Request Information				
Requestor	Ian John Lastimoso			
Implementing Team	Network Operations			
Ticket Number/s	201915324			
Change Classification	X	Major		Minor
After the fact		Yes	X	No
Emergency		Yes	X	No
Proposed Change Date	May 11, 2019			
Proposed Change Start/End Time	6:00 PM			
Proposed Change Verification Time	7:00 PM			

Objective of the change
Implementation of VLAN 228 on Core switch and Web Filter, Application Control & IPv4 policies for Firewall

Technical/Operational Impact of the change		
Negative:	Beneficial:	Neutral:
High Utilization of RAM and CPU usage on the Firewall during the Implementation	Segment Implementation for DATA_SCAN Clinic campaign FSSO user based access will be implemented	Access Switches connected to Core switch

Affected IT Infrastructure components			
Site	Hostname	IP Address	Function
G2	MKT-GL2-CSW-1	172.22.2.1	Core Switch
G2	MKT-GL2-FW-1	172.22.0.75	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 Environment needed as this was implemented before. *Please refer on this ticket #201914195*

Test Environment Results Summary
Implementation was a success based on the previous Implementations. *Please refer on this ticket #201914195*

Configuration Change Template

Baseline File	3.1.101, 3.1.401, 3.1.402, 3.1.403, 3.1.404
Baseline Version	As of March 01, 2019

Baseline File Changes:

Existing Configuration	Proposed Change	Impact	Section
No separate segment for DATA_SCAN campaign MKT-GL2-FW1: No existing IPv4 Policy for DataScan DHCP Server: No existing IP pool for DataScan	Create new VLAN, address group, ipv4 policy and WAN LLB Rules specially for DATA_SCAN DHCP Server: Create IP Pool for DataScan with an IP address of 172.22.28.0/24 FSSO Implementation for User Based Policy and Access	VLAN Database, Address Object, Ipv4 Policies, Address Group Web Filter	3.1.101, 3.1.102, 3.1.402, 3.1.403, 3.1.404, 3.1.405

Physical Implementation Procedures / Advisory
N/A

Backup Procedures

I. Part A (Switch Configuration)

1. Access G2 Core Switch via SSH (172.22.2.1)
2. Run the command "*Show run*".
3. Highlight all the text and paste it to notepad with the naming convention and save it inside \\172.17.0.124\it \Back Up\Network Backup Logs

II. Part B (Firewall Configuration)

1. Access G2 Firewall (https://172.22.0.75:10443)

2. Backup Configuration with the following naming convention and then save it inside \\172.17.0.124 \IT\Back up\G2_FW

3. BACKUP;Device;Date;Time,.Extension e.g. BACKUP_G2_07152017_17:45.cfg

III. Part C (DHCP Configuration)

1. Access G2 AD via RDP

2. Open the DHCP Management by typing *dhcpmgmt.msc*

3. Click on the DHCP Server then right click choose *Backup*

Create New folder and name it *DHCP<Date>* then click *OK* to save.

Physical Implementation Procedures

N/A

Technical Configuration Procedures

I. PART A (Switch Configuration)

A. Access G2 Core Switch via SSH (172.22.2.1)
B. Enter the following commands below line by line

en
conf t
vlan 228
name DATA_SCAN
exit
interface Vlan228
description GW_DATA_SCAN
ip address 172.22.28.253 255.255.255.0
ip helper-address 172.22.1.1
end
wr

II. PART B (Firewall Configuration)

A. Login to Fortigate G2 (https://172.22.0.75:10443)

B. **Policy & Object > Addresses >** Click on **Create new** and select **Addresses**

Name: INT_SUB_DATA_SCAN
Subnet/IPRange: 172.22.28.0/24

C. Click **Create New** and select **Address Group.**

Group name: **EXE_GR_DATA_SCAN_Managers_TLs**
Members: *Bypass NULL*

D. Go to **Security Profile > Web Filter**
Click the + button at the upper right corner to create new web filter.

Name: WF_DATA_SCAN

Follow the Category Filter

Category	Name	Action
Local Categories	OAM_Blocked	Block
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	Block
	Freeware and Software Downloads	Block
	Internet Radio and TV	Block
	Internet Telephony	Block
	Peer-to-peer File Sharing	Block
	Streaming Media and Download	Block
Security Risk	Dynamic DNS	Block
	Malicious Websites	Block
	Phishing	Block
	Spam URLs	Block
General Interest - Personal	Advertising	Allow
	Arts and Culture	Block
	Auction	Allow
	Brokerage and Trading	Allow
	Child Education	Allow
	Content Servers	Allow
	Digital Postcards	Allow
	Domain Parking	Allow
	Dynamic Content	Allow

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

	Information Technology	Allow
	Information and Computer Security	Block
	Search Engines and Portals	Allow
	Secure Websites	Block
	Web Hosting	Block
	Web-based Applications	Block
Unrated	Unrated	Warning

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

Set of tools and web links to be given any time soon

F. Create again DATA_SCAN Web Filter and name it as "**WF_DATA_SCAN_Managers_TLs**". Just copy all the category filter in step C.

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

Name: **AC_DATA_SCAN**

Copy the following Categories

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

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

H. On Application Overrides, click **add signatures** and copy the following configuration:

Application Signature	Category	Action
Adobe.Flash.Media.Playback	Video/Audio	Block
Adobe.Update	Update	Block
Arctic.Torrent	P2P	Block
AVI.Media.Player	Video/Audio	Block
Baidu.Player	Video/Audio	Block
BBC.iPlayer	Video/Audio	Block
BitTorrent	P2P	Block
Chrome.Update	Update	Block
Citrix.CDN	Collaboration	Allow
Citrix.ICA	General Interest	Allow
Citrix.Receiver	Remote.Access	Allow
CTorrent	P2P	Block
ExtraTorrent	P2P	Block
Facebook	Social.Media	Block
Facebook_AppNameParameters Required	Social.Media	Block
Facebook_Apps	Social.Media	Block
Facebook_Like.Button	Social.Media	Block
Facebook_Personal	Social.Media	Block

Facebook_Plugins	Social.Media	Block
Facebook_Search	Social.Media	Block
Facebook_Video.Play	Social.Media	Block
Firefox.Update	Update	Block
Flowplayer	Video/Audio	Block
G3.Torrent	P2P	Block
GOM.Player	Video/Audio	Block
Google.Play	General.Interest	Block
HTTP.Download.Accelerator	General.Interest	Block
HTTP.Segmented.Download	Network.Service	Block
Instagram	Social.Media	Block
Instagram_Video	Social.Media	Block
iTunes	Video/Audio	Block
iTunes_App.Download	Video/Audio	Block
iTunes_BroadCast	Video/Audio	Block
iTunes_Mobile	Video/Audio	Block
iTunes_Podcast	Video/Audio	Block
iTunes_Select.Play	Video/Audio	Block
iTunes_Store	Video/Audio	Block
LinkedIn	Social.Media	Block
LinkedIn_Message	Social.Media	Block
Microsoft.Authentication	Collaboration	Allow
Microsoft.Media.Server	Video/Audio	Block
Microsoft.Office.365	Collaboration	Allow
Microsoft.Portal	Collaboration	Allow
Microsoft.Outlook.Web.App	Collaboration	Allow
One Drive	Collaboration	Allow
Pipi.Player	P2P	Block
Playstation.Network	Game	Block
Skype	Collaboration	Allow
Skype.Portals	Collaboration	Allow

Skype.For.Business	Collaboration	Allow
Spotify	Video/Audio	Block
SVT.Play	Video/Audio	Block
TorrentLocker.Botnet	Botnet	Block
TorrentSpy	P2P	Block
Torrentz	P2P	Block
Twitter	Social.Media	Block
Twitter_Message	Social.Media	Block
Veoh.Player	Video/Audio	Block
Viber	VoIP	Block
Windows.Media.Player	Video/Audio	Block
YouTube	Video/Audio	Block
YouTube.Downloader.YTD	Video/Audio	Block
YouTube_Comment.Posting	Video/Audio	Block
YouTube_HD.Streaming	Video/Audio	Block
YouTube_Search.Safety.Mode.Off	Video/Audio	Block
YouTube_Search.Video	Video/Audio	Block
YouTube_Video.Embedded	Video/Audio	Block

I. Create again new Application Control profile and name it as "**AC_DATA_SCAN_Managers_TLs**". Just copy all the categories and application signature in step H.

J. Navigate to **Security Fabric** > **Fabric Connectors** , then click on **G2_FSSO** > **Groups** > Look for **FSSO_P_DATA_SCAN** , right click then click "**Add Selected"**

K. Navigate to User & Device > User Groups > Create New

Name: **FSSO_P_DATA_SCAN**
Type: **Fortinet Single Sign On**
Members: **FSSO_P_DATA_SCAN**

Click **OK.**

L. Navigate to **Security Fabric** > **Fabric Connectors** , then click on **G2_FSSO** > **Groups** > Look for **FSSO_P_DATA_SCAN_TLs** , right click then click "**Add Selected"**

M. Navigate to User & Device > User Groups > Create New

Name: **FSSO_P_DATA_SCAN_TLs**
Type: **Fortinet Single Sign On**
Members: **FSSO_P_DATA_SCAN**

Click **OK**

N. Go to **Policy & Objects** > **IPv4 Policy > Create New**

Name: *Privileged DATA_SCAN*
Incoming Interface: Internal(port16)
Outgoing Interface: wan-load-balance
Source: INT_GR_DATA_SCAN_Managers_TLs
FSS_P_DATA_SCAN_TLs
Destination Address: *all*
Schedule: *Always*
Service: *all*
Action: *ACCEPT*
NAT: *Enable*
Fixed Port: *Disable*
IP Pool Configuration: *Use Outgoing Interface*
AntiVirus: *Disable*
Web Filter: *WF_DATA_SCAN_Managers_TLs*
Application Control: *AC_DATA_SCAN_Managers_TLs*
IPS: *Disable*
SSL/SSH Inspection: *Disable*
Log Allowed Traffic: *Enable – Security Sessions*
Enable this policy: *Enable*

Click ***OK***.

O. Create DATA_SCAN IPv4 Policy.

Go to **Policy & Objects** > **IPv4 Policy > Create New**

Name: *CatchAll Policy DATA_SCAN*
Incoming Interface: Internal(port16)
Outgoing Interface: wan-load-balance
Source: INT_SUB_DATA_SCAN

FSSO_P_DATA_SCAN
Destination Address: ***ALL***
Schedule: *Always*
Service: ***ALL***
Action: *ACCEPT*
NAT: *Enable*
Fixed Port: *Disable*
IP Pool Configuration: *Use Outgoing Interface*
AntiVirus: *Disable*
Web Filter: *WF_DATA_SCAN*
Application Control: *AC_DATA_SCAN*
IPS: *Disable*
SSL/SSH Inspection: *Disable*
Log Allowed Traffic: *Enable – Security Events*
Enable this policy: *Enable*

Click ***OK***

P. Go to **Network** > **WAN LLB RULES** > **Create New**

Name: PR_INT_SUB_DATA_SCAN
Source Address: INT_SUB_DATA_SCAN
User Group: None
Destination: *Address*
Destination Address: *all*
Interface Members: Specify
port2(Gateway: 210.213.124.2)

PART C (DHCP Configuration)

Ask Systems Team for creating new DHCP Pool.

VLAN 228: DATA_SCAN
Network: 172.22.28.0/24
Range: 172.22.28.1 – 172.22.28.254
Exclusion: 172.22.28.252 – 172.22.28.254

Ask Systems Team to create new groups on FSSO folder in AD

Name: FSSO_P_DATA_SCAN
Name: FSSO_P_DATA_SCAN_TLs

Verification Procedures

- Do an "ipconfig" command in all DATA_SCAN workstations, to verify the network segment.

Test access the internet using Chrome or Firefox.

- IP address should be on 28 segments. Ex. 172.22.28.0

Back-out Procedures

I. Firewall Configuration

a. Go to **Policy & Objects** > **IPv4 Policy** > Right click on *CatchAll Policy DATA_SCAN* and *Privileged Access DATA_SCAN and* select **delete**.

b. Go to **Security Profile** > **Application Control** select *AC_ DATA_SCAN* and *AC_ DATA_SCAN _Managers_TLs*, then click the trash bin located at the upper right corner to delete. Click OK to confirm.

c. Go to **Security Profile** > **Web Filter,** click this icon select *WF_DATA_SCAN* and *WF_ DATA_SCAN _Managers_TLs* then click **delete**.

d. Go to **Network** > **WAN LLB RULES** then select **PR_INT_SUB_** *DATA_SCAN* delete.

e. Go to **Address** > **Create New** > **Address Group** select the group named ***EXE_GR_*** *DATA_SCAN* then click delete to remove the group.

f. Delete address object named **INT_SUB_** *DATA_SCAN*.

II. Switch Configuration

a. Access G2 core switch via SSH. Copy all commands below line by line.

en
conf t
no vlan 228
no interface Vlan228
end
wr

III. DHCP Configuration

Access Hercules via RDP.

Delete DHCP Pool named **Scope [172.22.28.0] DATA_SCAN**

IV. Firewall Configuration

a. Go to **Policy & Objects** > **IPv4 Policy** > Right click on *Privileged Access for DATA_SCAN* and select **delete**.

b. Go to **Security Profile** > **Application Control** select AC_ *DATA_SCAN* _Managers_TLs, then click the trash bin located at the upper right corner to delete. Click OK to confirm.

c. Go to **Security Profile** > **Web Filter,** click the and select WF_ *DATA_SCAN* _Managers_TLs then click **delete**.

d. Go to Policy & Objects > **Address** > Group. Select the group named ***EXE_GR_*** *DATA_SCAN* ***_Managers_TLs*** then click delete to remove the group.