

Process Owner: IT Operations	FORM	F-CMG-3.1
	2FA for FortiGate SSL VPN using DUO	

Request Information				
Requestor	Maurice Mendoza			
Implementing Team	Network Operations			
Ticket Number/s	201915572			
Change Classification	X	Major		Minor
After the fact		Yes	X	No
Emergency		Yes	X	No
Proposed Change Date	May 17, 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: No known negative impact.	Beneficial: Improved security: By requiring a second form of identification.	Neutral: Additional cabling and utilization of switchport of DMZ switch Additional power for Duo Auth Proxy and Radius server in Rack A

Affected IT Infrastructure components			
Site	Hostname	IP Address	Function
JAKA	ODYSSEUS	10.1.0.100	VPN Device

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 FortiGate 101E with SSL VPN, installed Duo Authentication proxy and daloRadius in the test server. Followed all the steps provided by Duo for FortiGate SSL VPN with Duo integration. https://duo.com/docs/fortinet

Test Environment Results Summary
Upon testing, whenever a user logs in to the FortiClient SSL VPN, DUO sends a Login request message to the registered device. If accepted, user will be logged in successfully. If not, FortiGate will drop and revert to the login page.

Process Owner: IT Operations	FORM	F-CMG-3.1
	<i>2FA for FortiGate SSL VPN using DUO</i>	

Configuration Change Template

Baseline File	3.1.407
Baseline Version	April 3, 2019

Baseline File Changes:

Existing Configuration	Proposed Change	Impact	Section
No existing 2 Factor Authentication configured in the VPN Device	Improved security: By adding the Factor Authentication using Duo	SSL-VPN portal and settings, Radius Server, User and Groups	3.1.407

Physical Implementation Procedures / Advisory

1. Place the configured Duo Authentication Proxy and Radius server in Rack A.
2. Connect a LAN cable from Radius server to port fa0/3 of DMZ Switch.
3. Connect a monitor, keyboard, and mouse to the Radius server.

Backup Procedures

Access Odyssey via web (<https://10.1.0.100:10443>)

Backup the configurations files using the naming conventions:

BACKUP_DEVICENAME_DATE.cfg

Example: BACKUP_ODYSSEUS_5172019.cfg

Technical Configuration Procedures

1. Access Odyssey via web(<https://10.1.0.100:10443>)
2. Navigate to User & Device > Radius Servers
3. Create new Radius Server with the following details:

Name	<input type="text" value="Duo Radius"/>	
Primary Server IP/Name	<input type="text" value="10.1.0.101"/>	
Primary Server Secret	<input type="password" value="*****"/>	<input type="button" value="Test Connectivity"/>
Secondary Server IP/Name	<input type="text"/>	
Secondary Server Secret	<input type="password"/>	<input type="button" value="Test Connectivity"/>
Authentication Method	Default <input type="button" value="Specify"/>	
Method	<input type="text" value="PAP"/>	
NAS IP	<input type="text"/>	
Include in every User Group	<input type="checkbox"/>	

4. Navigate to User & Device > User Groups
5. Create new User Group with the following details:

Process Owner: IT Operations	FORM	F-CMG-3.1
	2FA for FortiGate SSL VPN using DUO	

Name: Duo SSL VPN
 Type: ☒ Firewall ☐ Fortinet Single Sign-On (FSSO) ☐ Guest
 Members: Click to add...
 Remote groups:

Remote Server	
Duo Radius	Any

6. Go to VPN > SSL-VPN Settings. Scroll down to Authentication/Portal Mapping
 7. Create new mapping with the following details:

Users/Groups: Duo SSL VPN
 Portal: full-access

Verification Procedures

1. Using FortiClient, create new connection with the following details:

Edit VPN Connection

VPN: SSL-VPN IPsec VPN

Connection Name: OAMPI VPN

Description:

Remote Gateway: 10.1.0.100 ✕

[+Add Remote Gateway](#)

☒ Customize port: 443

Client Certificate: None

Authentication: ☐ Prompt on login ☒ Save login

Username: mmendoza

☒ Do not Warn Invalid Server Certificate

2. Once created and saved, key in the credentials in the SSL-VPN login page then click connect.

Process Owner: IT Operations	FORM	F-CMG-3.1
	2FA for FortiGate SSL VPN using DUO	

VPN Name

OAMPI VPN

Username

mmendoza

Password

.....|

Connect

Back-out Procedures

- Go to VPN > SSL-VPN Settings. Scroll down to Authentication/Portal Mapping
- Delete the previously created mapping with the following details:

Users/Groups

Duo SSL VPN

Portal

full-access
- Remove the configured Duo Authentication Proxy and Radius server from Rack A.
- Unplug the LAN cable from Radius server to port fa0/3 of DMZ Switch.