

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

Request Information				
Requestor	Maurice Mendoza			
Implementing Team	Network Operations			
Ticket Number/s	201915229			
Change Classification	X	Major		Minor
After the fact		Yes	X	No
Emergency		Yes	X	No
Proposed Change Date	May 4, 2019			
Proposed Change Start/End Time	4:00 PM – 10:00 PM			
Proposed Change Verification Time	9:00 PM			

Objective of the change
To have a VPN device in DMZ that will encrypt the Internal Management traffic

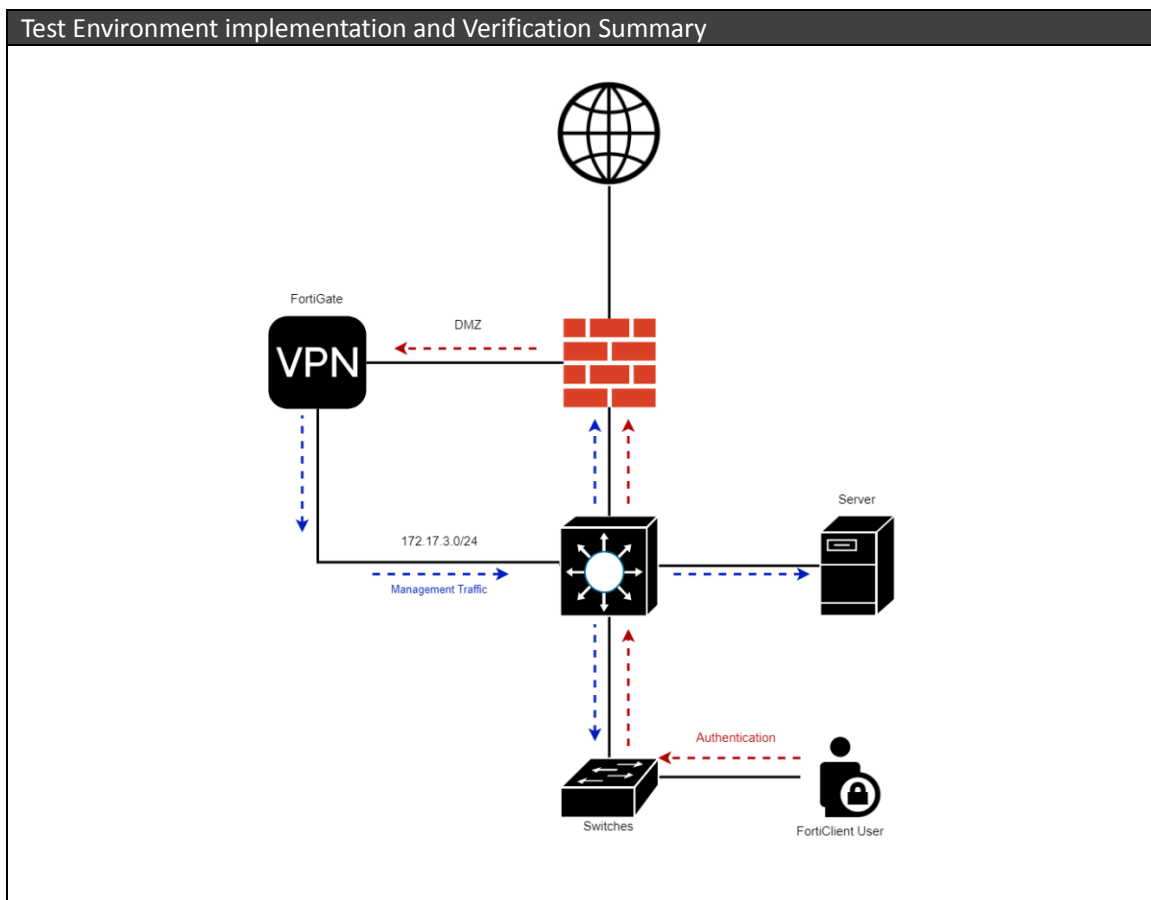
Technical/Operational Impact of the change		
Negative: All Switches and Servers with old IP addresses will be inaccessible.	Beneficial: To have another layer of security before accessing any manageable equipment. To encrypt all traffic of the Management Segment.	Neutral: Access to Access Switches via Console,

Affected IT Infrastructure components			
JAKA	Zeus	172.31.1.1	Core Switch
JAKA	Morpheus	172.31.1.17	Access Switch
JAKA	Poseidon	172.31.1.18	Access Switch
JAKA	Erebus	172.31.1.19	Access Switch
JAKA	Janus	172.31.1.24	Access Switch
JAKA	Cyclops	172.31.1.25	Access Switch
JAKA	Medusa	172.31.1.22	Access Switch
JAKA	Nyx	172.31.1.23	Access Switch
JAKA	Hera	172.31.1.21	Access Switch
JAKA	Switch5_1	172.31.1.29	Access Switch
JAKA	Switch5_2	172.31.1.30	Access Switch
JAKA	Switch5_3	172.31.1.31	Access Switch
JAKA	Switch5_4	172.31.1.32	Access Switch
JAKA	Switch5_5	172.31.1.36	Access Switch
JAKA	Switch5_6	172.31.1.37	Access Switch
JAKA	Switch5_7	172.31.1.38	Access Switch
JAKA	Switch3_1	172.31.1.33	Access Switch

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

JAKA	Switch3_2	172.31.1.34	Access Switch
JAKA	Switch3_3	172.31.1.35	Access Switch
G2	MKT-GL2-CSW-1	172.22.2.1	Core Switch
G2	MKT-GL2-SW-A1	172.22.2.11	Access Switch
G2	MKT-GL2-SW-A2	172.22.2.12	Access Switch
G2	MKT-GL2-SW-A3	172.22.2.13	Access Switch
G2	MKT-GL2-SW-A4	172.22.2.14	Access Switch
G2	MKT-GL2-SW-A5	172.22.2.15	Access Switch
G2	MKT-GL2-SW-B1	172.22.2.21	Access Switch
G2	MKT-GL2-SW-B2	172.22.2.22	Access Switch

Affected Departments and corresponding contact persons		
Department	Contact Name	Contact Info
IT	Rynel Yanes	09178535630
Network Operations	Maurice Mendoza	09176328103
Server Operations	Rovie Salvatierra	09176274325



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

Replicated the current network setup along with the actual VPN unit in the Test Environment. See topology above.

Test Environment Results Summary

The VPN was working upon testing using a FortiClient installed in a PC. After logged in, the test Laptop was able to reach the network 172.17.3.0/24 while still connected to the internet. This is due to the enabled split tunneling.

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

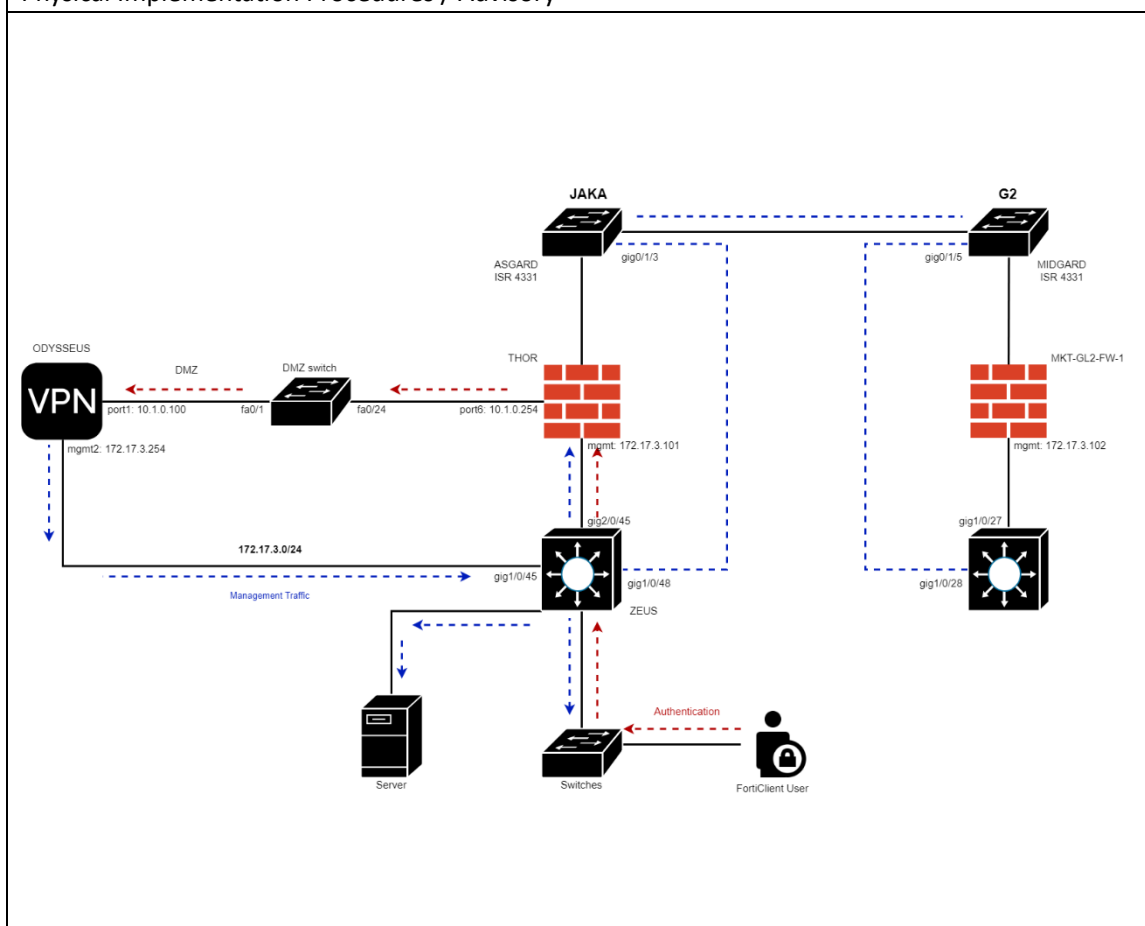
Configuration Change Template

Baseline File	3.1.402, see link for switches: Switch Baseline
Baseline Version	April 18, 2019

Baseline File Changes:

Existing Configuration	Proposed Change	Impact	Section
VLAN 1 is the existing Management VLAN	To add VLAN 1000 for Management Segment	IPv4 Policies, VLAN Database, Port VLAN membership, Switch interfaces	Switch Baseline
No existing VPN device for managing internal equipment	To add a VPN device for management		
	To add IPv4 Policies in Thor for Internal to DMZ and vice versa		

Physical Implementation Procedures / Advisory



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

Send an email to all the Switch and Server Administrators that will be affected after the implementation.

"Team,

Please be advised that we will change the way we access our Equipment. You may need to access the VPN first before accessing the Equipment. We'll provide a KB Article and send you your VPN credentials.

Thank you.

Regards,"

1. Connect port1(DMZ) of ODYSSEUS to port gig0/1 of DMZ SWITCH.
2. Connect mgmt2(Management) of ODYSSEUS to port gig1/0/45 of ZEUS.
3. Connect mgmt of FORTIGATE THOR to port gig2/0/45 of ZEUS.
4. Connect mgmt of MKT-GL2-FW-1 to port gig1/0/27 of MKT-GL2-CSW-1.
5. Connect port gig1/0/48 of ZEUS to port gig0/1/3 of ASGARD ISR 4331.
6. Connect port gig1/0/28 of MKT-GL2-CSW-1 to port gig0/1/5 of MIDGARD ISR 4331.

Backup Procedures

Access FortiGate Jaka and Access Switches.

Backup the configurations files using the naming conventions:

BACKUP_DEVICENAME_DATE.cfg


Example:

Thor	Backup_THOR_542019.cfg
MKT-GL2-FW-1	Backup_MKT-GL2-FW-1_542019.cfg
Zeus	Backup_Zeus_542019.cfg
Morpheus	Backup_Morpheus_542019.cfg
Poseidon	Backup_Poseidon_542019.cfg
Erebus	Backup_Erebus_542019.cfg
Janus	Backup_Janus_542019.cfg
Cyclops	Backup_Cyclops_542019.cfg
Medusa	Backup_Medusa_542019.cfg
Nyx	Backup_Nyx_542019.cfg
Hera	Backup_Hera_542019.cfg
Switch5_1	Backup_Switch5_1_542019.cfg

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

Switch5_2	Backup_Switch5_2_542019.cfg
Switch5_3	Backup_Switch5_3_542019.cfg
Switch5_4	Backup_Switch5_4_542019.cfg
Switch5_5	Backup_Switch5_5_542019.cfg
Switch5_6	Backup_Switch5_6_542019.cfg
Switch5_7	Backup_Switch5_7_542019.cfg
Switch3_1	Backup_Switch3_1_542019.cfg
Switch3_2	Backup_Switch3_2_542019.cfg
Switch3_3	Backup_Switch3_3_542019.cfg
MKT-GL2-CSW-1	Backup_MKT-GL2-CSW-1_542019.cfg
MKT-GL2-SW-A1	Backup_MKT-GL2-SW-A1_542019.cfg
MKT-GL2-SW-A2	Backup_MKT-GL2-SW-A2_542019.cfg
MKT-GL2-SW-A3	Backup_MKT-GL2-SW-A3_542019.cfg
MKT-GL2-SW-A4	Backup_MKT-GL2-SW-A4_542019.cfg
MKT-GL2-SW-A5	Backup_MKT-GL2-SW-A5_542019.cfg
MKT-GL2-SW-B1	Backup_MKT-GL2-SW-B1_542019.cfg
MKT-GL2-SW-B2	Backup_MKT-GL2-SW-B2_542019.cfg

Technical Configuration Procedures
<p>Network Configurations:</p> <p>Odysseus is already configured and ready for deployment.</p> <ol style="list-style-type: none"> Access FORTIGATE THOR via web (https://172.16.1.2:10443). Navigate to Network > Interfaces. Change the mgmt port IP address to the following: <p>IP/Network Mask: 172.17.3.101/255.255.255.0 Administrative Access: HTTPS, PING, FMG-ACCESS, SSH DHCP Server: disable</p> Navigate to Policy & Objects > Addresses. Create new Address Object and Group with the following details. <p>Address Object Name: DMZ_ODYSSEUS(VPN) Type: IP/Netmask Subnet/IP Range: 10.1.0.100</p>

 OPEN ACCESS WE SPEAK YOUR LANGUAGE	Proprietary and Confidential	Effectivity: April 1, 2019	Page 6
			Template Version : 02

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

Address Object

Name: INT_PC_RYANES

Type: IP/Netmask

Subnet/IP Range: 172.18.4.98

Address Group

Name: DMZ_ALLOWED_VPN_HOSTS

Members: INT_SUB_ITOPS, INT_PC_RYANES, INT_SUB_ITOPS_G2

4. Navigate to Policy & Objects > IPv4 Policy. Create new IPv4 Policy for INTERNAL TO DMZ.

Name: Internal To Odysseus(VPN)

Incoming Interface: Internal(port5)

Outgoing Interface: DMZ Network(port6)

Source: DMZ_ALLOWED_VPN_HOSTS

Destination: DMZ_ODYSSEUS(VPN)

Schedule: Always

Service: All

Action: Accept

NAT: Disabled

Log Allowed Traffic: Enabled - All Sessions

Enable this policy: Enabled

5. Navigate to Policy & Objects > IPv4 Policy. Create new IPv4 Policy for DMZ TO INTERNAL.

Name: Odysseus(VPN) To Internal

Incoming Interface: DMZ Network(port6)

Outgoing Interface: Internal(port5)

Source: DMZ_ODYSSEUS(VPN)

Destination: DMZ_ALLOWED_VPN_HOSTS

Schedule: Always

Service: All

Action: Accept

NAT: Disabled

Log Allowed Traffic: Enabled - All Sessions

Enable this policy: Enabled

6. Access MKT-GL2-FW-1 via web (<https://172.22.0.75:10443>)

7. Navigate to Network > Interfaces. Change the mgmt port IP address to the following:

IP/Network Mask: 172.17.3.102/255.255.255.0

Administrative Access: HTTPS, PING, FMG-ACCESS, SSH

DHCP Server: disable

8. Access all switches in the table below via console then copy and paste the commands

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

per switch.

Zeus	configure terminal interface vlan 1 no description no ip address vlan 1000 name MANAGEMENT_SEGMENT interface vlan 1000 description MANAGEMENT_SEGMENT ip address 172.17.3.106 255.255.255.0 interface gigabitEthernet 1/0/45 description TO ODYSSEUS(VPN) switchport access vlan 1000 switchport mode access interface gigabitEthernet 1/0/48 description TO ASGARD switchport access vlan 1000 switchport mode access ip default-gateway 172.17.3.254
Morpheus	configure terminal interface vlan 1 no description no ip address interface vlan 1000 ip address 172.17.3.107 255.255.255.0 ip default-gateway 172.17.3.254
Poseidon	configure terminal interface vlan 1 no description no ip address interface vlan 1000 ip address 172.17.3.108 255.255.255.0 ip default-gateway 172.17.3.254
Erebus	configure terminal interface vlan 1 no description no ip address interface vlan 1000 ip address 172.17.3.109 255.255.255.0 ip default-gateway 172.17.3.254
Janus	configure terminal interface vlan 1 no description no ip address interface vlan 1000

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

		ip address 172.17.3.110 255.255.255.0 ip default-gateway 172.17.3.254	
	Cyclops	configure terminal interface vlan 1 no description no ip address interface vlan 1000 ip address 172.17.3.111 255.255.255.0 ip default-gateway 172.17.3.254	
	Medusa	configure terminal interface vlan 1 no description no ip address interface vlan 1000 ip address 172.17.3.112 255.255.255.0 ip default-gateway 172.17.3.254	
	Nyx	configure terminal interface vlan 1 no description no ip address interface vlan 1000 ip address 172.17.3.113 255.255.255.0 ip default-gateway 172.17.3.254	
	Hera	configure terminal interface vlan 1 no description no ip address interface vlan 1000 ip address 172.17.3.114 255.255.255.0 ip default-gateway 172.17.3.254	
	Switch5_1	configure terminal interface vlan 1 no description no ip address interface vlan 1000 ip address 172.17.3.115 255.255.255.0 ip default-gateway 172.17.3.254	
	Switch5_2	configure terminal interface vlan 1 no description no ip address interface vlan 1000 ip address 172.17.3.116 255.255.255.0 ip default-gateway 172.17.3.254	

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

	Switch5_3	configure terminal interface vlan 1 no description no ip address interface vlan 1000 ip address 172.17.3.117 255.255.255.0 ip default-gateway 172.17.3.254
	Switch5_4	configure terminal interface vlan 1 no description no ip address interface vlan 1000 ip address 172.17.3.118 255.255.255.0 ip default-gateway 172.17.3.254
	Switch5_5	configure terminal interface vlan 1 no description no ip address interface vlan 1000 ip address 172.17.3.119 255.255.255.0 ip default-gateway 172.17.3.254
	Switch5_6	configure terminal interface vlan 1 no description no ip address interface vlan 1000 ip address 172.17.3.120 255.255.255.0 ip default-gateway 172.17.3.254
	Switch5_7	configure terminal interface vlan 1 no description no ip address interface vlan 1000 ip address 172.17.3.121 255.255.255.0 ip default-gateway 172.17.3.254
	Switch3_1	configure terminal interface vlan 1 no description no ip address interface vlan 1000 ip address 172.17.3.122 255.255.255.0 ip default-gateway 172.17.3.254
	Switch3_2	configure terminal interface vlan 1 no description

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

		no ip address interface vlan 1000 ip address 172.17.3.123 255.255.255.0 ip default-gateway 172.17.3.254
	Switch3_3	configure terminal interface vlan 1 no description no ip address interface vlan 1000 ip address 172.17.3.124 255.255.255.0 ip default-gateway 172.17.3.254
	MKT-GL2-CSW-1	configure terminal interface vlan 1 no description no ip address vlan 1000 name MANAGEMENT_SEGMENT interface vlan 1000 description MANAGEMENT_SEGMENT ip address 172.17.3.125 255.255.255.0 interface gigabitEthernet 1/0/27 description TO ODYSSEUS(VPN) switchport access vlan 1000 switchport mode access interface gigabitEthernet 1/0/28 description TO MIDGARD switchport access vlan 1000 switchport mode access ip default-gateway 172.17.3.254
	MKT-GL2-SW-A1	configure terminal interface vlan 1 no description no ip address interface vlan 1000 ip address 172.17.3.126 255.255.255.0 ip default-gateway 172.17.3.254
	MKT-GL2-SW-A2	configure terminal interface vlan 1 no description no ip address interface vlan 1000 ip address 172.17.3.127 255.255.255.0 ip default-gateway 172.17.3.254
	MKT-GL2-SW-A3	configure terminal interface vlan 1 no description

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

		no ip address interface vlan 1000 ip address 172.17.3.128 255.255.255.0 ip default-gateway 172.17.3.254	
	MKT-GL2-SW-A4	configure terminal interface vlan 1 no description no ip address interface vlan 1000 ip address 172.17.3.129 255.255.255.0 ip default-gateway 172.17.3.254	
	MKT-GL2-SW-A5	configure terminal interface vlan 1 no description no ip address interface vlan 1000 ip address 172.17.3.130 255.255.255.0 ip default-gateway 172.17.3.254	
	MKT-GL2-SW-B1	configure terminal interface vlan 1 no description no ip address interface vlan 1000 ip address 172.17.3.131 255.255.255.0 ip default-gateway 172.17.3.254	
	MKT-GL2-SW-B2	configure terminal interface vlan 1 no description no ip address interface vlan 1000 ip address 172.17.3.132 255.255.255.0 ip default-gateway 172.17.3.254	
	ASGARD ISR 4331 JAKA	configure terminal vlan 1000 name MANAGEMENT_SEGMENT int gig0/1/3 description TO ZEUS switchport access vlan 1000 switchport mode access	
	MIDGARD ISR 4331 G2	configure terminal vlan 1000 name MANAGEMENT_SEGMENT int gig0/1/5 description TO MKT-GL2-CSW-1 switchport access vlan 1000	

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

	switchport mode access
--	------------------------

Server Configurations:

1. Log on to ESXi using the root account.
2. From the main page of the ESXi management console, click on **Networking**.
3. Select **VM Network** from the list and **Edit Settings**.

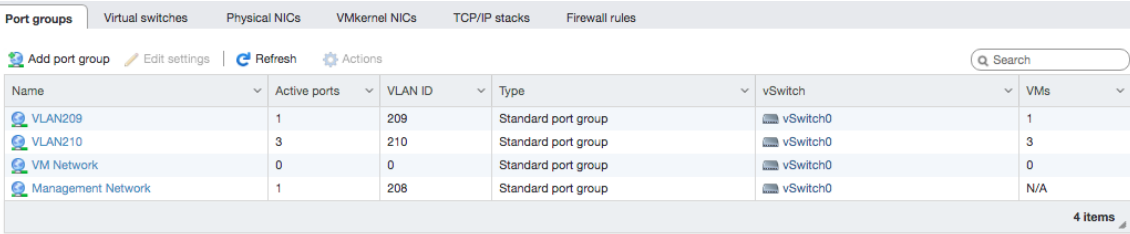



Figure 1: The VM Network port group is currently available and no IP is assigned yet.

4. Enter the VLANID. Save.
5. Next, Add virtual NIC to each virtual machine. From the Management console, go to the **Virtual Machine** section.
6. Right click on the virtual machine > Edit Settings.
7. Click on Add network adapter > scroll down to edit the New Network Adapter > assign the new VLAN ID.
8. Repeat steps 6-7 for each virtual machine.
9. Log on to each virtual machine and set the second virtual adapter to a static IP address from the range 172.17.3.1-172.17.3.100.

Verification Procedures			
<ol style="list-style-type: none"> 1. Install FortiClient in PC. 2. In the FortiClient, select Remote Access then click the gear button to add new connection. Use the following details below: VPN: SSL-VPN Connection Name: OAMPI VPN Remote Gateway: 10.1.0.100 Then Save. 3. Login to FortiClient (10.1.0.100) using the given credentials. 4. After logged in, you should be given an IP address from the range 172.17.3.240-172.17.3.250. 5. Due to split tunneling, only connections that matches the Management Segment 172.17.3.0/24 will pass thru the VPN while other destination will pass thru directly to one of our ISPs. To verify ran traceroute towards any website then check the 1st hop. It should be passing thru the default gateway 172.18.133.254 instead of 10.1.0.254. 6. Try to access the any website from the internet, it should be accessible. 7. Run Ping and Putty to the Switches and Servers below. It should all be accessible. 			
	Proprietary and Confidential	Effectivity: April 1, 2019	Page 13
			Template Version : 02

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

1. Disconnect port1(DMZ) of ODYSSEUS to port gig0/1 of DMZ SWITCH.
2. Disconnect mgmt2(Management) of ODYSSEUS to port gig1/0/45 of ZEUS.
3. Disconnect mgmt of FORTIGATE THOR to port gig2/0/45 of ZEUS.
4. Disconnect mgmt of MKT-GL2-FW-1 to port gig1/0/27 of MKT-GL2-CSW-1.
5. Disconnect port gig1/0/48 of ZEUS to port gig0/1/3 of ASGARD ISR 4331.
6. Disconnect port gig1/0/28 of MKT-GL2-CSW-1 to port gig0/1/5 of MIDGARD ISR 4331.
7. Access FortiGate THOR then navigate to Policy & Objects and disable the IPv4 Policies:

Internal To Odysseus(VPN)

Odysseus(VPN) To Internal

8. Access all switches in the table below via console then copy and paste the commands per switch.

Zeus	configure terminal interface vlan 1 no description ip address 172.31.1.1 no vlan 1000 no interface vlan 1000 interface gigabitEthernet 1/0/45 no description TO ODYSSEUS(VPN) no switchport access vlan 1000 no switchport mode access interface gigabitEthernet 1/0/48 no description TO ASGARD no switchport access vlan 1000 no switchport mode access
Morpheus	configure terminal interface vlan 1 no description ip address 172.31.1.17 no interface vlan 1000 ip default-gateway 172.31.1.1
Poseidon	configure terminal interface vlan 1 no description ip address 172.31.1.18 no interface vlan 1000 ip default-gateway 172.31.1.1
Erebus	configure terminal interface vlan 1 no description ip address 172.31.1.19 no interface vlan 1000 ip default-gateway 172.31.1.1

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

	Janus	configure terminal interface vlan 1 no description ip address 172.31.1.24 no interface vlan 1000 ip default-gateway 172.31.1.1
	Cyclops	configure terminal interface vlan 1 no description ip address 172.31.1.25 no interface vlan 1000 ip default-gateway 172.31.1.1
	Medusa	configure terminal interface vlan 1 no description ip address 172.31.1.22 no interface vlan 1000 ip default-gateway 172.31.1.1
	Nyx	configure terminal interface vlan 1 no description ip address 172.31.1.23 no interface vlan 1000 ip default-gateway 172.31.1.1
	Hera	configure terminal interface vlan 1 no description ip address 172.31.1.21 no interface vlan 1000 ip default-gateway 172.31.1.1
	Switch5_1	configure terminal interface vlan 1 no description ip address 172.31.1.29 no interface vlan 1000 ip default-gateway 172.31.1.1
	Switch5_2	configure terminal interface vlan 1 no description ip address 172.31.1.30 no interface vlan 1000 ip default-gateway 172.31.1.1
	Switch5_3	configure terminal interface vlan 1 no description

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

		ip address 172.31.1.31 no interface vlan 1000 ip default-gateway 172.31.1.1	
	Switch5_4	configure terminal interface vlan 1 no description ip address 172.31.1.32 no interface vlan 1000 ip default-gateway 172.31.1.1	
	Switch5_5	configure terminal interface vlan 1 no description ip address 172.31.1.36 no interface vlan 1000 ip default-gateway 172.31.1.1	
	Switch5_6	configure terminal interface vlan 1 no description ip address 172.31.1.37 no interface vlan 1000 ip default-gateway 172.31.1.1	
	Switch5_7	configure terminal interface vlan 1 no description ip address 172.31.1.38 no interface vlan 1000 ip default-gateway 172.31.1.1	
	Switch3_1	configure terminal interface vlan 1 no description ip address 172.31.1.33 no interface vlan 1000 ip default-gateway 172.31.1.1	
	Switch3_2	configure terminal interface vlan 1 no description ip address 172.31.1.34 no interface vlan 1000 ip default-gateway 172.31.1.1	
	Switch3_3	configure terminal interface vlan 1 no description ip address 172.31.1.35 no interface vlan 1000 ip default-gateway 172.31.1.1	

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

	MKT-GL2-CSW-1	configure terminal interface vlan 1 no description ip address 172.22.2.1 no vlan 1000 no interface vlan 1000 interface gigabitEthernet 1/0/27 no description TO ODYSSEUS(VPN) no switchport access vlan 1000 no switchport mode access interface gigabitEthernet 1/0/28 no description TO MIDGARD no switchport access vlan 1000 no switchport mode access
	MKT-GL2-SW-A1	configure terminal interface vlan 1 no description ip address 172.22.2.11 no interface vlan 1000 ip default-gateway 172.22.2.1
	MKT-GL2-SW-A2	configure terminal interface vlan 1 no description ip address 172.22.2.12 no interface vlan 1000 ip default-gateway 172.22.2.1
	MKT-GL2-SW-A3	configure terminal interface vlan 1 no description ip address 172.22.2.13 no interface vlan 1000 ip default-gateway 172.22.2.1
	MKT-GL2-SW-A4	configure terminal interface vlan 1 no description ip address 172.22.2.14 no interface vlan 1000 ip default-gateway 172.22.2.1
	MKT-GL2-SW-A5	configure terminal interface vlan 1 no description ip address 172.22.2.15 no interface vlan 1000 ip default-gateway 172.22.2.1

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

	MKT-GL2-SW-B1	configure terminal interface vlan 1 no description ip address 172.22.2.21 no interface vlan 1000 ip default-gateway 172.22.2.1
	MKT-GL2-SW-B2	configure terminal interface vlan 1 no description ip address 172.22.2.22 no interface vlan 1000 ip default-gateway 172.22.2.1
	ASGARD ISR 4331 JAKA	configure terminal interface vlan 1 no description no interface vlan 1000
	MIDGARD ISR 4331 G2	configure terminal interface vlan 1 no description no interface vlan 1000
<p>9. After backout, run ping and SSH to the old Management IP address. It should be accessible.</p>		