

FortiGate 60C										
<div> <div>System</div> <div> <div>Policy</div> <div>Proxy Options</div> <div>SSL Inspection</div> <div>Monitor</div> </div> </div> <div> <div>Create New</div> <div>Edit</div> <div>Delete</div> </div> <div>Section View Global View</div> <div>Search</div>										
Seq.#	Source	Destination	Schedule	Service	Authentication	Action	Security Profiles	Log	NAT	Count
dmz (Server_Zone) - internal (Office_Zone) (1 - 2)										
1	AD_WS2008	Staff_HQ	always	ALL		Accept				603 Packets / 79.12 KB
2	File_Server	IT_HQ	always	ALL		Accept				0 Packets / 0 B
dmz (Server_Zone) - wan1 (3BB_FTTx) (3 - 3)										
3	all	all	always	ALL		Accept				187,897,528 Packets / 151.24 GB
internal (Office_Zone) - dmz (Server_Zone) (4 - 5)										
4	Staff_HQ	AD_WS2008	always	ALL		Accept				4,228 Packets / 1.00 MB
5	IT_HQ	VMWare_ESXi	always	ALL		Accept				123,386 Packets / 39.13 MB
internal (Office_Zone) - wan1 (3BB_FTTx) (6 - 6)										
6	Office_Subnet	all	always	ALL		Accept				22,012,510 Packets / 14.21 GB
Implicit (7 - 7)										

FortiGate 60C

System

Policy

Policy

Proxy Options

SSL Inspection

Monitor

Create New

Edit

Delete

Section View

Global View

Search

Seq.#	From	To	Source	Destination	Schedule	Service	Authentication	Action	Security Profiles	Log	NAT
1	internal	wan1	Office_Subnet	all	always	ALL		Accept			
2	dmz	wan1	AD_WS2008 File_Server FortiAnalyst	all	always	ALL		Accept			
3	internal	dmz	Staff_HQ IT_HQ	AD_WS2008 File_Server	always	ALL		Accept			
4	dmz	internal	AD_WS2008 File_Server	Staff_HQ IT_HQ	always	ALL		Accept			
5	internal	dmz	IT_HQ	VMWare_ESXi FortiAnalyst	always	ALL		Accept			
6	dmz	internal	VMWare_ESXi FortiAnalyst	IT_HQ	always	ALL		Accept			
7	any	any	any	any	always	ALL		Deny			

FortiGate 60C

Help

Wizard

Logout

FORTINET

System

Policy

Proxy Options

SSL Inspection

Monitor

Create New

Edit

Delete

Section View Global View Search

Seq.#	From	To	Source	Destination	Schedule	Service	Authentication	Action	Security Profiles	Log	NAT
1	internal	wan1	AD_WS2008	all	always	ALL		Accept			
2	dmz	wan1	AD_WS2008	all	always	ALL		Accept			
3	internal	dmz	Staff_HQ	AD_WS2008	always	ALL		Accept			
4	dmz	internal	AD_WS2008	Staff_HQ	always	ALL		Accept			
5	internal	dmz	IT_HQ	VMWare_ESXi	always	ALL		Accept			
6	dmz	internal	VMWare_ESXi	IT_HQ	always	ALL		Accept			
7	any	any	any	any	always	ALL		Deny			

หัวข้อที่ควรทราบ

1. Policy นั้นใช้สำหรับสร้าง Firewall Policy ซึ่งจะมี Address ,User Identify ,Device Identify
2. สำหรับการอ่าน Policy นั้น FortiGate จะมี Option ให้ผ่านได้ 2 แบบ
 - a. Session View จะเป็นการอ่าน Policy ตาม Interface เช่น Intrnal => Wan1
 - b. Global View จะเป็นการอ่าน Policy ตาม Sequent การทำงานของ Firewall

หมายเหตุ : สำหรับการ View ทั้ง 2 แบบสามารถเพิ่ม Filed ได้ ที่ใช้งานบ่อยๆ ได้แก่ ID ,Count ,Status



FortiGate 60C					
<div> <div>System</div> <div>Policy</div> <div>Firewall Objects</div> <div>Address</div> <div>Group</div> <div>Service</div> <div>Schedule</div> </div>					
Create New					
Name	Address/FQDN	Interface	Type	Show in Address List	
AD_WS2008	100.100.100.101	Any	Subnet	✓	
File_Server	100.100.100.253	Any	Subnet	✓	
FortiAnalyst	100.100.100.252	Any	Subnet	✓	
IT_HQ	192.168.1.254	Any	Subnet	✓	
Office_Subnet	192.168.1.0/255.255.0	Any	Subnet	✓	
SSLVPN_TUNNEL_ADDR1	10.212.134.200-10.212.134.210	Any	IP Range	✓	
Staff_HQ	192.168.1.1-192.168.1.253	Any	IP Range	✓	
VMWare_ESXi	100.100.100.254	Any	Subnet	✓	
all	0.0.0.0/0.0.0.0	Any	Subnet	✓	

FortiGate 60C

System

Policy

Firewall Objects

Address

Group

Service

Schedule

New Address

Name

Type

Subnet / IP Range

Interface

Show in Address List

Comments

Subnet

0.0.0.0/0.0.0.0

Any

☒

Write a comment...

Please Select

FQDN

Geography

IP Range

Subnet

OK

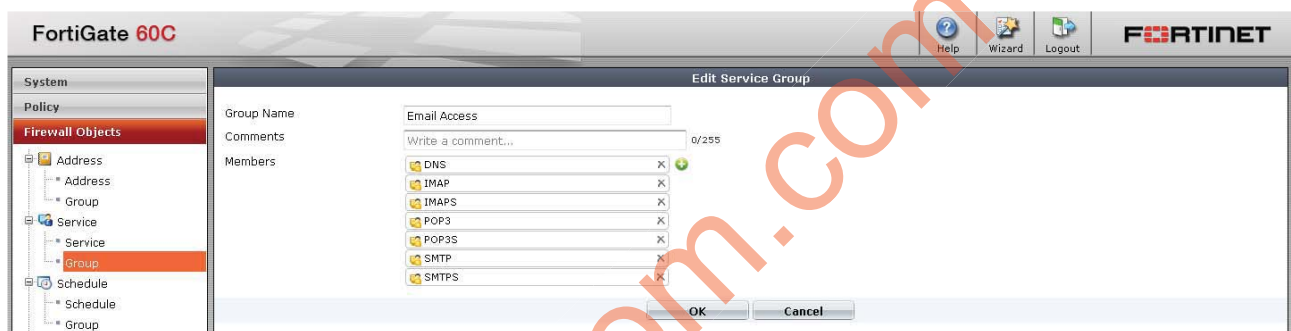
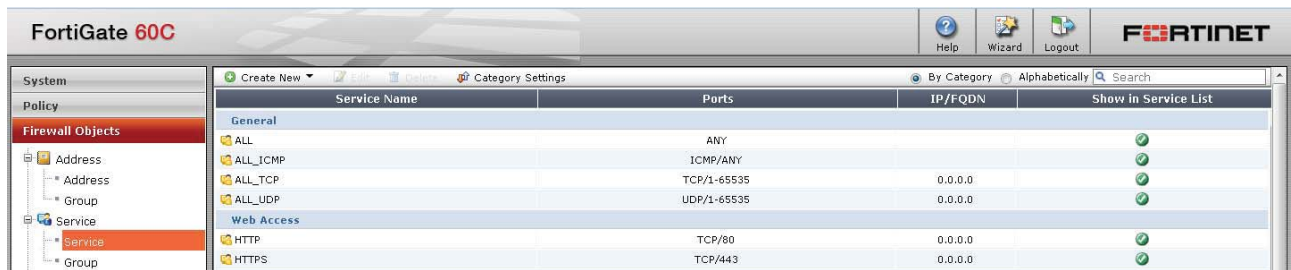
Cancel

หัวข้อที่ควรทราบ Firewall Objects (Address)

- สำหรับสร้าง Object ที่เป็น Address ขึ้นมาสำหรับไปใช้งานใน Firewall Policy
 - FQDN คือ Fully Qualified Domain Name เช่น facebook.com ,youtube.com
 - Geography คือ IP Address ที่ถูก Assign ให้ประเทศต่างๆ
 - IP-Range คือ ช่วงของ IP Address เช่น 192.168.100.1-192.168.1.50
 - Subnet คือ กลุ่มของ IP Address ทั้งหมายเลข Subnet เช่น 192.168.100.0/24

หมายเหตุ :

ตัวเลือก Interface กรณีมีการเลือกไว้ Object Address นี้จะสามารถใช้งานได้ต่อเมื่อเลือก Interface นั้นๆ ขึ้นมาใช้งานใน Firewall Policy กรณี ต้องการใช้งานรวมๆ ให้เลือกเป็น “Any”



หัวข้อที่ควรทราบ Firewall Objects (Service)

สำหรับการสร้าง Object ที่เป็น Service นั้นโดยส่วนใหญ่ FortiGate จะมี Service มาตรฐานที่เป็น Pre-Define มาให้แล้ว แต่กรณีที่ต้องการสร้าง Custom Service ขึ้นมาใช้งานเองใน Service Object ก็สามารที่จะสร้างขึ้นมาได้ โดย กำหนดชื่อ รวมถึง Protocol ใช้งาน และ Source Port ,Destination Port เองตาม Custom Service ที่ลูกค้าต้องการใช้งาน กรณีที่ต้องการรวม Service หลายๆ ตัวเข้าเป็น Group นั้นก็สามารถทำขึ้นมาได้โดยการ Create “Group Service” และรวม Service หลายๆตัวเข้าด้วยกัน

FortiGate 60C

Help Wizard Logout FORTINET

System

Policy

Firewall Objects

Address

Service

Schedule

Create New

Name	Type	Day	Start	End	Ref.
August_Only	One-Time		2013/07/01 00:00	2013/07/31 00:00	0
Mon_Fri	Recurring	monday tuesday wednesday thursday friday	00:00	00:00	0
always	Recurring	sunday monday tuesday wednesday thursday friday saturday	00:00	00:00	6

FortiGate 60C

Help Wizard Logout FORTINET

System

Policy

Firewall Objects

Address

Service

Schedule

New Recurring Schedule

Name: Mon_Fri

Day of the Week: ☐ Sunday ☒ Monday ☒ Tuesday ☒ Wednesday ☒ Thursday ☒ Friday ☐ Saturday

Start Time: Hour 00 Minute 00

Stop Time: Hour 00 Minute 00

Notes: If the stop time is set earlier than the start time, the stop time will be during the next day. If the start time is equal to the stop time, the schedule will run for 24 hours.

OK Cancel

FortiGate 60C

Help Wizard Logout FORTINET

System

Policy

Firewall Objects

Address

Service

Schedule

New One-time Schedule

Name: August_Only

Start: Year 2013 Month 07 Day 01 Hour 00 Minute 00

Stop: Year 2013 Month 07 Day 31 Hour 00 Minute 00

Notes: Start time should be earlier than stop time.

☒ Generate event log when schedule is about to expire

3 days before

OK Cancel

หัวข้อที่ควรทราบ Firewall Objects (Schedule)

สำหรับการสร้าง Object ที่เป็น Schedule นั้นโดย ค่ามาตรฐานของ FortiGate จะมี “Always” มาให้ใช้งานเป็นค่าเริ่มต้น สำหรับกรณีที่ลูกค้าต้องการสร้าง Schedule ขึ้นมาเพื่อให้ Firewall ทำงานสำหรับ Policy นั้นๆตามช่วงเวลาที่เรากำหนดขึ้นมาเอาที่สามารถทำได้ โดย FortiGate นั้นจะรองรับรูปแบบการสร้าง Schedule ทั้งแบบ “Recurring” ช่วงเวลานั้นๆตลอดไป และ แบบ One-Time คือช่วงเวลาตามที่กำหนดเท่านั้น และสำหรับ Object Schedule นั้นก็สามารถที่จะรวมเป็น Group ได้



FortiGate 60C

Help Wizard Logout FORTINET

System

Policy

Firewall Objects

Address

Service

Schedule

Traffic Shaper

Shared

Per-IP

Virtual IP

New Shared Traffic Shaper

Name: 2Mbps_Per_Policy

Apply Shaper: ☒ Per Policy ☐ For All Policies Using This Shaper

Traffic Priority: Medium

☒ Maximum Bandwidth: 2048 (1-16776000 kbit/s)

☐ Guaranteed Bandwidth: 0 (1-16776000 kbit/s)

☐ DSCP: 000000 (000000 - 111111)

OK Cancel

FortiGate 60C

Help Wizard Logout FORTINET

System

Policy

Firewall Objects

Address

Service

Schedule

Traffic Shaper

Shared

Per-IP

Virtual IP

New Shared Traffic Shaper

Name: 2Mbps_All_Policy

Apply Shaper: ☐ Per Policy ☒ For All Policies Using This Shaper

Traffic Priority: Medium

☒ Maximum Bandwidth: 2048 (1-16776000 kbit/s)

☐ Guaranteed Bandwidth: 0 (1-16776000 kbit/s)

☐ DSCP: 000000 (000000 - 111111)

OK Cancel

FortiGate 60C

Help Wizard Logout FORTINET

System

Policy

Firewall Objects

Address

Service

Schedule

Traffic Shaper

Shared

Per-IP

Virtual IP

New Per-IP Traffic Shaper

Name: 1Mbps_Per_IP

☒ Maximum Bandwidth: 1024 (1-16776000 kbit/s)

☐ Maximum Concurrent Connections: 0 (1-2097000)

☐ Forward DSCP: 000000 (000000 - 111111)

☐ Reverse DSCP: 000000 (000000 - 111111)

OK Cancel

หัวข้อที่ควรทราบ Firewall Objects (Traffic Shaper)

สำหรับการสร้าง Object ที่เป็น Traffic Shaper นั้นจะมีอยู่ด้วยกัน 2 แบบ “Shared ,Per IP” โดยสำหรับ Shared นั้นจะแบ่งย่อยเป็น “Per Policy” กรณีนำไปใช้งานจะเป็น Traffic ที่ถูกนำไปใช้งานเฉพาะ Policy นั้นๆ เท่านั้น ส่วน “For All Policy” นั้นจะเป็นต่อ Traffic Shaper ที่ใช้งานร่วมกันทุก Policy ที่ใช้งาน Object Traffic Shaper ตัวนี้ คือ รวมกันไปทุก Policy ในตอนนี้เพียงข้อเดียว สำหรับ Per IP นั้นจะเป็น Object Traffic Shaper ที่ใช้งานลักษณะต่อ IP จะใช้ Traffic Maximum ได้เท่านั้นถ้ามีการนำ Object Traffic Shaper “Per IP” นั้นๆ ไปใช้งานใน Firewall Policy

FortiGate 60C						
<div> <div>System</div> <div>Policy</div> <div>Firewall Objects</div> <div>Address</div> <div>Service</div> <div>Schedule</div> <div>Traffic Shaper</div> <div>Virtual IP</div> <div>Virtual IP</div> <div>VIP Group</div> <div>IP Pool</div> </div>						
Name	IP	Service Port	Map to IP/IP Range	Map to Port	Src Filter	
OwaMail	wan2/61.1.30.42	0-65535/tcp	192.168.1.201	0-65535/tcp		
WebApps	wan2/61.1.30.43	0-65535/tcp	192.168.1.202	0-65535/tcp		
FortiAnalyzer	wan2/61.1.30.41	8000/tcp	192.168.1.254	8000/tcp		
IP_Cam1	wan2/61.1.30.41	8001/tcp	192.168.1.251	8001/tcp		
IP_Cam2	wan2/61.1.30.41	8002/tcp	192.168.1.252	8002/tcp		
IP_Cam3	wan2/61.1.30.41	8003/tcp	192.168.1.253	8003/tcp		

FortiGate 60C		Help	Wizard	Logout	FORTINET
System	Policy				
Firewall Objects					
Address					
Service					
Schedule					
Traffic Shaper					
Virtual IP					
Virtual IP					
VIP Group					
IP Pool					

Name	WebApps				
Comments	Write a comment... 0/255				
External Interface	wan2 (CAT_Static)				
Type	Static NAT				
Source Address Filter	<input type="checkbox"/>				
External IP Address/Range	61.1.30.44 - 61.1.30.44				
Mapped IP Address/Range	192.168.1.202 - 192.168.1.202				
Port Forwarding	<input type="checkbox"/>				
OK Cancel					

FortiGate 60C		Help	Wizard	Logout	FORTINET
System	Policy				
Firewall Objects					
Address					
Service					
Schedule					
Traffic Shaper					
Virtual IP					
Virtual IP					
VIP Group					
IP Pool					
Monitor					
Traffic Shaper Monitor					

Name	IP_Cam1				
Comments	Write a comment... 0/255				
External Interface	wan2 (CAT_Static)				
Type	Static NAT				
Source Address Filter	<input type="checkbox"/>				
External IP Address/Range	61.1.30.41 - 61.1.30.41				
Mapped IP Address/Range	192.168.1.251 - 192.168.1.251				
Port Forwarding	<input checked="" type="checkbox"/>				
Protocol	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> SCTP				
External Service Port	8001 - 8001				
Map to Port	8001 - 8001				
OK Cancel					

หัวข้อที่ควรทราบ Firewall Objects (VIP)

สำหรับการสร้าง Object ที่เป็น VIP นั้นจะมีอยู่ด้วยกัน 2 แบบ คือ “Static NAT 1:1” คือจาก Real IP ภายนอกมาเป็น Private IP ภายในโดยตรง “Static NAT 1:1” และ สำหรับอีกแบบจะเป็น ลักษณะการ Forward Port เข้ามาที่ Private IP ภายใน IP ต่างๆ เฉพาะ Port ใด Port หนึ่ง หรืออาจจะ ทำการ Forward Port เป็นช่วงเข้ามาหา Private IP ภายในก็ได้กรณี Apps หรือ Server นั้นๆ ต้องการ

หมายเหตุ

Real IP ที่ได้ Assign มาสำหรับตัวอย่างนี้

	Subnet ID	Host Addresses	Subnet Broadcast
9157	61.1.30.40	61.1.30.41 - 61.1.30.46	61.1.30.47



เบื้องต้นเกี่ยวกับ Security Profile (UTM Profile)

การทำการตรวจสอบของ Security Profile ของ FortiGate มี 2 แบบ Flow Based ,Proxy Based โดย Flow Based ตรวจสอบเป็น Packets ส่วน Proxy Based จะตรวจสอบแบบ Complete Content

Feature	Stateful	Flow	Proxy
Inspection unit per session	first packet	selected packets	complete content
Memory, CPU required	low	medium	high
Level of threat protection	good	better	best

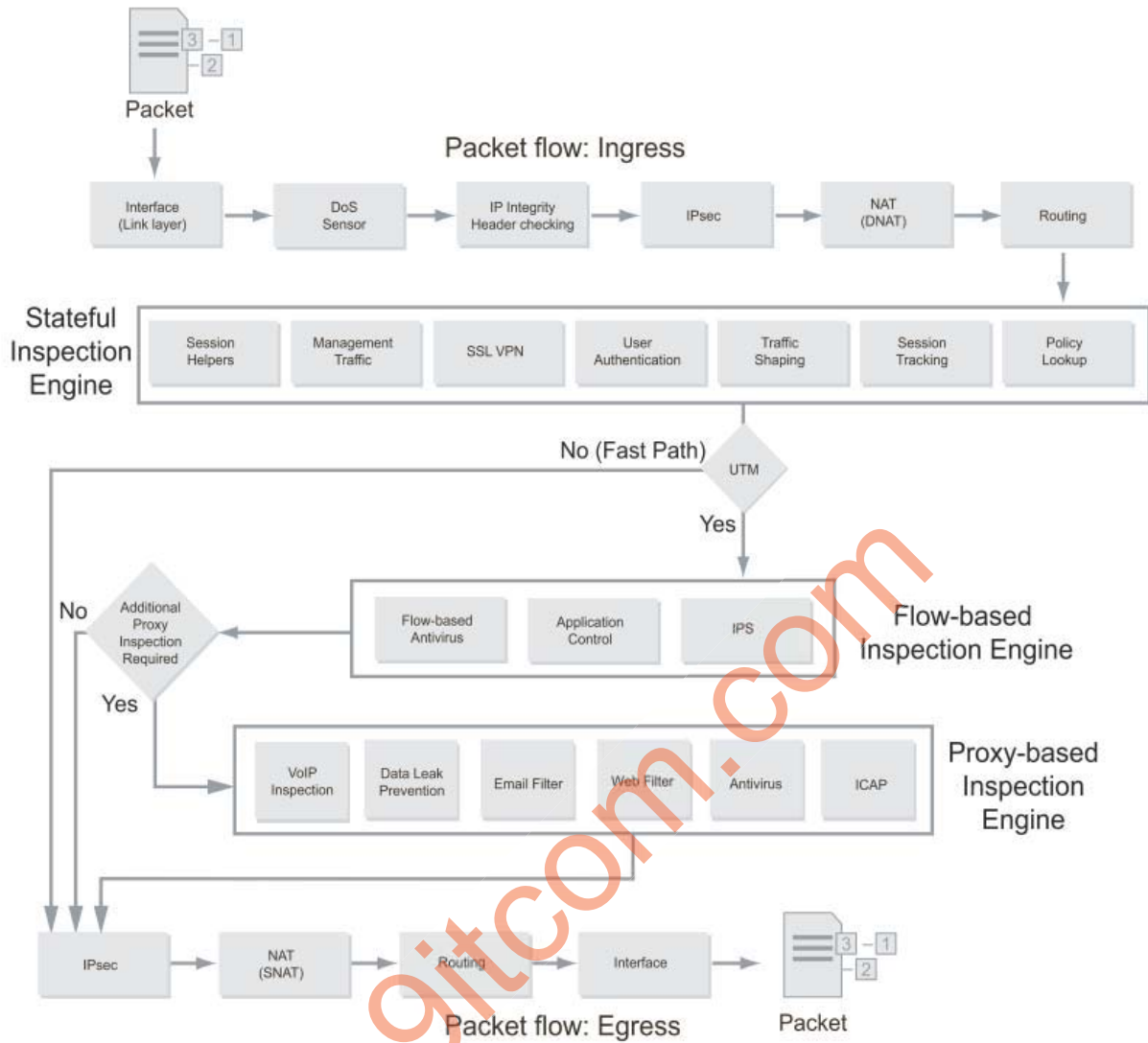
ชนิดของ Security Profile กับลักษณะการตรวจสอบ

FortiOS security functions and security layers

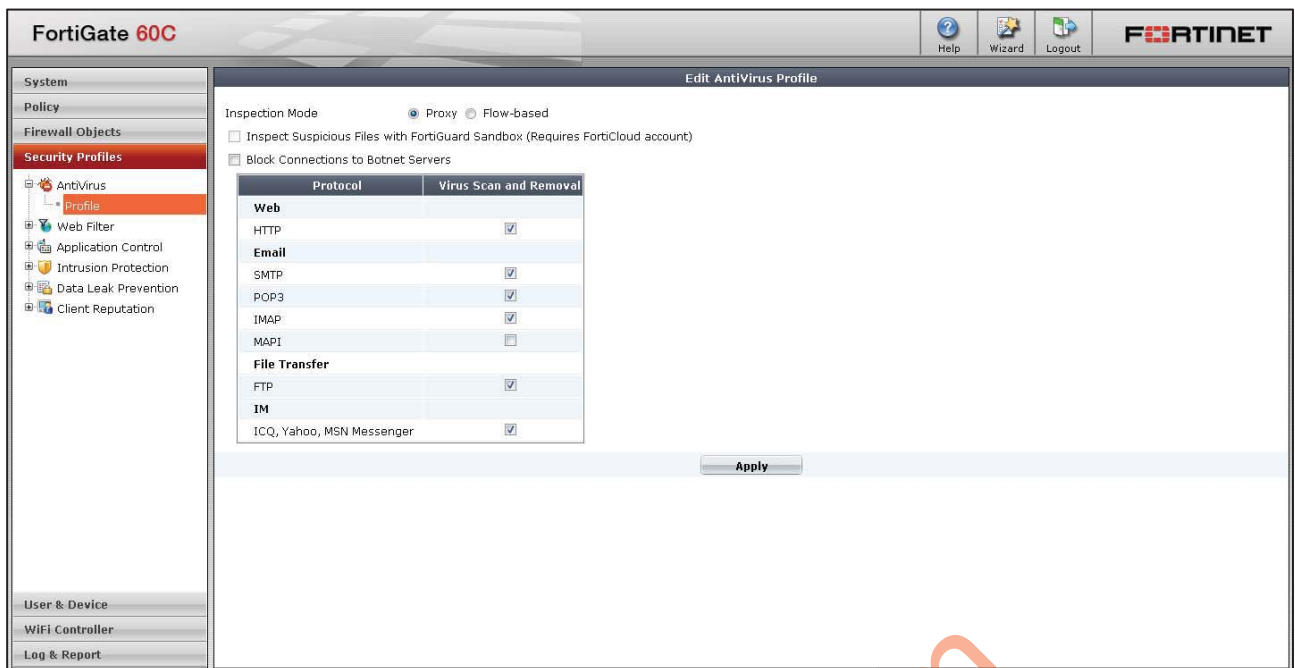
Security Function	Stateful	Flow	Proxy
Firewall	ü		
IPsec VPN	ü		
Traffic Shaping	ü		
User Authentication	ü		
Management Traffic	ü		
SSL VPN	ü		
Intrusion Prevention		ü	
Flow-based Antivirus		ü	
Application Control		ü	
VoIP inspection			ü
Proxy Antivirus			ü
Email Filtering			ü
Web Filtering (Antispam)			ü
Data Leak Prevention			ü



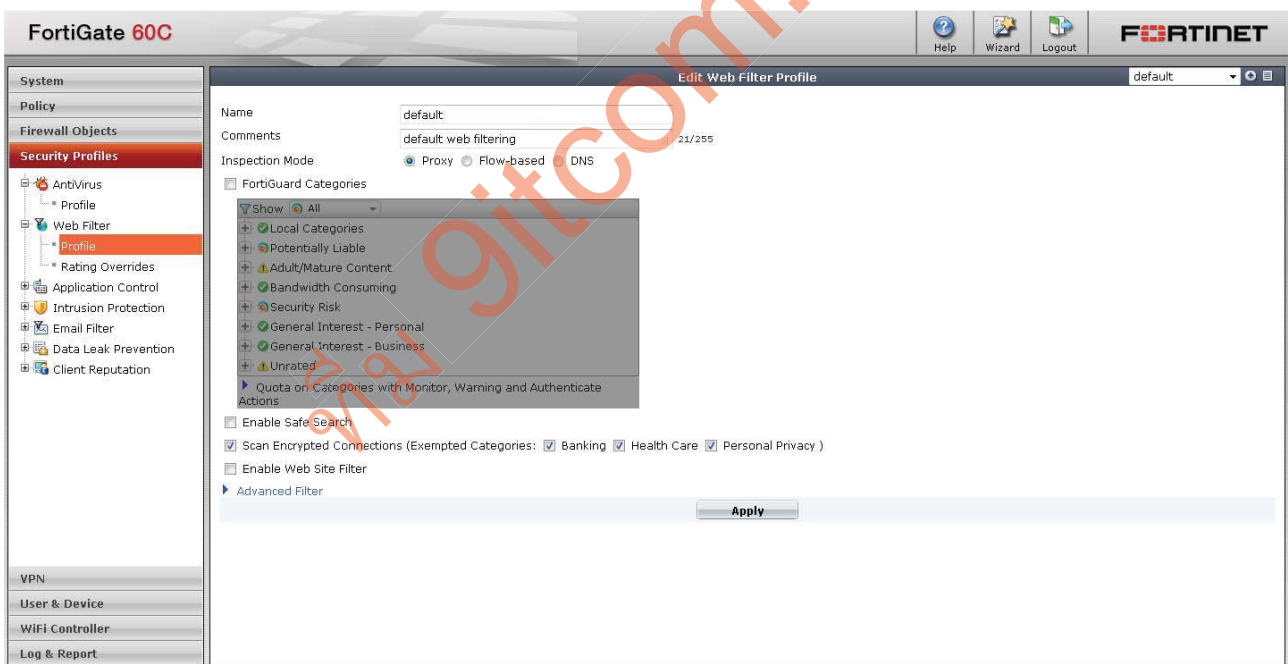
Packet flow



โครงสร้างการทำงาน Packets Flow ภายใน FortiGate

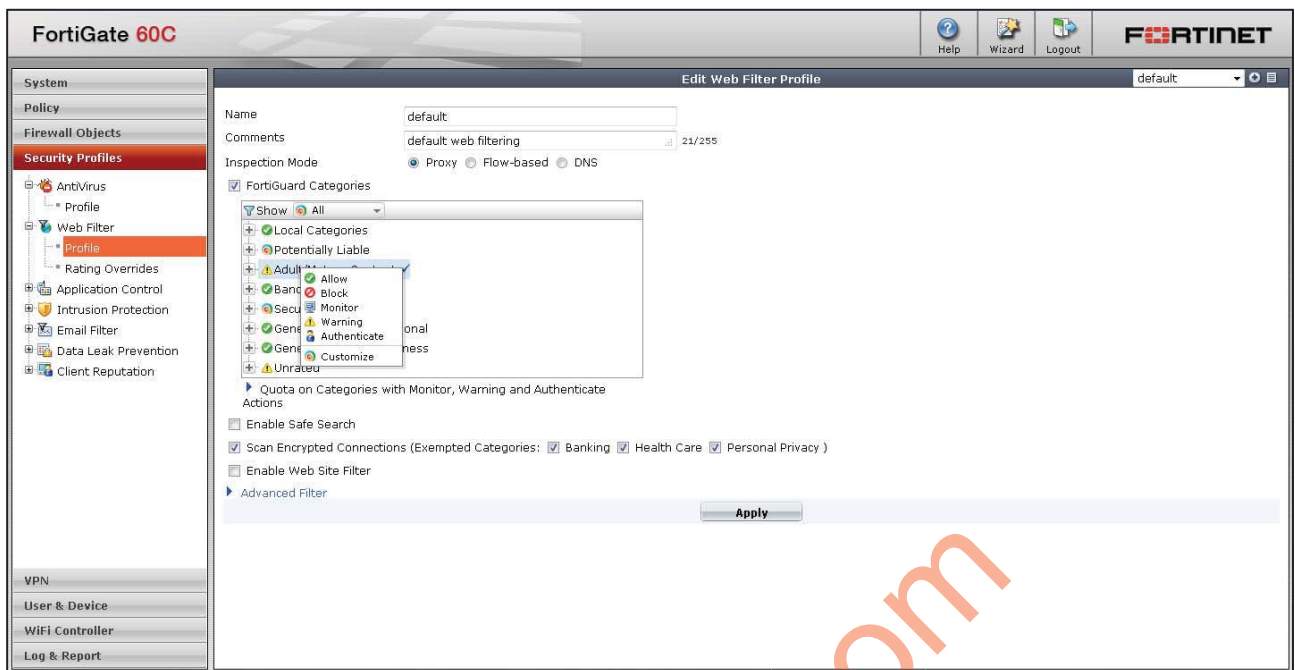


สำหรับ AntiVirus Security Profile นั้นจะรองรับการ Scan ทั้ง 2 แบบ คือ Flow Base และ Proxy Base และจะสามารถเลือกได้ว่าจะให้ Scan ที่ Protocol ใหนบ้าง สามารถเลือกตามการใช้งานที่เหมาะสมได้



สำหรับ WebFilter นั้นจะสามารถใช้งานส่วนของ FortiGuard Categories เลขก็ได้ อาจจะเพิ่ม URL บางตัวเข้าไปใน WebSite Filter หรือ อาจจะใช้งานเฉพาะ WebSite Filter ก็สามารทำได้

ตัวอย่างการใช้ FortiGuard ทำการ Block WebSite ไม่เหมาะสมทั้ง Categories



ทดสอบเปิด WebSite ที่เกี่ยวกับ Alcohol โดยใช้ Action = Block (<http://www.johnniewalker.com>)

