

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

Request Information				
Requestor	Network Operations			
Implementing Team	Network Operations			
Ticket Number/s	201914920			
Change Classification	X	Major		Minor
After the fact		Yes	X	No
Emergency	X	Yes		No
Proposed Change Date	April 23, 2019			
Proposed Change Start/End Time	21:00			
Proposed Change Verification Time	21:10			

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: Allowing of GTI Team Public IP Address inbound to all subnets.	Beneficial: The team will be able to proceed for External VAPT scan.	Neutral: Network Firewall Core Switch

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
N/A

Test Environment Results Summary
N/A

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

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
No Inbound IPv4 policy for External VAPT Scan.	Creation of Inbound IPv4 policy; Source: GTI Public IP (WAN) Destination: All subnets (LAN)	Firewall IPv4 policy	3.1.402 3.1.10.2

Physical Implementation 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 Public IP Office
Type: IP Range
Subnet / IP Range: 64.39.96.0-64.39.111.254
Interface: any
Show in Address List: Enable
Static Route Configuration: Disable
Comments: GTI Office Address

Press **OK**.

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

Repeat Step 2 for IP Address 122.180.254.231 named GTI Public IP Scanner

3. Navigate to **Policy & Objects > IPv4 Policy** with the following:
Name: *External VAPT Policy*
Incoming Interface: *SD-WAN*
Outgoing Interface: *Internal (port5)*
Source: *GTI Public IP Office*
GTI Public IP Scanner
Destination: *all*
Schedule: *always*
Service: *all*
Action: *Accept*
NAT: *Disabled*
Proxy Options: *Default*
Security Profiles: *All disable*
Logging options: *Enable – Security Events*
Capture Packets – Disable
Enable this policy: *Enable*

Once created, put the policy on sequence number 2.

Verification Procedures
<ol style="list-style-type: none"> 1. Navigate to Policy & Objects > IPv4 Policy 2. The policy “External VAPT Policy” should be on sequence number 2. 3. Coordinate with GTI team if the scanner is now interacting with 2 of our Firewalls (JAKA and G2).

Back-out Procedures
<ol style="list-style-type: none"> 1. Access both JAKA and G2 firewall. 2. Disable the 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.