

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

Request Information				
Requestor	Alvis Bajal			
Implementing Team	Network Operations			
Ticket Number/s	201914540			
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	19:00			
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 Incoming Interface: Internal(port5)

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


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

This is a pilot testing. If successful, the changes will be implemented.

Configuration Change Template

	Proprietary and Confidential	Effectivity: April 1, 2019	Page 2
			Template Version : 02

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

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
<ol style="list-style-type: none"> 1. Email GTL's for campaign UAT 2. Setup Test Computer to be used for the activity.

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

Technical Configuration Procedures

I. PART A (Firewall Configuration)

1. Access **THOR** and **G2 FW** via https.

2. Go to **Services > Create New > Category** > then create the following:

New Service Category	Open Access BPO Services	
Name:	ICMP	
Protocol Type:	ICMP	
Type:	<blank>	

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

Code:	<blank>	
Name:	6780 - 6781 / TCP	5228 / TCP (Google Service)
Protocol Type:	TCP/UDP	TCP/UDP
Destination Port:	TCP 6780 - 6781	TCP 5228
Name:	443 / TCP (HTTPS)	8083 / TCP & UDP (us-srv)
Protocol Type:	TCP/UDP	TCP/UDP
Destination Port:	TCP 443	TCP 8083 UDP 8083
Name:	10000 - 65535 / UDP (RTP)	5091 / TCP (CXTP)
Protocol Type:	TCP/UDP	TCP/UDP
Destination Port:	UDP 10000 - 65535	TCP 5091
Name:	5060 / TCP & UDP (SIP)	5091 / SCTP (SIP)
Protocol Type:	TCP/UDP	TCP/UDP
Destination Port:	TCP 5060 UDP 5060	SCTP 5091

3. Navigate to **Policy & Objects > IPv4 Policy**

Create the following policies:

Policy for UAT – **Privileged Access USColo**
 Policy for UAT – **Privileged Access FSSO Zenefits**
 Policy for UAT – **CatchAll Policy FSSO Zenefits**
 Policy for UAT – **CatchAll Policy FSSO BackOffice (#HR)**
 Policy for UAT – **Bypass Policy for Postmates RC**
 Policy for UAT – **Privileged Access FSSO Postmates**
 Policy for UAT – **CatchAll Policy FSSO Postmates**
 Policy for UAT – **CatchAll Policy RA_QA**
 Policy for UAT – **CatchAll Policy Workforce**
 Policy for UAT – **CatchAll Policy Security**
 Policy for UAT – **CatchAll Policy Executive**

Once the policies were created, place them to the highest sequence number.

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

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

Name: Test Policy for UAT – **Campaign Name**

Incoming Interface: Internal(port5)

Outgoing Interface: SD-WAN

Source: "**10.20.1.0 /24**"

Destination: "**EXT_SUB_USCOLO
EXT_GR_CEBUPAC_SSH
EXT_GR_VOIPPHONE**"

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

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**

	Proprietary and Confidential	Effectivity: April 1, 2019	Page 5
			Template Version : 02

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

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 #6 for **G2 FW**.

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 created UAT 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**.

II. Core Switch Configuration

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

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
```

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 the following:

THOR 172.16.1.2

- Policy for UAT – **Privileged Access USColo**
- Policy for UAT – **Privileged Access FSSO Zenefits**
- Policy for UAT – **CatchAll Policy FSSO Zenefits**
- Policy for UAT – **CatchAll Policy FSSO BackOffice (#HR)**
- Policy for UAT – **Bypass Policy for Postmates RC**
- Policy for UAT – **Privileged Access FSSO Postmates**
- Policy for UAT – **CatchAll Policy FSSO Postmates**
- Policy for UAT – **CatchAll Policy RA_QA**
- Policy for UAT – **CatchAll Policy Workforce**
- Policy for UAT – **CatchAll Policy Security**
- Policy for UAT – **CatchAll Policy Executive**

MKT-GL2-FW1 172.22.0.74

- Policy for UAT – **Privilege Access USColo**
- Policy for UAT – **Bypass Policy for WV Apps**
- Policy for UAT – **Privilege Access WorldVentures**
- Policy for UAT – **CatchAll WorldVentures**
- Policy for UAT – **Privilege Access AVA**
- Policy for UAT – **CatchAll AVA**

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

Policy for UAT – **CatchAll Quora International**
Policy for UAT – **CatchAll Quora English**
Policy for UAT – **CatchAll Recruitment**
Policy for UAT – **Privileged Access UIPath**
Policy for UAT – **CatchAll UIPath**
Policy for UAT – **Privileged Access NDY**
Policy for UAT – **CatchAll Policy NDY**

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
SIP – TCP & UDP
SIP 2 – TCP & UDP
Google Service – TCP
STUN - UDP
SNMP – UDP

C. Access **ZEUS** and **G2-MKT-CSW** via **SSH**.

Type the following commands to delete VLAN 500

no vlan 500
no int vlan 500
do wr