

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 – 27, 2019			
Proposed Change Start/End Time	5 PM of April 20 until the UAT is completed			
Proposed Change Verification Time	Until the UAT is completed			

Objective of the change
To limit all the specific outbound TCP/UDP ports of all Business units that are in scope of PCI DSS.

Technical/Operational Impact of the change		
Negative: Additional CPU, Memory, and Disk utilization due to added Ipv4 Policies.	Beneficial: To limit all the specific outbound TCP/UDP ports of all Business units that are in scope of PCI DSS. Mitigation of any security threats like IP Spoofing.	Neutral: N/A

Affected IT Infrastructure components			
Site	Hostname	IP Address	Function
JAKA	THOR	172.16.1.2	Site Firewall
G2	MIDAS	172.22.0.74	Site Firewall

Affected Departments and corresponding contact persons		
Department	Contact Name	Contact Info
Zenefits	Allan Madarico	amadarico@openaccessbpo.com
Postmates, Quora	Myka Florendo	mflorendo@openaccessbpo.com
World Ventures	Clint Ortiz	cortiz@openaccessbpo.com
UI Path	Nate Martinez	nmartinez@openaccessbpo.com
Ava Women	Crissy Tuazon	ctuazon2@openaccessbpo.com
IT	Rynel Yanes	09178535630
Network Operations	Maurice Mendoza	09176328103

Test Environment implementation and Verification Summary
<ol style="list-style-type: none"> 1. Coordinate with GTLs and Campaign Managers that are in the above contacts regarding the names of Agents that will do the UAT per campaigns. 2. Get the station's IP address of the Agent. 3. Create a test IPv4 Policy in Jaka and G2 Firewall with the following details: <p>Name: UAT Policy Incoming Interface: Internal(port5)</p>

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

Outgoing Interface: SD-WAN
 Source: "IP Address of the station that the Agent is using"
 Destination: All
 Schedule: Always
 Service: "Service ports per 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

- Have the Agent do a UAT including Campaign tools and Website Accesses.
- Repeat steps 2 to 4 then change the Source, Web Filter, and Application Control per Campaign.
- Once verified and accepted by the representative of each Campaign, proceed to the implementation then delete the Test IPv4 Policy.

Test Environment Results Summary

Results will be based on the User Acceptance Testing. Once completed and accepted, the implementation will be conducted.

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

Configuration Change Template

Baseline File	3.1.401, 3.1.402
Baseline Version	April 3, 2019

Baseline File Changes:

Existing Configuration	Proposed Change	Impact	Section
All IPv4 policies are using the Outbound port "All".	To set all Outbound ports of all Business units that are in scope of PCI DSS to Campaign Specifics. Check the link for list of Service ports.	IPv4 Policies, Services	3.1.401, 3.1.402

Physical Implementation Procedures / Advisory

Send an email to all the GTLs and Campaign Managers that will be affected during the implementation.

"Everyone,

We will be having Network Maintenance and testing this coming Saturday, April 27 between 6 pm - 9 pm. No expected downtime for the said maintenance. The IT team will be on standby for support.

For any concerns please email us at itgroup@openaccessmarketing.com

Thank you.

Regards,"

Backup Procedures

Access FortiGate Jaka and G2 via Web Browser.

Backup the configurations files using the naming conventions:

BACKUP_DEVICENAME_DATE.cfg

Example: BACKUP_THOR_4272019.cfg, BACKUP_MIDAS_4272019.cfg

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

Physical Implementation Procedures
No physical implementations for this change.

Technical Configuration Procedures
<p>I. PART A (THOR Configuration)</p> <ol style="list-style-type: none"> 1. Access ZEUS via https 172.16.1.2. 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.</p> <p>Name: HTTPS - TCP Category: Open Access BPO Services PCI-DSS Protocol Type: TCP/UDP IP/FQDN: <blank> Destination Port: TCP 443</p> <p>Press OK.</p> <p>Name: RTP - UDP Category: Open Access BPO Services PCI-DSS Protocol Type: TCP/UDP</p>

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

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

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**

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

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

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

IP/FQDN: <blank>

Destination Port: **SCTP | 5091**

Press **OK**.

3. Navigate to Policy & Objects > IPv4 Policy

Locate the following policies:

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

4. Change the Services of “Privilege Access USColo” from all to the following:

6780 – 6781 - TCP
SIP – TCP & UDP
HTTPS - TCP
HTTP
RTP - UDP
ICMP

5. Change the Services of “Privileged Access FSSO Zenefits” from all to the following:

HTTPS - TCP
ICMP
Google Service – TCP
STUN - UDP

6. Change the Services of “CatchAll Policy for FSSO Zenefits” from all to the following:

HTTPS - TCP
ICMP
Google Service – TCP

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

STUN - UDP

7. Change the Services of “**CatchAll Policy FSSO BackOffice**” from **all** to the following:

HTTPS - TCP
ICMP

8. Change the Services of “**Bypass Policy for Postmates RC**” from **all** to the following:

EXT_SVC_RingCentral_Ports:

HTTPS - TCP
us-srv – TCP & UDP
RTP - UDP
CXTP – TCP
ICMP

9. Change the Services of “**Privilege Access FSSO Postmates**” from **all** to the following:

HTTPS
Google Service – TCP
ICMP

10. Change the Services of “**Privilege Access FSSO Postmates**” from **all** to the following:

HTTPS
Google Service – TCP
ICMP

11. Change the Services of “**CatchAll Policy RA_QA**” from **all** to the following:

443 / TCP (HTTPS)
ICMP

12. Change the Services of “**CatchAll Policy Workforce**” from **all** to the following:

443 / TCP (HTTPS)
ICMP

13. Change the Services of “**CatchAll Policy Security**” from **all** to the following:

443 / TCP (HTTPS)
ICMP

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

14. Change the Services of “CatchAll Policy Executive” from **all** to the following:

443 / TCP (HTTPS)
ICMP

II. PART C (MKT-GL2-FW1 Configuration)

1. Access **MKT-GL2-FW1** via https **172.22.0.74**
2. Go to **Services > Create New > Category >** then type the following:

New Service Category

Name: Open Access BPO Services | PCI-DSS
Comments: <blank>

Press **OK**.

Once created, create new **Services** with the following:

Name: **ICMP**
Category: **Open Access BPO Services | PCI-DSS**
Protocol Type: **ICMP**
Type: <blank> #blank means **ALL** for this service
Code: <blank>

Press **OK**.

Create another **Services** with the following:

Name: **6780 – 6781 - TCP**
Category: **Open Access BPO Services | PCI-DSS**
Protocol Type: **TCP/UDP**
IP/FQDN: <blank>
Destination Port: **TCP | 6780 - 6781**

Press **OK**.

Name: **HTTPS - TCP**
Category: **Open Access BPO Services | PCI-DSS**
Protocol Type: **TCP/UDP**
IP/FQDN: <blank>
Destination Port: **TCP | 443**

Press **OK**.

Name: **RTP - UDP**
Category: **Open Access BPO Services | PCI-DSS**

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

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

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**.

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

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. Navigate to Policy & Objects > IPv4 Policy

Locate the following policies:

Privileged Access USColo
Bypass Policy for WV Apps
Privilege Access WorldVentures
CatchAll AVA
CatchAll Quora International
CatchAll Quora English
CatchAll Recruitment
Privileged Access UIPath
CatchAll UIPath
Privileged Access NDY
CatchAll Policy NDY

4. Change the Services of “Privilege Access USColo” from all to the following:

6780 – 6781 - TCP
SIP – TCP & UDP
HTTPS - TCP
HTTP
RTP - UDP
ICMP

5. Change the Services of “Bypass Policy for WV Apps” from all to the following:

HTTPS - TCP
ICMP
RTP - UDP

6. Change the Services of “Privilege Access WorldVentures” from all to the following:

HTTPS - TCP
ICMP
Google Service – TCP

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

7. Change the Services of “**CatchAll WorldVentures**” from **all** to the following:

HTTPS - TCP
ICMP
Google Service – TCP

8. Change the Services of “**Privileged Access AVA**” from **all** to the following:

HTTPS - TCP
ICMP
STUN - UDP

9. Change the Services of “**CatchAll AVA**” from **all** to the following:

HTTPS - TCP
ICMP
STUN - UDP

10. Change the Services of “**CatchAll Quora International**” from **all** to the following:

HTTPS - TCP
ICMP
Google Service – TCP
STUN - UDP

11. Change the Services of “**CatchAll Quora English**” from **all** to the following:

HTTPS - TCP
ICMP
Google Service – TCP
STUN - UDP

15. Change the Services of “**CatchAll Policy Recruitment**” from **all** to the following:

443 / TCP (HTTPS)
ICMP

12. Change the Services of “**Privileged Access UIPath**” from **all** to the following:

HTTPS - TCP
ICMP
STUN - UDP
SIP_2 – Sctp
Google Service – TCP

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

13. Change the Services of “**CatchAll UIPath**” from **all** to the following:

HTTPS - TCP
ICMP
STUN - UDP
SIP_2 – SCTP
Google Service – TCP

14. Change the Services of “**Privileged Access NDY**” from **all** to the following:

HTTPS - TCP
ICMP

15. Change the Services of “**CatchAll Policy NDY**” from **all** to the following:

HTTPS - TCP
ICMP

Verification Procedures

I. Firewall Configuration

1. Login to **THOR** and **MKT-GL2-FW1** via **https** respectively.
2. **Navigate to Policies & Objects > IPv4 Policy**, verify that the ports properly assigned to the “**Service**” of the following:

(THOR) 172.16.1.2

Privileged Access USColo
 Bypass Policy for WV Apps
 Privilege Access WorldVentures
 CatchAll AVA
 CatchAll Quora International
 CatchAll Quora English
 CatchAll Recruitment
 Privileged Access UIPath
 CatchAll UIPath
 Privileged Access NDY
 CatchAll Policy NDY

(MKT-GL2-FW-1) 172.22.0.74

Privileged Access USColo
 Bypass Policy for WV Apps
 Privilege Access WorldVentures
 CatchAll AVA
 CatchAll Quora International
 CatchAll Quora English

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

Privileged Access UIPath CatchAll UIPath Privileged Access NDY CatchAll Policy NDY 3. Get a PC from each campaigns that policies were recently configured and check the internet connection. 4. Do a test browsing that is included in the policy, once traffic is generated, check the "Bytes" column on the IPv4 policy . <div style="border: 1px solid #ccc; padding: 5px; width: fit-content; margin: 10px auto;"> <div style="background-color: #f0f0f0; padding: 2px 10px; text-align: center;">Bytes</div> <div style="border-top: 1px solid #ccc; padding-top: 2px;"> 60.28 GB </div> </div>

Back-out Procedures
<p>A. Locate the following IPv4 policies then change the Services to all.</p> <p>THOR: Privileged Access USColo Bypass Policy for WV Apps Privilege Access WorldVentures CatchAll AVA CatchAll Quora International CatchAll Quora English CatchAll Recruitment Privileged Access UIPath CatchAll UIPath Privileged Access NDY CatchAll Policy NDY</p> <p>MKT-GL2-FW1: Privileged Access USColo Bypass Policy for WV Apps Privilege Access WorldVentures CatchAll AVA CatchAll Quora International CatchAll Quora English CatchAll Recruitment Privileged Access UIPath CatchAll UIPath Privileged Access NDY</p>

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

CatchAll Policy NDY

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

THOR:

6780 – 6781 - TCP

SIP – TCP & UDP

HTTPS - TCP

RTP - UDP

ICMP

Google Service – TCP

STUN – UDP

us-srv – TCP & UDP

CXTP – TCP

MKT-GL2-FW1:

6780 – 6781 - TCP

SIP – TCP & UDP

HTTPS - TCP

RTP - UDP

ICMP

Google Service – TCP

STUN – UDP

us-srv – TCP & UDP

CXTP – TCP

SIP_2 – SCTP