Request Information				
Requestor	Network Operations			
Implementing Team	Network Operations			
Ticket Number/s	201916556			
Change Classification	X	Major		Minor
After the fact		Yes	X	No
Emergency		Yes	X	No
Proposed Change Date	June 22, 2019			
Proposed Change Start/End Time	18:00			
Proposed Change Verification Time	18:30			

Objective of the change
To implement the changes for the recommended allowed ports and access to InContact servers on our G2 firewall IPv4 policy.

Technical/Operational Impact of the change		
Negative: Business unit downtime due to misconfiguration.	Beneficial: Allowing of mentioned InContact servers and service ports outbound.	Neutral: Isolation of problem if it will persist after the change,

Affected IT Infrastructure components			
Site	Hostname	IP Address	Function
G2	MKT-GL2-FW1	172.17.3.102	Network Firewall

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

Test Environment implementation and Verification Summary
No test environment is needed for the change as this was previously done by the Network Ops team. Referenced change: **T-CMG-3.1-Configuration-Change-Template – InContact New Address.docx** | Submitted on January 3, 2019

Test Environment Results Summary
Expected change result are the IP addresses mentioned by **InContact** through Kandy that is not currently in our policy will be added.

Configuration Change Template

Baseline File	3.1.10.2, 3.1.10.3, 3.1.10.4
Baseline Version	May 24, 2019

Baseline File Changes:

Existing Configuration	Proposed Change	Impact	Section
MKT-GL2-FW1: Bypass Policy for WV Apps: No outbound IP for **199.172.8.0/24, 199,172.9.0/24, 61.14.30.129/27, 210.25.25.128/28, 200.15.3.0/24, 61.14.30.16/28**	**MKT-GL2-FW1:** Bypass Policy for WV Apps: Add the following Network Addresses: **199.172.8.0/24, 199,172.9.0/24, 61.14.30.129/27, 210.25.25.128/28, 200.15.3.0/24, 61.14.30.16/28**	Network Uplinks of InContact servers will be added on the policy	3.1.10.2

Physical Implementation Procedures / Advisory
No Physical Implementation will be conducted for this change.

Backup Procedures
1. Login to **MKT-GL2-FW1** via **https**. 2. Click on the **user > Backup configuration** 3. Save the file to \\172.17.0.124\it\Backup\Network Backup Logs   With naming convention: HOSTNAME_201906XX

Technical Configuration Procedures
1. Login to **MKT-GL2-FW1 172.17.3.102:10443** via **https**. 2. Navigate to **Policy & Objects** > **Addresses** > **Create New Address** with the following info: Name: **EXT_SVR_InContact_34 (++)** Type: **Subnet** Subnet / IP Range: **199.172.8.0/24** Interface: **Any** Show in Address List: **Enabled** Static Route Configuration: Disabled

Click **OK**.

Note: Repeat the steps for the following network addresses:
199.172.9.0/24
61.14.30.129/27
210.25.25.128/28
200.15.3.0/24
61.14.30.16/28

3. Navigate to **Policy & Objects** > **Addresses** search for Address Group **EXT_SVR_INCONTACT**.

4. Once opened, add the created Address Objects **EXT_SVR_InContact_34**up to **39.**

Verification Procedures

1. Navigate to **Policy & Objects** > **Addresses** search for Address Group **EXT_SVR_INCONTACT**.

2. Verify by looking if the **EXT_SVR_InContact_34**up to **39** address objects are added on the group.

3. Test on WV Workstations if their current issue on InContact persist.

Back-out Procedures

1. Navigate to **Policy & Objects** > **Addresses** search for Address Group **EXT_SVR_INCONTACT**.

2. Remove the **Address Objects EXT_SVR_InContact_34**up to **39** in the address group.

3. Go to **Address Objects,** search and delete for **EXT_SVR_InContact_34**up to **39.**