Request Information				
Requestor	Alvis Bajal			
Implementing Team	Network Operations			
Ticket Number/s	201914302			
Change Classification	X	Major		Minor
After the fact		Yes	X	No
Emergency		Yes	X	No
Proposed Change Date	April 19, 2019			
Proposed Change Start/End Time	15:00			
Proposed Change Verification Time	15:10			

Objective of the change

To setup new network configurations (Firewall Policies, Address Objects, Web and App filtering, VLANs, ACLs) for Executives and Backoffice.

Technical/Operational Impact of the change

Negative:	Beneficial:	Neutral:
Added memory and CPU usage in Zeus and Jupiter.	Backoffice and Executives will have separate broadcast domain.	N/A

Affected IT Infrastructure components

Site	Hostname	IP Address	Function
JAKA	ZEUS	172.31.1.1	Network Core Switch
JAKA	JUPITER	172.31.1.252	Network Core Switch
JAKA	THOR	172.16.1.2	Network Firewall

Affected Departments and corresponding contact persons

Department	Contact Name	Contact Info
IT Department	Rynel Yanes	09178535630
Network Operations	Maurice Mendoza	09176881085

Test Environment implementation and Verification Summary

No test environment implementation was needed since this was already done before by the Network Operations Team.

Test Environment Results Summary

N/A

Configuration Change Template

Baseline File	3.1.101, 3.1.102, 3.1.103, 3.1.104, 3.1.113
Baseline Version	N/A

Baseline File Changes:

Existing Configuration	Proposed Change	Impact	Section
No existing config in Zeus and Jupiter for Executive and backoffice.	To create a separate VLAN segment for Executive, Back Office and own IPv4 policy for back office.	VLAN, Address Object, IPv4 Policy Group, Web and Application Filter	3.1.101 3.1.102 3.1.103 3.1.104 3.1.113

Physical Implementation Procedures / Advisory
No physical implementation is needed for this change docs.

Backup Procedures

I. **Part A.** (**Firewall Configuration**)

1. Access THOR.
2. Backup configuration with the following naming convention and then save it inside:
   \\fs.oampi.com\It\IT_Backup\Back Up\Network Operations
3. BACKUP_<device>_<DATE>_<TIME>.EXTENSION, eg.
   BACKUP_THOR_07152017_17:00.cfg

II. **Part B.** (**Switch Configuration**)

1. Access Zeus/Jupiter
2. Run the command "*show run*" then highlight all and paste it to the notepad then Save with the naming convention:
3. BACKUP_<device>_<DATE>_<TIME>, eg: BACKUP_ZEUS_07152017_17:00

Physical Implementation Procedures
No physical implementation is needed for this change docs.

Technical Configuration Procedures

I. PART A. (Switch Configuration)

1. Access Zeus via SSH
2. Copy and paste the commands below:

```
int vlan 70
description EXEC_BACKOFFICE
ip address 172.18.70.253 255.255.255.0
ip helper-address 172.17.0.121
standby version 2
standby 70 ip 172.18.70.254
standby 70 timers 1 3
standby 70 priority 180
standby 70 preempt
standby 70 track 1 decrement 50

spanning-tree vlan 70 24576
spanning-tree vlan 70 forward-time 4
spanning-tree vlan 70 max-age 6
```

3. Access Jupiter via SSH
4. Copy and paste the commands below:

```
int vlan 70
description EXEC_BACKOFFICE
ip address 172.18.70.252 255.255.255.0
ip helper-address 172.17.0.121
standby version 2
standby 70 ip 172.18.70.254
standby 70 timers 1 3
standby 70 priority 150
standby 70 preempt
standby 70 track 1 decrement 10

spanning-tree vlan 70 priority 36384
spanning-tree vlan 70 forward-time 4
spanning-tree vlan 70 max-age 6
```

5. Request help from the server team to create DHCP pool for this address:

INT_EXEC_BACKOFFICE
Network: 172.18.70.0/24
Scope: 172.18.70.1/172.18.70.245
Router: 172.18.70.254

6. Login to FortiGate Thor via Web

7. Access **THOR** via **https,** go to **Security Profile > Web Filter**
Click the + button at the upper right corner to create new web filter.

Name: WF_CAPABILITY

Follow the Category Filter

Category	**Name**	**Action**
Local Categories	Custom1	Allow
	Custom2	Allow
Potentially Liable	Child Abuse	Block
	Discrimination	Block
	Drug Abuse	Block
	Explicit Violence	Block
	Extremist Groups	Block
	Hacking	Block
	Illegal or Unethical	Block
	Plagiarism	Block
	Proxy Avoidance	Block
Adult / Mature Content	Abortion	Block
	Advocacy Organizations	Block
	Alcohol	Block
	Alternative Beliefs	Block
	Dating	Block
	Gambling	Block
	Lingerie and Swimsuit	Block

		Marijuana	Block
		Nudity and Risque	Block
		Other Adult Materials	Block
		Pornography	Block
		Sex Education	Block
		Sports Hunting and War Games	Block
		Tobacco	Block
		Weapons (Sales)	Block
	Bandwidth Consuming	File Sharing and Storage	Allow
		Freeware and Software Downloads	Block
		Internet Radio and TV	Block
		Internet Telephony	Allow
		Peer-to-peer File Sharing	Block
		Streaming Media and Download	Block
	Security Risk	Dynamic DNS	Block
		Malicious Websites	Block
		Newly Observed Domain	Block
		Newly Registered Domain	Block
		Phishing	Block
		Spam URLs	Block
	General Interest - Personal	Advertising	Block
		Arts and Culture	Block
		Auction	Block
		Brokerage and Trading	Block
		Child Education	Block
		Content Servers	Allow
		Digital Postcards	Block
		Domain Parking	Block
		Dynamic Content	Block
		Education	Block
		Entertainment	Block

		Folklore	Block
		Games	Block
		Global Religion	Block
		Health and Wellness	Block
		Instant Messaging	Allow
		Job Search	Block
		Meaningless Content	Block
		Medicine	Block
		News and Media	Allow
		Newsgroups and Message Boards	Block
		Personal Privacy	Block
		Personal Vehicles	Block
		Personal Websites and Blogs	Block
		Political Organizations	Block
		Real Estate	Block
		Reference	Block
		Restaurant and Dining	Block
		Shopping	Block
		Social Networking	Block
		Society and Lifestyles	Block
		Sports	Block
		Travel	Block
		Web Chat	Allow
		Web-based Email	Allow
	General Interest - Business	Armed Forces	Block
		Business	Allow
		Finance and Banking	Block
		General Organizations	Allow
		Government and Legal Organizations	Allow
		Information Technology	Allow
		Information and Computer Security	Allow

	Search Engines and Portals	Allow
	Secure Websites	Allow
	Web Hosting	Allow
	Web-based Applications	Allow
Unrated	Unrated	Block

a. Create new URL Filter and copy the lists of websites below.

spotify.com	-	wildcard	-	block
facebook.com	-	wildcard	-	block
lazada.com	-	wildcard	-	block
youtube.com	-	wildcard	-	Allow
viber.com	-	wildcard	-	block
vimeo.com	-	wildcard	-	block
twitter.com	-	wildcard	-	block
instagram.com	-	wildcard	-	block
soundcloud.com	-	wildcard	-	block
freemoviedownloads6.com	-	wildcard	-	block

Click APPLY button.

b. Go to **Security Profile** > **Application Control.** Click the + to add new application sensor.

Name: **AC_CAPABILITY**

Copy the following Categories

Categories	**Action**
Business	Allow
Cloud.IT	Allow
Collaboration	Allow
Email	Allow
Game	Block
General.Interest	Allow
Mobile	Allow
Network.Service	Allow
P2P	Block

Proxy	Block
Remote.Access	Block
Social.Media	Block
Storage.Backup	Block
Update	Block
Video/Audio	Block
VoIP	Allow
Web.Client	Allow
Unknown Applications	Block

c. On Application Override, click **add signatures** and copy the following configuration:

Application Signature	**Category**	**Action**
Adobe.Update	Update	Block
AVI.Media.Player	Video/Audio	Block
Baidu.Player	Video/Audio	Block
BBC.iPlayer	Video/Audio	Block
Chrome.Update	Update	Block
Facebook_Messenger.Image.Transfer	Collaboration	Block
Facebook_Messenger.Video.Transfer	Collaboration	Block
Facebook_Messenger.Voice.Message	Collaboration	Block
Facebook_Messenger.VoIP.Call	Collaboration	Block
Facebook_Video.Play	Social.Media	Block
Firefox.Update	Update	Block
Flowplayer	Video/Audio	Block
GOM.Player	Video/Audio	Block
Google.Play	General.Interest	Block
Google.Drive	Storage.Backup	Allow
Google.Drive_Edit	Storage.Backup	Allow
Google.Drive_File.Download	Storage.Backup	Allow

Google.Drive_File.Upload	Storage.Backup	Allow
Google.Drive_File.Sharing	Storage.Backup	Allow
Instagram	Social.Media	Block
Instagram_Video	Social.Media	Block
iTunes_Select.Play	Video/Audio	Block
iTunes_Update	Update	Block
Java.Update	Update	Block
LinkedIn	Social.Media	Block
LinkedIn_Message	Social.Media	Block
Microsoft.Office.Update	Update	Block
Microsoft.Outlook	Email	Allow
Microsoft.Outlook.Web.App	Email	Allow
Microsoft.Outlook_Attachment	Email	Allow
MS.Windows.Update	Update	Block
Outlook.Anywhere	Business	Allow
Pipi.Player	P2P	Block
Playstation.Network	Game	Block
Real.Player	Video/Audio	Block
SoundCloud	Video/Audio	Block
Spotify	Video/Audio	Block
SVT.Play	Video/Audio	Block
Twitter	Social.Media	Block
Twitter_Message	Social.Media	Block
Ubuntu.Update	Update	Block
UEFA_Video.Play	Video/Audio	Block
Veoh.Player	Video/Audio	Block
Viber	VoIP	Block
Windows.Media.Player	Video/Audio	Block
YouTube	Video/Audio	Allow
YouTube.Downloader.YTD	Video/Audio	Block
YouTube_Comment.Posting	Video/Audio	Block

YouTube_HD.Streaming	Video/Audio	Allow
YouTube_Search.Safety.Mode.Off	Video/Audio	Allow
YouTube_Search.Video	Video/Audio	Allow
YouTube_Video.Embedded	Video/Audio	Allow

8. Go to Policy & Objects > Address then create address objects using the following details below:

Name: INT_WORKFORCE
Type: Subnet
Subnet: 172.18.70.0/26

Name: INT_RA_QA
Type: Subnet
Subnet: 172.18.70.64/26

Name: INT_SECURITY
Type: Subnet
Subnet: 172.18.70.128/26

Name: INT_EXECUTIVE
Type: Subnet
Subnet: 172.18.70.192/26

9. Add the following address objects to the address group EXE_GR_Managers:

INT_EXECUTIVE

10. Add the following address objects to the Source of policy Privileged Access US COLO:

INT_RA_QA
INT_WORKFORCE
INT_SECURITY

11. Create new IPv4 Policy with the following information:

Name: CatchAll RA_QA
Incoming Interface: Internal (port5)
Outgoing Interface: SD-WAN
Source: INT_RA_QA
Destination: all

Schedule: always
Service: 443 TCP
ICMP
Action: ACCEPT

Firewall / Network Options
NAT: Enable
IP Pool Config: Use Outgoing Interface Address
Proxy Options: Default

Security Profiles:
Web Filter (enable): BOFC
Application Filter (enable): BOFC

Logging Options:
Log Allowed Traffic (enable) [Security Events]

Enable this policy (enable)

Name: CatchAll WORKFORCE
Incoming Interface: Internal (port5)
Outgoing Interface: SD-WAN
Source: INT_WORKFORCE
Destination: all
Schedule: always
Service: 443 TCP
ICMP
Action: ACCEPT

Firewall / Network Options
NAT: Enable
IP Pool Config: Use Outgoing Interface Address
Proxy Options: Default

Security Profiles:
Web Filter (enable): BOFC
Application Filter (enable): BOFC

Logging Options:
Log Allowed Traffic (enable) [Security Events]

Enable this policy (enable)

Name: CatchAll CAPABILITY

Incoming Interface: Internal (port5)
Outgoing Interface: SD-WAN
Source: INT_CAPABILITY
Destination: all
Schedule: always
Service: 443 TCP
ICMP
Action: ACCEPT

Firewall / Network Options
NAT: Enable
IP Pool Config: Use Outgoing Interface Address
Proxy Options: Default

Security Profiles:
Web Filter (enable): BOFC
Application Filter (enable): BOFC

Logging Options:
Log Allowed Traffic (enable) [Security Events]

Enable this policy (enable)

Verification Procedures

I. Part A. (Switch Configuration)

1. Access Zeus and Jupiter via SSH
2. Run the commands below:

show vlan brief - This command will show all the VLANs in the database. VLAN 70.

show spanning-tree vlan 70 - This command will show the current spanning tree details. The details below should be the same;

```
For VLAN 70 in Zeus
Root ID    Priority    24646
           Address     0042.5a39.da00
           This bridge is the root
           Hello Time   2 sec  Max Age  6 sec  Forward Delay  4 sec

Bridge ID  Priority    24646  (priority 24576 sys-id-ext 70)
           Address     0042.5a39.da00
           Hello Time   2 sec  Max Age  6 sec  Forward Delay  4 sec
           Aging Time  300 sec

For VLAN 70 in Jupiter
Root ID    Priority    24646
           Address     0042.5a39.da00
           Cost        3
           Port        488 (Port-channel1)
           Hello Time   2 sec  Max Age  6 sec  Forward Delay  4 sec

Bridge ID  Priority    36454  (priority 36864 sys-id-ext 70)
           Address     0021.a13c.4180
           Hello Time   2 sec  Max Age  6 sec  Forward Delay  4 sec
           Aging Time 300
```

3. Configure port GigabitEthernet2/0/29 of Zeus

```
interface GigabitEthernet2/0/29
switchport access vlan 70
switchport mode access
```

4. Connect a test laptop to port GigabitEthernet2/0/29 of Zeus, the device should obtain the ip address 172.18.70.1 and should have internet connection.

Back-out Procedures

I. PART A. (Firewall Configuration)

a. Login to THOR via web.

b. Go to Policy & Object and remove the following address group from "EXE_GR_Managers".

INT_EXECUTIVE

c. Locate the IPv4 Policy "Privileged Access USCOLO", remove the following address objects from the SOURCE:

INT_WORKFORCE
INT_CAPABILITY
INT_RA_QA

d. Go to Policy & Objects > Addresses then delete the following:

INT_EXECUTIVE
INT_WORKFORCE
INT_CAPABILITY
INT_RA_QA

e. Locate the IPv4 Policy "CatchAll RA_QA", right click > delete.

f. Locate the IPv4 Policy "CatchAll WORKFORCE", right click > delete.

g. Locate the IPv4 Policy "CatchAll CAPABILITY", right click > delete.

h. Ask server team to remove the DHCP Pool with the address:
EXECUTIVE
INT_WORKFORCE
INT_CAPABILITY
INT_RA_QA

i. Login to Zeus and Jupiter via SSH.

j. Copy and paste the following command to remove the VLAN interface in both switch:

```
conf t
no interface vlan 70

exit
wr
```