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

Request Information					
Requestor	Net	work Operations			
Implementing Team	Network Operations				
Ticket Number/s	201	914920			
Change Classification	Х	Major		Minor	
After the fact		Yes	Х	No	
Emergency	Х	Yes		No	
Proposed Change Date		April 24, 2019			
Proposed Change Start/End Time	22:0	00			
Proposed Change Verification Time	22:10				

Objective of the change

Creation of IPv4 policy to allow GTI Team for the External VAPT on our Firewall. (**THOR and MKT-GL2-FW**)

Technical/Operational Impact of the change				
Negative:	Beneficial:	Neutral:		
Allowing of GTI Team Public IP Address inbound to all subnets.	The team will be able to proceed for External VAPT scan.	Network Segments (LAN)		

Affected IT Infrastructure components				
Site	Hostname	IP Address	Function	
JAKA	THOR	115.85.25.4	Network Firewall	
G2	MKT-GL2-FW1	210.213.124.2	Network Firewall	

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

Test Environment implementation and Verification Summary

This is an emergency implementation; this will be directly implemented due to the emergency nature of the change.

Expected Results Summary

GTI Team will be able to proceed with their External VAPT scan.



Dun anna Outra an	FORM	
Process Owner: IT Operations	Configuration Change Request	F-CMG-3.1

Configuration Change Template

Baseline File	3.1.402, 3.1.10.2
Baseline Version	April 18, 2019

Baseline File Changes:

Existing Configuration	Proposed Change	Impact	Section
JAKA and G2:	Creation of Inbound IPv4 policy for GTI External VAPT:	Firewall IPv4 policy	3.1.402 3.1.10.2
No Inbound IPv4 policy for External VAPT Scan.	JAKA and G2:		
	Source: 64.39.96.0/20 Destination: Subnets that are under PCI Scope		

Physical	Imp	lementation	Procedures,	/ Advisory
----------	-----	-------------	-------------	------------

No advisory was implemented for this policy.

Backup Procedures

Access FortiGate Jaka and G2 via Web Browser. Backup the configurations files using the naming conventions:

BACKUP_DEVICENAME_DATE.cfg Example:

BACKUP_THOR_4272019.cfg, BACKUP_MIDAS_4272019.cfg

Technical Configuration Procedures

1. Access THOR and MKT-GL2-FW1 via https.

2. Navigate to **Policy & Objects > Addresses > Create New** with the following:

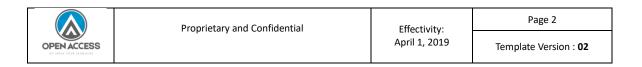
Name: GTI Office
Type: Subnet

Subnet / IP Range: 64.39.96.0/20

Interface: any

Show in Address List: Enable
Static Route Configuration: Disable
Comments: GTI Office Address

Press OK.



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

3. Navigate to **Policy & Objects** > **IPv4 Policy** with the following:

THOR

Name: External VAPT Policy **Incoming Interface:** SD-WAN **Outgoing Interface:** *Internal (port5)*

Source: GTI Office

Destination: INT SUB ZEN (172.18.132.0/24)

INT SUB POSTMATES (172.18.137.0/24) INT_SUB_EXECUTIVE (172.18.70.0 /24) INT_SUB_BOFC_9TH (172.18.9.0/24)

Schedule: always Service: all **Action**: Accept **NAT:** Disabled

Proxy Options: Default **Security Profiles**: All disable

Logging options: Enable – All sessions

Capture Packets – *Disable* **Enable this policy**: Enable

Press OK.

Once created, put the policy on sequence number 1.

G2

Name: External VAPT Policy **Incoming Interface:** SD-WAN **Outgoing Interface:** *Internal (port5)*

Source: GTI Office

Destination: INT SUB G2 WV (172.22.11.0/24)

Proprietary and Confidential

INT_SUB_G2_QUORA (172.22.12.0/24) INT_SUB_G2_AVA (172.22.13.0/24) INT_SUB_EXECUTIVE (172.22.16.0/24) INT_SUB_UIPATH (172.22.24.0/24) INT_SUB_NDY (172.22.26.0/24)

INT_SUB_RECRUITMENT (172.22.15.0/24)

Schedule: always Service: all **Action**: Accept **NAT:** Disabled



Dun anna Outra ann	FORM	
Process Owner: IT Operations	Configuration Change Request	F-CMG-3.1

Proxy Options: Default **Security Profiles**: *All disable*

Logging options: Enable – All sessions

Capture Packets – *Disable* **Enable this policy**: *Enable*

Press OK.

Once created, put the policy on sequence number 1.

Verification Procedures

- 1. Access both **THOR** and **MKT-GL2-FW1** via https.
- 2. Navigate to Policy & Objects > IPv4 Policy
- 3. The policy "External VAPT Policy" should be on sequence number 1.
- 4. Coordinate with **GTI team** if the scanner is now interacting with 2 of our Firewalls (**JAKA and G2**).

Back-out Procedures

- 1. Access both JAKA and G2 firewall.
- 2. Disable the IPv4 policy "External VAPT Policy" on both of JAKA and G2 firewall.
- 3. Once disabled, delete the policy.
- 3. Delete the created address object *GTI Public IP Office, GTI Public IP Scanner*.

