Request Information				
Requestor	Ian John Lastimoso			
Implementing Team	Network Operations			
Ticket Number/s	201916990			
Change Classification	X	Major		Minor
After the fact	X	Yes		No
Emergency	X	Yes		No
Proposed Change Date	June 04, 2019			
Proposed Change Start/End Time	8:30 AM			
Proposed Change Verification Time	9:00 AM			

Objective of the change
To Add VMWare Ports for Digicast Service Ports

Technical/Operational Impact of the change		
Negative: High Utilization of CPU and Memory since this require configuration inside the firewall	Beneficial: Digicast will now be able to use the VMWare Application since service ports will be added to their Ipv4 policy.	Neutral: Web Filter, Application Control and Respective Ipv4 policy of other Business unit.

Affected IT Infrastructure components			
Site	Hostname	IP Address	Function
Jaka	THOR	172.17.3.101:10443 or https://thor.openaccessbpo.com	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
No test can take place since this is an Emergency Change Document

Test Environment Results Summary
No test can take place since this is an Emergency Change Document

Configuration Change Template

Baseline File	3.1.10.2 , 3.1.11.3
Baseline Version	As of March 01, 2019

Baseline File Changes:

Existing Configuration	Proposed Change	Impact	Section
No Existing Service Ports on Digicast for VMWare since this is a new Application for the Business Unit	Adding of Ports for Digicast Service Ports TCP / UDP – 4172 UDP – 50002 TCP – 55000	VMWare Application will now be accessible	3.1.402

Backup Procedures

I. Part A (Firewall Configuration)

1. Access THOR Firewall (https://172.17.0.101:10443)
2. Backup Configuration with the following naming convention and then save it inside \\172.17.0.124 \IT\Back up\THOR_FW
3. BACKUP;Device;Date;Time,.Extension e.g. BACKUP_G2_07152017_17:45.cfg

Technical Configuration Procedures

I. PART A (Firewall Configuration)

A. Login to Fortigate THOR (https://172.17.3.101:10443)

B. Go to **Policy & Objects** > **Services** > **Create New** > **Service** >

Name: VMWare Port_1
Category: Open Access BPO
Protocol Type: TCP/UDP/SCTP
Destination Port: TCP | 4172
Destination Port: UDP | 4172

Name: VMWare Port_2
Category: Open Access BPO
Protocol Type: TCP/UDP/SCTP
Destination Port: UDP | 50002

Name: VMWare Port_3
Category: Open Access BPO
Protocol Type: TCP/UDP/SCTP
Destination Port: TCP | 55000

C. Go to **Policy & Objects** > **Services** > **Zenefits Service Ports**

Add the following Ports to its Members, **VMWare Port_1, VMWare Port_2, VMWare Port_3**

Verification Procedures

1. To Verify tonight on Geoff's shift because Geoff's Team uses the mentioned Application.
2. User should be able to connect to the VM Desktop on the VMWare Application without any issues.

Back-out Procedures

I. PART A (Firewall Configuration)

1. Access Firewall via Web browser *https://172.17.3.101:10443*

2. Go to **Policy & Objects** > **Services** > **Zenefits Service Ports**

   Remove the following Ports to its Members, **VMWare Port_1, VMWare Port_2, VMWare Port_3**

   Click **OK.**