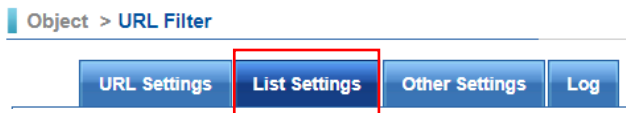




STEP 1. เข้าเมนู [Object / URL Filtering]

- Object
 - IP Address
 - Services
 - Schedule
 - QoS
 - Application Control
 - **URL Filter**
 - DNS Filter
 - Firewall Protection
 - Authentication
 - Bulletin Board

1.1 เข้าเมนู List Settings



1.2 กดปุ่ม Add

● **Basic Setting**
 Name
 List Mode Blacklist Whitelist
 Match Mode Exact Fuzzy

● **Sandstorm (Active)**
 Sandstorm (Risk Setting : High)

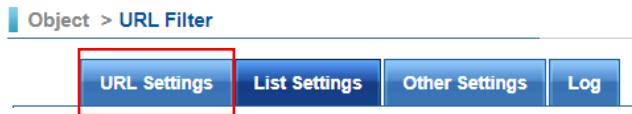
Security Risks & Criminal (0/6) Select All
 Pornography & Violence (0/9) Select All
 Organizations & Education (0/5) Select All
 Network & Cloud Service (0/19) Select All
 Life Information (0/17) Select All
 Others (0/6) Select All

● **Create Blacklist**
 URL Blacklist
 IPv4 IP Blacklist
 IPv6 IP Blacklist
 Domain Blacklist

- Name ชื่อกลุ่มของ URL listing
- List Mode ให้เลือก Blacklist
- Match Mode คือวิธีการตรวจสอบ
 - Exact คือต้องมีคำที่ต้องการ Block เท่านั้น
 - Fuzzy คือใช้คำตรงกับที่ต้องการ จะมีอักษรหน้าหลังเป็นอะไรก็ได้
- Sandstorm คือการตรวจสอบ Malware ที่แนบมากับไฟล์จากการโหลดข้อมูลทางเว็บ
- URL Database คือฐานข้อมูลที่รวบรวมเป็นหมวดหมู่
- URL Blacklist ให้ใส่ URL หรือคำวลีที่ต้องการ Block เช่น porn.com, Pornhub
- IPv4 Blacklist ให้ใส่ IP Address ที่ต้องการ Block
- IPv6 Blacklist ให้ใส่ IP v6 ที่ต้องการ Block
- Domain Blacklist ให้ใส่โดเมน เช่น *.porn.com



STEP 2. เข้า [URL Settings]



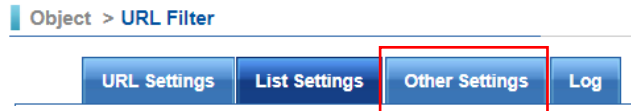
2.1 กดปุ่ม Add

Group Name

Create block warning message

List Select

- Group name ให้ใส่ชื่อกลุ่มจะถูกนำไปเรียกใช้ที่ Policy
- Create block warning message ถ้าไม่คลิกถูกข้อความเตือนจะแสดงตาม Other Settings



- List Select ให้เลือกจากการสร้างในหัวข้อ List Settings

STEP 3. เข้าเมนู [Policy / Security Policy/Outgoing]

3.1 Edit Policy เฉพาะที่เป็น HTTP policy โดยกดที่รูปดินสอ

DEST Service Group Port

Action

Policy

Schedule

QoS

Application Control

Max. Concurrent Sessions for Each Source IP Address

Authentication

Bulletin Board

URL Access Control

- DEST Service Group ต้องเป็น HTTP port 80 เท่านั้น
- URL Access Control ให้เลือกชื่อกลุ่มที่สร้างที่ STEP 2

3.2 กดปุ่ม Edit



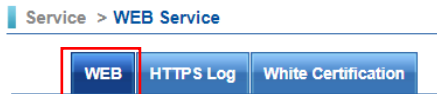
การ Block เว็บต้องห้าม HTTPS

STEP 4. ถ้าต้องการ Block เว็บต้องห้ามผ่าน HTTPS ให้เพิ่มขึ้นในการติดตั้ง Certificate บนเครื่องคอมพิวเตอร์

4.1 เข้าเมนู [Service/Web service]

- Service
 - ▣ DHCP
 - ▣ DDNS
 - ▣ SNMP
 - ▣ DNS Server
 - ▣ Anti-Virus Engine
 - ▣ Sandstorm
 - ▣ **WEB Service**
 - ▣ High Availability
 - ▣ Remote Syslog

4.2. เลือกเมนู [WEB]

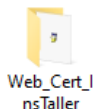
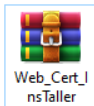


4.3 ให้ Download Software ไปติดตั้งบนเครื่องคอมพิวเตอร์ที่ต้องการ Block เว็บต้องห้าม

► **Encryption Connect Setting :**

SSL Listen Port	<input type="text" value="443"/> (Range: 1 ~ 65535) ?
Certificate Time	2020-09-17 22:24:48
Download SSL Certificate	<input type="button" value="Download"/> <input type="button" value="Re-generate Certificate"/>
Certificate Download Link	https:// Wan IP Address or Domain : [HTTPS Port] /myca.crt (https://192.168.111.1/myca.crt)
Certification Installer Download Link	https:// Wan IP Address or Domain : [HTTPS Port] /download_certinstaller.php <input type="button" value="Download Installer"/> (https://192.168.111.1/download_certinstaller.php)

- คลิกที่ปุ่ม Download Installer จะได้เป็น Zip ไฟล์ให้คลาย Zip แล้ว



- เข้า Folder แล้วคลิกที่ File Web_Cert_InsTaller.exe เพื่อติดตั้ง

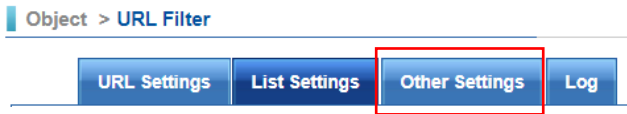
STEP 5. เข้าเมนู [Policy / Security Policy/Outgoing]

DEST Service Group	<input type="text" value="HTTPS"/> Port <input type="text" value="443"/>
Action	<input type="button" value="Permit"/>
► Policy	
Schedule	<input type="button" value="None"/>
QoS	<input type="button" value="None"/>
Application Control	<input type="button" value="None"/>
Max. Concurrent Sessions for Each Source IP Address	<input type="text" value="0"/>
Authentication	<input type="button" value="None"/>
Bulletin Board	<input type="button" value="None"/>
URL Access Control ?	<input type="button" value="BL"/>

*** แก้ไข Policy เหมือน HTTP แต่เปลี่ยน DEST Service Group เป็น HTTPS port 443



STEP 6. เข้า [Other Settings]



2.1 หน้าจอจะแสดงข้อความที่เป็น Default ให้ดำเนินการแก้ไขตามที่ต้องการ

Default Block Page Settings

Warning message [View](#)

Warning Subject

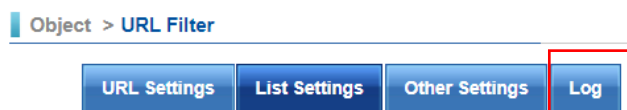
Warning content

2.2. ให้กด View เพื่อดูสิ่งที่เราแก้ไข



Access to the page has been denied because the following page is blacklisted

STEP 7. ดู Log ผู้ฝ่าฝืนใช้งานเว็บตั้งห้าม



Source IP	Protocol	Destination
192.168.111.78	HTTPS	https://xxxporn7.com/category/%E0%B9%80%E0%B8%AD%E0%B...
192.168.111.78	HTTPS	https://xxxporn7.com/favicon.ico
192.168.111.78	HTTPS	https://xn--72czpj1fd3b9a3a8g3d.com/%E0%B9%81%E0%B8%9...
192.168.111.78	HTTPS	https://www.porn.com/favicon.ico
192.168.111.78	HTTPS	https://www.porn.com/

*** สามารถค้นหาได้ตาม IP Address / Date