Request Information				
Requestor	Ian John Lastimoso			
Implementing Team	Network Operations			
Ticket Number/s	201915367			
Change Classification	X	Major		Minor
After the fact		Yes	X	No
Emergency		Yes	X	No
Proposed Change Date	May 19, 2019			
Proposed Change Start/End Time	6:00 PM			
Proposed Change Verification Time	7:00 PM			

Objective of the change
To Add Ring Central Ports on Service on Ipv4 Policy of UIPath To Add Citrix Receiver Ports on Service on Ipv4 Policy of NDY

Technical/Operational Impact of the change		
Negative: High Utilization of CPU and Memory since this require configuration inside the firewall	Beneficial: Ring Central calls will push through since we are able to add the right port number on our end Citrix will be able to run more smoothly once all the ports required are allowed on our end	Neutral: Other Ipv4 policies on G2 Firewall

Affected IT Infrastructure components			
Site	Hostname	IP Address	Function
G2	MKT-GL2-FW-1	172.22.0.75	Firewall

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

Test Environment implementation and Verification Summary
N/A

Test Environment Results Summary
N/A

Configuration Change Template

Baseline File	3.1.10.2
Baseline Version	As of March 01, 2019

Baseline File Changes:

Existing Configuration	Proposed Change	Impact	Section
Services consists of HTTPS – TCP , ICMP , STUN – UDP , SIP_2 SCTP , Google Services - TCP Temporarily on a all service to monitor connectivity to Citrix	Adding of Ring Central Ports namely *port 8801 , 8802 , SRTP – 5097 , RTP* Allow / Add the following Citrix Ports – Port 21 , 53, 123 , 80 , 443 , 389 , 514 , 636 , 1494 , 1812 , 2598 , 3268 , 3269, 9080 , 30001 , 9443 , 45000 , 8443 , 27000 , 161 . All ports included above are need for Citrix	Coming calls will be handled properly without issues.	3.1.10.2

Physical Implementation Procedures / Advisory
N/A

Backup Procedures
I. Part A (Firewall Configuration) 1. Access G2 Firewall (https://172.22.0.75:10443) 2. Backup Configuration with the following naming convention and then save it inside \\172.17.0.124 \IT\Back up\G2_FW 3. BACKUP;Device;Date;Time,.Extension e.g. BACKUP_G2_07152017_17:45.cfg

Physical Implementation Procedures

N/A

Technical Configuration Procedures

I. PART A (UIPATH) (Firewall Configuration)

A. Login to Fortigate G2 (https://172.22.0.75:10443)
B. Go to **Policy & Objects** > **Services** > **Create New** > **Service** >

Name: 8801 – TCP
Category: Open Access BPO
Protocol Type: TCP/UDP/SCTP
Destination Port: TCP | 8801

Name: 8802 – TCP
Category: Open Access BPO
Protocol Type: TCP/UDP/SCTP
Destination Port: TCP | 8802

C. Navigate to *Policy & Objects > IPv4 Policy > Click on By Sequence > Find ID #19 & #20 "CatchAll UIPath and #11 Privileged Access UIPath*
D. Click on "*CatchAll UIPath and Privileged Access UIPath" then Edit*
E. Navigate to Services > Click on it > Click on ***HTTPS – TCP , ICMP , STUN – UDP, SCTP , 5228 – TCP , 10000 – 65535 / UDP , 8802 – TCP , 8801 – TCP***
F. Click on **OK**
G. ***Repeat Step C to E for Privileged Access UIPATH***

II. PART B (NDY) (Firewall Configuration)

A. Navigate to Policy & Object > Services > Create New > Services

Name: 21 – TCP
Category: Open Access BPO
Protocol Type: TCP
Destination Port: TCP | 21

Name: 53 – TCP
Category: Open Access BPO
Protocol Type: TCP
Destination Port: TCP | 53

Name: 123 – TCP
Category: Open Access BPO
Protocol Type: TCP
Destination Port: TCP | 123 / UDP | 213

Name: 389 – TCP
Category: Open Access BPO
Protocol Type: TCP
Destination Port: TCP | 389

Name: 514 – TCP
Category: Open Access BPO
Protocol Type: TCP
Destination Port: TCP | 514

Name: 1494 – TCP
Category: Open Access BPO
Protocol Type: TCP
Destination Port: TCP | 1494

Name: 1812 – TCP
Category: Open Access BPO
Protocol Type: TCP
Destination Port: TCP | 1812

Name: 2598 – TCP
Category: Open Access BPO
Protocol Type: TCP
Destination Port: TCP | 2598

Name: 3268 – TCP
Category: Open Access BPO
Protocol Type: TCP
Destination Port: TCP | 3268

Name: 3269 – TCP
Category: Open Access BPO
Protocol Type: TCP
Destination Port: TCP | 3269

Name: 9080 – TCP
Category: Open Access BPO
Protocol Type: TCP
Destination Port: TCP | 9080

Name: 30001 – TCP
Category: Open Access BPO
Protocol Type: TCP
Destination Port: TCP | 30001

Name: 9443 – TCP
Category: Open Access BPO
Protocol Type: TCP
Destination Port: TCP | 9443

Name: 8443 – TCP
Category: Open Access BPO
Protocol Type: TCP
Destination Port: TCP | 8443

Name: 27000 – TCP
Category: Open Access BPO
Protocol Type: TCP
Destination Port: TCP | 27000

Name: 7279 – TCP
Category: Open Access BPO
Protocol Type: TCP
Destination Port: TCP | 7279

Name: 161 – TCP
Category: Open Access BPO
Protocol Type: TCP
Destination Port: TCP | 161

Name: 162 – TCP
Category: Open Access BPO
Protocol Type: TCP
Destination Port: TCP | 162

B. Navigate to *Policy & Objects > IPv4 Policy > Click on By Sequence > Find ID #22 & #23 "CatchAll NDY and #11 Privileged Access NDY*
C. Click on "*CatchAll UIPath and Privileged Access UIPath" then Edit*
Navigate to Services > Click on it > Click on **HTTPS , HTTP , PORT 21, 53 , 123, 123, 389, 514, 636, 1494, 1812, 2598, 3268, 3269, 9080, 30001, 9443, 8443, 27000, 7279, 161 & 162.**
D. Click **OK.**
E. Repeat **B** to **C** for ***Privileged Access NDY Policy***

Verification Procedures

I. Verification for UIPATH

1. Most important verification must be, Call should be passing thru already after the change has been made, Customer must be able to hear agent – Agent should be able to hear customer.

2. Test call first agent to agent if they will be able to call each other and will be able to hear each other

3. Ask agent if they can call outbound, As confirming with an agent their ring central can call a local mobile phone number. Ask an agent to call IT mobile number or your personal number to test if you will be able to hear other.

4. If all test fails. Proceed with backout procedure.

II. Verification for NDY

1. Confirm on users that the Citrix loads normally even after removing the *All options* On the services.
2. Verification may last for two day just for confirmation that It really loads and works normally.
3. If verification fails and the Citrix loads slowly, Proceed with the back-out procedure

Back-out Procedures

I. Back-out Procedures for UIPATH

A. Navigate to *Policy & Objects > IPv4 Policy > Click on By Sequence > Find ID #19 & #20 "CatchAll UIPath and #11 Privileged Access UIPath*
B. Click on "*CatchAll UIPath and Privileged Access UIPath" then Edit*
C. Navigate to Services > Click on it > Click on ***All***
D. Click on **OK**
E. ***Repeat Step D to E for Privileged Access UIPATH***

II. Back-out Procedures for NDY

A. Navigate to *Policy & Objects > IPv4 Policy > Click on By Sequence > Find ID #22 & #23 "CatchAll NDY and #11 Privileged Access NDY*
A. Click on "*CatchAll NDY and Privileged Access NDY" then Edit*
B. Navigate to Services > Click on it > Click on ***All***

C. Click on **OK**

E. ***Repeat Step D to E for Privileged Access NDY***