

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

Request Information				
Requestor	Network Operations			
Implementing Team	Network Operations			
Ticket Number/s	201904302			
Change Classification	X	Major		Minor
After the fact		Yes	X	No
Emergency		Yes	X	No
Proposed Change Date	April 15, 2019			
Proposed Change Start/End Time	17:00 / Until the UAT for affected campaigns/department is complete			
Proposed Change Verification Time	Until the UAT for affected campaigns/department is complete			

Objective of the change
Restrict the outbound TCP/UDP ports only to the Business Unit/Department needs as outlined on PCI-DSS requirement.

Technical/Operational Impact of the change		
Negative:	Beneficial:	Neutral:
N/A	Network team will be able to know if the IPv4 policy needs to be modified as needed.	N/A

Affected IT Infrastructure components			
Site	Hostname	IP Address	Function
JAKA	THOR	172.16.1.2	Network Firewall
	ZEUS	172.31.1.2	Network Core Switch
G2	MKT-GL2-CSW-1	172.22.2.1	Network Core Switch

Affected Departments and corresponding contact persons		
Department	Contact Name	Contact Info
All	Rynel Yanes	09178535630
Network Operations	Maurice Mendoza	09176881085

Test Environment implementation and Verification Summary
<p>UAT Procedures:</p> <ol style="list-style-type: none"> 1. Coordinate with the Campaign manager to do a test for each campaign before implementation. 2. Setup a test PC and join it in the VLAN of the Campaign. 3. Create a test IPv4 Policy with the following details: Name: Test Policy for UAT

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

Incoming Interface: Internal(port5)
Outgoing Interface: SD-WAN
Source: "IP ADDRESS OF THE TEST PC"
Destination: all

Schedule: always
Service: "SPECIFIC OUTBOUND PORTS FOR THE CAMPAIGN"
Action: Accept
NAT: Enabled
Web Filter: "WEB FILTERING OF THE CAMPAIGN"
Application Control: "APPLICATION CONTROL OF THE CAMPAIGN"
Log Allowed Traffic: Enabled – All Sessions
4. Have the user do a UAT. (Campaign tools, website accesses)
5. Repeat steps 3 to 4 for all Campaigns.
6. Once verified and accepted by the representative of each Campaign, delete the "Test Policy for UAT" policy then proceed to the configuration procedure.
7. Change the IPv4 policy perimeter as the campaign changes for the UAT.

Test Environment Results Summary

#To be filled up once the UAT is done.

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

Configuration Change Template

Baseline File	3.1.402, 3.1.403, 3.1.404
Baseline Version	April 3, 2019

Baseline File Changes:

Existing Configuration	Proposed Change	Impact	Section
No IPv4 Policy for UAT of campaigns to be deployed on THOR and MKT-GL2-FW1 .	IPv4 Policy creation for UAT of campaigns to be deployed on THOR and MKT-GL2-FW1 .	IP Policies for each business units/departments will be more defined; increased security	3.1.402, 3.1.403, 3.1.404

Physical Implementation Procedures / Advisory

1. Email GTL's for campaign UAT
2. Setup Test Computer to be used for the activity.

Backup Procedures

I. Part A (Firewall Configuration)

1. Access **THOR**, **MKT-GL2-CSW**, **ZEUS**, **MKT-GL2-CSW** using your given credentials.
2. Backup Configuration with the following naming convention and then save it inside <\\172.17.0.124\IT\NOC>
3. BACKUP;Device;Date;Time,.Extension e.g.
BACKUP_THOR_20190129_17:45.cfg

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

Physical Implementation Procedures
N/A

Technical Configuration Procedures
<p>I. PART A (Firewall Configuration)</p> <ol style="list-style-type: none"> 1. Access THOR and G2 FW via https. 2. Go to Services > Create New > Category > then type the following: <p>New Service Category</p> <p>Name: Open Access BPO Services PCI-DSS Comments: <blank></p> <p>Press OK.</p> <p>Once created, create new Services with the following:</p> <p>Name: ICMP Category: Open Access BPO Services PCI-DSS Protocol Type: ICMP Type: <blank> #blank means ALL for this service Code: <blank></p> <p>Press OK.</p> <p>Create another Services with the following:</p> <p>Name: 6780 – 6781 - TCP Category: Open Access BPO Services PCI-DSS Protocol Type: TCP/UDP IP/FQDN: <blank> Destination Port: TCP 6780 - 6781</p> <p>Press OK. Name: HTTPS - TCP Category: Open Access BPO Services PCI-DSS</p>

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

Protocol Type: **TCP/UDP**
IP/FQDN: <blank>
Destination Port: **TCP | 443**

Press **OK**.

Name: **RTP - UDP**
Category: **Open Access BPO Services | PCI-DSS**
Protocol Type: **TCP/UDP**
IP/FQDN: <blank>
Destination Port: **UDP | 10000 - 65535**

Press **OK**.

Name: **SIP – TCP & UDP**
Category: **Open Access BPO Services | PCI-DSS**
Protocol Type: **TCP/UDP**
IP/FQDN: <blank>
Destination Port: **TCP | 5060**
UDP | 5060

Press **OK**.

Name: **Google Service – TCP**
Category: **Open Access BPO Services | PCI-DSS**
Protocol Type: **TCP/UDP**
IP/FQDN: <blank>
Destination Port: **TCP | 5228**

Press **OK**.

Name: **STUN - UDP**
Category: **Open Access BPO Services | PCI-DSS**
Protocol Type: **TCP/UDP**
IP/FQDN: <blank>
Destination Port: **UDP | 3478**

Press **OK**.

Name: **us-srv – TCP & UDP**
Category: **Open Access BPO Services | PCI-DSS**
Protocol Type: **TCP/UDP**
IP/FQDN: <blank>
Destination Port: **TCP | 8083**
UDP | 8083

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

Press **OK**.

Name: **CXTP – TCP**

Category: **Open Access BPO Services | PCI-DSS**

Protocol Type: **TCP/UDP**

IP/FQDN: <blank>

Destination Port: **TCP | 5091**

Press **OK**.

Name: **SIP_2 – SCTP**

Category: **Open Access BPO Services | PCI-DSS**

Protocol Type: **TCP/UDP/SCTP**

IP/FQDN: <blank>

Destination Port: **SCTP | 5091**

Press **OK**.

3. Access **THOR** via **https**, go to **Security Profile > Web Filter**
Click the + button at the upper right corner to create new web filter.

Name: WF_CAPABILITY

Follow the Category Filter

Category	Name	Action
Local Categories	Custom1	Allow
	Custom2	Allow
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

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

	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	Allow	
		Freeware and Software Downloads	Block	
		Internet Radio and TV	Block	
		Internet Telephony	Allow	
		Peer-to-peer File Sharing	Block	
		Streaming Media and Download	Block	
	Security Risk	Dynamic DNS	Block	
		Malicious Websites	Block	
		Newly Observed Domain	Block	
		Newly Registered Domain	Block	
		Phishing	Block	
		Spam URLs	Block	
	General Interest - Personal	Advertising	Block	
		Arts and Culture	Block	
		Auction	Block	
		Brokerage and Trading	Block	

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

	Child Education	Block	
	Content Servers	Allow	
	Digital Postcards	Block	
	Domain Parking	Block	
	Dynamic Content	Block	
	Education	Block	
	Entertainment	Block	
	Folklore	Block	
	Games	Block	
	Global Religion	Block	
	Health and Wellness	Block	
	Instant Messaging	Allow	
	Job Search	Block	
	Meaningless Content	Block	
	Medicine	Block	
	News and Media	Allow	
	Newsgroups and Message Boards	Block	
	Personal Privacy	Block	
	Personal Vehicles	Block	
	Personal Websites and Blogs	Block	
	Political Organizations	Block	
	Real Estate	Block	
	Reference	Block	
	Restaurant and Dining	Block	
	Shopping	Block	
	Social Networking	Block	
	Society and Lifestyles	Block	
	Sports	Block	
	Travel	Block	
	Web Chat	Allow	
	Web-based Email	Allow	

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

General Interest - Business	Armed Forces	Block
	Business	Allow
	Finance and Banking	Block
	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

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

spotify.com	-	wildcard	-	block
facebook.com	-	wildcard	-	block
lazada.com	-	wildcard	-	block
youtube.com	-	wildcard	-	Allow
viber.com	-	wildcard	-	block
vimeo.com	-	wildcard	-	block
twitter.com	-	wildcard	-	block
instagram.com	-	wildcard	-	block
soundcloud.com	-	wildcard	-	block
freemoviedownloads6.com	-	wildcard	-	block

Click APPLY button.

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

Name: **AC_CAPABILITY**

Copy the following Categories

Categories	Action
Business	Allow
Cloud.IT	Allow

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

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

- c. On Application Override, click **add signatures** and copy the following configuration:

Application Signature	Category	Action
Adobe.Update	Update	Block
AVI.Media.Player	Video/Audio	Block
Baidu.Player	Video/Audio	Block
BBC.iPlayer	Video/Audio	Block
Chrome.Update	Update	Block
Facebook_Messenger.Image.Transfer	Collaboration	Block
Facebook_Messenger.Video.Transfer	Collaboration	Block
Facebook_Messenger.Voice.Message	Collaboration	Block
Facebook_Messenger.VoIP.Call	Collaboration	Block
Facebook_Video.Play	Social.Media	Block

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

	Firefox.Update	Update	Block
	Flowplayer	Video/Audio	Block
	GOM.Player	Video/Audio	Block
	Google.Play	General.Interest	Block
	Google.Drive	Storage.Backup	Allow
	Google.Drive_Edit	Storage.Backup	Allow
	Google.Drive_File.Download	Storage.Backup	Allow
	Google.Drive_File.Upload	Storage.Backup	Allow
	Google.Drive_File.Sharing	Storage.Backup	Allow
	Instagram	Social.Media	Block
	Instagram_Video	Social.Media	Block
	iTunes_Select.Play	Video/Audio	Block
	iTunes_Update	Update	Block
	Java.Update	Update	Block
	LinkedIn	Social.Media	Block
	LinkedIn_Message	Social.Media	Block
	Microsoft.Office.Update	Update	Block
	Microsoft.Outlook	Email	Allow
	Microsoft.Outlook.Web.App	Email	Allow
	Microsoft.Outlook_Attachment	Email	Allow
	MS.Windows.Update	Update	Block
	Outlook.Anywhere	Business	Allow
	Pipi.Player	P2P	Block
	Playstation.Network	Game	Block
	Real.Player	Video/Audio	Block
	SoundCloud	Video/Audio	Block
	Spotify	Video/Audio	Block
	SVT.Play	Video/Audio	Block
	Twitter	Social.Media	Block
	Twitter_Message	Social.Media	Block
	Ubuntu.Update	Update	Block

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

UEFA_Video.Play	Video/Audio	Block
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	Block
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

4. Navigate to Policy & Objects > IPv4 Policy

Create the following policies:

Test Policy for UAT – **Privileged Access USColo**

Test Policy for UAT – **Campaign Policy**

Once the policies were created, set them in order above to the lowest sequence # (above Implicit Deny).

5. Create a test IPv4 Policy with the following details:

Name: Test Policy for UAT – **Privileged Access USColo**

Incoming Interface: Internal(port5)

Outgoing Interface: SD-WAN

Source: "**10.20.1.0 /24**"

Destination: "**EXT_SUB_USCOLO
EXT_GR_CEBUPAC_SSH
EXT_GR_VOIPFONE**"

Schedule: always

Service: "**6780 – 6781 - TCP**

SIP – TCP & UDP

HTTPS – TCP

HTTP – TCP

10000 – 65535 / UDP

ICMP"

Action: Accept

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

NAT: Enabled
Web Filter: <blank>
Application Control: <blank>
Log Allowed Traffic: Enabled – All Sessions

6. Create a test IPv4 Policy with the following details:
Name: Test Policy for UAT – **Campaign Policy** (#insert campaign name)
Incoming Interface: Internal(port5)
Outgoing Interface: SD-WAN
Service: “**SPECIFIC OUTBOUND PORTS FOR THE CAMPAIGN**”
Action: Accept
NAT: Enabled
Web Filter: “**WEB FILTERING OF THE CAMPAIGN**”
Application Control: “**APPLICATION CONTROL OF THE CAMPAIGN**”
Log Allowed Traffic: Enabled – All Sessions

Note: Change the Service Port, Web Filter, Application Control as needed by the campaign/business unit.

7. Access **G2FW** via https **172.22.0.74**, then create the USColo policy:
Create a test IPv4 Policy with the following details:
Name: Test Policy for UAT – **Privileged Access USColo**
Incoming Interface: Internal(port5)
Outgoing Interface: SD-WAN
Source: “**10.30.1.0 /24**”
Destination: “**EXT_SUB_USCOLO**”

Schedule: always
Service: “**6780 – 6781 - TCP**
SIP – TCP & UDP
HTTPS – TCP
HTTP – TCP
10000 – 65535 / UDP
ICMP”

Action: Accept
NAT: Enabled
Web Filter: <blank>
Application Control: <blank>
Log Allowed Traffic: Enabled – All Sessions

8. Create another policy with the similar format on #5 for **G2 FW**.

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

II. PART B (Core Switch Configuration)

1. Access **ZEUS** and **MKT-GL2-CSW** via **SSH**.
2. Create the following VLAN by typing the commands:

```

!
vlan 500
int vlan 500
description <TEST_VLAN_UAT>
ip address 10.20.1.254 255.255.255.0 (#10.20.30.1.254 for G2)
spanning-tree vlan 500 24576
spanning-tree vlan 500 forward-time 4
spanning-tree vlan 500 max-age 6
!

```

Verification Procedures

- A. Login to **THOR** and **G2 FW** via **https** respectively.
- B. **Navigate to Policies & Objects > IPv4 Policy**, verify that the ports properly assigned to the “**Service**” of the following:

THOR 172.16.1.2
 Test Policy for UAT – **Privileged Access USColo**
 Test Policy for UAT – **Campaign Policy**
- C. Use the test PC for each campaigns/departments that policies were recently configured and check the internet connection.
- D. Do a test browsing that is included in the policy, once traffic is generated, check the “**Bytes**” column on the **IPv4 policy**.

Bytes
60.28 GB 

II. Core Switch Configuration

- A. Access **ZEUS** and **MKT-GL2-CSW** via **SSH**.
Type the following commands for test VLAN verification:

```

show run int vlan 500
show vlan br

```

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

The output should display vlan 500 created and with an IP address of 10.X.10.0/24.

show spanning-tree vlan 70 - This command will show the current spanning tree details. The details below should be the same;

For VLAN 500 in Zeus
Root ID Priority 25076
Address 0042.5a39.da00
This bridge is the root
Hello Time 2 sec Max Age 6 sec Forward Delay 4 sec

Bridge ID Priority 25076 (priority 25076 sys-id-ext 70)
Address 0042.5a39.da00
Hello Time 2 sec Max Age 6 sec Forward Delay 4 sec
Aging Time 300 sec

Back-out Procedures

A. Locate the following IPv4 policies then delete all of the following:

THOR 172.16.1.2

Test Policy for UAT – **Privileged Access USColo**

Test Policy for UAT – **Campaign Policy**

MKT-GL2-FW1 172.22.0.74

Test Policy for UAT – **Privileged Access USColo**

Test Policy for UAT – **Campaign Policy**

B. Locate the following **Services** then delete all.

THOR:

6780 – 6781 - TCP
HTTPS - TCP
RTP - UDP
SIP – TCP & UDP
SIP 2 – TCP & UDP
Google Service – TCP
STUN - UDP
SNMP – UDP

MKT-GL2-FW:

6780 – 6781 - TCP
HTTPS - TCP
RTP - UDP

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

<p>SIP – TCP & UDP SIP 2 – TCP & UDP Google Service – TCP STUN - UDP SNMP – UDP</p> <p>C. Access THOR via https, go to Security Profiles > Web Filter > click the Change view button on the rightest part of Web Profile.</p> <p>Locate the following Web Filter and then delete:</p> <p>WF_CAPABILITY</p> <p>Go to Application Control > click the Change view button on the rightest part of Web Profile.</p> <p>Locate the following Web Filter and then delete:</p> <p>WF_CAPABILITY</p> <p>D. Access ZEUS and G2-MKT-CSW via SSH.</p> <p>Type the following commands to delete VLAN 500</p> <p>no vlan 500 no int vlan 500 do wr</p>
