Request Information				
Requestor	Network Operations			
Implementing Team	Network Operations			
Ticket Number/s	201914723			
Change Classification	X	Major		Minor
After the fact		Yes	X	No
Emergency		Yes	X	No
Proposed Change Date	April 20, 2019			
Proposed Change Start/End Time	17:00 / 19:00			
Proposed Change Verification Time	18:00			

Objective of the change
To create new IPv4 Policy for G2 conference

Technical/Operational Impact of the change		
Negative: Addition RAM of Firewall will be consumed for this policy.	Beneficial: G2 Conference will have a different policy separated to the production	Neutral: N/A

Affected IT Infrastructure components			
Site	Hostname	IP Address	Function
G2	Midas	172.22.0.74	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
UIPath	Nate Martinez	nmartinez@openaccessbpo.com
Ava Women	Crissy Tuazon	ctuazon@openaccessbpo.com

Test Environment implementation and Verification Summary
No testing needed for this request since we already implemented IPv4 policy before.

Test Environment Results Summary
N/A

Configuration Change Template

Baseline File	3.1.10.2, 3.1.10.3, 3.1.10.4
Baseline Version	N/A

Baseline File Changes:

Existing Configuration	Proposed Change	Impact	Section
No existing IPv4 for conference in MKT-GL2-FW-1 firewall	To create new IPv4 Policy for Conference in G2 separated to the production.	VLAN, Address Object, IPv4 Policy Group, Web and Application Filter	3.1.10.2 3.1.10.3 3.1.10.4

Physical Implementation Procedures / Advisory
N/A

Backup Procedures
1. Access G2 Firewall (MKT-GL2-FW-1). 2. Backup configuration with the following naming convention and then save it inside: \\fs.oampi.com\It\IT_Backup\Back Up\Network Operations 3. BACKUP_<device>_<DATE>_<TIME>.EXTENSION, eg. BACKUP_GL2-Firewall_07152017_17:00.cfg

Physical Implementation Procedures
N/A

Technical Configuration Procedures

1. Access GL2 Firewall (https://172.22.0.74:10443).

2. Go to **Policy & Object** > **Addresses** > **Create New address** > **Address Group**

    Group Name: *EXE_GR_CONFERENCE*
    Member: *INT_PC_CONF_1*
        INT_PC_CONF_2
        INT_PC_CONF_3
        INT_PC_CONF_4
        INT_PC_CONF_5

    Click **OK.**

3. Go to **Security** > **Web Filter**
    Click "**+**" button at the upper right corner to add new web filter.

    Name: **WF_CONFERENCE**

    Follow the Category Filters:

Category	Name	Action
Local Categories	OAM_Blocked	Allow
Potentially Liable	Child Abuse	Allow
	Discrimination	Allow
	Drug Abuse	Allow
	Explicit Violence	Allow
	Extremist Groups	Allow
	Hacking	Block
	Illegal or Unethical	Allow
	Plagiarism	Allow
	Proxy Avoidance	Block
Adult / Mature Content	Abortion	Allow
	Advocacy Organizations	Allow
	Alcohol	Allow

		Alternative Beliefs	Allow
		Dating	Allow
		Gambling	Allow
		Lingerie and Swimsuit	Allow
		Marijuana	Allow
		Nudity and Risque	Allow
		Other Adult Materials	Allow
		Pornography	Block
		Sex Education	Allow
		Sports Hunting and War Games	Allow
		Tobacco	Allow
		Weapons (Sales)	Allow
	Bandwidth Consuming	File Sharing and Storage	Allow
		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	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	Allow
		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	Allow

URL FILTER:

URL	Type	Action	Status
video.fbcdn.net	Wildcard	Block	Enable
fbcdn.net	Wildcard	Exempt	Enable
dl.tehmovies.com	Wildcard	Block	Enable
freemoviedownloads6.com	Wildcard	Block	Enable
youtube.com	Wildcard	Exempt	Enable
spotify.com	Wildcard	Exempt	Enable
recruitment.openaccessbpo.com	Wildcard	Exempt	Enable
aboutworldlanguages.com	Wildcard	Exempt	Enable
silentblade.com	Wildcard	Exempt	Enable
skype.com	Wildcard	Exempt	Enable
facebook.com	Wildcard	Exempt	Enable
microsoft.portal	Wildcard	Exempt	Enable
microsoft.authentication	Wildcard	Exempt	Enable
login.microsoftonline.com	Wildcard	Exempt	Enable

Click **APPLY**.

4. Under Security Profile, select Application Control. Click "**+**" to add new application sensor.

Name: **AC_CONFERENCE**
Copy the following Categories

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

5. On Application overrides, click **add signatures** and copy the following configuration:

Application Signature	Category	Action
Adobe.Flash.Media.Playback	Video/Audio	Allow
Adobe.Update	Update	Allow
Arctic.Torrent	P2P	Block
AVI.Media.Player	Video/Audio	Allow
Baidu.Player	Video/Audio	Block
BBC.iPlayer	Video/Audio	Block
BitTorrent	P2P	Block
Chrome.Update	Update	Block

Citrix.CDN	Collaboration	Allow
Citrix.ICA	General Interest	Allow
Citrix.Receiver	Remote.Access	Allow
CTorrent	P2P	Block
ExtraTorrent	P2P	Block
Facebook	Social.Media	Allow
Facebook_AppNameParameters Required	Social.Media	Allow
Facebook_Apps	Social.Media	Allow
Facebook_Like.Button	Social.Media	Allow
Facebook_Personal	Social.Media	Allow
Facebook_Plugins	Social.Media	Allow
Facebook_Search	Social.Media	Allow
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	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	Allow
LinkedIn_Message	Social.Media	Block

Microsoft.Authentication	Collaboration	Allow
Microsoft.Media.Server	Video/Audio	Block
Microsoft.Office.365	Collaboration	Allow
Microsoft.Portal	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	Allow
Twitter_Message	Social.Media	Block
Veoh.Player	Video/Audio	Block
Viber	VoIP	Block
Windows.Media.Player	Video/Audio	Block
YouTube	Video/Audio	Allow
YouTube.Downloader.YTD	Video/Audio	Allow
YouTube_Comment.Posting	Video/Audio	Allow
YouTube_HD.Streaming	Video/Audio	Allow
YouTube_Search.Safety.Mode.Off	Video/Audio	Allow
YouTube_Search.Video	Video/Audio	Allow
YouTube_Video.Embedded	Video/Audio	Allow

6. Go to **Policy & Object** > **IPv4 Policy** > **Create New**.

> Name: **CatchAll Conference**
> Incoming interface: *Internal (port16)*
> Outgoing Interface: *sd-wan*
> Source: *EXE_GR_CONFERENCE*
> Destination: *all*
> Schedule: *always*
> Service: *all*
> Action: *ACCEPT*
> NAT: *Enable*
> IP Pool Configuration: *Use Outgoing Interface Address*
> Web Filter: *WF_CONFERENCE*
> App Control: *AC_CONFERENCE*
> Log Allowed Traffic: *All Sessions*
> Enable this policy: *Enable*
>
> Hit **OK**.

7. Access G2 Core Switch via SSH (172.22.2.1)
8. Execute the following command:

> *en*
> *conf t*
> *int vlan 217*
> *ip helper-address 172.22.1.1*
> *no shutdown*
> *exit*
> *wr*

Verification Procedures

1. Check if the firewall IPv4 policies are successfully saved.
2. Check all the conference PC, try to browse and it should have internet connection.
3. Check some websites including Youtube must be accessible for training.

Back-out Procedures

1. Login to **MKT-GL2-FW-1** via web.
2. Go to Policy & Object and remove the address object named: "*INT_SUB_CONFERENCE*".
3. Locate the IPv4 Policy "**CatchAll CONFERENCE**" and click **Delete**.
4. Go to **Security Profile** > **Web Filter** and Select **WF_CONFERENCE** and click the trash icon on the upper right corner.
5. Go to **Security Profile** > **Application Control** and Select **AC_CONFERENCE** and click the trash icon on the upper right corner.