conf t
vlan 225
name ADVENT_SEGMENT
int vlan 225
ip address 172.22.25.254 255.255.255.0
```

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

*ip access-list ALLOWED\_NETWORKS\_225*

*10 permit 172.22.1.0 0.0.0.255*

*20 permit 172.22.7.0 0.0.0.255*

*30 permit 172.22.25.0 0.0.0.255*

*40 deny any*

*exit*

*vlan access-map ACL\_225 10*

*match ip address ALLOWED\_NETWORKS\_225 ANTISPOOFING*

*action forward*

*exit*

*wr*

*exit*

4. Coordinate with Systems Team:

#### **PART C (DHCP Configuration)**

*Ask Systems Team for creating new DHCP Pool.*

*VLAN 225: ADVENT*

*Network: 172.22.25.0/24*

*Range: 172.22.25.1 – 172.22.25.254*

*Exclusion: 172.22.25.240 – 172.22.25.254*

#### **PART D (FSSO Configuration)**

*Ask Systems Team for creating new OU and FSSO Group.*

*FSSO Name = FSSO\_ADVENT*

5. Access **MKT-GL2-FW1 172.17.3.102** via **HTTPS**.
6. Navigate to **Policy & Object > Addresses** > Click on **Create new** and select **Addresses**, create new Address Object with the following:

**Name:** INT\_SUB\_ADVENT

**Subnet/IPRange:** 172.22.25.0/24

7. Create new **Address Group** with the following:

**Name:** GR\_SRC\_ADVENT

**Members:** INT\_SUB\_ADVENT

**Show in Address List:** Enabled

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

Click OK.

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

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

**Name: WF\_ADVENT**

Follow the Category Filter

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

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

		Weapons (Sales)	Monitor	
		File Sharing and Storage	Allow	
	Bandwidth Consuming	Freeware and Software Downloads	Block	
		Internet Radio and TV	Allow	
		Internet Telephony	Allow	
		Peer-to-peer File Sharing	Block	
		Streaming Media and Download	Allow	
	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	
		Global Religion	Allow	
		Health and Wellness	Allow	
		Instant Messaging	Allow	
		Job Search	Block	
		Meaningless Content	Allow	
		Medicine	Allow	
		News and Media	Allow	

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

	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	Allow	
	Web Chat	Allow	
	Web-based Email	Allow	
	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	
Web Hosting		Allow	
Web-based Applications		Allow	
Unrated	Unrated	Block	

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

\*skype.com\*

-

wildcard

-

block

\*pinterest.com\*

-

wildcard

-

block

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

*lazada.com*	-	wildcard	-	block
*youtube.com*	-	wildcard	-	allow
*facebook.com*	-	wildcard	-	block
*vimeo.com*	-	wildcard	-	block
*twitter.com*	-	wildcard	-	allow
*instagram.com*	-	wildcard	-	block
*soundcloud.com*	-	wildcard	-	block
*messenger.com*	-	wildcard	-	block
*hdeuropix.com*	-	wildcard	-	block
*accuradio.com*	-	wildcard	-	block
*whatapps.com*	-	wildcard	-	block
*freemoviedownloads6.com*	-	wildcard	-	block

Click APPLY button.

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

Name: **AC\_ADVENT**

Copy the following Categories

Categories	Action
Botnet	Block
Business	Monitor
<a href="#">Cloud.IT</a>	Monitor
Collaboration	Monitor
Email	Monitor
Game	Monitor
General.Interest	Monitor
Mobile	Monitor
Network.Service	Monitor
P2P	Block
Proxy	Block
Remote.Access	Monitor
Social.Media	Monitor
Storage.Backup	Monitor
Update	Monitor

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

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

11. 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	Allow
Facebook_AppNameParameters Required	Social.Media	Block
Facebook_Apps	Social.Media	Allow
Facebook_Like.Button	Social.Media	Block
Facebook_Personal	Social.Media	Block
Facebook_Plugins	Social.Media	Block
Facebook_Search	Social.Media	Allow
Facebook_Video.Play	Social.Media	Block
Firefox.Update	Update	Block
Flowplayer	Video/Audio	Block
G3.Torrent	P2P	Block
GOM.Player	Video/Audio	Block



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

Google.Play	General.Interest	Block
HTTP.Download.Accelerator	General.Interest	Block
HTTP.Segmented.Download	Network.Service	Block
Instagram	Social.Media	Allow
Instagram_Video	Social.Media	Allow
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.Media.Server	Video/Audio	Block
Microsoft.Office.365	Collaboration	Block
Microsoft.Portal	Collaboration	Allow
Netflix	Video/Audio	Block
Pinterest	Social.Media	Allow
Pipi.Player	P2P	Block
Playstation.Network	Game	Block
Skype	Collaboration	Allow
Skype.Portals	Collaboration	Allow
SoundCloud	Video/Audio	Block
Spotify	Video/Audio	Block
SVT.Play	Video/Audio	Block
TorrentLocker.Botnet	Botnet	Block
TorrentSpy	P2P	Block
Torrentz	P2P	Block
Twitter	Social.Media	Allow

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

Twitter_Message	Social.Media	Allow
Veoh.Player	Video/Audio	Block
Viber	VoIP	Block
Windows.Media.Player	Video/Audio	Block
YouTube	Video/Audio	Allow
YouTube.Downloader.YTD	Video/Audio	Block
YouTube_Comment.Posting	Video/Audio	Allow
YouTube_HD.Streaming	Video/Audio	Block
YouTube_Search.Safety.Mode.Off	Video/Audio	Allow
YouTube_Search.Video	Video/Audio	Allow
YouTube_Video.Embedded	Video/Audio	Allow

## 12. Create ADVENT IPv4 Policy.

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

Name: *CatchAll Policy FSSO ADVENT*  
 Incoming Interface: *Internal(port5)*  
 Outgoing Interface: *wan-load-balance*  
 Source: *FSSO\_USERS\_ADVENT*  
           *GR\_SRC\_ADVENT*  
 Destination Address: **ALL**  
 Schedule: *Always*  
 Service: **ALL**  
 Action: *ACCEPT*  
 NAT: *Enable*  
 Fixed Port: *Disable*  
 IP Pool Configuration: *Use Outgoing Interface*  
 AntiVirus: *Disable*  
 Web Filter: *WF\_ADVENT*  
 Application Control: *AC\_ADVENT*  
 IPS: *Disable*  
 SSL/SSH Inspection: *Disable*  
 Log Allowed Traffic: *Enable – All Sessions*  
 Enable this policy: *Enable*

Click **OK**

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

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


Name: PR\_INT\_SUB\_ADVENT  
Source Address: INT\_SUB\_ADVENT  
User Group: None  
Destination: *Address*  
Destination Address: *all*  
Interface Members: Specify  
port2(Gateway: 210.213.124.2)

Verification Procedures

1. Check if the IPv4 policies are saved.
2. Go to **Logs and Report > Forward Traffic** click **Add filter** select **Source** and add IP from VLAN 225 and check if there are any traffic logs.
3. Check the ADVENT computers and it should have internet connections. Browse any website/tools using Chrome or Firefox browser and should be accessible with no error.
4. Check also if email sites are accessible. Social Medias such as Facebook should be blocked and Youtube should be accessible

Back-out Procedures

**I. Firewall Configuration**

- a. Go to **Policy & Objects > IPv4 Policy** > Right click on *CatchAll Policy ADVENT* and select **delete**.
- b. Go to **Security Profile > Application Control** select *AC\_ADVENT* 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\_ADVENT* and then click **delete**.
- d. Go to **Network > WAN LLB RULES** then select **PR\_INT\_SUB\_ADVENT** delete.
- e. Delete address object named **INT\_SUB\_ADVENT**.
- f. Delete address group named **GR\_SRC\_ADVENT**.