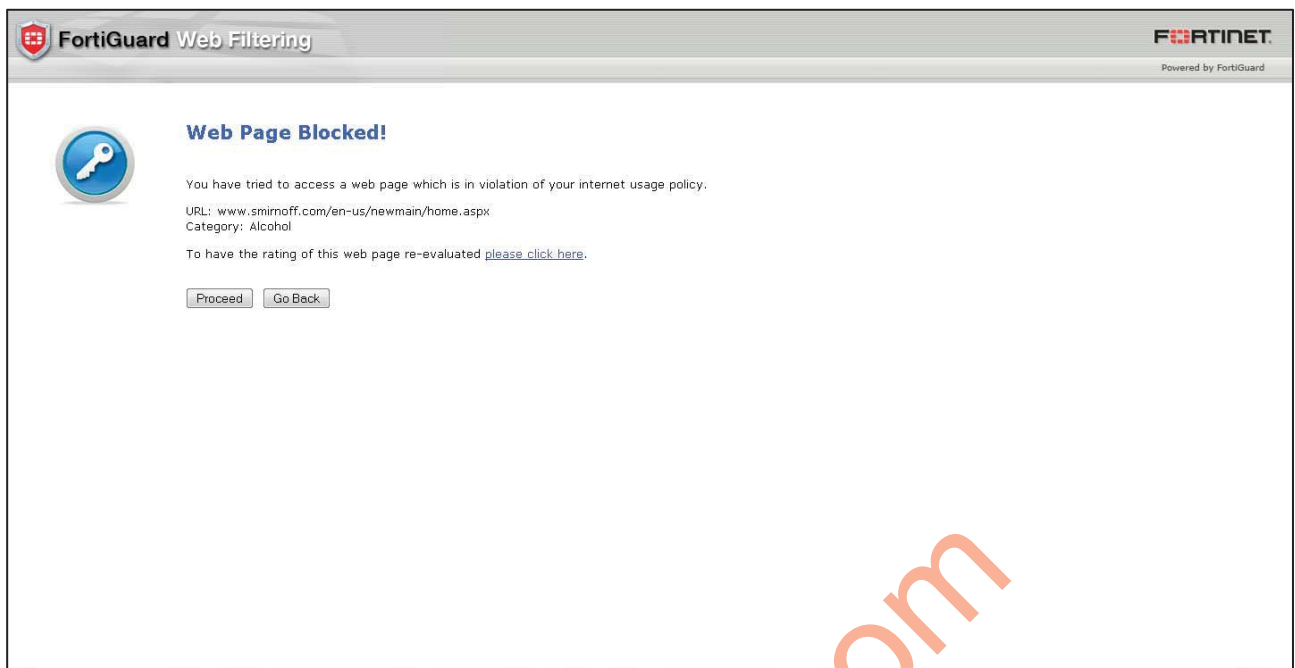
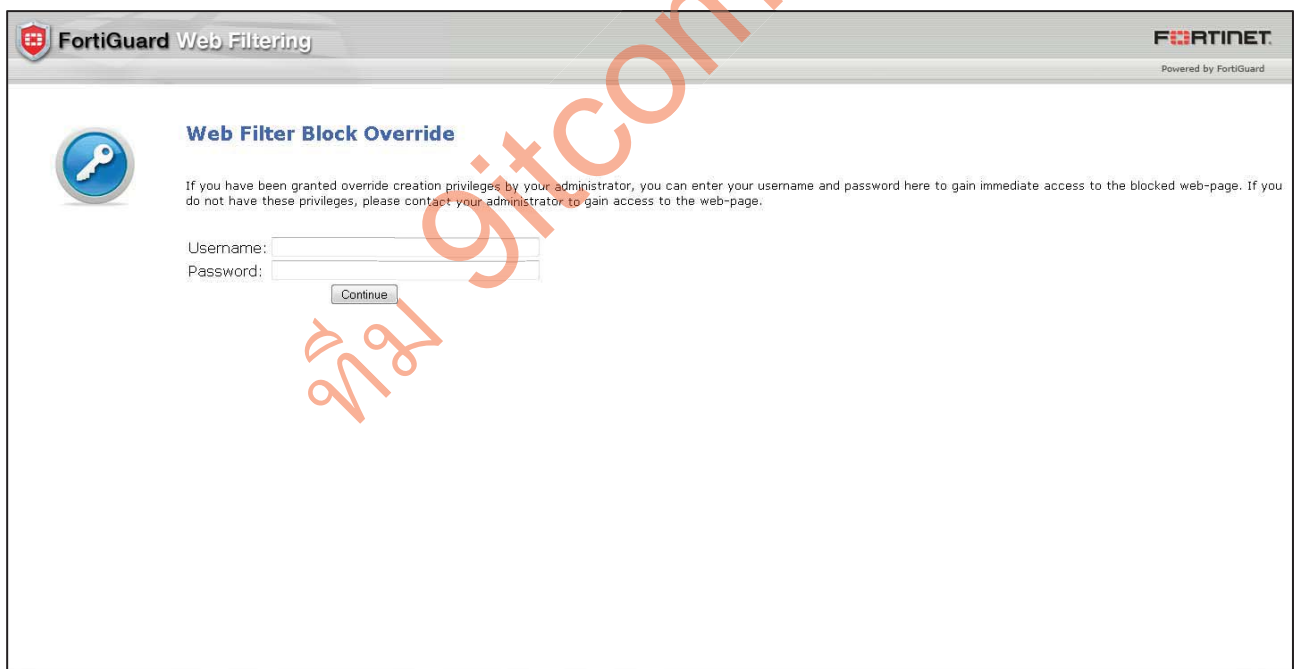


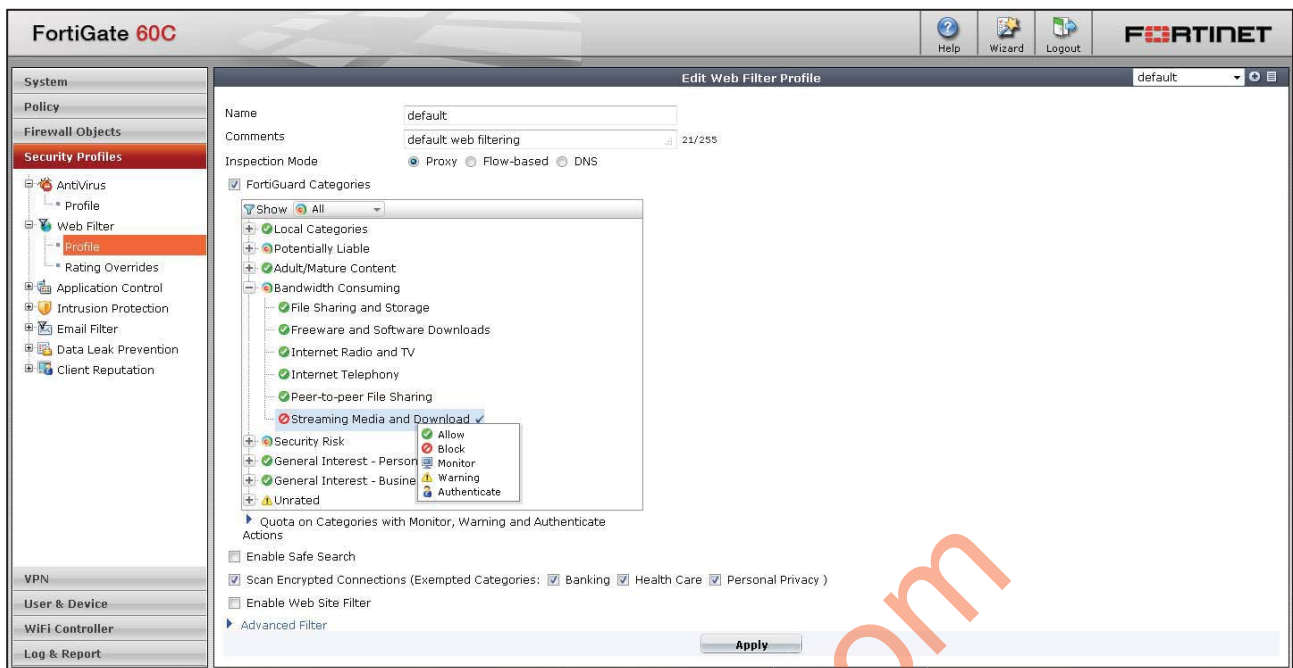
ทดสอบเปิด WebSite ที่เกี่ยวกับ Alcohol โดยใช้ Action = Warning (<http://www.smirnoff.com>)



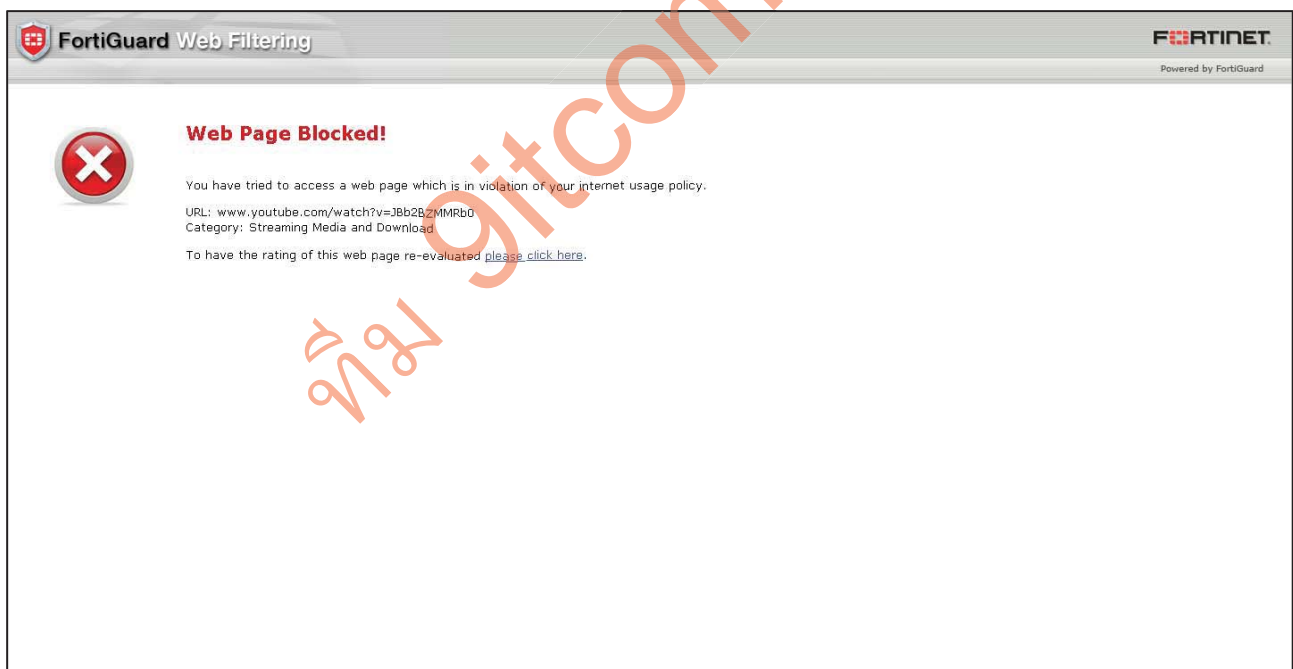
ทดสอบเปิด WebSite ที่เกี่ยวกับ Alcohol โดยใช้ Action = Authenticate (<http://www.smirnoff.com>)



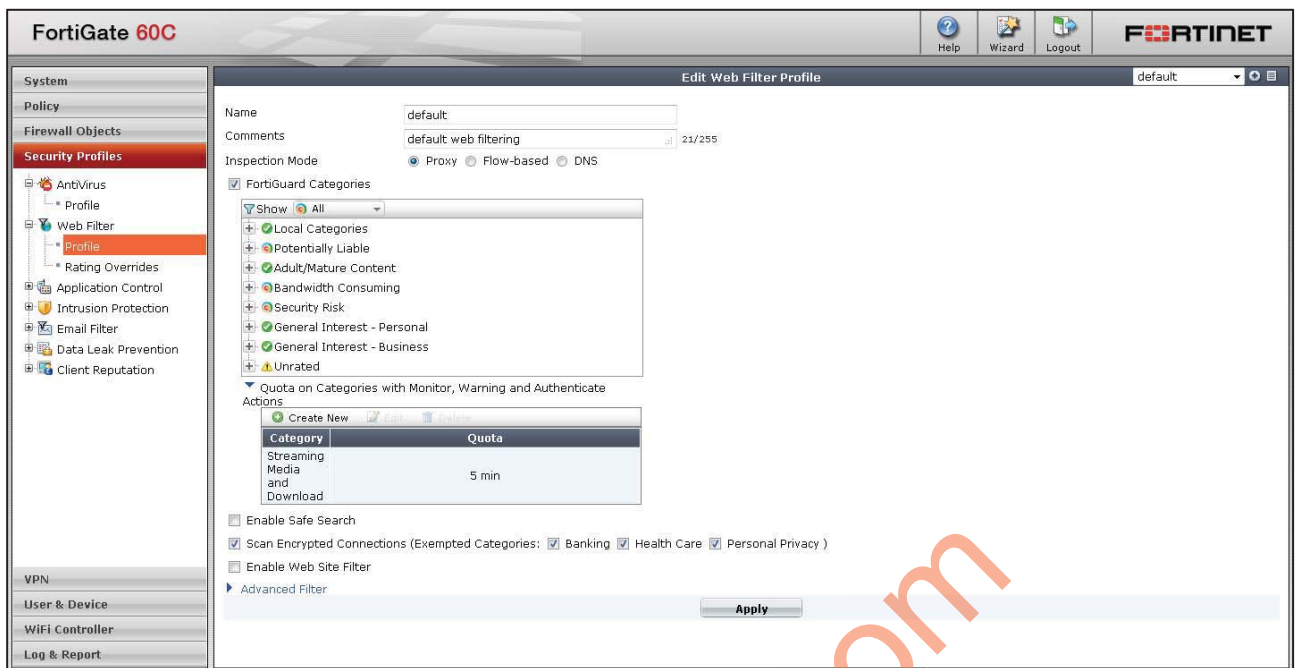
ตัวอย่างการใช้ FortiGuard ทำการ Block WebSite ไม่เหมาะสมบางส่วนของ Categories



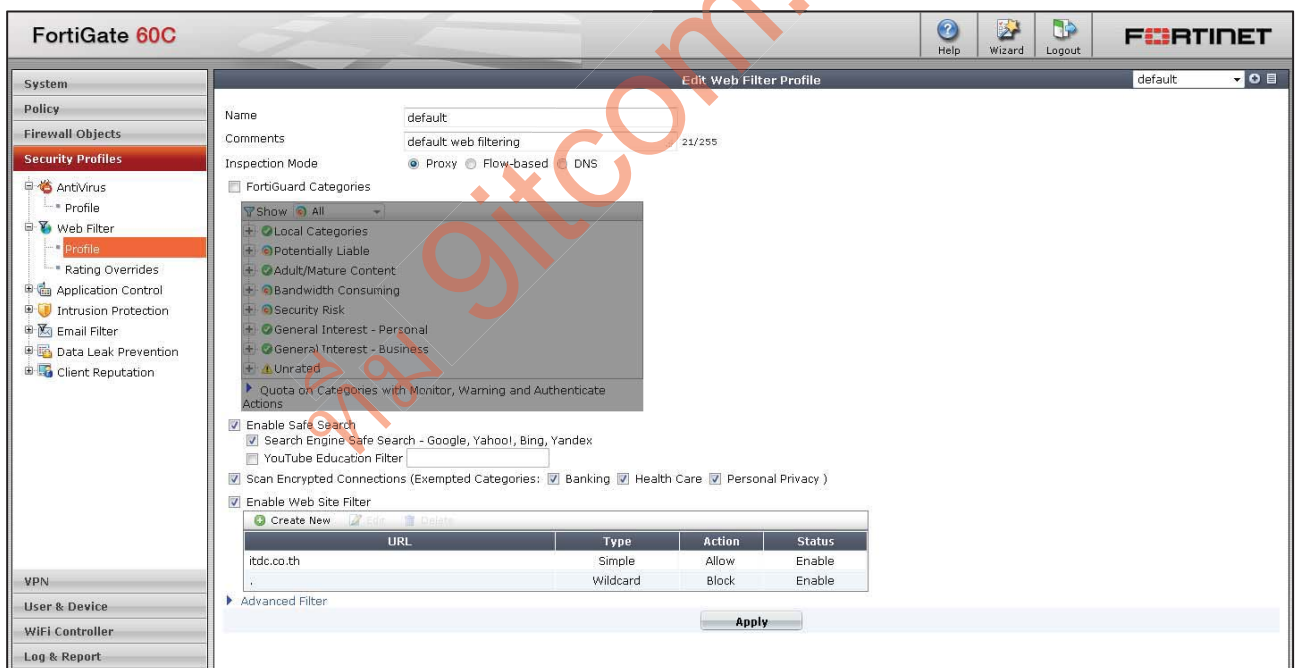
ทดสอบเปิด WebSite ที่เกี่ยวกับ Streaming โดยใช้ Action = Block



สำหรับ Action อื่นๆ เช่นการกำหนด Quota ในการ Access WebSite นั้นๆ ได้นานเท่าใด

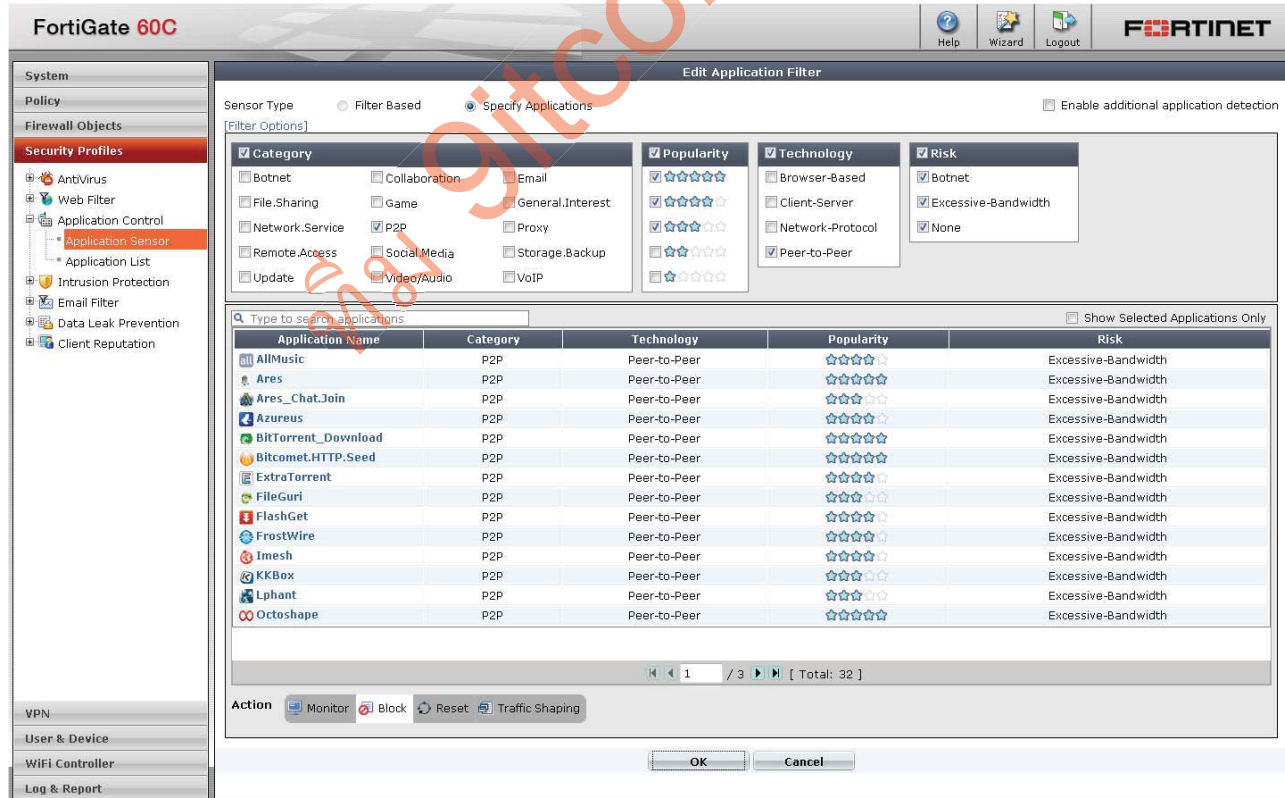
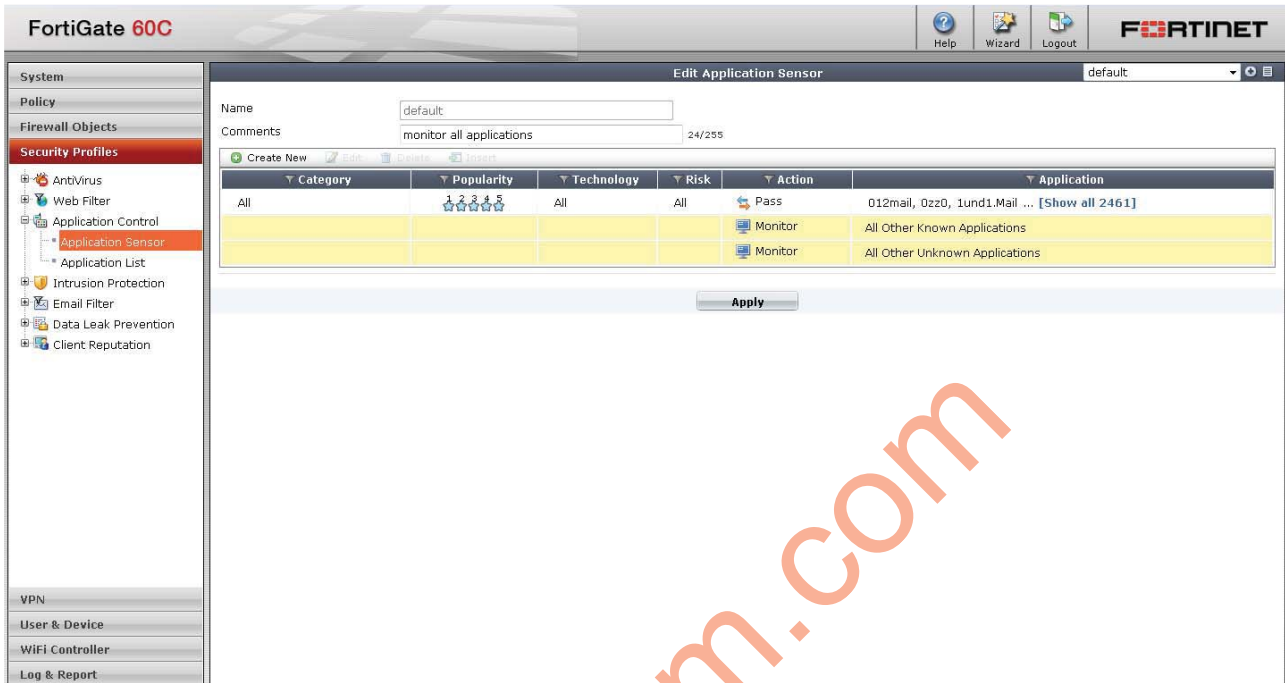


ตัวอย่างการใช้งาน URL Filter

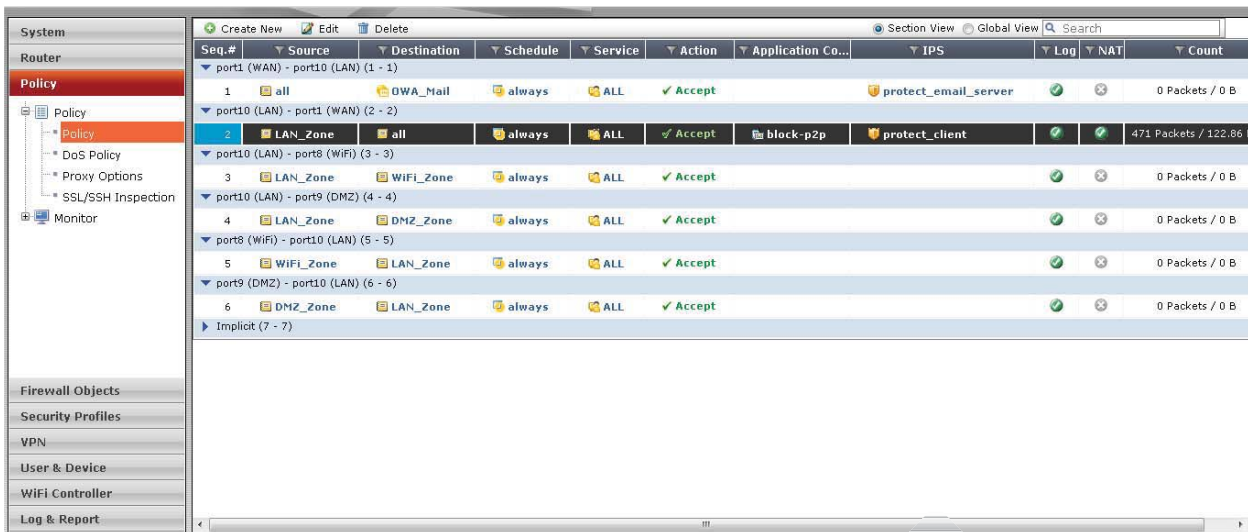


สำหรับ Application Control

เป็นการสร้าง Profile สำหรับการควบคุม Application ที่ผ่าน Firewall เช่น Monitor ,Block เพื่อที่จะนำ Profile เหล่านั้นมาใช้งานใน Policy ต่อไป ซึ่งสามารถเลือกเป็น Application ก็ได้



ตัวอย่างการใช้งาน Application Control (Block P2P)



Seq.#	Source	Destination	Schedule	Service	Action	Application Co...	IPS	Log	NAT	Count
1	all	OWA_Mail	always	ALL	Accept	protect_email_server				0 Packets / 0 B
2	port1 (WAN) - port10 (LAN) (1 - 1)									
3	port10 (LAN) - port1 (WAN) (2 - 2)									
4	port10 (LAN) - port8 (WiFi) (3 - 3)									
5	port10 (LAN) - port9 (DMZ) (4 - 4)									
6	port8 (WiFi) - port10 (LAN) (5 - 5)									
7	port9 (DMZ) - port10 (LAN) (6 - 6)									
8	Implicit (7 - 7)									

จะเห็นว่าเมื่อสร้าง Application Sensor แล้วก็จะนำไปใส่ใน Policy ที่ต้องการใช้งาน

ดังตัวอย่าง ลูกค้านำต้องการให้ Block Bit ไม่ให้เครื่อง Client ในวง LAN สามารถ Load Bit ได้

ก็จะนำ Application Sensor ชื่อ Block P2P ไปใส่ใน Policy ชื่อที่อนุญาตให้ Client ออก Internet

สำหรับ IPS Sensor

FortiGate จะมี Profile Default อยู่แล้ว ซึ่งมีการกำหนด Action เป็น Signature Default คือ กรณี Attack ใดที่มีความรุนแรงและมีควมอันตรายระบบจะทำการ Block ให้ ส่วน Attack ใดที่อยู่ในขั้นที่ปลอดภัยระบบจะทำการ Monitor สำหรับการ Attack นั้นๆ ในที่นี้อาจจะใช้ Profile Default เลยก็ได้

FortiGate 60C

System
Policy
Firewall Objects
Security Profiles
Antivirus
Profile
Web Filter
Application Control
Intrusion Protection
IPS Sensor
IPS Signatures
Email Filter
Data Leak Prevention
Client Reputation

VPN
User & Device
WiFi Controller
Log & Report

Edit IPS Filter

Sensor Type: ☒ Filter Based ☐ Specify Signatures

[Filter Options]

Severity

- ☒ critical
- ☒ high
- ☒ medium
- ☐ low
- ☐ info

Target

- ☒ client
- ☒ server

OS

- ☒ BSD
- ☒ Linux
- ☒ MacOS
- ☒ Other
- ☒ Solaris
- ☒ Windows

Name	Severity	Target	OS	Default
2Wire.Wireless.Router.XSRF.Password.Reset	medium	server, client	BSD	Block
3Com.3Cdaemon.FTP.Server.Buffer.Overflow	high	server	Linux	Block
3Com.Intelligent.Management.Center.Directory.Traversal	medium	server	Linux	Block
3Com.Intelligent.Management.Center.Information.Disclosure	medium	server	Linux	Block
3Com.OfficeConnect.ADSL.Wireless.Firewall.Router.DoS	medium	server	BSD	Monitor
3D.Life.Player.WebPlayer.ActiveX.Control.Buffer.Overflow	high	client	Linux	Monitor
3ivx.MPEG4.File.Processing.Buffer.Overflow	high	client	Linux	Block
4D.WebStar.FTP.Command.Buffer.Overflow	high	server	Linux	Block
4D.WebStar.Tomcat.Plugin.Remote.Buffer.Overflow	medium	server	Linux	Monitor
7T.IGSS.ODBC.Server.Memory.Corruption	medium	server	Linux	Block
7Technologies.IGSS.SCAD.A.System.Directory.Traversal	critical	server	Linux	Monitor
427BB.Cookie.Based.Authentication.Bypass	medium	server	Windows	Block
427BB.Showthread.PHP.ForumID.Parameter.SQL.Injection	medium	server	Windows	Block
1024CMS.Standard.PHP.File.Inclusion	high	server	Linux, BSD	Block

1 / 414 [Total: 5795]

Action ☒ Signature Defaults ☐ Monitor All ☐ Block All ☐ Reset ☐ Quarantine

☐ Packet Logging

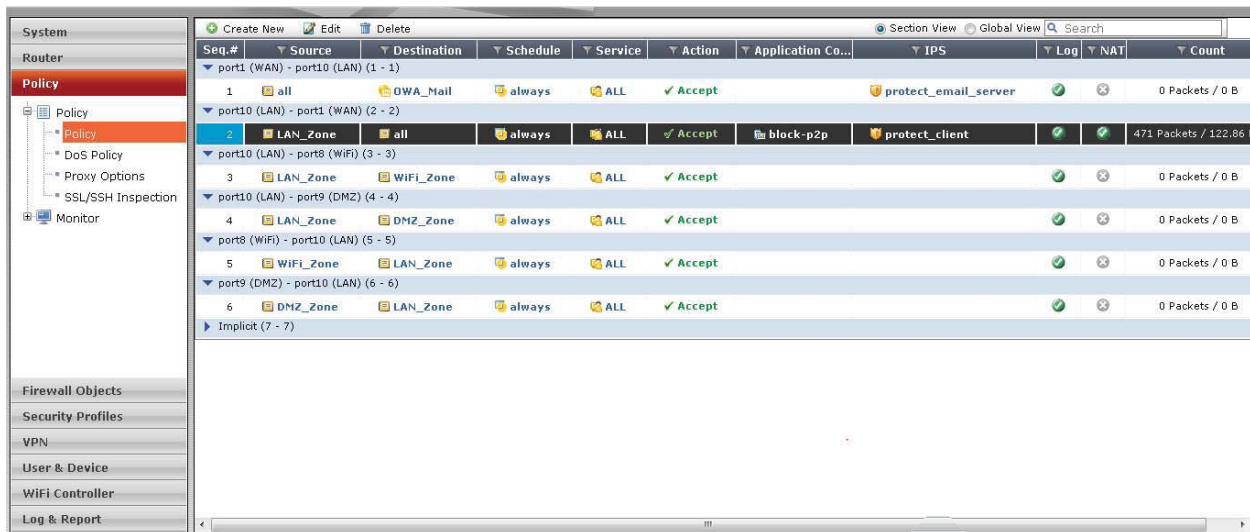
OK Cancel

หรือ อาจจะมีการเก็บ Package Log

Action ☒ Signature Defaults ☐ Monitor All ☐ Block All ☐ Reset ☐ Quarantine

☐ Packet Logging

ตัวอย่างการใช้งาน IPS



The screenshot shows the FortiGate Policy Map configuration. The left sidebar contains the navigation menu with 'Policy' selected. The main area displays a table of policies with columns for Seq.#, Source, Destination, Schedule, Service, Action, Application Control, IPS, Log, NAT, and Count. The following table represents the data shown in the screenshot:

Seq.#	Source	Destination	Schedule	Service	Action	Application Co...	IPS	Log	NAT	Count
1	all	OWA_Mail	always	ALL	Accept		protect_email_server	✓	✗	0 Packets / 0 B
2	port1 (WAN) - port10 (LAN) (1 - 1)									
3	port10 (LAN) - port1 (WAN) (2 - 2)									
4	port10 (LAN) - port8 (WiFi) (3 - 3)									
5	port10 (LAN) - port9 (DMZ) (4 - 4)									
6	port8 (WiFi) - port10 (LAN) (5 - 5)									
7	port9 (DMZ) - port10 (LAN) (6 - 6)									
8	Implicit (7 - 7)									

จะเห็นว่าสำหรับ Case นี้ลูกค้าต้องการ Protect Mail Server และวง Client ที่ออก Internet

จึงนำเอา IPS Profile ชื่อ Protect eMail Server ไปไว้ใน Policy Map VIP จาก WAN เข้า Mail Server

และใช้ IPS Profile ชื่อ Protect Client ไว้สำหรับ Policy ที่อนุญาต Client ออก Internet

สำหรับ Email Filter

FortiGate จะมี Profile Default อยู่แล้ว แต่อาจจะเพิ่ม “Enable Spam Detection and Filtering”
“FortiGuard Spam Filtering” หรือ “Local Spam Filtering” เข้าใน Profile Default เลขก็ได้

FortiGate 60C

System
Policy
Firewall Objects
Security Profiles
Antivirus
Web Filter
Application Control
Intrusion Protection
Email Filter
Profile
Email List
Data Leak Prevention
Client Reputation

VPN
User & Device
WiFi Controller
Log & Report

FortiGate 60C

Help Wizard Logout

FortINET

Edit Email Filter Profile default

Name: default

Comments: malware and phishing URL filtering 34/255

Inspection Mode: Proxy Flow-based

☒ Enable Spam Detection and Filtering

	☒ IMAP	☒ POP3	☒ SMTP
Spam Action	Tagged	Tagged	Discard
Tag Location	Subject	Subject	Subject
Tag Format	Spam	Spam	Spam

☒ FortiGuard Spam Filtering

☒ IP Address Check ☒ URL Check ☒ Detect Phishing URLs in Email

☒ E-mail Checksum Check ☒ Spam Submission

☐ Local Spam Filtering

☒ HELO DNS Lookup ☐ Return E-mail DNS Check

☐ BWL Check -- None --

Apply

หมายเหตุ

สำหรับ Email Filter ในตัว FortiGate นั้นจะมี Action ได้ 2 แบบคือ Tag Subject และ Discard เท่านั้น

Enable Spam Detection and Filtering

=> FortiGuard License

FortiGuard Spam Filtering

=> FortiGuard License



System	Create New Section View Global View Search										
	Seq.#	Source	Destination	Schedule	Service	Authentication	Action	Email Filter	Log	NAT	Count
Router	▼ port1 (WAN) - port10 (LAN) (1 - 1)										
	1	all	OWA_Mail	always	ALL		✓ Accept	FDS_AntiSpam	✓	✗	0 Packets / 0 B
Policy	▼ port10 (LAN) - port1 (WAN) (2 - 2)										
	2	LAN_Zone	all	always	ALL		✓ Accept		✓	✓	3,988 Packets / 2.33 MB
Policy	▼ port10 (LAN) - port8 (WiFi) (3 - 3)										
	3	LAN_Zone	WiFi_Zone	always	ALL		✓ Accept		✓	✗	0 Packets / 0 B
Policy	▼ port10 (LAN) - port9 (DMZ) (4 - 4)										
	4	LAN_Zone	DMZ_Zone	always	ALL		✓ Accept		✓	✗	0 Packets / 0 B
Policy	▼ port8 (WiFi) - port10 (LAN) (5 - 5)										
	5	WiFi_Zone	LAN_Zone	always	ALL		✓ Accept		✓	✗	0 Packets / 0 B
Policy	▼ port9 (DMZ) - port10 (LAN) (6 - 6)										
	6	DMZ_Zone	LAN_Zone	always	ALL		✓ Accept		✓	✗	0 Packets / 0 B
Policy	▼ Implicit (7 - 7)										
Firewall Objects											
Security Profiles											
VPN											
User & Device											
WAN Opt. & Cache											
WiFi Controller											
Log & Report											

ตัวอย่างการใช้งาน FortiGuard AntiSpam

เมื่อสร้าง FortiGuard AntiSpam เรียบร้อยแล้ว จากนั้นสามารถนำ Profile ดังกล่าว

มาใช้งานใน Policy ที่ต้องการ Protect ได้เลย ตัวอย่างนี้คือใช้งานใน Policy VIP

ที่ทำการ Map IP Public มาให้ Mail Server ภายใน



Local User Auth

ขั้นตอนที่ 1 : สร้าง User Group

System

Router

Policy

Firewall Objects

Security Profiles

VPN

User & Device

- User
 - User Definition
 - User Group**
 - Guest Management
- Device
- Authentication
- Two-factor Authentication
- Vulnerability Scan
- Monitor

WAN Opt. & Cache

WiFi Controller

Log & Report

New User Group

Name: firewall_local

Type: ☒ Firewall ☐ Fortinet Single Sign-On (FSSO) ☐ Guest ☐ RADIUS Single Sign-On (RSSO)

Members: Click to set...

Remote authentication servers

Remote Server	Group Name
No matching entries found	

OK Cancel

ขั้นตอนที่ 2 : สร้าง User ใส่ใน User Group โดยทำตามขั้นตอนไปเรื่อยๆ

System

Router

Policy

Firewall Objects

Security Profiles

VPN

User & Device

- User
 - User Definition
 - User Group**
 - Guest Management
- Device
- Authentication
- Two-factor Authentication
- Vulnerability Scan
- Monitor

WAN Opt. & Cache

WiFi Controller

Log & Report

User Creation Wizard

1 Choose User Type 2 Specify Login Credentials 3 Provide Contact Info 4 Provide Extra Info

☒ Local User

☐ Remote RADIUS User

☐ Remote TACACS+ User

☐ Remote LDAP User

< Back Next > Cancel