Request Information				
Requestor	Maurice Mendoza			
Implementing Team	Network Operations			
Ticket Number/s	201915358			
Change Classification		Major	X	Minor
After the fact		Yes	X	No
Emergency		Yes	X	No
Proposed Change Date	May 11, 2019			
Proposed Change Start/End Time	18:00 – 21:00			
Proposed Change Verification Time	20:00			

Objective of the change
To point all Network Equipment to Syslog Server

Technical/Operational Impact of the change		
Negative: There will be no logs during the configuration.	Beneficial: To ease network troubleshooting. To log all network configuration changes and status.	Neutral: Usage of Switch console port for configuration.

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
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

Test Environment implementation and Verification Summary

Configured a test switch with the following commands:

enable
configure terminal
logging ip-address-of-wazuh
exit
wr

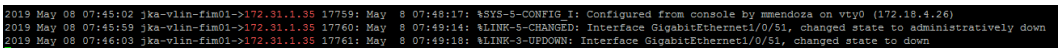
Accessed Wazuh via CLI and ran the command:

tail -f /var/ossec/logs/archives/archives.log | grep ip-address-of-test-switch

Ran the test configurations below on the test switch:

interface gigabitEthernet1/0/51
shutdown
no shutdown

After running some test configurations, the logs appeared in Wazuh in /var/ossec/logs/archives/archives.log



Test Environment Results Summary

Upon testing, all network equipment can successfully send the logs to Wazuh Syslog Server.

Configuration Change Template

Baseline File	See link for switches: Switch Baseline
Baseline Version	April 3, 2019

Baseline File Changes:

Existing Configuration	Proposed Change	Impact	Section
All Network Equipments are currently pointed to the old syslog server 172.17.0.102	All Network Equipments will be pointed to Wazuh Syslog Server	Switch Configurations (Logging hosts)	Switch Baseline

Physical Implementation Procedures / Advisory
No physical implementation. No advisory since this is a non-service affecting implementation.

Backup Procedures

Access FortiGate Jaka, G2 and all Access Switches via console.
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
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

1. Access all access switches both in Jaka and G2 via Console.
2. Copy and run the commands below to all access switches listed in the table.

```
enable
configure terminal
logging traps notification
logging 172.17.3.3
logging 172.17.3.25
exit
wr
```

JAKA	Zeus	172.17.3.106	Core Switch
JAKA	Morpheus	172.17.3.107	Access Switch
JAKA	Poseidon	172.17.3.108	Access Switch
JAKA	Erebus	172.17.3.109	Access Switch
JAKA	Janus	172.17.3.110	Access Switch
JAKA	Cyclops	172.17.3.111	Access Switch
JAKA	Medusa	172.17.3.112	Access Switch
JAKA	Nyx	172.17.3.113	Access Switch
JAKA	Hera	172.17.3.114	Access Switch

JAKA	Switch5_1	172.17.3.115	Access Switch
JAKA	Switch5_2	172.17.3.116	Access Switch
JAKA	Switch5_3	172.17.3.117	Access Switch
JAKA	Switch5_4	172.17.3.118	Access Switch
JAKA	Switch5_5	172.17.3.119	Access Switch
JAKA	Switch5_6	172.17.3.120	Access Switch
JAKA	Switch5_7	172.17.3.121	Access Switch
JAKA	Switch3_1	172.17.3.122	Access Switch
JAKA	Switch3_2	172.17.3.123	Access Switch
JAKA	Switch3_3	172.17.3.124	Access Switch
G2	MKT-GL2-CSW-1	172.17.3.125	Core Switch
G2	MKT-GL2-SW-A1	172.17.3.126	Access Switch
G2	MKT-GL2-SW-A2	172.17.3.127	Access Switch
G2	MKT-GL2-SW-A3	172.17.3.128	Access Switch
G2	MKT-GL2-SW-A4	172.17.3.129	Access Switch
G2	MKT-GL2-SW-A5	172.17.3.130	Access Switch
G2	MKT-GL2-SW-B1	172.17.3.131	Access Switch
G2	MKT-GL2-SW-B2	172.17.3.132	Access Switch

3. Access FortiGate Thor and G2 via CLI.
4. Apply the commands below:

```
config log syslogd setting
set status enable
set server 172.17.3.3
set reliable disable
set port 514
set csv disable
set facility syslog

config log syslogd2 setting
set status enable
set server 172.17.3.25
set reliable disable
set port 514
set csv disable
set facility local7
```

Verification Procedures

1. Access Wazuh (ip-address-of-wazuh-Jaka and G2) using root via CLI then run the commands below:

   tail -f /var/ossec/logs/archives/archives.log | grep ip-address-of-test-switch

2. Access any access switch then run the following commands below:

   enable
   configure terminal
   interface gigabitEthernet 1/0/52
   shutdown
   no shutdown

   The commands above will display the logs below:

```
2019 May 08 08:52:03 jka-vlin-fim01->172.31.1.35 17980: May  8 08:55:19: %SYS-5-
CONFIG_I: Configured from console by mmendoza on vty0 (172.18.4.26)
2019 May 08 08:52:14 jka-vlin-fim01->172.31.1.35 17981: May  8 08:55:30: %LINK-5
-CHANGED: Interface GigabitEthernet1/0/52, changed state to administratively dow
n
2019 May 08 08:52:21 jka-vlin-fim01->172.31.1.35 17982: May  8 08:55:37: %LINK-3
-UPDOWN: Interface GigabitEthernet1/0/52, changed state to down
```

3. Access FortiGate Jaka and G2 via CLI
4. Run the commands below:

   diag log test

   The command above will display the following logs below:

Wazuh Logs:

```
2019 May 08 10:14:46 jka-vlin-fim01->10.1.0.100 date=2019-05-07 time=19:18:00 de
vname=ODYSSEUS devid=FGT3HD3916802421 logid=0000000013 type=traffic subtype=forw
ard level=notice vd=root srcip=1.1.1.1 srcport=30002 srcintf="mgmt1" dstip=2.2.2
.2 dstport=20 dstintf="mgmt2" sessionid=30002 proto=6 action=accept policyid=1 p
olicytype=policy dstcountry="France" srccountry="Australia" trandisp=noop servic
e="tcp/20" duration=10 sentbyte=2000 rcvdbyte=1000 sentpkt=0 rcvdpkt=0 appcat="u
nscanned" utmaction=block countweb=1 crscore=60 craction=4194312
2019 May 08 10:14:47 jka-vlin-fim01->10.1.0.100 date=2019-05-07 time=19:18:01 de
vname=ODYSSEUS devid=FGT3HD3916802421 logid=0100038404 type=event subtype=system
 level=error vd=root logdesc="FortiGuard hostname unresolvable" hostname="servic
e.fortiguard.net" msg="unable to resolve FortiGuard hostname"
2019 May 08 10:14:47 jka-vlin-fim01->10.1.0.100 date=2019-05-07 time=19:18:01 de
vname=ODYSSEUS devid=FGT3HD3916802421 logid=0100038404 type=event subtype=system
 level=error vd=root logdesc="FortiGuard hostname unresolvable" hostname="servic
e.fortiguard.net" msg="unable to resolve FortiGuard hostname"
```

Back-out Procedures

1. Access all access switches both in Jaka and G2 via Console.
2. Copy and run the commands below to all access switches listed in the table.

```
enable
configure terminal
logging traps notification
logging 172.17.0.102
exit
wr
```

JAKA	Zeus	172.17.3.106	Core Switch
JAKA	Morpheus	172.17.3.107	Access Switch
JAKA	Poseidon	172.17.3.108	Access Switch
JAKA	Erebus	172.17.3.109	Access Switch
JAKA	Janus	172.17.3.110	Access Switch
JAKA	Cyclops	172.17.3.111	Access Switch
JAKA	Medusa	172.17.3.112	Access Switch
JAKA	Nyx	172.17.3.113	Access Switch
JAKA	Hera	172.17.3.114	Access Switch
JAKA	Switch5_1	172.17.3.115	Access Switch
JAKA	Switch5_2	172.17.3.116	Access Switch
JAKA	Switch5_3	172.17.3.117	Access Switch
JAKA	Switch5_4	172.17.3.118	Access Switch
JAKA	Switch5_5	172.17.3.119	Access Switch
JAKA	Switch5_6	172.17.3.120	Access Switch
JAKA	Switch5_7	172.17.3.121	Access Switch
JAKA	Switch3_1	172.17.3.122	Access Switch
JAKA	Switch3_2	172.17.3.123	Access Switch
JAKA	Switch3_3	172.17.3.124	Access Switch
G2	MKT-GL2-CSW-1	172.17.3.125	Core Switch
G2	MKT-GL2-SW-A1	172.17.3.126	Access Switch
G2	MKT-GL2-SW-A2	172.17.3.127	Access Switch
G2	MKT-GL2-SW-A3	172.17.3.128	Access Switch
G2	MKT-GL2-SW-A4	172.17.3.129	Access Switch
G2	MKT-GL2-SW-A5	172.17.3.130	Access Switch
G2	MKT-GL2-SW-B1	172.17.3.131	Access Switch
G2	MKT-GL2-SW-B2	172.17.3.132	Access Switch

3. Access FortiGate Thor and G2 via CLI.
4. Apply the commands below:

```
config log syslogd setting
```

```
set status enable
set server 172.17.0.102
set reliable disable
set port 514
set csv disable
set facility syslog

config log syslogd2 setting
set status disable
```