Request Information				
Requestor	Network Operations			
Implementing Team	Network Operations			
Ticket Number/s	20191577			
Change Classification	X	Major		Minor
After the fact	X	Yes		No
Emergency	X	Yes		No
Proposed Change Date	This config request was already implemented.			
Proposed Change Start/End Time	This config request was already implemented.			
Proposed Change Verification Time	This config request was already implemented.			

Objective of the change
To restrict the specific network which can access the core, access switch. Hardening of access of Network Firewalls.

Technical/Operational Impact of the change		
Negative: Possible switch lockout due to misconfiguration. Possible firewall lockout due to misconfiguration	Beneficial: Core, Access Switch, Firewall Hardening,	Neutral: Workstations, User Accounts

Affected IT Infrastructure components			
Site	Hostname	IP Address	Function
JAKA	THOR	172.16.1.2	Network Firewall
G2	MKT-GL2-FW1	172.22.0.75	Network Firewall
JAKA	ODYSSEUS	10.1.0.254	Network Firewall
JAKA	ZEUS	172.31.1.1	Network Core Switch
G2	MKT-GL2-CSW1	172.22.2.1	Network Core Switch
JAKA	Morpheus	172.17.3.107	Network Access Switch
JAKA	Poseidon	172.17.3.108	Network Access Switch
JAKA	Erebus	172.17.3.109	Network Access Switch
JAKA	Janus	172.17.3.110	Network Access Switch
JAKA	Cyclops	172.17.3.111	Network Access Switch
JAKA	Medusa	172.17.3.112	Network Access Switch
JAKA	Nyx	172.17.3.113	Network Access Switch
JAKA	Hera	172.17.3.114	Network Access Switch
JAKA	Switch5_1	172.17.3.115	Network Access Switch
JAKA	Switch5_2	172.17.3.116	Network Access Switch
JAKA	Switch5_3	172.17.3.117	Network Access Switch
JAKA	Switch5_4	172.17.3.118	Network Access Switch
JAKA	Switch5_5	172.17.3.119	Network Access Switch
JAKA	Switch5_6	172.17.3.120	Network Access Switch
JAKA	Switch5_7	172.17.3.121	Network Access Switch
JAKA	Switch3_1	172.17.3.122	Network Access Switch

JAKA	Switch3_2	172.17.3.123	Network Access Switch
JAKA	Switch3_3	172.17.3.124	Network Access Switch
G2	MKT-GL2-CSW-1	172.17.3.125	Network Access Switch
G2	MKT-GL2-SW-A1 -	172.17.3.126	Network Access Switch
G2	MKT-GL2-SW-A2 -	172.17.3.127	Network Access Switch
G2	*MKT-GL2-SW-A3	172.17.3.128	Network Access Switch
G2	*MKT-GL2-SW-A4	172.17.3.129	Network Access Switch
G2	*MKT-GL2-SW-A5	172.17.3.130	Network Access Switch
G2	*MKT-GL2-SW-B2	172.17.3.132	Network Access Switch
G2	MKT-GL2-SW-B3 -	172.17.3.133	Network Access Switch

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

Test Environment implementation and Verification Summary
No test environment was implemented since this is emergency ATF change.

Test Environment Results Summary
Expected results is network restriction of access via SSH.

Configuration Change Template

Baseline File	3.1.401, 3.1.10.1
Baseline Version	April 30,2019, Nov 15 2018

Baseline File Changes:

Existing Configuration	Proposed Change	Impact	Section
Firewall Config: Password Policy Special Char: 0 Password expiration: 60 **No existing config on Core/Access Switches for SSH ACL.**	**Firewall Config:** Password Policy Special Char: 1 Password expiration: 60 **Core / Access SW Config:** Access-list extended SSH_IN	Firewall password security improvement. Switches: SSH can only be access from 172.17.3.0/24 network.	3.1.401, 3.1.10.1, 3.1.101, 3.1.11.3

Physical Implementation Procedures / Advisory
No physical implementation and advisory were needed for this change.

Backup Procedures
I. Firewall Backup 1. Access **THOR, MKT-GL2-FW1, ODYSSEUS** Save the backup config to: \\172.17.0.124\it\Backup\Network Backup Logs With the following naming convention: BACKUP_HOSTNAME_201905XX II. Switches Backup 1. Access **ZEUS, MKT-GL2-CSW1, JAKA, G2 switches.** Save the backup config to: \\172.17.0.124\it\Backup\Network Backup Logs With the following naming convention: BACKUP_HOSTNAME_201905XX

Technical Configuration Procedures

I. Firewall Configuration

1. Connect to Fortigate SSL VPN using the dedicated user account.
2. Access **THOR, MKT-GL2-FW1, ODYSSEUS.**
3. Navigate to **System > Settings > System Settings,** configure the **Administration Settings** and **Password Policy**.

Administration Settings:
HTTP port: 8080
Redirect to HTTPS: Enabled
HTTPS port: 10443
HTTPS server certificate: thor.openaccess.bpo/MKT-GL2-FW-1.openaccess.bpo/Odysseus
SSH Port: 4422
Telnet port: 4423
Idle timeout: 5 (Minutes)

Password Policy:
Password scope: Admin
Minimum length: 8
Character requirements: Enabled
Upper Case: 1
Lower Case: 1
Numbers: 1
Special: 1
Allow password reuse: Disabled
Password expiration: Enabled – 90 Days

II. Core Switch Configuration

1. Connect to **FortiGate SSL VPN** using the dedicated user account.
2. Access **ZEUS 172.17.3.106, MKT-GL2-CSW1 172.22.2.1, Jupiter 172.31.1.252** and the following Access switches:

Poseidon	172.17.3.108
Morpheus	172.17.3.107
Erebus	172.17.3.109

Janus	172.17.3.110
Cyclops	172.17.3.111
Medusa	172.17.3.112
Nyx	172.17.3.113
Hera	172.17.3.114

Switch5_1	172.17.3.115
Switch5_2	172.17.3.116
Switch5_3	172.17.3.117
Switch5_4	172.17.3.118
Switch5_5	172.17.3.119
Switch5_6	172.17.3.120
Switch5_7	172.17.3.121

Switch3_1	172.17.3.122
Switch3_2	172.17.3.123
Switch3_3	172.17.3.124

MKT-GL2-SW-A1	172.17.3.126
MKT-GL2-SW-A2	172.17.3.127
MKT-GL2-SW-A3	172.17.3.128
MKT-GL2-SW-A4	172.17.3.129
MKT-GL2-SW-A5	172.17.3.130
MKT-GL2-SW-B2	172.17.3.132
MKT-GL2-SW-B3	172.17.3.133

3. Type the following commands to apply the **ACL** on **SSH** :

Access-list extended SSH_IN
10 permit udp 172.17.3.0 0.0.0.255 any eq 22
20 permit tcp 172.17.3.0 0.0.0.255 any eq 22
90 deny tcp any any
91 deny udp any any
Exit

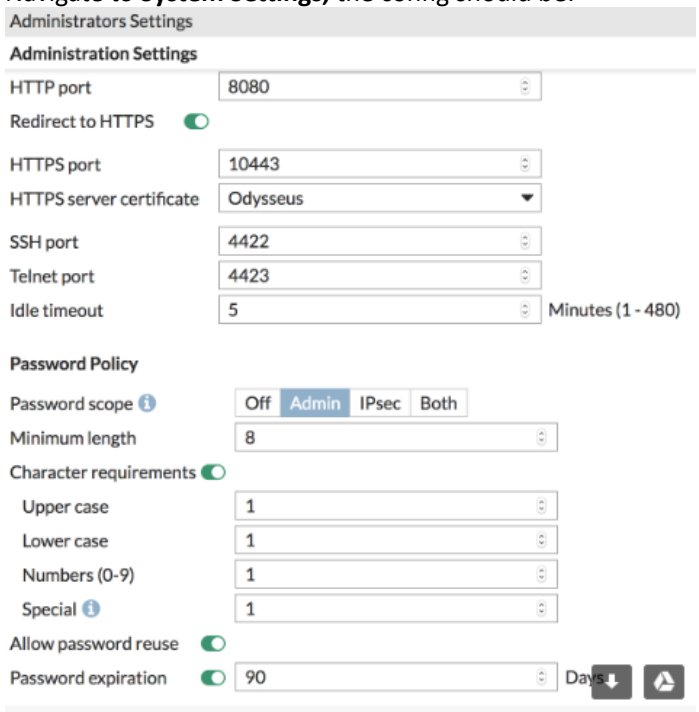
Line vty 0 3
Access-class SSH_IN in
Logging synchronous
Login local
Transport input SSH
Line vty 0 4
Access-class SSH_IN in
Logging synchronous

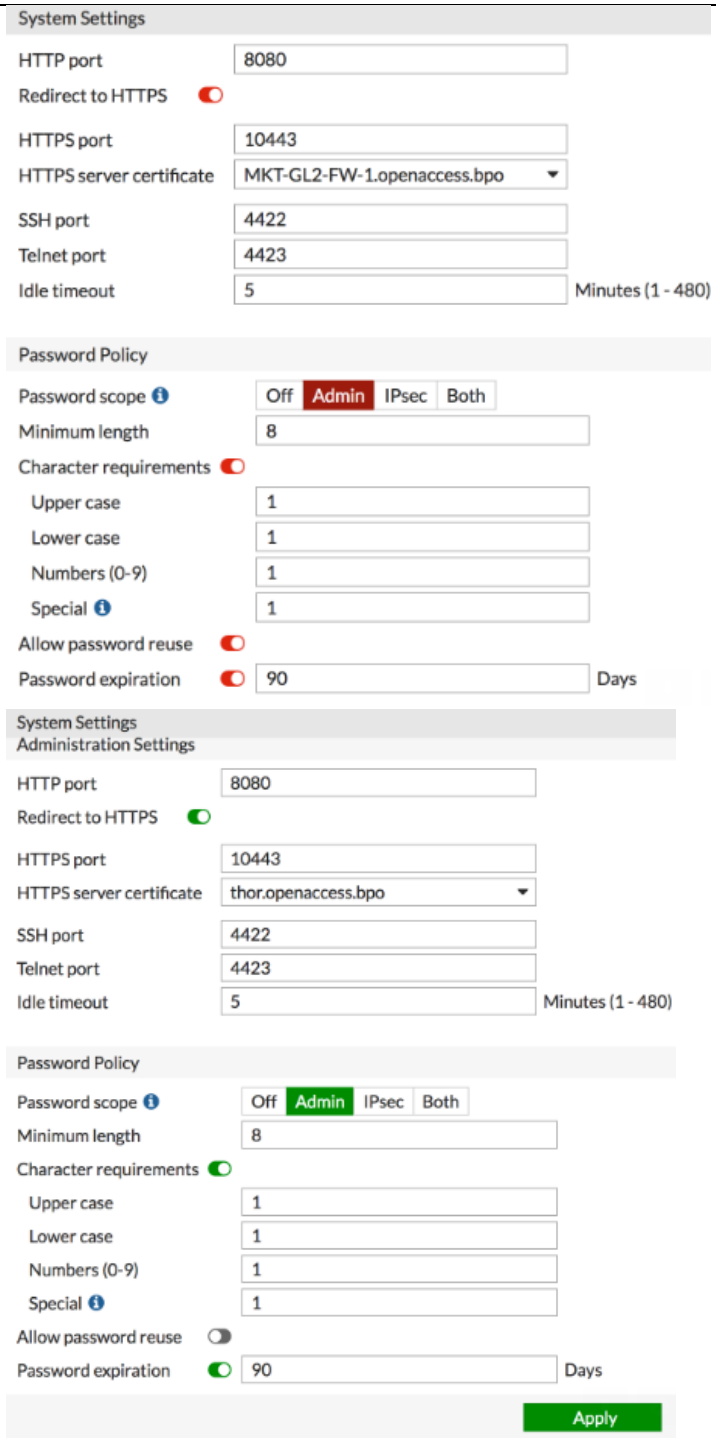
Login local
Transport input none
Line vty 5 15
Access-class SSH_IN in
Login
Transport input none

Verification Procedures

I. Firewall Verification:

1. Access **THOR, MKT-GL2-FW1, ODYSSEUS**.
2. Navigate to **System Settings,** the config should be:





II. Switch Verification

1. Connect to **Fortigate SSL VPN.**
2. Access the switches via **SSH** on their Management (172.17.3.0/24) SVI since the inside IP address of VPN is 172.17.3.0/24.

Back-out Procedures
No back-out procedure was done on this config since this is an ATF.