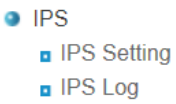
NetinforTech Co.,Ltd.

การติดตั้ง IPS (Intrusion Prevention System)

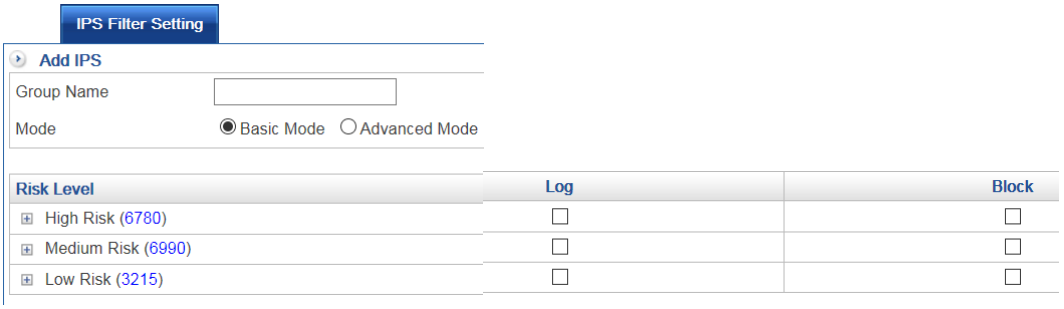
การ Setup IPS มีขั้นตอนดังนี้

1. เปิดเมนู IPS



2. คลิกที่เมนูย่อย IPS Setting และกดปุ่ม  เพื่อสร้างกลุ่มของ IPS

3. จะปรากฏหน้าจอดังรูป 3.1



รูปที่ 3.1

3.1 Group Name คือชื่อของกลุ่ม IPS โดยจะไปแสดงให้เลือกใช้ใน Security Policy

3.2 Mode มีให้เลือกอยู่ 2 Mode คือ

3.2.1 Basic Mode คือการเลือกจะตรวจสอบและป้องกันแยกตามระดับความเสี่ยง (High, Medium, Low) และสามารถจะเลือกเก็บ Log อย่างเดียวหรือทั้งป้องกันความเสี่ยง

3.2.2 Advanced Mode คือ สามารถเลือกที่จะเก็บ Log หรือ ป้องกันแยกตามความเสี่ยง (Signature)

3.3 Rick Level จะเป็นระดับของรูปแบบความเสี่ยงจะมีอยู่ 3 ระดับ เช่น High, Medium, Low

3.4 Log เมื่อคลิกเครื่องหมายถูกที่ Log ความหมายคือเมื่อระบบตรวจสอบข้อมูลว่ากับรูปแบบความเสี่ยงระบบจะเก็บ Log ไว้

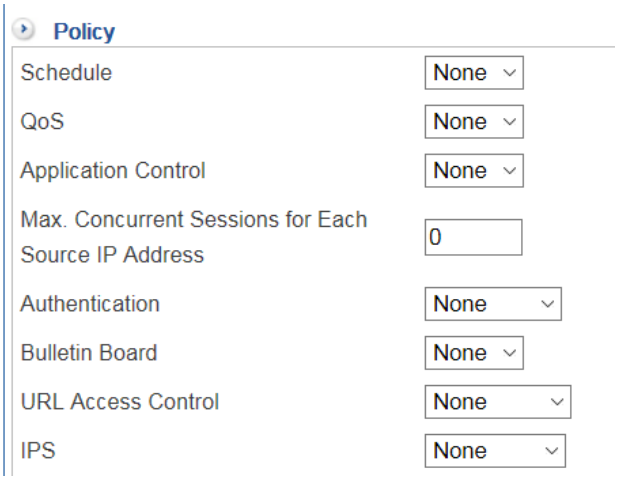
3.5 Block คือเมื่อคลิกเครื่องหมายถูก และตรวจสอบว่าข้อมูลตรงกับความเสี่ยงระบบจะทำการ Block ไม่ให้รับเข้าและส่งออกทันที

3.6 กดปุ่ม 

4. ไปที่เมนู Security Policy และเลือกเมนู Outgoing

4.1 เข้าไปแก้ไข Policy ตามกลุ่มที่เราต้องการตรวจสอบโดยกดปุ่ม 

4.2 หน้าจอจะปรากฏดังรูปที่ 4.2

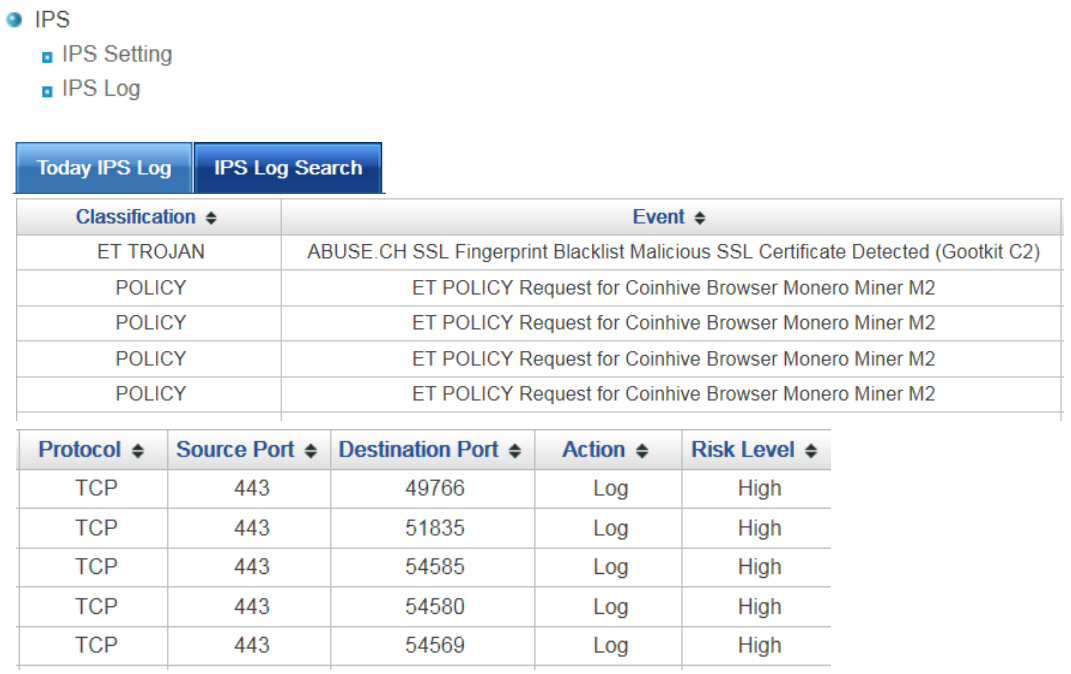


4.3 ให้คลิกที่ข้อความ Policy เพื่อขยายหน้าจอแล้วให้ไปตรงบันทัด IPS ให้กด Menu List เพื่อเลือก Group ของ IPS ที่เราสร้างไว้

4.4 กดปุ่ม 

หมายเหตุ: ปล่อยให้ระบบทำงานตรวจสอบประมาณ 5 นาที ระบบจะเริ่มบันทึกข้อมูลลง Databe เพื่อแสดงใน IPS Log

5.คลิกที่เมนู IP Log เพื่อดู Log ว่ามีการตรวจสอบแล้วเจอความเสี่ยงหรือไม่



Classification	Event
ET TROJAN	ABUSE.CH SSL Fingerprint Blacklist Malicious SSL Certificate Detected (Gootkit C2)
POLICY	ET POLICY Request for Coinhive Browser Monero Miner M2
POLICY	ET POLICY Request for Coinhive Browser Monero Miner M2
POLICY	ET POLICY Request for Coinhive Browser Monero Miner M2
POLICY	ET POLICY Request for Coinhive Browser Monero Miner M2

Protocol	Source Port	Destination Port	Action	Risk Level
TCP	443	49766	Log	High
TCP	443	51835	Log	High
TCP	443	54585	Log	High
TCP	443	54580	Log	High
TCP	443	54569	Log	High