

คู่มือการใช้งาน Virtual Firewall FortiGate



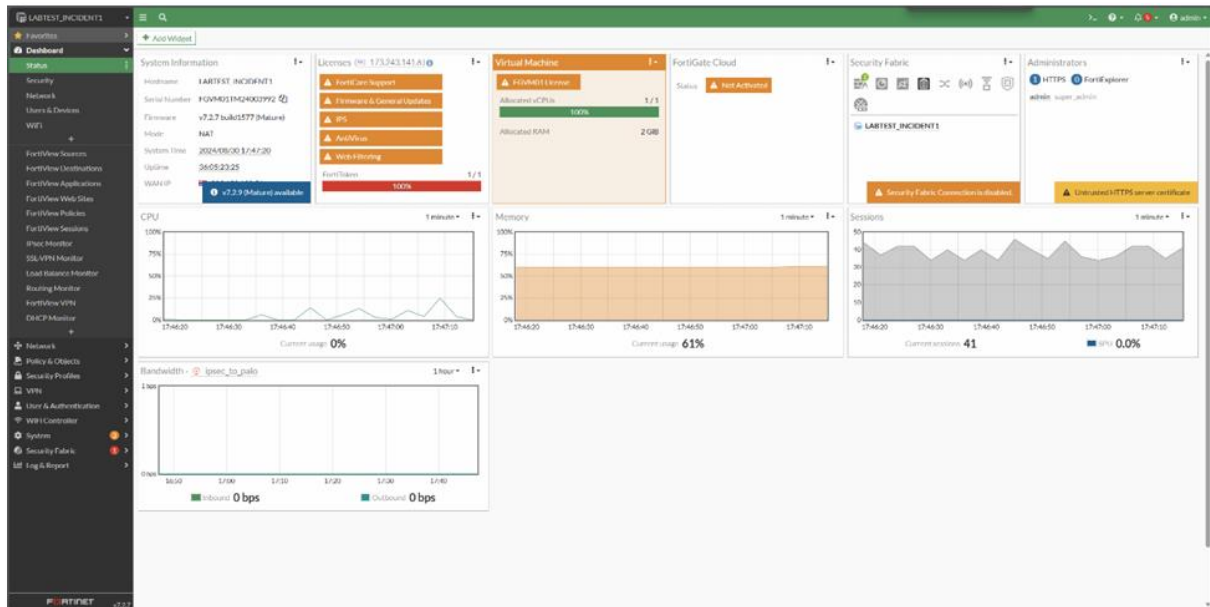
สารบัญ

เนื้อหา	หน้า
Dashboard FORTIGATE.....	3
Network Interface FORTIGATE.....	3
Policy FORTIGATE.....	4
SSL VPN FORTIGATE.....	13
Log & Report FORTIGATE.....	20

Firewall: FortiGate

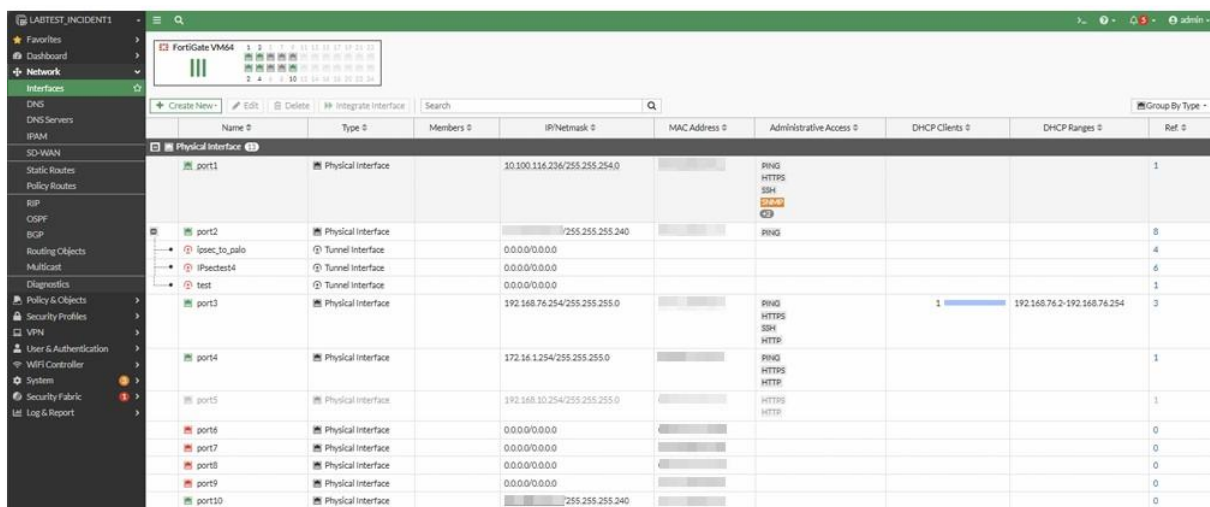
Dashboard FORTIGATE

Dashboard > Status คือหน้าหลักเมื่อเข้าใช้งานระบบ vFW FortiGate จะแสดงข้อมูลภาพรวมของ Firewall



Network Interface FORTIGATE

เมนู Network > Interface ใช้แสดง Interface ที่เชื่อมต่อกับ IP Network หรือ VLAN ต่างๆ รวมถึง IPSEC ที่เชื่อมอยู่ภายใต้ Firewall ด้วย



The screenshot displays the FortiGate Network > Interface page. The table lists the following interfaces:

Name	Type	Members	IP/Netmask	MAC Address	Administrative Access	DHCP Clients	DHCP Ranges	Ref
port1	Physical Interface		10.100.116.236/255.255.254.0		RING			1
port2	Physical Interface		255.255.255.240		RING			8
port2	Physical Interface		0.0.0.0/0.0.0.0					4
port2	Physical Interface		0.0.0.0/0.0.0.0					6
port2	Physical Interface		0.0.0.0/0.0.0.0					1
port3	Physical Interface		192.168.76.254/255.255.255.0		RING	1	192.168.76.2-192.168.76.254	3
port4	Physical Interface		172.16.1254/255.255.255.0		RING			1
port5	Physical Interface		192.168.10.254/255.255.255.0		HTTPS			1
port6	Physical Interface		0.0.0.0/0.0.0.0					0
port7	Physical Interface		0.0.0.0/0.0.0.0					0
port8	Physical Interface		0.0.0.0/0.0.0.0					0
port9	Physical Interface		0.0.0.0/0.0.0.0					0
port10	Physical Interface		255.255.255.240					0

Policy FORTIGATE

เข้าเมนู Policy & Objects > Firewall Policy เพื่อดูหรือตั้งค่า Policy ต่างๆ โดยลำดับการทำงานของ Policy จะเรียงลำดับเริ่มจาก ลำดับบนสุด > ลำดับล่างสุด ในการสร้าง Policy จะแบ่งเป็น Policy ขา เข้า Inbound Policy [DNAT] และ ขาออก Outbound [SNAT]

Q													
Q													
Name	From	To	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes	Type	
test-dp	DOD	WAN	172.16.1.10	all	always	ALL	✓ ACCEPT	Enabled	DLP-deep-inspection VDP test	All	1.65 GB	Standard	
A	Floppod Cloud	WAN	192.168.76.135	VIP_203.150.108.49_8080	always	ALL	✓ ACCEPT	Enabled	no-inspection	Disabled	0 B	Standard	
B	WAN	Floppod Cloud	Thailand	VIP_203.150.108.49_8080	always	ALL	✓ ACCEPT	Disabled	no-inspection	All	1.26 MB	Standard	
C	Floppod Cloud	Floppod Cloud	192.168.76.135	VIP_192.168.76.10	always	ALL	✓ ACCEPT	Enabled	no-inspection	All	0 B	Standard	
D	Floppod Cloud	Floppod Cloud	192.168.76.135	VIP_203.150.108.49_8080	always	ALL	✓ ACCEPT	Enabled	no-inspection	All	0 B	Standard	
Flow to DOD	Floppod Cloud	DOD	192.168.20.0/24	172.16.10.2/4	always	ALL	✓ ACCEPT	Disabled	no-inspection	All	0 B	Standard	
Schedules	VIP_203.150.108.49_8080	WAN	Floppod Cloud	VIP_203.150.108.49_8080	always	ALL_8080	✓ ACCEPT	Disabled	no-inspection	All	1.99 MB	Standard	
Virtual IPs	DOD to Flox	DOD	Floppod Cloud	172.16.10.2/4	always	ALL	✓ ACCEPT	Disabled	no-inspection	All	0 B	Standard	
IP Pools	Request to DOD	Floppod Cloud	DOD	192.168.76.10/32 192.168.76.15/32	always	HTTP HTTPS	✓ ACCEPT	Disabled	no-inspection	All	0 B	Standard	
Protocols Options	Request to DOD	Floppod Cloud	DOD	192.168.76.10/32 192.168.76.15/32	always	HTTP HTTPS TCP-21030 UDP-21030	✓ ACCEPT	Disabled	no-inspection	All	0 B	Standard	
Traffic Shaping													
Virtual Servers													
Health-Check													
Security Profiles													
VPN													
User & Authentication													
VPN Controller													
System													
Security Fabric													
Log & Report													
VPN2	any	DOD	Incident SSLVPN_TUNNEL_ADDR1	172.16.1.0/24 192.168.76.0/24	always	ALL	✓ ACCEPT	Disabled	no-inspection	All	173.87 MB	Standard	
VPN	SSLVPN tunnel interface (af-root)	DOD	Incident SSLVPN_TUNNEL_ADDR1	172.16.1.0/24 192.168.76.0/24	always	ALL	✓ ACCEPT	Disabled	no-inspection	All	0 B	Standard	
WAN-192.168.76.135	Floppod Cloud	WAN	Midcomscom	all	always	ALL	✓ ACCEPT	Enabled	no-inspection	All	0 B	Standard	
palo to LAN	Spec to palo	Floppod Cloud	all	all	always	ALL	✓ ACCEPT	Disabled	no-inspection	All	0 B	Standard	
LAN to palo	Spec to palo	Floppod Cloud	all	all	always	ALL	✓ ACCEPT	Disabled	no-inspection	All	0 B	Standard	
VPN to B	SSLVPN tunnel interface (af-root)	Floppod Cloud	LoadB01	192.168.76.0/24	always	DNS HTTPS TCP-8080	✓ ACCEPT	Disabled	no-inspection	All	0 B	Standard	
IPsec test 4 Site to test DR	IPsec test 4	Floppod Cloud	all	all	always	ALL	✓ ACCEPT	Disabled	no-inspection	All	0 B	Standard	
IPsec test 4 Site to test DR	IPsec test 4	Floppod Cloud	all	all	always	ALL	✓ ACCEPT	Disabled	no-inspection	All	0 B	Standard	
Implicit Deny	any	any	all	all	always	ALL	DENY	Enabled	no-inspection	Enabled	82.66 MB	Standard	

Policy ขาออก / Outbound Policy [SNAT]

Step 1: เริ่มที่ตรวจสอบ Interface เครื่องที่ต้องการว่าอยู่ที่ Interface ไต โดยดูได้จากแถบ Network >> Interface

Step 2: ให้เริ่มดู Zone ที่ต้องการทำ ตัวอย่างเช่น:

ต้องการให้เครื่อง IP: 192.168.76.11 ออก Internet ได้ zone Flexpod Cloud และ Interface port3

Step 3: Create Policy โดยเลือกแถบ Policy & Object > Firewall Policy

The screenshot shows the FortiGate VM64 web interface. On the left, the 'Policy & Objects' menu is expanded, with 'IPv4 Policy' selected. The main area displays a table of existing policies. The table has columns for ID, Name, From, To, Source, Destination, Schedule, Service, Action, NAT, Security Profiles, Log, and Bytes. The first policy listed is ID 0, named 'Implicit Deny', with 'any' for both From and To, 'all' for both Source and Destination, 'always' for the Schedule, 'ALL' for the Service, 'DENY' for the Action, and 'Disabled' for the Log status. The Bytes column shows '698 B'.

ID	Name	From	To	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
0	Implicit Deny	any	any	all	all	always	ALL	DENY			Disabled	698 B

Step 4: Create policy SNAT

New Policy

ID

0

Name

SNAT-192.168.76.11

Incoming Interface

Flexpod Cloud

+

✕

Outgoing Interface

WAN

+

✕

Source

192.168.76.11/32

+

✕

Negate Source

☐

Destination

all

+

✕

Negate Destination

☐

Schedule

always

Service

ALL

Action

ACCEPT

DENY

Inspection Mode

Flow-based

Proxy-based

Firewall/Network Options

NAT

☒

IP Pool Configuration

Use Outgoing Interface Address

Use Dynamic IP Pool

Preserve Source Port

☐

Protocol Options

PROT

default

✎

Disclaimer Options

Display Disclaimer

☐

Security Profiles

AntiVirus

☐

Web Filter

☐

DNS Filter

☐

Application Control

☐

IPS

☐

File Filter

☐

SSL Inspection

SSL

no-inspection

✎

Logging Options

Log Allowed Traffic

☒

Security Events

All Sessions

Generate Logs when Session Starts

☐

Capture Packets

☐

Advanced

WCCP

☐

Exempt from Captive Portal

☐

Workflow Management

Policy expiration

☐

Comments

Write a comment...

0/1023

Enable this policy

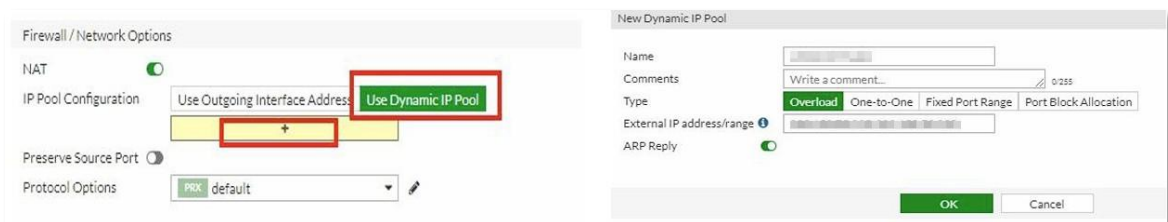
☒

5 | Page

 TEL +66 2017 7777
 FAX +66 2017-7778
 CALL CENTER +66 2017 7770

ในหน้าต่าง New Policy ให้กรอกข้อมูลดังนี้

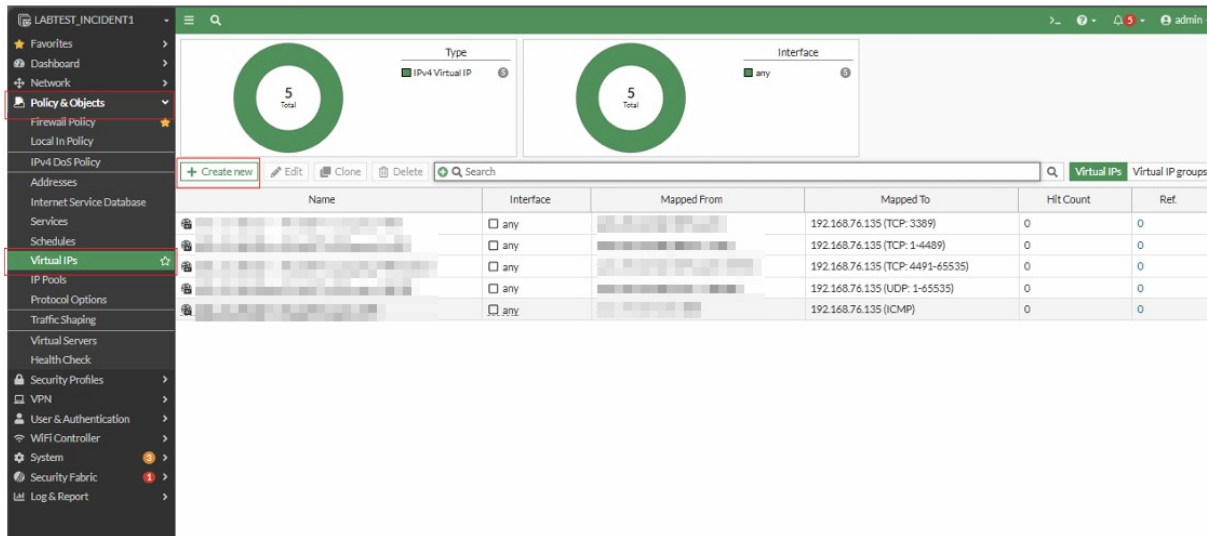
- **Name:** ตั้งชื่อให้กับ Policy ให้สื่อถึงการใช้งานตาม IP เช่น SNAT-192.168.76.11 เป็นต้น
- **Incoming Interface:** เลือก Interface ที่ Traffic จะเข้ามา (เช่น Flexpod Cloud).
- **Outgoing Interface:** เลือก Interface ที่ Traffic จะออกไป (เช่น WAN).
- **Source:** ระบุแหล่งที่มาของ Traffic (IP Address, Subnet, หรือ Object) หากยังไม่มีจะต้องสร้าง Object ก่อน
- **Destination:** ระบุปลายทางของ Traffic (IP Address, Subnet, หรือ Object) หากยังไม่มีจะต้องสร้าง Object ก่อน
- **Schedule:** กำหนดเวลาที่ Policy จะทำงาน (เช่น Always หากต้องการให้ทำงานตลอดเวลา).
- **Service:** เลือกประเภทบริการที่ต้องการควบคุม (เช่น HTTP, HTTPS, หรือ All หากต้องการควบคุมทุก Service) หากยังไม่มีจะต้องสร้าง Object ก่อน
- **Security Profile** กรณีลูกค้ามีการใช้งานพวก Feature App control หรือ Web filter เป็นต้น
- **Logging Option** การเก็บ Log ให้เลือกเก็บแบบ All Session
- **Action:** เลือก Allow เพื่ออนุญาต หรือ Deny เพื่อปฏิเสธ Traffic
- **ID** ไม่จำเป็นต้องกรอก โดยหลังจาก Create New Policy ID จะเริ่มนับต่อจาก ID ล่าสุดที่ถูกสร้างขึ้น



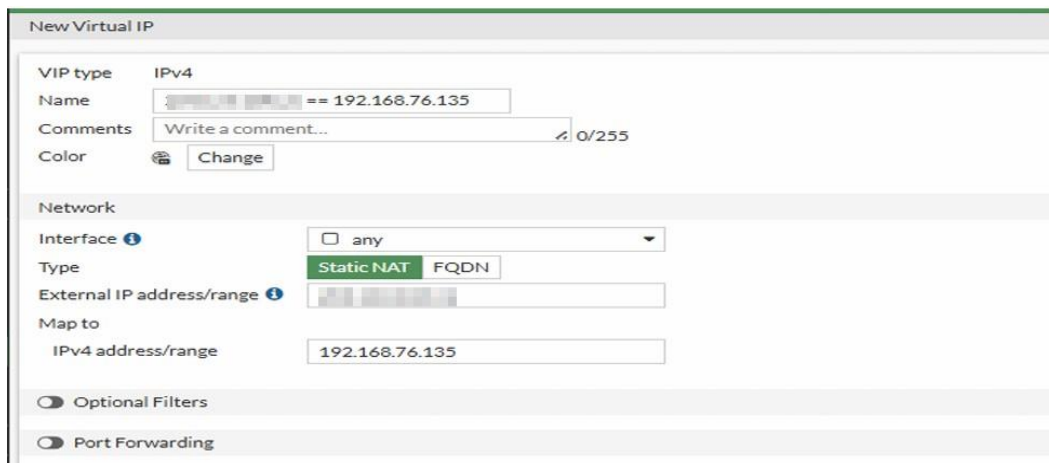
- **NAT:** เปิดใช้งานหากต้องการทำ Network Address Translation.
โดยการ NAT จะเป็นการเปลี่ยน IP source เดิมให้เป็น IP ใหม่ ที่นี้จะเลือกใช้งานเป็น IP interface ตาม interface outgoing ในข้อ 2 จะออกเป็น IP 203.150.79.227 ทั้งนี้หากต้องการ NAT เป็น IP อื่นๆตามที่ทางลูกค้า request
ให้เลือก Dynamic pool แล้วจึงสร้าง pool public ใหม่หากยังไม่มี object
- หากกำหนดค่าต่างๆ เรียบร้อยแล้ว อย่าลืมที่จะ Enable Policy

Policy ขาเข้า Inbound Policy [DNAT]

Step 1: สร้าง Virtual IP (VIP) โดยการ MAP IP [WAN] เข้ากับ IP [LAN] โดยไปยังแถบ Policy & Object
> Virtual IPs จากนั้นเลือก Create



- การ MAP IP จะได้ผลออกมาเป็น Object ที่ภายในมีการ Forward packet จาก ขา WAN ไปยัง ขา LAN



New Virtual IP

VIP type: IPv4

Name: [Redacted] == 192.168.76.135

Comments: Write a comment... 0/255

Color: [Redacted] Change

Network

Interface: any

Type: Static NAT FQDN

External IP address/range: [Redacted]

Map to: IPv4 address/range 192.168.76.135

Optional Filters: [Off]

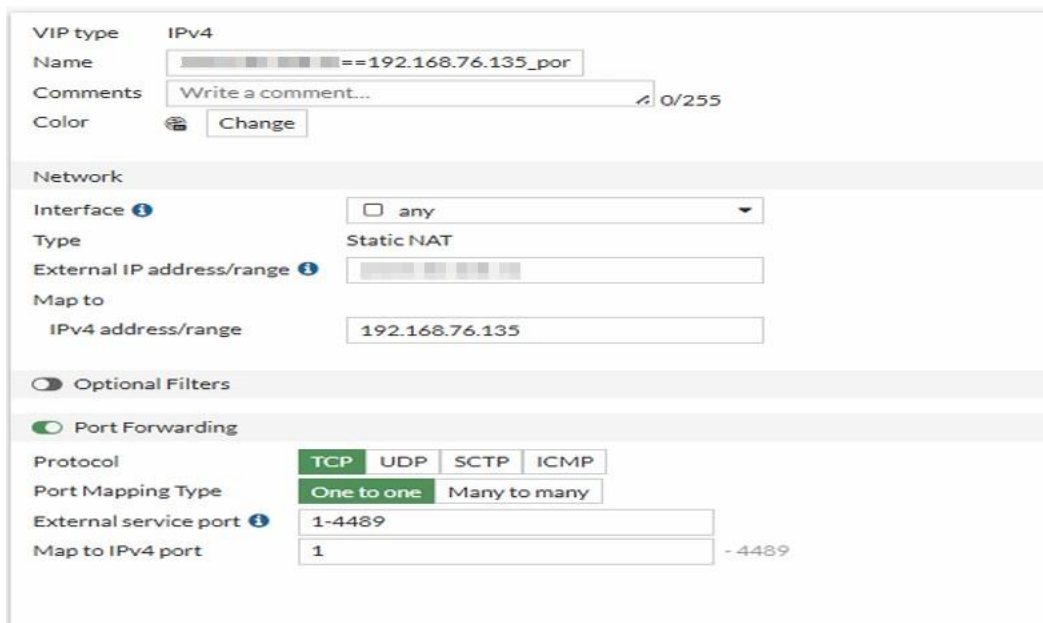
Port Forwarding: [Off]

*** ในหัวข้อ External IP จะเป็น IP WAN ที่เราต้องการใช้งาน MAP กับ LAN IP address

Step 2: กรณีหากลูกค้าต้องการจะทำ port forwarding ให้ดำเนินการ MAP เหมือนขั้นตอนปกติ แต่จะเพิ่มในส่วนของ Port Forwarding

โดยส่วน Port Forwarding จะมีให้เลือกส่วน 4 ส่วน

- **Protocol:** ชนิดของ Protocol ที่ต้องการ Forward Port
- **Port Mapping Type:** ประเภทของการ Mapping Port ปกติจะเลือก one to one
- **External service port:** Port ที่จะเรียกเข้ามาจากภายนอก
- **Map to IPv4 port:** Port ที่ต้องการ Forward ต่อ



VIP type: IPv4

Name: ==192.168.76.135_por

Comments: Write a comment... 0/255

Color:  Change

Network

Interface:  any

Type: Static NAT

External IP address/range: 

Map to:

IPv4 address/range: 192.168.76.135

Optional Filters

☒ Port Forwarding

Protocol: **TCP** UDP SCTP ICMP

Port Mapping Type: **One to one** Many to many

External service port:  1-4489

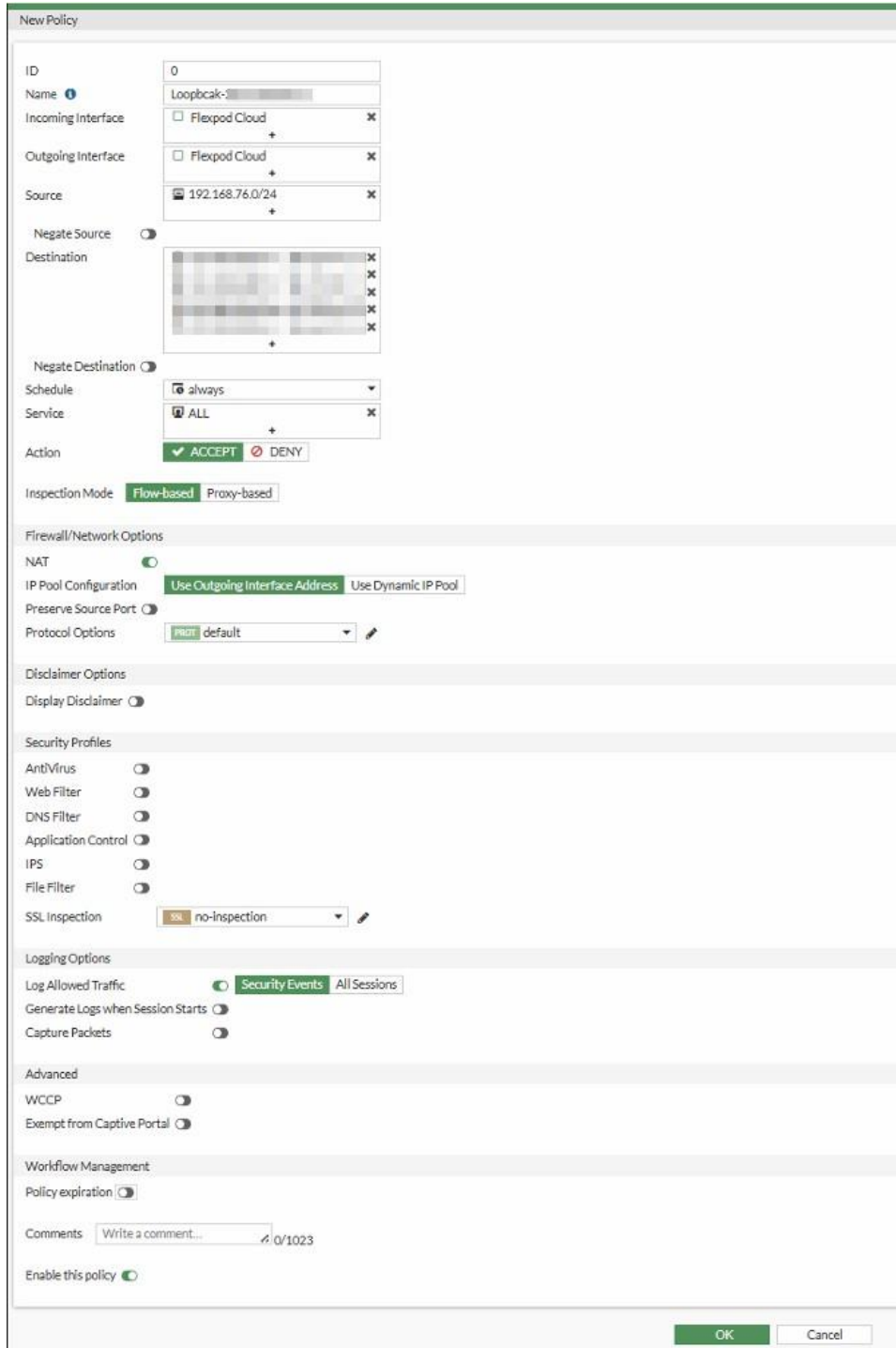
Map to IPv4 port: 1 - 4489

โดยในหน้าต่าง New Policy ให้กรอกข้อมูลดังนี้:

- ID ไม่จำเป็นต้องกรอก โดยหลังจาก Create New Policy ID จะเริ่มนับต่อจาก ID ล่าสุดที่ถูกสร้างขึ้นมา
- Name: ตั้งชื่อให้กับ Policy
- Incoming Interface: เลือก Interface ที่ Traffic จะเข้ามา (เช่น WAN).
โดยปกติของ Policy DNAT ส่วนใหญ่จะเข้ามาจาก Interface Wan แต่ก็สามารถเข้ามาจาก Interface อื่นๆได้ เช่น LAN จะเป็นส่วนของ Policy Loopback
- Outgoing Interface: เลือก Interface ที่ Traffic จะออกไป (เช่น Flexpod Cloud).
จะต้องเลือกจาก Interface ที่เครื่องปลายทางอยู่เช่น 192.168.76.135 อยู่ Flexpod Cloud เป็นต้น
- Source: ระบุแหล่งที่มาของ Traffic (IP Address, Subnet, หรือ Object). หากยังไม่มีจะต้องสร้าง Object ก่อน
- Destination: ระบุปลายทางของ Traffic (IP Address, Subnet, หรือ Object). หากยังไม่มีจะต้องสร้าง Object ก่อน
- Schedule: กำหนดเวลาที่ Policy จะทำงาน (เช่น Always หากต้องการให้ทำงานตลอดเวลา).
- Service: เลือกประเภทบริการที่ต้องการควบคุม (เช่น HTTP, HTTPS, หรือ All หากต้องการควบคุมทุก Service). หากยังไม่มีจะต้องสร้าง Object ก่อน
- Security Profile กรณีลูกค้ามีการใช้งานพวก Feature App control หรือ Web filter
การใช้งาน Feature ต่างๆ *** มีข้อควรระวัง คือหากมีการเปิดใช้อาจส่งผลกระทบต่อการใช้งานเพราะอาจมีบาง feature ที่เป็นการ block service เป็นต้น
- Logging Option การเก็บ Log ให้เลือกเก็บแบบ All Session
- Action: เลือก Allow เพื่ออนุญาต หรือ Deny เพื่อปฏิเสธ Traffic
- NAT: เปิดใช้งานหากต้องการทำ Network Address Translation.
โดยการ NAT จะเป็นการเปลี่ยน IP source เดิมให้เป็น IP ใหม่ หากมีการเปิดใช้งาน source ดังกล่าว จะถูกเปลี่ยนเป็น IP ตามที่กำหนด และ บางทีอาจจะทำให้ไม่ทราบ Source IP ที่แท้จริงที่เรียกเข้ามาได้
- หากกำหนดค่าต่างๆ เรียบร้อยแล้ว อย่าลืมที่จะ Enable Policy เป็นอันเรียบร้อย

Step 4: Policy Loopback

กรณีที่เครื่องอยู่ภายใต้ Firewall เดียวกัน เรียกมายัง IP Public ของที่ภายใต้ Firewall เดียวกัน เช่นกัน โดยลักษณะของ Policy จะสร้างคล้ายๆของ Policy DNAT แต่จะแตกต่างที่ Source Interface จะเป็น Interface ภายใต้ Firewall ไม่ใช่ WAN และ มีการ NAT Source เพิ่มเพื่อให้สามารถเรียกไปยัง IP Public ที่อยู่ภายใต้ Firewall เดียวกันได้

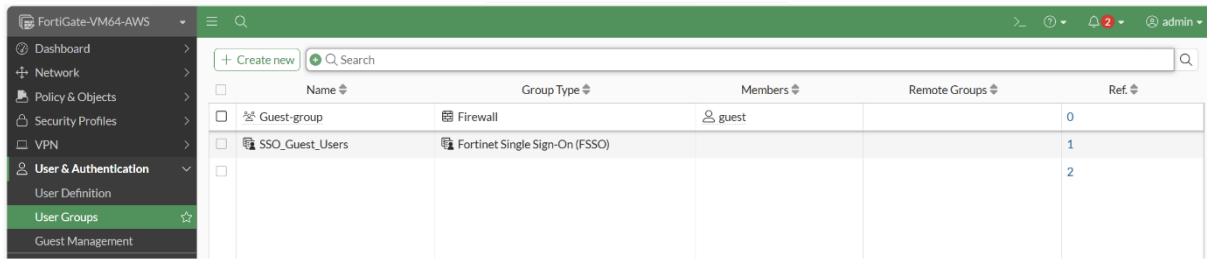


โดยในหน้าต่าง **New Policy** ให้กรอกข้อมูลดังนี้:

- **ID** ไม่จำเป็นต้องกรอก โดยหลังจาก **Create New Policy** ID จะเริ่มนับต่อจาก ID ล่าสุดที่ถูกสร้างขึ้นมา
- **Name:** ตั้งชื่อให้กับ Policy
- **Incoming Interface:** เลือก Interface ที่ Traffic จะเข้ามา (เช่น Flexpod Cloud).
โดยปกติของ Policy DNAT ส่วนใหญ่จะเข้ามาจาก Interface Wan แต่ก็สามารถเข้ามาจาก Interface อื่นๆได้ เช่น LAN จะเป็นส่วนของ Policy Loopback
- **Outgoing Interface:** เลือก Interface ที่ Traffic จะออกไป (เช่น Flexpod Cloud).
จะต้องเลือกจาก Interface ที่เครื่องปลายทางอยู่เช่น 192.168.76.135 อยู่ Flexpod Cloud เป็นต้น
- **Source:** ระบุแหล่งที่มาของ Traffic (IP Address, Subnet, หรือ Object). หากยังไม่มีจะต้องสร้าง Object ก่อน
- **Destination:** ระบุปลายทางของ Traffic (IP Address, Subnet, หรือ Object). หากยังไม่มีจะต้องสร้าง Object ก่อน
- **Schedule:** กำหนดเวลาที่ Policy จะทำงาน (เช่น Always หากต้องการให้ทำงานตลอดเวลา).
- **Service:** เลือกประเภทบริการที่ต้องการควบคุม (เช่น HTTP, HTTPS, หรือ All หากต้องการควบคุมทุก Service).
- **Security Profile** กรณีลูกค้ามีการใช้งานพวก Feature App control หรือ Web filter
การใช้งาน Feature ต่างๆ *** มีข้อควรระวัง คือหากมีการเปิดใช้อาจส่งผลกระทบต่อการใช้งานเพราะอาจมีบาง feature ที่เป็นการ block service เป็นต้น
- **Logging Option** การเก็บ Log ให้เลือกเก็บแบบ All Session
- **Action:** เลือก Allow เพื่ออนุญาต หรือ Deny เพื่อปฏิเสธ Traffic
- **NAT:** เปิดใช้งานหากต้องการทำ Network Address Translation.
โดยการ NAT จะเป็นการเปลี่ยน IP source เดิมให้เป็น IP ใหม่ให้เป็น วง Network ภายใต้ Firewall เพื่อให้สามารถเรียกไปยังปลายทางที่เป็น IP Public ที่อยู่ภายใต้ Firewall เดียวกันได้ ตัวอย่างเช่น 192.168.76.135 NAT 192.168.76.254 เป็นต้น
- หากกำหนดค่าต่างๆ เรียบร้อยแล้ว อย่าลืมที่จะ **Enable Policy** เป็นอันเรียบร้อย

SSL VPN FORTIGATE

Step 1: เริ่มต้นด้วยการสร้าง User VPN Group User & Authentication > User Groups > Create New



Name	Group Type	Members	Remote Groups	Ref
Guest-group	Firewall	guest		0
SSO_Guest_Users	Fortinet Single Sign-On (FSSO)			1
				2

- กำหนดชื่อ Group > จากนั้นกดที่ OK

New User Group

Name

Type

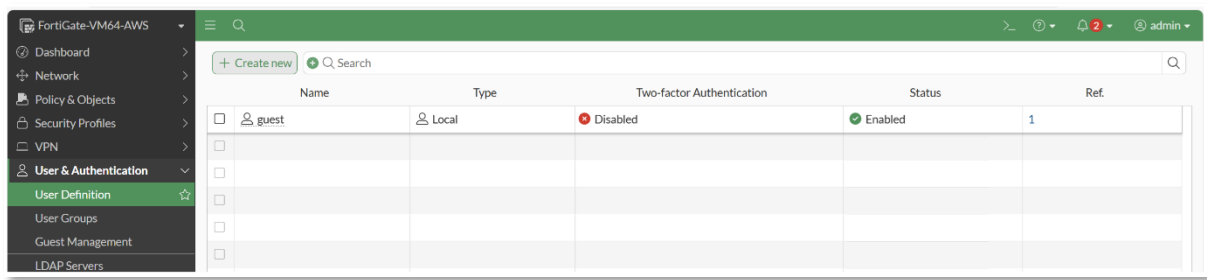
Firewall
Fortinet Single Sign-On (FSSO)
RADIUS Single Sign-On (RSSO)
Guest

Members

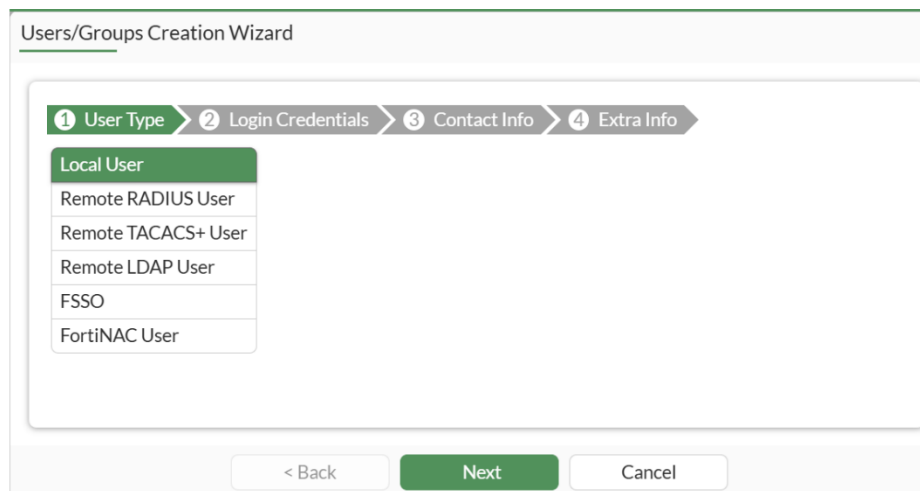
OK

Cancel

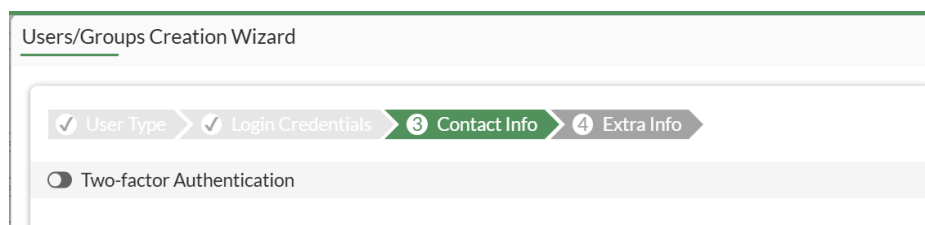
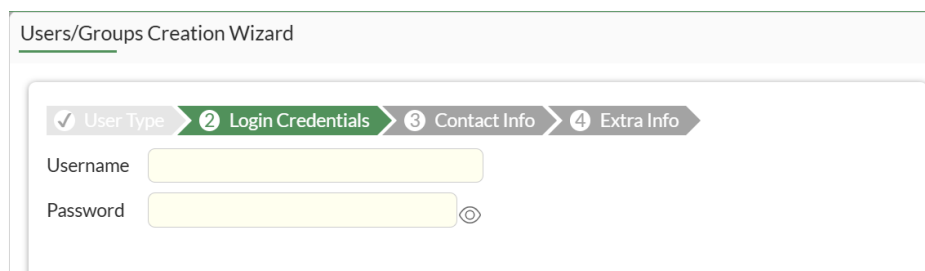
Step 2: สร้าง User ใหม่ ไปที่ User & Authentication > User Definition > Create New



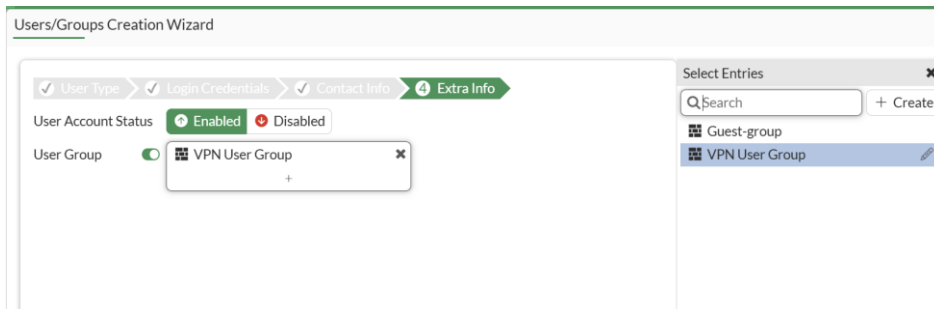
- เลือกไปที่ Local User > Next



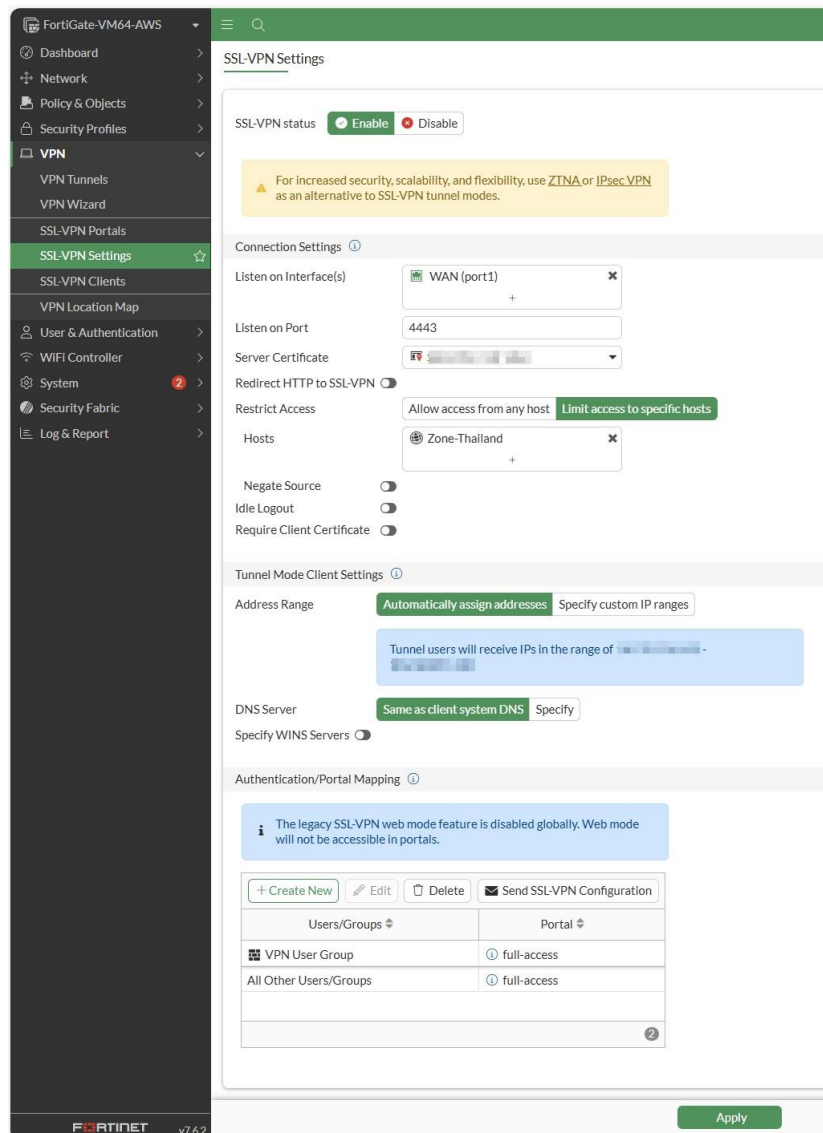
- กำหนด Username / Password ให้เรียบร้อย > Next // หากไม่มี 2FA ให้ Next ข้ามไปก่อนได้เลย



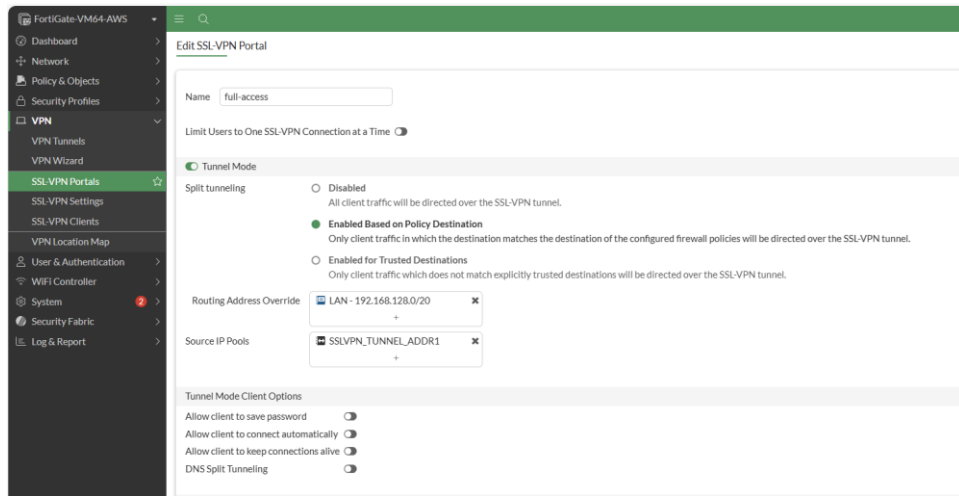
- เลือก Enable กดเลือก User Group เป็น group ที่สร้างไว้ตอน Step 1 แล้วกด OK เป็นอันเสร็จสมบูรณ์ ในการสร้าง User VPN



Step 3: ที่ SSL-VPN Setting ตรง Authentication/Portal Mapping กด Create New Group ที่เราสร้างแล้วเลือก Full Access



- ไปที่หน้า SSL-VPN Portal กดที่ full access แล้วกด edit จากนั้น Enable Split Tunneling ออก แล้วกด OK



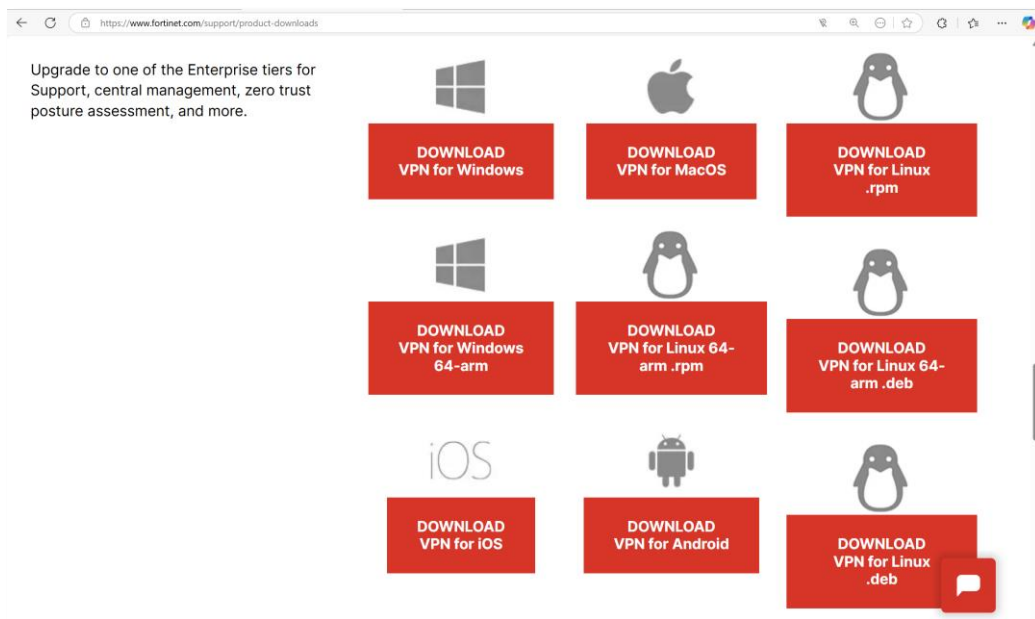
Step 4: สร้าง Policy สำหรับการใช้งาน SSL-VPN โดยในหน้าต่าง New Policy ให้กรอกข้อมูลดังนี้:

- ID ไม่จำเป็นต้องกรอก โดยหลังจาก Create New Policy ID จะเริ่มนับต่อจาก ID ล่าสุดที่ถูกสร้างขึ้น
- Name: ตั้งชื่อให้กับ Policy ให้สื่อถึงการใช้งานตาม IP เช่น VPN TO CLOUD เป็นต้น
- Incoming Interface: เลือก Interface ที่ Traffic จะเข้ามา (เช่น SSL-VPN tunnel interface (ssl.root)). โดยปกติของ Policy ของ SSL VPN จะเลือก SSL-VPN tunnel interface (ssl.root) เป็น Interface
- Outgoing Interface: เลือก Interface ที่ Traffic จะออกไป (เช่น Flexpod Cloud). จะต้องเลือกจาก Interface ที่เครื่องปลายทางอยู่เช่น 192.168.76.0/24 อยู่ Flexpod Cloud
- Source: ระบุแหล่งที่มาของ Traffic (IP Address, Subnet, หรือ Object). หากยังไม่มีจะต้องสร้าง Object ก่อน
- Destination: ระบุปลายทางของ Traffic (IP Address, Subnet, หรือ Object). หากยังไม่มีจะต้องสร้าง Object ก่อน
- Schedule: กำหนดเวลาที่ Policy จะทำงาน (เช่น Always หากต้องการให้ทำงานตลอดเวลา).
- Service: เลือกประเภทบริการที่ต้องการควบคุม (เช่น HTTP, HTTPS, หรือ All หากต้องการควบคุมทุก Service).
- Logging Option การเก็บ Log ให้เลือกเก็บแบบ All Session
- Action: เลือก Allow เพื่ออนุญาต หรือ Deny เพื่อปฏิเสธ Traffic
- หากกำหนดค่าต่างๆ เรียบร้อยแล้ว อย่าลืมที่จะ Enable Policy เป็นอันเรียบร้อย

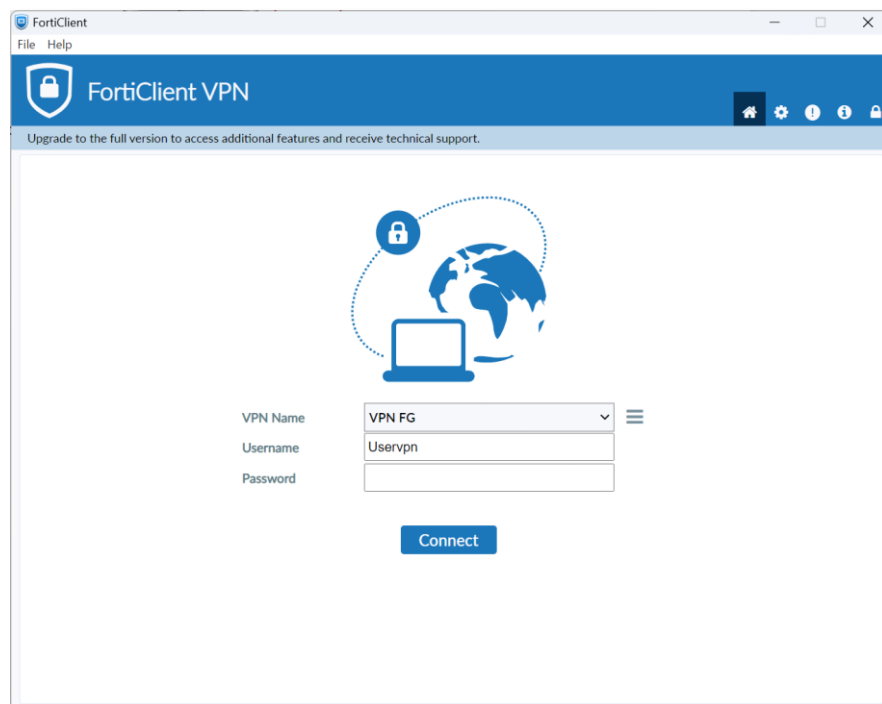
FortiClient VPN

Download Client VPN จาก <https://www.fortinet.com/support/product-downloads>

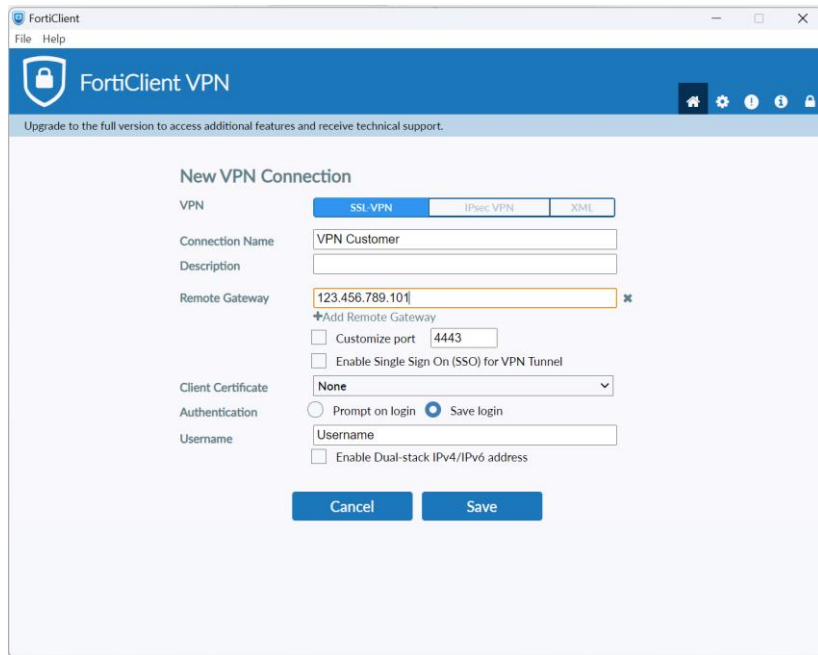
- เลือก Product Download > Forticlient VPN Only



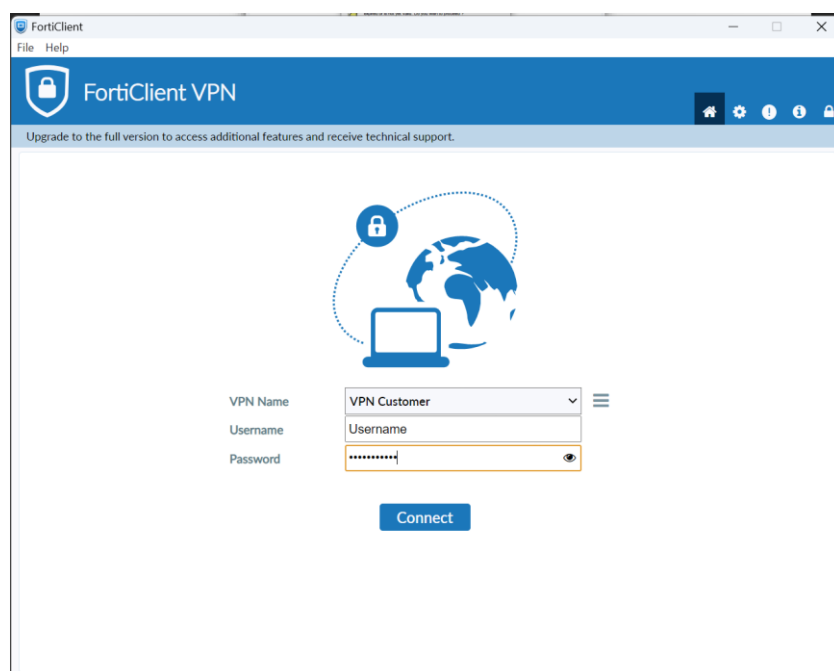
- หลังจากติดตั้ง Forticlient ที่เป็น Program สำหรับการ VPN เรียบร้อยแล้ว
- เลือก แถบ 3 ขีด > Add a new Connection



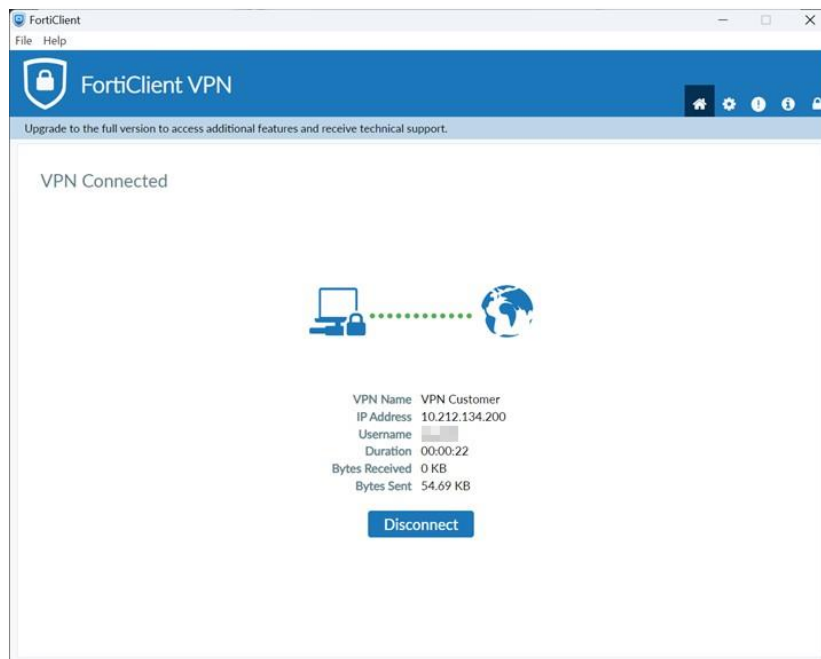
- กำหนดค่า SSL-VPN Connection ตามที่ระบบ Firewall กำหนดไว้ดังนี้
 - 1) Connection Name: CPN customer
 - 2) Remote Gateway: xxx.xxx.xxx.xxx (IP Public ของ Firewall)
 - 3) ทำเครื่องหมายถูกที่ช่อง Customize port และระบุค่าเป็น 4443
 - 4) คลิกปุ่ม Save



- กรอก Username และ Password ที่ใช้ Login เข้าเครื่องคอมพิวเตอร์ที่ทำงาน
- คลิกปุ่ม Connect

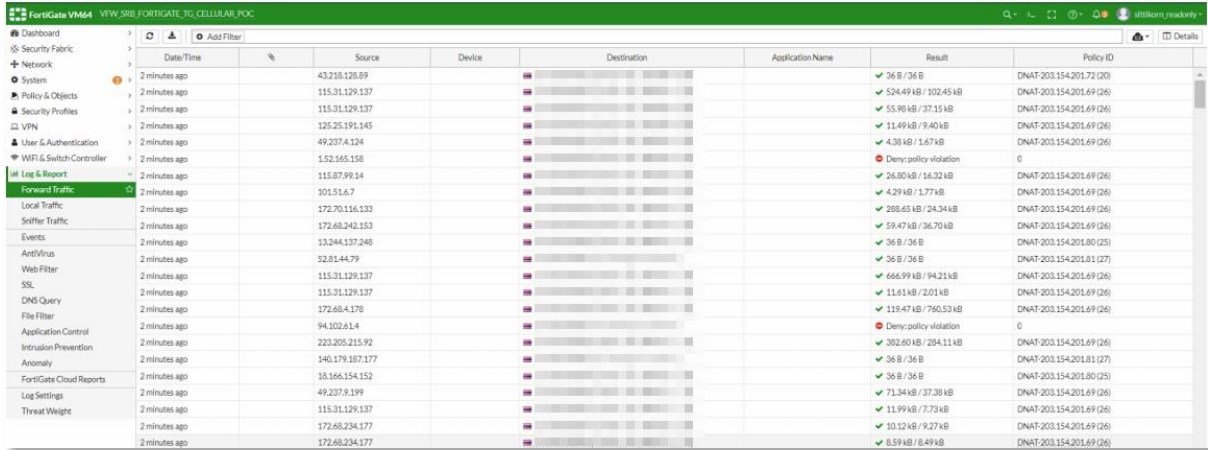


- หาก Config SSL VPN ถูกต้อง และ Login สำเร็จจะได้ผลตามรูปด้านล่าง



Log & Report FORTIGATE

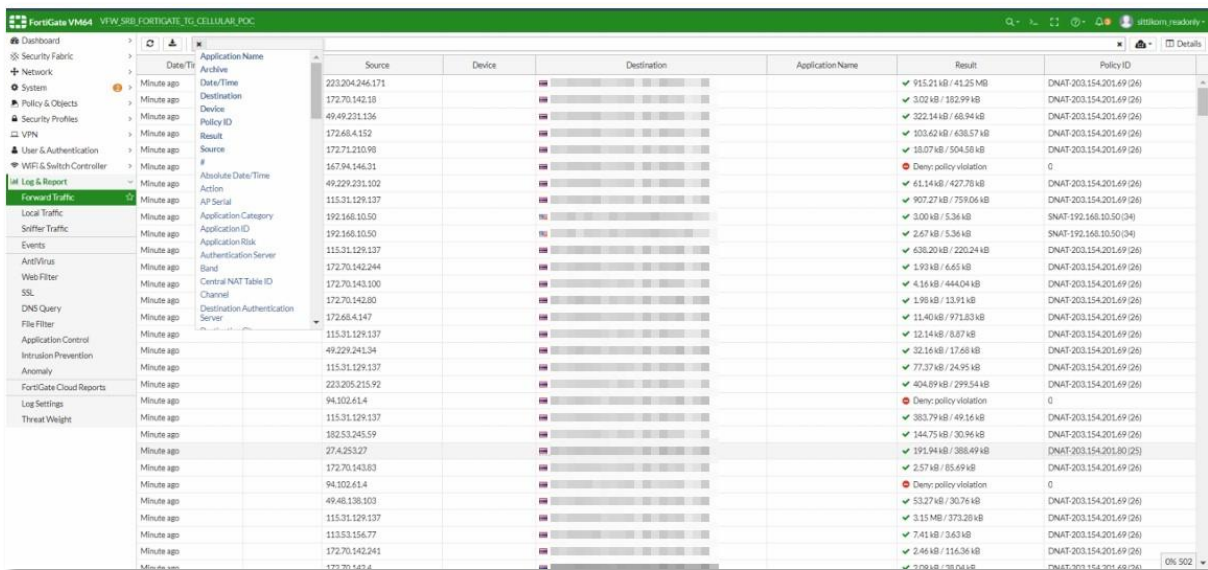
Step 1: ในการดู Log จะเข้ามาที่แถบ Log&Report > Forward Traffic โดยจะโชว์ Log ขึ้นมาดังภาพ



	Date/Time	Source	Device	Destination	Application Name	Result	Policy ID
Forward Traffic	2 minutes ago	43.218.128.89				✓ 36 B / 36 B	DNAT-203.154.201.69 (26)
Local Traffic	2 minutes ago	115.31.129.137				✓ 524.49 KB / 102.45 KB	DNAT-203.154.201.69 (26)
Sniffer Traffic	2 minutes ago	115.31.129.137				✓ 55.98 KB / 37.15 KB	DNAT-203.154.201.69 (26)
Events	2 minutes ago	125.25.191.145				✓ 11.49 KB / 9.40 KB	DNAT-203.154.201.69 (26)
AntiVirus	2 minutes ago	49.237.4.124				✓ 4.38 KB / 1.67 KB	DNAT-203.154.201.69 (26)
Web Filter	2 minutes ago	115.67.99.14				Deny: policy violation	0
SSL	2 minutes ago	101.51.6.7				✓ 26.80 KB / 16.32 KB	DNAT-203.154.201.69 (26)
DNS Query	2 minutes ago	172.70.116.133				✓ 4.29 KB / 1.77 KB	DNAT-203.154.201.69 (26)
File Filter	2 minutes ago	172.68.242.153				✓ 280.65 KB / 24.34 KB	DNAT-203.154.201.69 (26)
Application Control	2 minutes ago	13.244.137.248				✓ 59.47 KB / 36.70 KB	DNAT-203.154.201.69 (26)
Intrusion Prevention	2 minutes ago	52.81.44.79				✓ 36 B / 36 B	DNAT-203.154.201.69 (26)
Anomaly	2 minutes ago	115.31.129.137				✓ 666.99 KB / 94.21 KB	DNAT-203.154.201.69 (26)
FortiGate Cloud Reports	2 minutes ago	115.31.129.137				✓ 11.61 KB / 2.01 KB	DNAT-203.154.201.69 (26)
Log Settings	2 minutes ago	172.68.4.178				✓ 119.47 KB / 760.53 KB	DNAT-203.154.201.69 (26)
Threat Weight	2 minutes ago	94.102.61.4				Deny: policy violation	0
	2 minutes ago	223.205.215.92				✓ 302.60 KB / 204.11 KB	DNAT-203.154.201.69 (26)
	2 minutes ago	140.179.187.177				✓ 36 B / 36 B	DNAT-203.154.201.69 (26)
	2 minutes ago	18.166.154.152				✓ 36 B / 36 B	DNAT-203.154.201.69 (26)
	2 minutes ago	49.237.9.199				✓ 71.34 KB / 37.38 KB	DNAT-203.154.201.69 (26)
	2 minutes ago	115.31.129.137				✓ 11.99 KB / 7.73 KB	DNAT-203.154.201.69 (26)
	2 minutes ago	172.68.234.177				✓ 10.12 KB / 9.27 KB	DNAT-203.154.201.69 (26)
	2 minutes ago	172.68.234.177				✓ 8.59 KB / 8.49 KB	DNAT-203.154.201.69 (26)

Step 2: ตัวอย่างการใช้แถบค้นหาข้อมูล

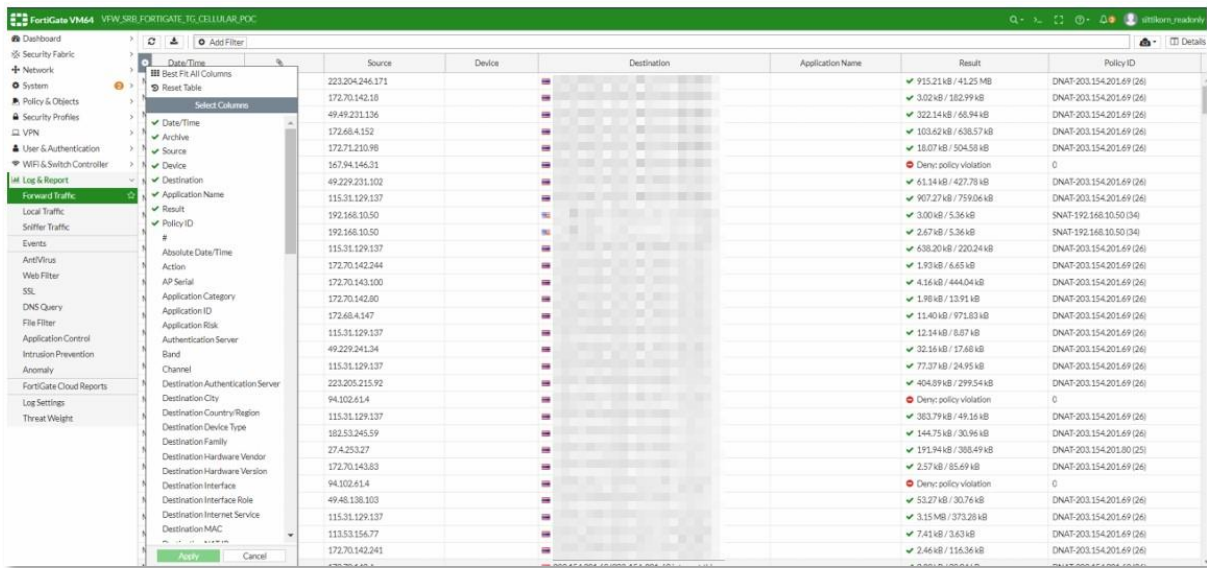
ในแถบค้นหาสามารถกด add filter เพื่อกำหนดขอบเขตการค้นหาได้ จะมีหัวข้อให้เลือกดังภาพ



	Date/Time	Source	Device	Destination	Application Name	Result	Policy ID
Forward Traffic	Minute ago	223.204.246.171				✓ 915.21 KB / 41.25 MB	DNAT-203.154.201.69 (26)
Local Traffic	Minute ago	172.70.142.18				✓ 3.02 KB / 182.99 KB	DNAT-203.154.201.69 (26)
Sniffer Traffic	Minute ago	49.49.231.136				✓ 322.14 KB / 68.94 KB	DNAT-203.154.201.69 (26)
Events	Minute ago	172.68.4.152				✓ 103.62 KB / 638.57 KB	DNAT-203.154.201.69 (26)
AntiVirus	Minute ago	172.71.210.98				✓ 18.07 KB / 504.58 KB	DNAT-203.154.201.69 (26)
Web Filter	Minute ago	167.94.146.31				Deny: policy violation	0
SSL	Minute ago	49.229.231.102				✓ 61.14 KB / 427.78 KB	DNAT-203.154.201.69 (26)
DNS Query	Minute ago	115.31.129.137				✓ 907.27 KB / 759.06 KB	DNAT-203.154.201.69 (26)
File Filter	Minute ago	192.168.10.50				✓ 3.00 KB / 5.36 KB	SNAT-192.168.10.50 (34)
Application Control	Minute ago	192.168.10.50				✓ 2.67 KB / 5.36 KB	SNAT-192.168.10.50 (34)
Intrusion Prevention	Minute ago	115.31.129.137				✓ 638.20 KB / 220.24 KB	DNAT-203.154.201.69 (26)
Anomaly	Minute ago	172.70.142.244				✓ 1.93 KB / 6.65 KB	DNAT-203.154.201.69 (26)
FortiGate Cloud Reports	Minute ago	172.70.143.100				✓ 4.16 KB / 444.04 KB	DNAT-203.154.201.69 (26)
Log Settings	Minute ago	172.70.142.80				✓ 1.99 KB / 13.91 KB	DNAT-203.154.201.69 (26)
Threat Weight	Minute ago	172.68.4.147				✓ 11.40 KB / 971.83 KB	DNAT-203.154.201.69 (26)
	Minute ago	115.31.129.137				✓ 12.14 KB / 8.87 KB	DNAT-203.154.201.69 (26)
	Minute ago	49.229.241.34				✓ 32.16 KB / 17.68 KB	DNAT-203.154.201.69 (26)
	Minute ago	115.31.129.137				✓ 77.37 KB / 24.95 KB	DNAT-203.154.201.69 (26)
	Minute ago	223.205.215.92				✓ 404.69 KB / 299.54 KB	DNAT-203.154.201.69 (26)
	Minute ago	94.102.61.4				Deny: policy violation	0
	Minute ago	115.31.129.137				✓ 383.79 KB / 49.16 KB	DNAT-203.154.201.69 (26)
	Minute ago	182.53.245.59				✓ 144.75 KB / 30.96 KB	DNAT-203.154.201.69 (26)
	Minute ago	27.4.253.27				✓ 191.94 KB / 388.49 KB	DNAT-203.154.201.69 (26)
	Minute ago	172.70.143.83				✓ 2.57 KB / 85.69 KB	DNAT-203.154.201.69 (26)
	Minute ago	94.102.61.4				Deny: policy violation	0
	Minute ago	49.48.138.103				✓ 53.27 KB / 30.76 KB	DNAT-203.154.201.69 (26)
	Minute ago	115.31.129.137				✓ 3.15 MB / 373.26 KB	DNAT-203.154.201.69 (26)
	Minute ago	115.53.156.77				✓ 7.41 KB / 3.63 KB	DNAT-203.154.201.69 (26)
	Minute ago	172.70.142.241				✓ 2.46 KB / 116.36 KB	DNAT-203.154.201.69 (26)
	Minute ago	172.70.142.4				✓ 3.08 KB / 38.04 KB	DNAT-203.154.201.69 (26)

ตัวอย่างการใช้แถบค้นหาข้อมูล

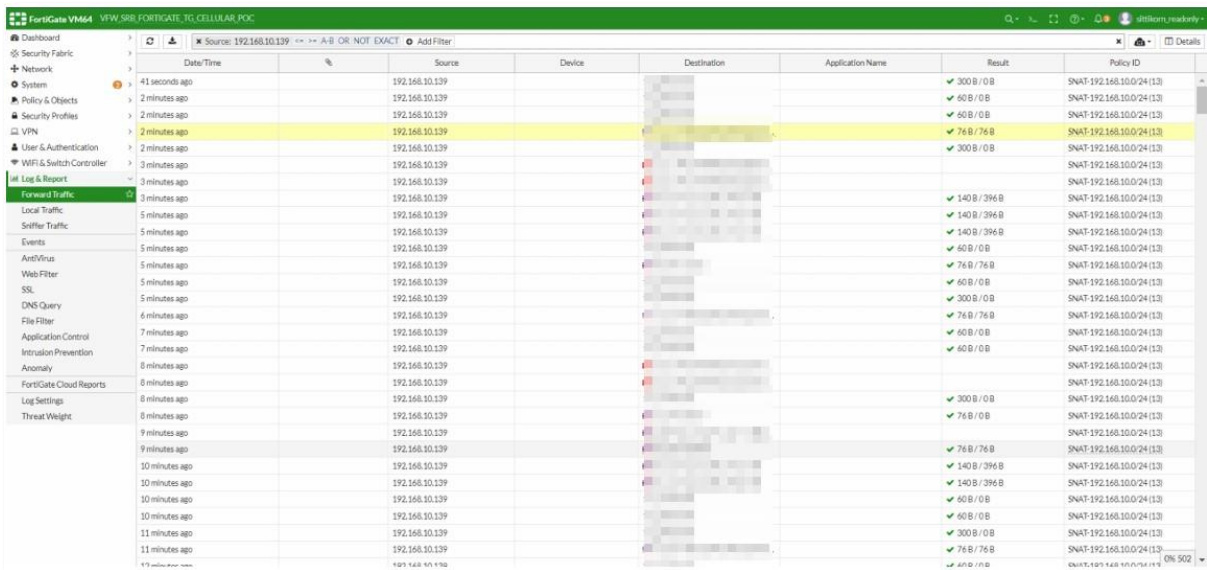
สามารถ คลิกขวาที่แถบ column เพื่อทำการเพิ่ม/ลด column ที่ต้องการแสดงได้



Source	Device	Destination	Application Name	Result	Policy ID
223.204.246.171				✓ 915.21 KB / 41.25 MB	DNAT-203.154.201.69 (26)
172.70.142.18				✓ 3.02 KB / 182.99 KB	DNAT-203.154.201.69 (26)
49.49.231.136				✓ 222.14 KB / 68.94 KB	DNAT-203.154.201.69 (26)
172.68.4.152				✓ 103.42 KB / 638.57 KB	DNAT-203.154.201.69 (26)
172.71.210.96				✓ 18.07 KB / 504.58 KB	DNAT-203.154.201.69 (26)
167.94.146.31				Deny: policy violation	0
49.229.231.102				✓ 61.14 KB / 427.78 KB	DNAT-203.154.201.69 (26)
115.31.129.137				✓ 907.27 KB / 759.06 KB	DNAT-203.154.201.69 (26)
192.168.10.50				✓ 3.00 KB / 5.36 KB	SNAT-192.168.10.50 (34)
192.168.10.50				✓ 2.67 KB / 5.36 KB	SNAT-192.168.10.50 (34)
115.31.129.137				✓ 638.20 KB / 220.24 KB	DNAT-203.154.201.69 (26)
172.70.142.244				✓ 1.93 KB / 6.65 KB	DNAT-203.154.201.69 (26)
172.70.143.100				✓ 4.16 KB / 444.04 KB	DNAT-203.154.201.69 (26)
172.70.142.80				✓ 1.98 KB / 13.91 KB	DNAT-203.154.201.69 (26)
172.68.4.147				✓ 11.40 KB / 971.83 KB	DNAT-203.154.201.69 (26)
115.31.129.137				✓ 12.34 KB / 8.87 KB	DNAT-203.154.201.69 (26)
49.229.241.134				✓ 32.16 KB / 17.68 KB	DNAT-203.154.201.69 (26)
115.31.129.137				✓ 77.37 KB / 24.95 KB	DNAT-203.154.201.69 (26)
223.205.215.92				✓ 404.89 KB / 299.54 KB	DNAT-203.154.201.69 (26)
94.102.61.4				Deny: policy violation	0
115.31.129.137				✓ 383.79 KB / 49.16 KB	DNAT-203.154.201.69 (26)
182.53.245.59				✓ 144.75 KB / 30.96 KB	DNAT-203.154.201.69 (26)
27.4.253.27				✓ 191.94 KB / 306.49 KB	DNAT-203.154.201.69 (26)
172.70.143.83				✓ 2.57 KB / 85.69 KB	DNAT-203.154.201.69 (26)
94.102.61.4				Deny: policy violation	0
49.48.136.103				✓ 53.27 KB / 30.76 KB	DNAT-203.154.201.69 (26)
115.31.129.137				✓ 3.15 KB / 373.28 KB	DNAT-203.154.201.69 (26)
115.31.156.77				✓ 7.41 KB / 3.63 KB	DNAT-203.154.201.69 (26)
172.70.142.241				✓ 2.46 KB / 116.36 KB	DNAT-203.154.201.69 (26)

ตัวอย่างการใช้แถบค้นหาข้อมูล

ตัวอย่างการค้นหาโดยกำหนด filter เป็น IP source



Date/Time	Source	Device	Destination	Application Name	Result	Policy ID
41 seconds ago	192.168.10.139				✓ 300 B / 0 B	SNAT-192.168.10.0/24 (13)
2 minutes ago	192.168.10.139				✓ 60 B / 0 B	SNAT-192.168.10.0/24 (13)
2 minutes ago	192.168.10.139				✓ 60 B / 0 B	SNAT-192.168.10.0/24 (13)
2 minutes ago	192.168.10.139				✓ 76 B / 76 B	SNAT-192.168.10.0/24 (13)
2 minutes ago	192.168.10.139				✓ 300 B / 0 B	SNAT-192.168.10.0/24 (13)
3 minutes ago	192.168.10.139				✓ 300 B / 0 B	SNAT-192.168.10.0/24 (13)
3 minutes ago	192.168.10.139				✓ 140 B / 396 B	SNAT-192.168.10.0/24 (13)
5 minutes ago	192.168.10.139				✓ 140 B / 396 B	SNAT-192.168.10.0/24 (13)
5 minutes ago	192.168.10.139				✓ 140 B / 396 B	SNAT-192.168.10.0/24 (13)
5 minutes ago	192.168.10.139				✓ 60 B / 0 B	SNAT-192.168.10.0/24 (13)
5 minutes ago	192.168.10.139				✓ 76 B / 76 B	SNAT-192.168.10.0/24 (13)
5 minutes ago	192.168.10.139				✓ 60 B / 0 B	SNAT-192.168.10.0/24 (13)
5 minutes ago	192.168.10.139				✓ 300 B / 0 B	SNAT-192.168.10.0/24 (13)
5 minutes ago	192.168.10.139				✓ 300 B / 0 B	SNAT-192.168.10.0/24 (13)
6 minutes ago	192.168.10.139				✓ 76 B / 76 B	SNAT-192.168.10.0/24 (13)
7 minutes ago	192.168.10.139				✓ 60 B / 0 B	SNAT-192.168.10.0/24 (13)
7 minutes ago	192.168.10.139				✓ 60 B / 0 B	SNAT-192.168.10.0/24 (13)
8 minutes ago	192.168.10.139				✓ 60 B / 0 B	SNAT-192.168.10.0/24 (13)
8 minutes ago	192.168.10.139				✓ 300 B / 0 B	SNAT-192.168.10.0/24 (13)
8 minutes ago	192.168.10.139				✓ 76 B / 0 B	SNAT-192.168.10.0/24 (13)
9 minutes ago	192.168.10.139				✓ 76 B / 76 B	SNAT-192.168.10.0/24 (13)
10 minutes ago	192.168.10.139				✓ 140 B / 396 B	SNAT-192.168.10.0/24 (13)
10 minutes ago	192.168.10.139				✓ 140 B / 396 B	SNAT-192.168.10.0/24 (13)
10 minutes ago	192.168.10.139				✓ 60 B / 0 B	SNAT-192.168.10.0/24 (13)
10 minutes ago	192.168.10.139				✓ 60 B / 0 B	SNAT-192.168.10.0/24 (13)
11 minutes ago	192.168.10.139				✓ 300 B / 0 B	SNAT-192.168.10.0/24 (13)
11 minutes ago	192.168.10.139				✓ 76 B / 76 B	SNAT-192.168.10.0/24 (13)