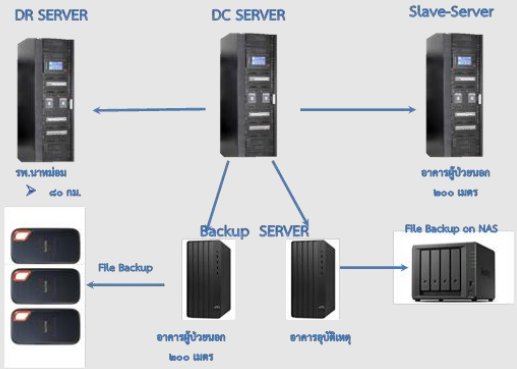
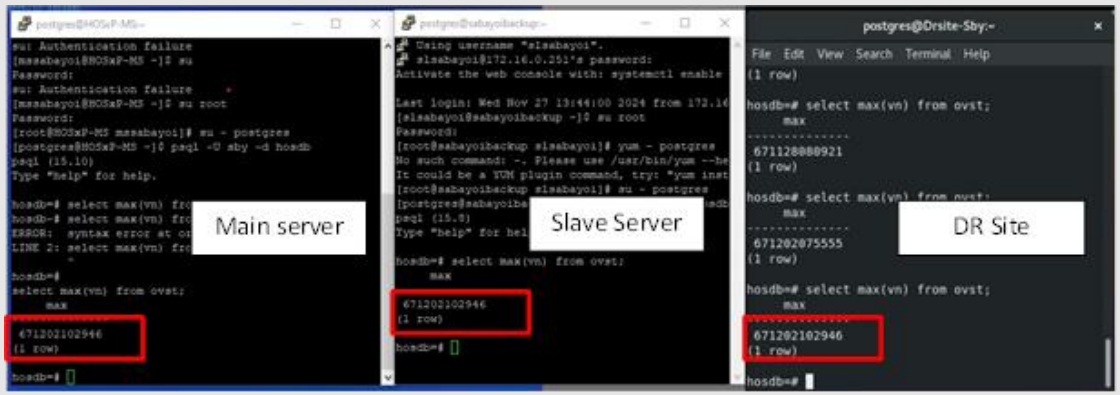
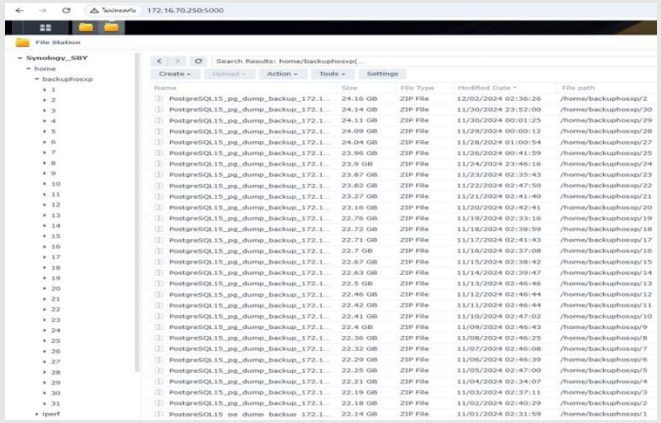
CS.3.1 มีการจัดทำแนวปฏิบัติด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ (Specific information security policy) มีหัวข้อ อย่างน้อยต่อไปนี้ 1) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ (Access Control) 2)การสำรองข้อมูลเพื่อให้สารสนเทศอยู่ใน สภาพพร้อมใช้งานและการจัดทำแผนเตรียมความพร้อมรับมือภัย คุกคาม 3) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

<table>
<tr><th>ลำดับ</th><th>หัวข้อ</th><th>ขอบเขตการดำเนินการ</th><th>การแก้ไข</th><th>ประเมิน</th><th>ผู้รับผิดชอบ</th></tr>
<tr><td>1.</td><td>Backup
: การสำรองข้อมูลเก็บไว้ที่อื่น เพื่อให้สามารถใช้เพื่อกู้คืนข้อมูลเดิมหลังจากเหตุการณ์ข้อมูลสูญหาย</td><td>มีการสำรองข้อมูลอย่างน้อยวันละ 1 ครั้ง และสามารถย้อนหลังได้ 7 วัน เป็นอย่างน้อยตามมาตรฐาน โดยจัดเก็บบนระบบ Logical HDD หรือ Physical HDD และ จัดเก็บ Backup ในรูปแบบ 3-2-1 1. สำเนาข้อมูลไว้บนระบบ 3 ชุด 2. สำเนาข้อมูลไว้บนเทคโนโลยีต่างกัน 2 ชุด 3. สำเนาข้อมูลไว้แบบ Offline หรือ Offsite หรือ Cloud 1 ชุด</td><td></td><td></td><td></td></tr>
<tr><td colspan="5">หลักฐาน
แผนผังการสำรองข้อมูล
 

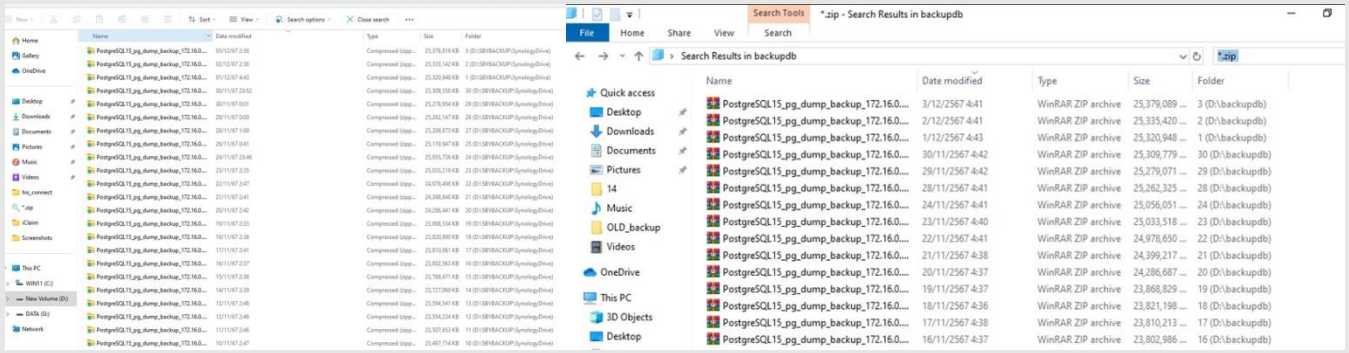
1. สำเนาข้อมูลไว้บนระบบ 3 ชุด
 

2. สำเนาข้อมูลไว้บนเทคโนโลยีต่างกัน</td></tr>
</table>

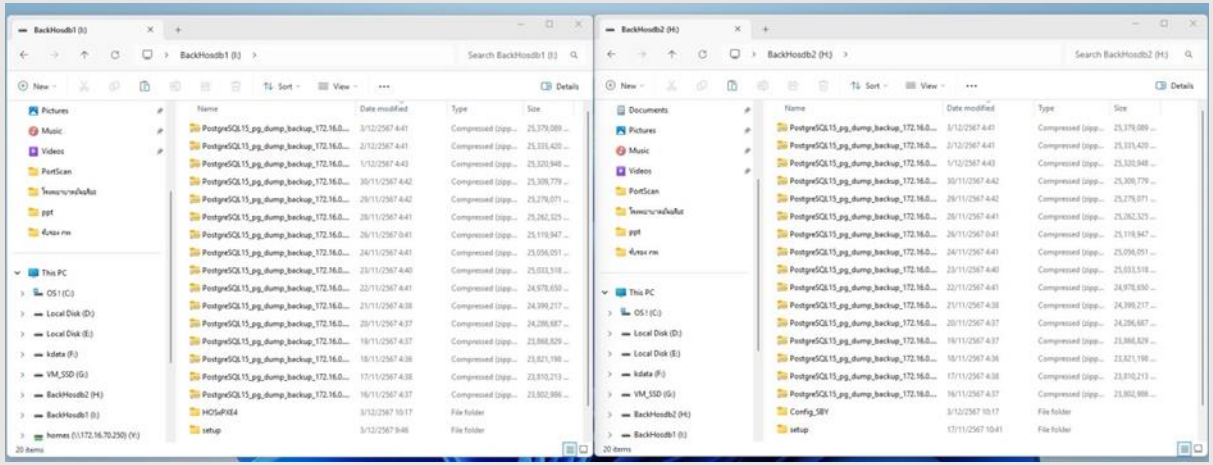
2.1 ไฟล์สำรองฐานข้อมูล HIS บน Nas



2.2ไฟล์สำรองฐานข้อมูล HIS บน PC 1 อาคารอุบัติเหตุ,ไฟล์สำรองฐานข้อมูล HIS บน PC 1 อาคารผู้ป่วยนอก

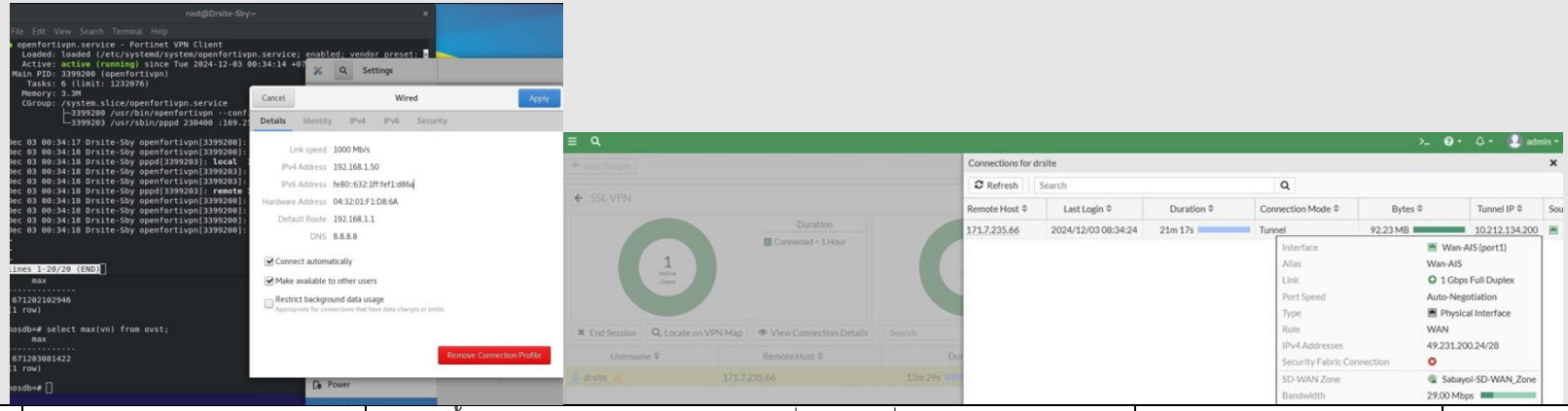


2.3 ไฟล์สำรองฐานข้อมูล HIS บน External Hard Disk



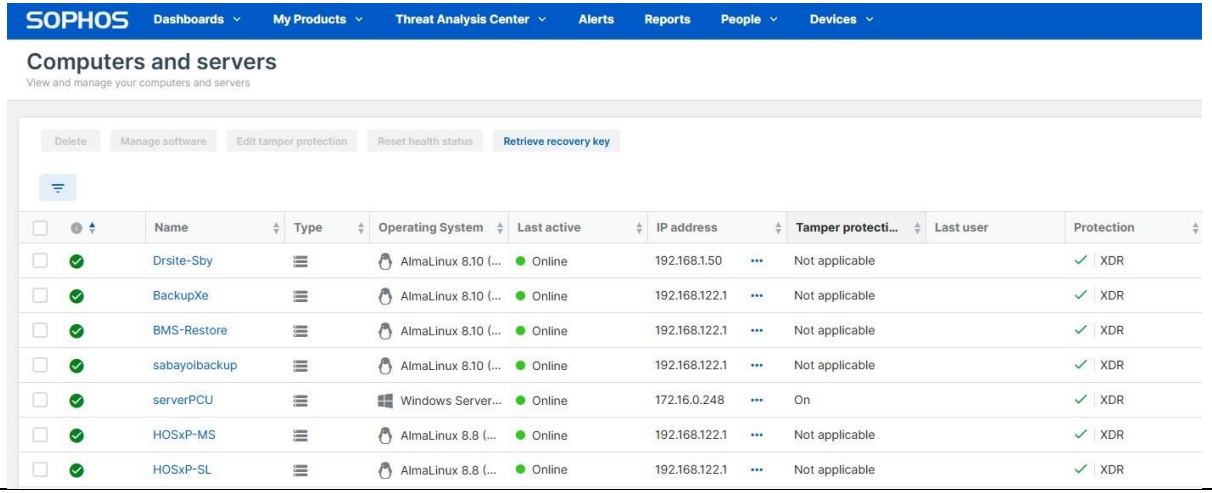
3. สำเนาข้อมูลไว้แบบ Offline หรือ Offsite หรือ Cloud 1 ชุด

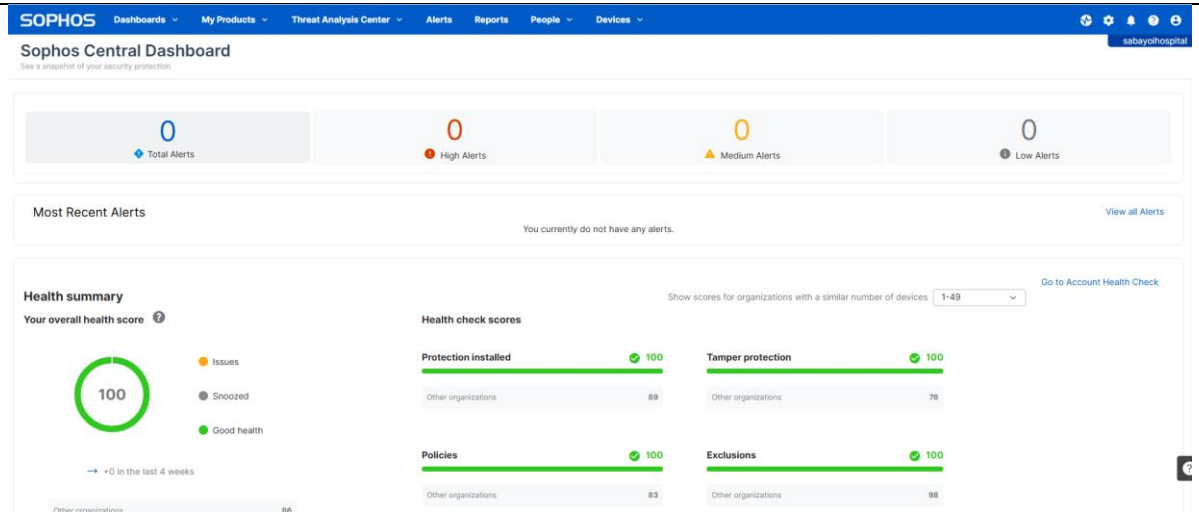
ข้อมูล DR Site Server ตั้งอยู่ที่ รพ.นาหม่อม ระยะทาง 81 กิโลเมตร การ Sync ข้อมูลผ่านระบบ VPN



2.	**Antivirus Software** : โปรแกรมป้องกันไวรัส หรือ แอนติไวรัส คอยตรวจจับ ป้องกัน และกำจัดโปรแกรมคุกคามทางคอมพิวเตอร์หรือมัลแวร์	มีการติดตั้ง Anti-Virus หรือ EDR หรือ XDR บนเครื่องอุปกรณ์ที่สำคัญ 1. Review Alert Report 2. Update Program Anti-Virus, EDR/XER 3. Schedule Update Database Signature			

หลักฐาน



					
3.	Access Control (Public และ Private) : การควบคุมอุปกรณ์หรือการเข้าถึงระบบผ่านทางช่องทาง Public/Private ทั้งภายใน ประเทศ และ ต่างประเทศ	มีการควบคุม Policy การเข้าถึงระบบที่สำคัญทั้งทาง Public และ Private 1. มีการควบคุมการเข้าถึงห้องเครื่องคอมพิวเตอร์แม่ข่าย 2. IP Address Filter กำหนดขอบเขตการใช้งาน IP Address ที่สามารถเข้าใช้งานในระบบได้ เช่น IP Location, Geometric 3. 3. ดำเนินการกำหนด White list Port และไม่เปิด Port ที่ ที่มี มีความเสี่ยงต่อการโดนโจมตี ตี ปัจจุบันได้แก่ 7, 19, 20, 21, 22, 23, 25, 37, 53, 69, 79, 80, 110, 111, 135, 137, 138, 139,445, 161, 443, 512, 513, 514, 1433, 1434,1723,3 389, 8080 (หากมี มีความจำเป็นในการเปิดจะต้องทำ การกำ หนด Source และ Destination ให้ชัดเจน) 4. .มีการแบ่งโซน Network ระหว่างอุปกรณ์แม่ข่าย (Server) และอุปกรณ์ลูกข่าย 5. มีการใช้งาน VPN ในการเข้าถึงอุปกรณ์แม่ข่าย (Server) แทนการใช้งานผ่าน Public 6. User Access Accounts กำหนดสิทธิการใช้งานเท่าที่จำเป็น เช่น Role Base / Group Base 7. User Password Policy กำหนดการใช้งานพาสเวิค เช่น กำหนดความยาวอย่างน้อย 12 ตัวอักษร, Hash MD5, SHA-256 8. Time Sync			

หลักฐาน

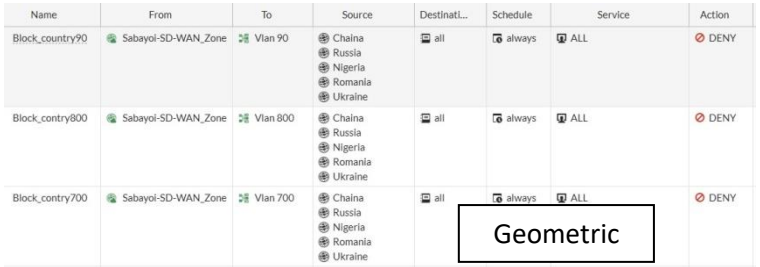
3.1 การควบคุมการเข้าถึงห้องเครื่องคอมพิวเตอร์แม่ข่าย

สแกนลายนิ้วมือ

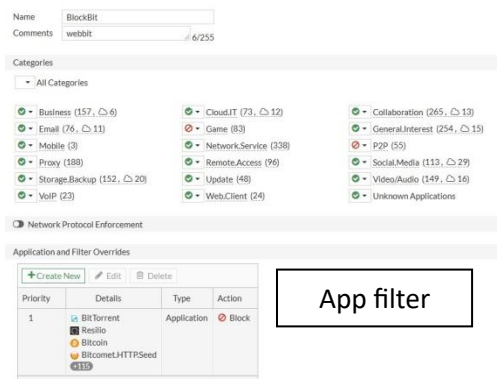
กล้องวงจรปิด

การเข้าถึง Network

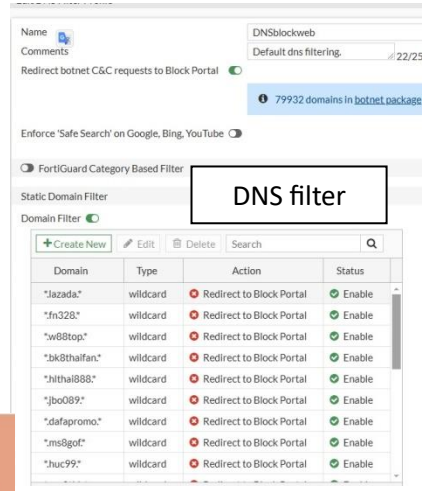
3.2. IP Address Filter กำหนดขอบเขตการใช้งาน IP Address ที่สามารถเข้าใช้งานในระบบได้ เช่น IP Location, Geometric



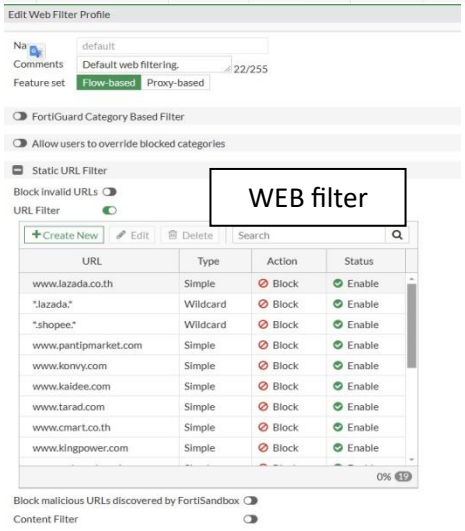
Geometric



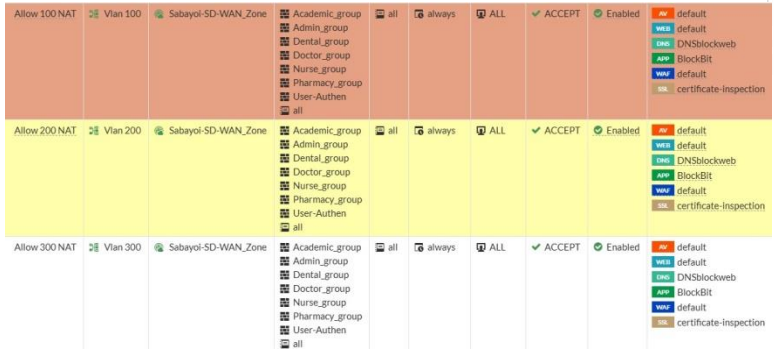
App filter



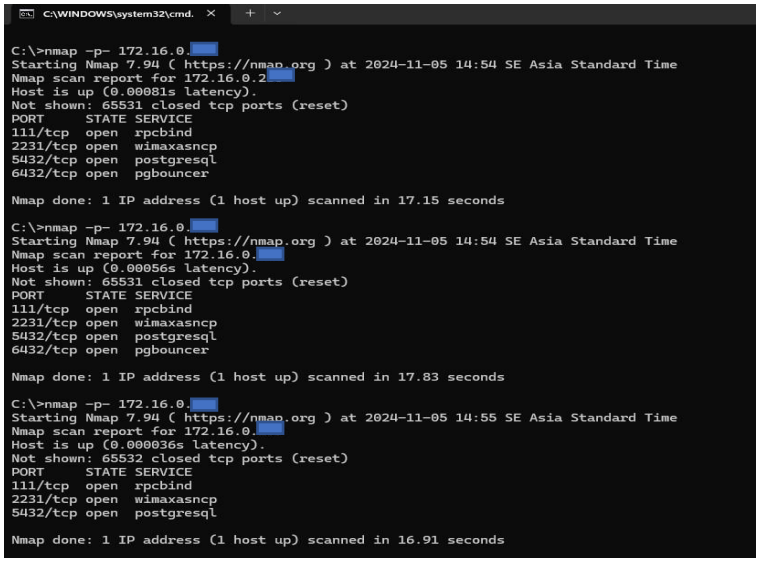
DNS filter

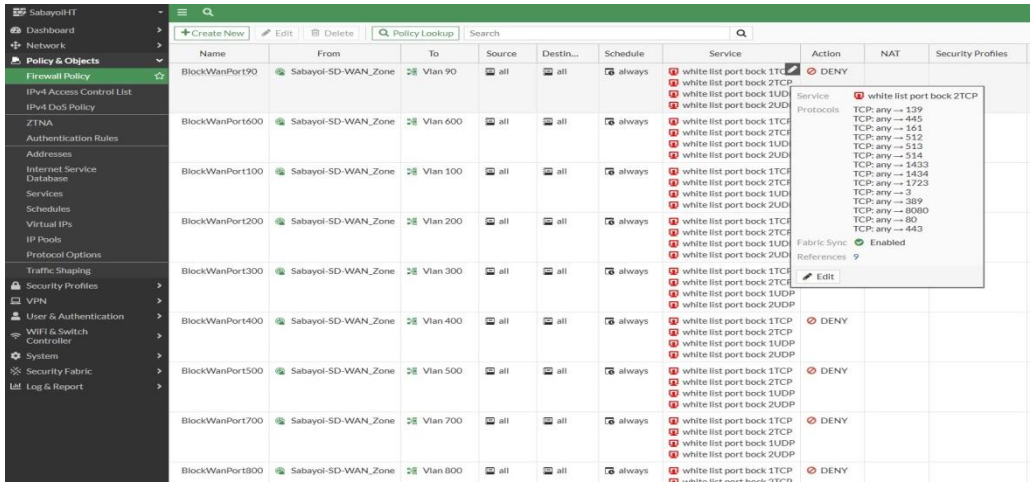


WEB filter

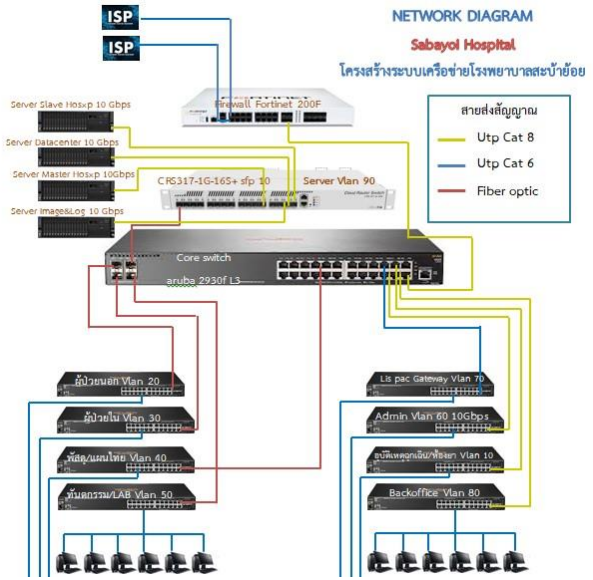


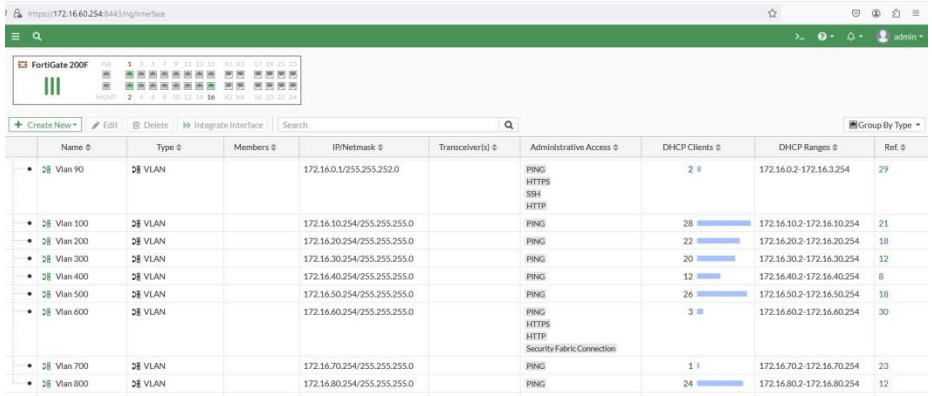
3.3 ดำเนินการกำหนด White list Port และไม่เปิด Port ที่ ที่มี มีความเสี่ยงต่อการโดนโจมตี



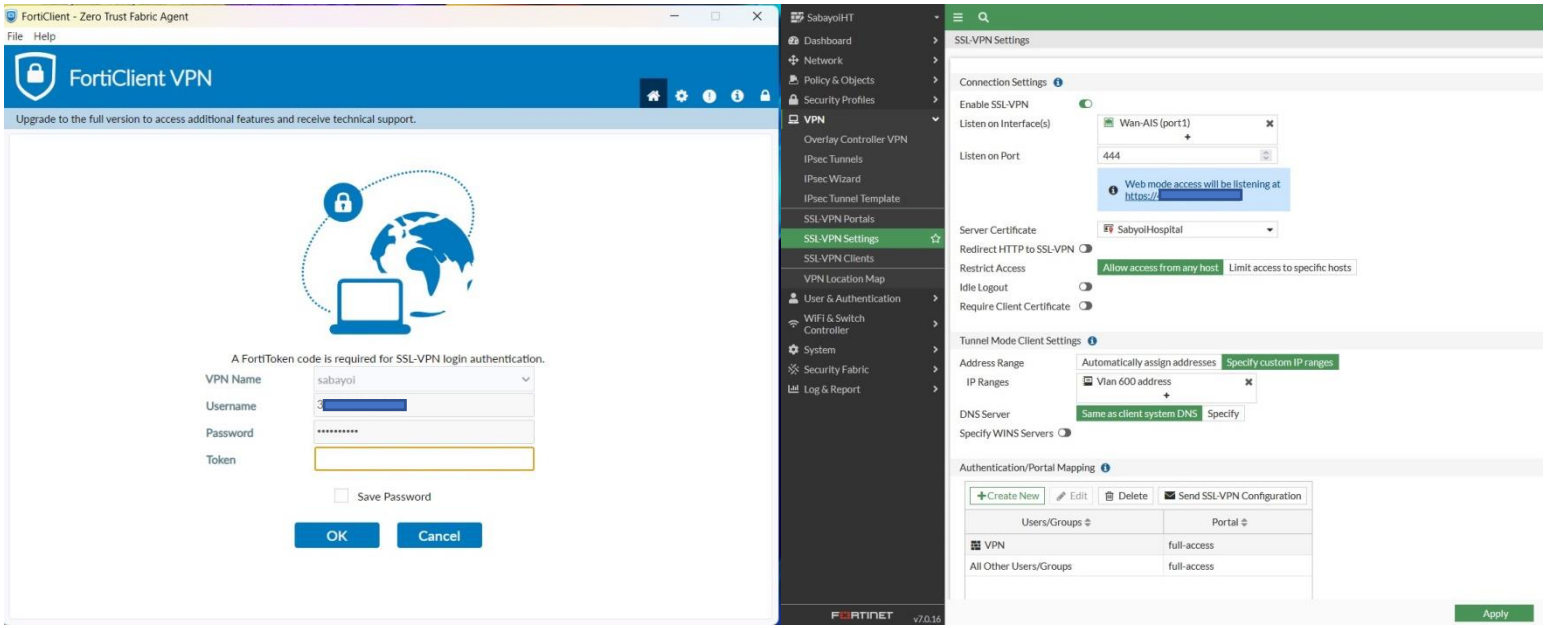


3.4 มีการแบ่งโซน Network ระหว่างอุปกรณ์แม่ข่าย (Server) และอุปกรณ์ลูกข่าย



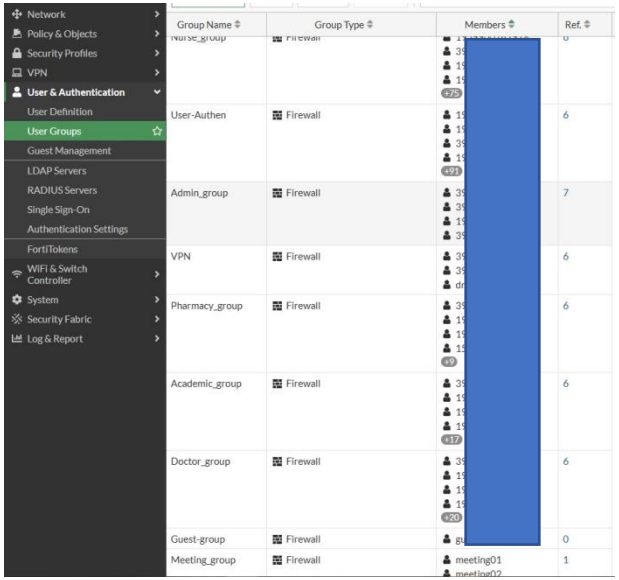


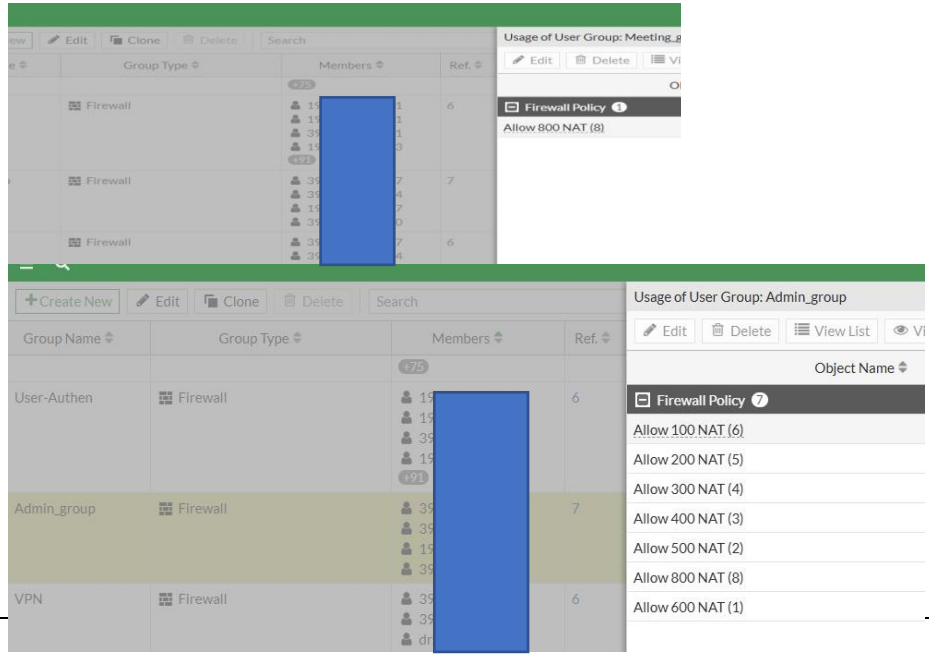
3.5 มีการใช้งาน VPN ในการเข้าถึงอุปกรณ์แม่ข่าย (Server) แทนการใช้งานผ่าน Public



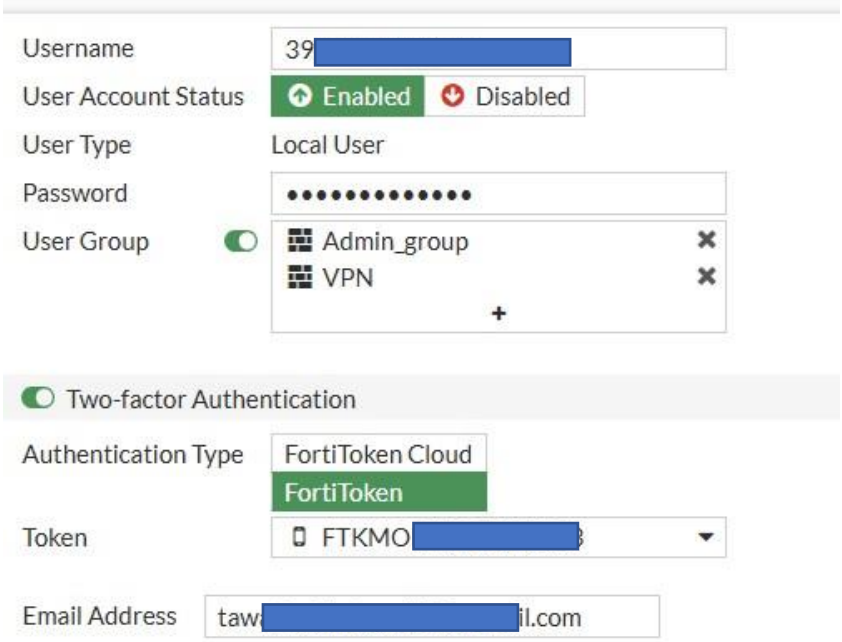
การใช้งาน VPN to factor authentication

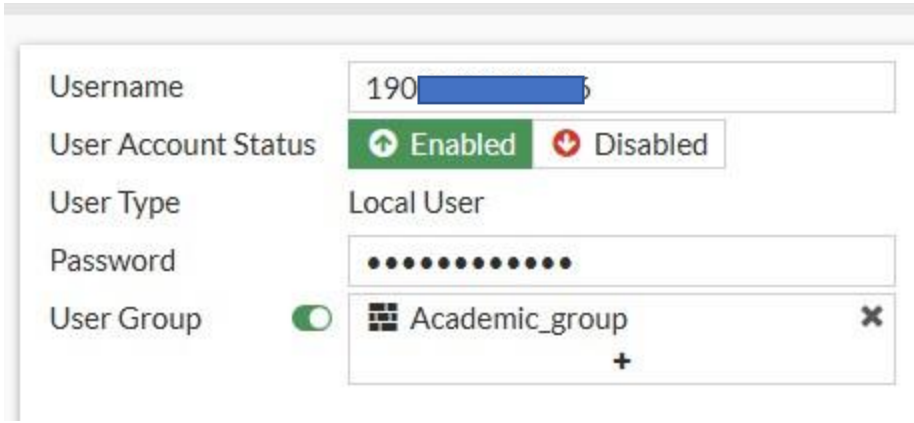
3.6 User Access Accounts กำหนดสิทธิการใช้งานเท่าที่จำเป็น เช่น Role Base / Group Base



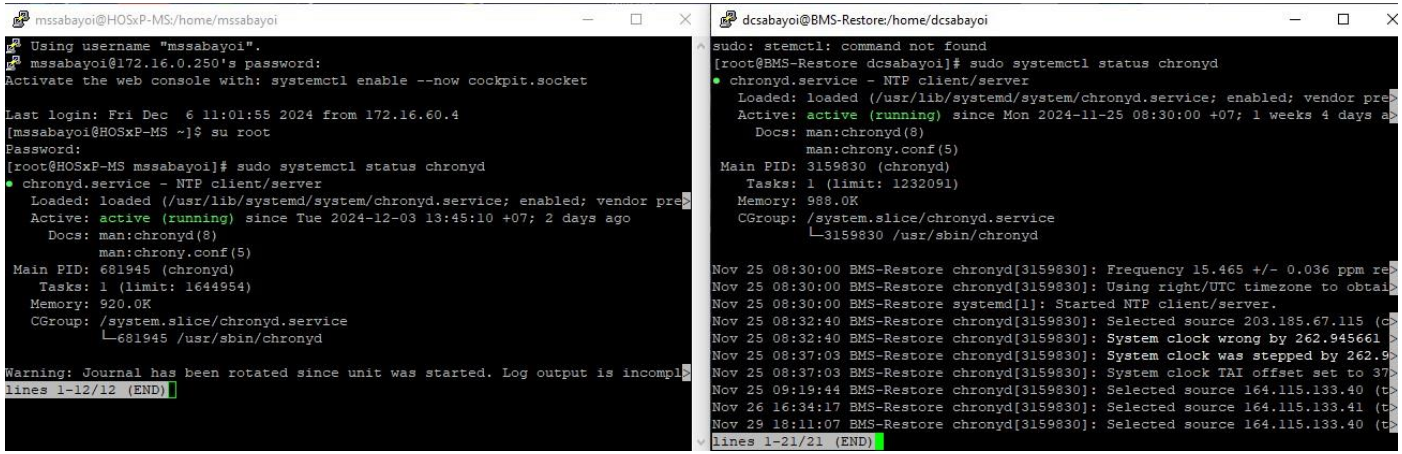


3.7 User Password Policy กำหนดการใช้งานพาสเวิด เช่น กำหนดความยาวอย่างน้อย 12 ตัวอักษร, Hash MD5, SHA-256





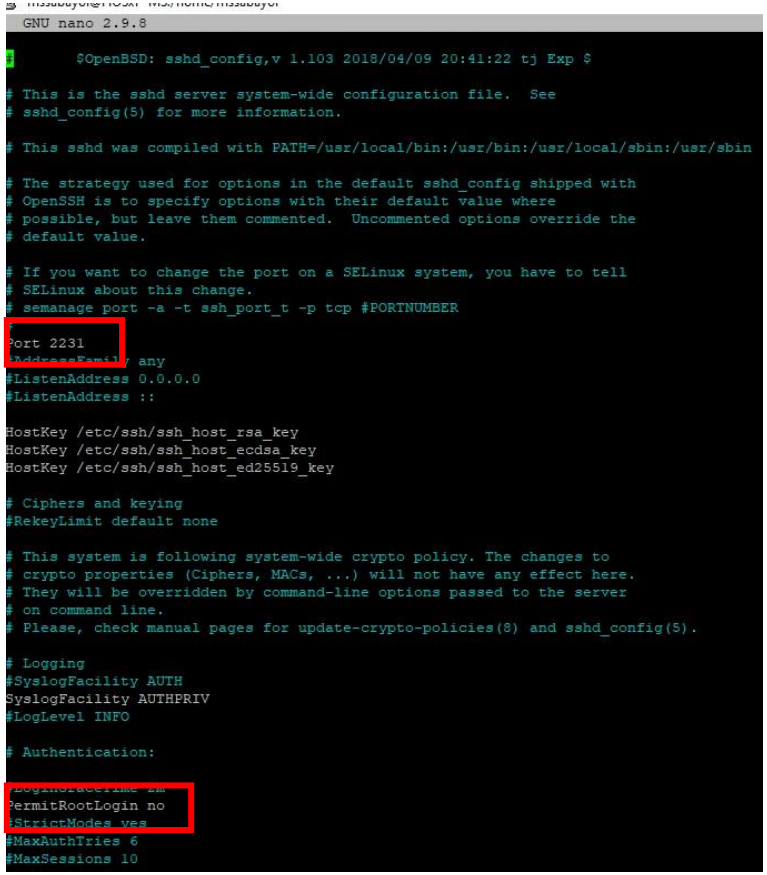
3.8 Time Sync

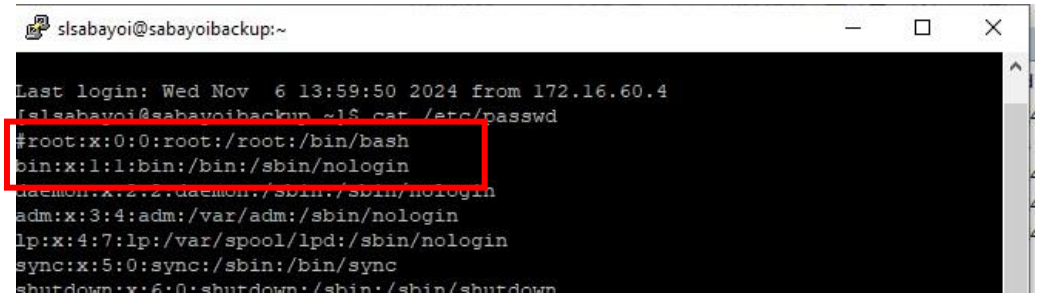


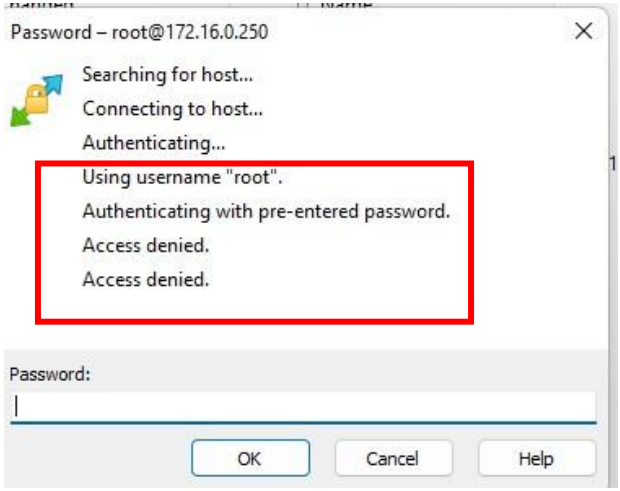
4.	Privileged Access Management (PAM) : โซลูชั่นการรักษาความปลอดภัยของข้อมูลประจำตัวที่ช่วยปกป้องค์กรจากภัย คุกคามทางไซเบอร์ด้วยการ ติดตาม ตรวจหา และป้องกัน การใช้สิทธิ์การเข้าถึงทรัพยากรที่สำคัญในระดับสูง	มีการควบคุมการเข้าถึงระบบโดยใช้งานสิทธิ์ระดับ Least Privilege ดังนี้ 1. ดำเนินการ Disable Administrator / Root / Admin 2. มีการกำหนด Role-base access ในการเข้าถึงระบบเท่าที่มีจำเป็น 3. มีการตั้ง Password อย่างน้อย 12 ตัว (ตัวอักษรใหญ่, เล็ก, อักขระพิเศษ, ตัวเลข) 12, มีการเข้ารหัส Password MD5,SHA-256 4. Expire Sessions Time out			

หลักฐาน

4.1 ดำเนินการ Disable Administrator / Root / Admin

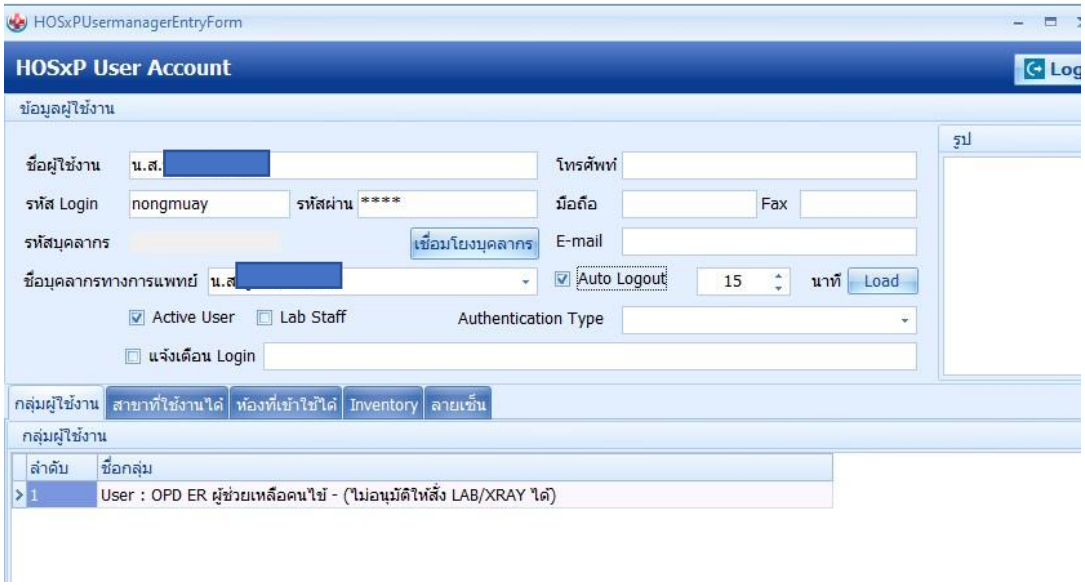




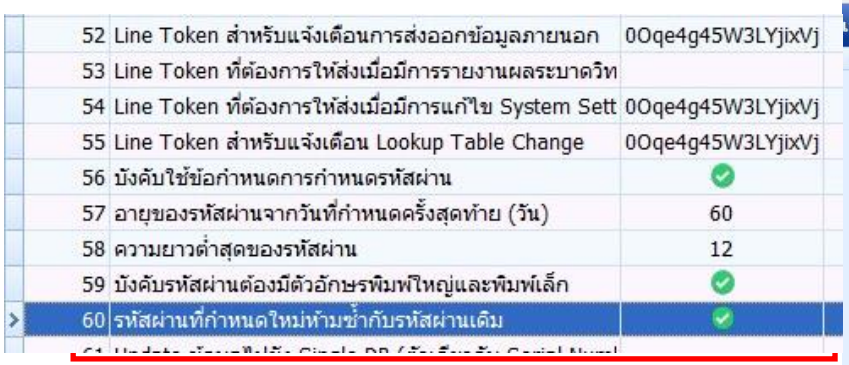


4.2 มีการกำหนด Role-base access ในการเข้าถึงระบบเท่าที่มีจำเป็น

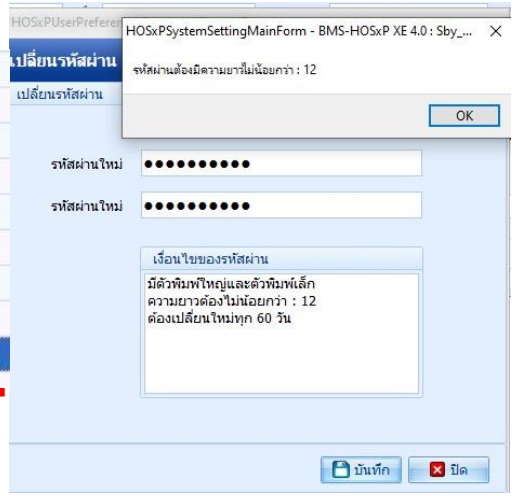
ลำดับ	รหัสกลุ่ม	ชื่อกลุ่ม	จำนวน Us
1	OPD	User : OPD พยาบาล	85
2	REFER	User : REFER ศูนย์ส่งต่อ	68
3	IPD	User : IPD พยาบาล	66
4	FINANCE	User : FN การเงิน	63
5	ER	User : ER ห้องฉุกเฉิน	33
6	DOCTOR	User : DOCTOR ห้องตรวจแพทย์	29
7	IPD	User : IPD LR ห้องคลอด	26
8	LAB	User : LAB ห้องปฏิบัติการ	19
9	OPD	User : ผู้ช่วยเหลือคนไข้	17
10	SUPER USER	Super User : ผู้ดูแลระบบ (ADMIN)	17
11	CARD	User : CARD ห้องเวชระเบียน	16
12	PCU	User : PCU พยาบาล	12
13	PT OT	User : PT กายภาพบำบัด	12
14	LAB	User : LAB - ดูข้อมูลปกปิด	11
15	DENT	User : DENT ทันตแพทย์	10
16	RX	User : RX เภสัชกรรม	10
17	DENT	User : DENT เจ้าพนักงานทันตสาธารณสุข	10
18	LAB	User : LAB - ดูข้อมูลปกปิดกลุ่ม 1 (คนไข้ HIV)	9

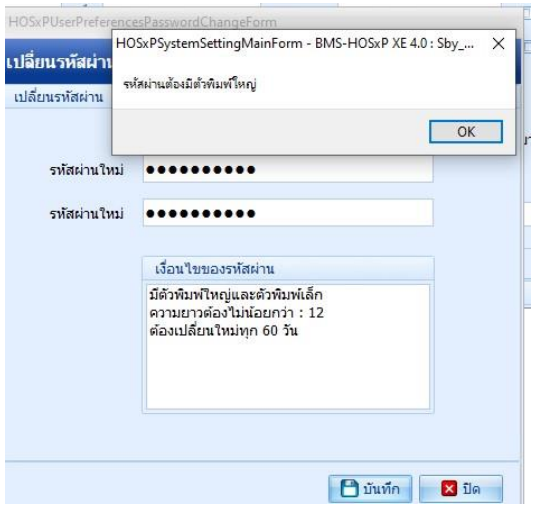


4.3 มีการตั้ง Password อย่างน้อย 12 ตัว (ตัวอักษรใหญ่, เล็ก, อักขระพิเศษ, ตัวเลข) 12

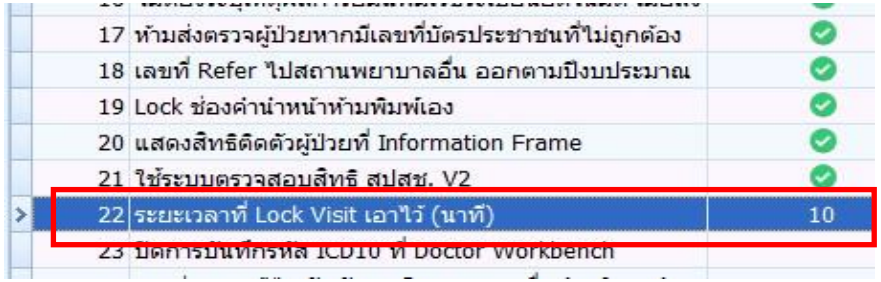


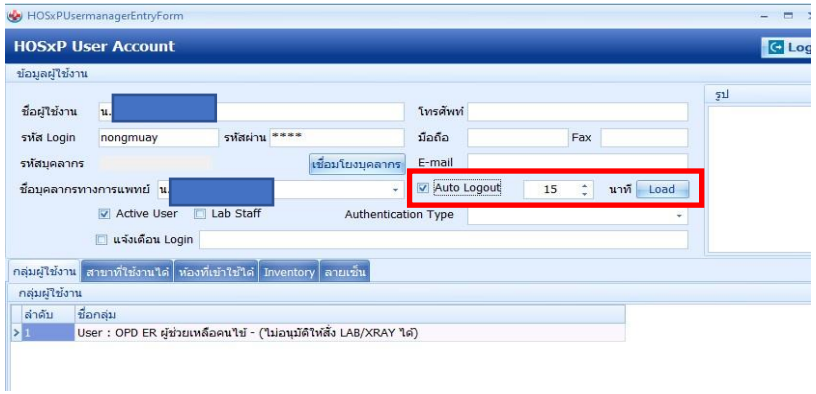
52	Line Token สำหรับแจ้งเตือนการส่งออกข้อมูลภายนอก	0Oqe4g45W3LYjixVj
53	Line Token ที่ต้องการให้ส่งเมื่อมีการรายงานผลระบาดวิท	
54	Line Token ที่ต้องการให้ส่งเมื่อมีการแก้ไข System Sett	0Oqe4g45W3LYjixVj
55	Line Token สำหรับแจ้งเตือน Lookup Table Change	0Oqe4g45W3LYjixVj
56	บังคับใช้ข้อกำหนดการกำหนดรหัสผ่าน	✓
57	อายุของรหัสผ่านจากวันที่กำหนดครั้งสุดท้าย (วัน)	60
58	ความยาวต่ำสุดของรหัสผ่าน	12
59	บังคับรหัสผ่านต้องมีตัวอักษรพิมพ์ใหญ่และพิมพ์เล็ก	✓
60	รหัสผ่านที่กำหนดใหม่ห้ามซ้ำกับรหัสผ่านเดิม	✓





4.4 Expire Sessions Time out





5.	Business Continuity Plan (BCP) และ Disaster Recovery Plan (DRP) : แผนที่กำหนดแนวทางการ ดำเนินการของหน่วยงาน เมื่อเกิดสภาวะวิกฤต หรือภัยต่าง ๆ ที่ ส่งผลให้กระบวนการทำงานของ หน่วยงานหยุดชะงัก เพื่อให้ สามารถกลับมาดำเนินการได้อย่าง ต่อเนื่อง	มีการทดสอบ Business Continuity Plan (BCP) และ Disaster Recovery Plan (DRP) อย่างน้อย ปีละ 1 ครั้ง และ มีการจัดทำรายงานถึง ขั้นตอนการดำเนินการที่ชัดเจนรวมถึงระยะเวลาดำเนินการและผู้ที่ เกี่ยวข้องในการดำเนินการงานดังนี้ 1. การบริหารจัดการความเสี่ยง (Risk Management) 2. การบริการจัดการด้าน Resource (Resource Management) 3. การวางแผนความต่อเนื่องจากธุรกิจที่เกิดขึ้น (Business Continuity Planning) 4. การทดสอบ (Testing)			

หลักฐาน

แผนแผนบริหารความต่อเนื่องในการให้บริการ (BCP)

http://sabayoihospital.com/th/?p=4926

แผนกู้คืนระบบสารสรเทศโรงพยาบาล (DRP)

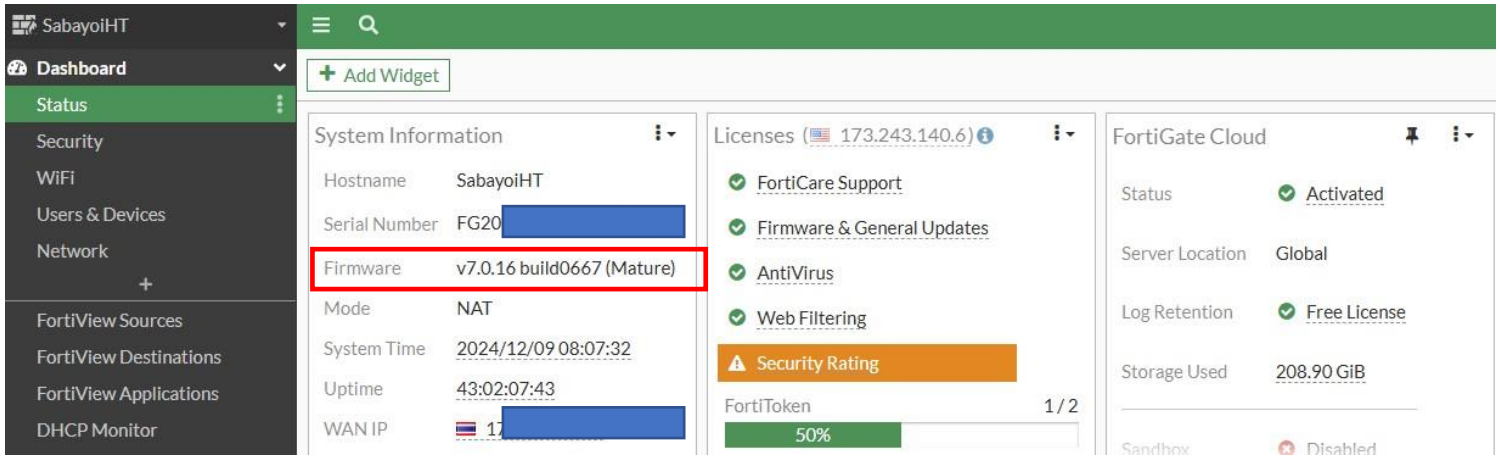
http://sabayoihospital.com/th/?p=4929

การซ้อมแผน

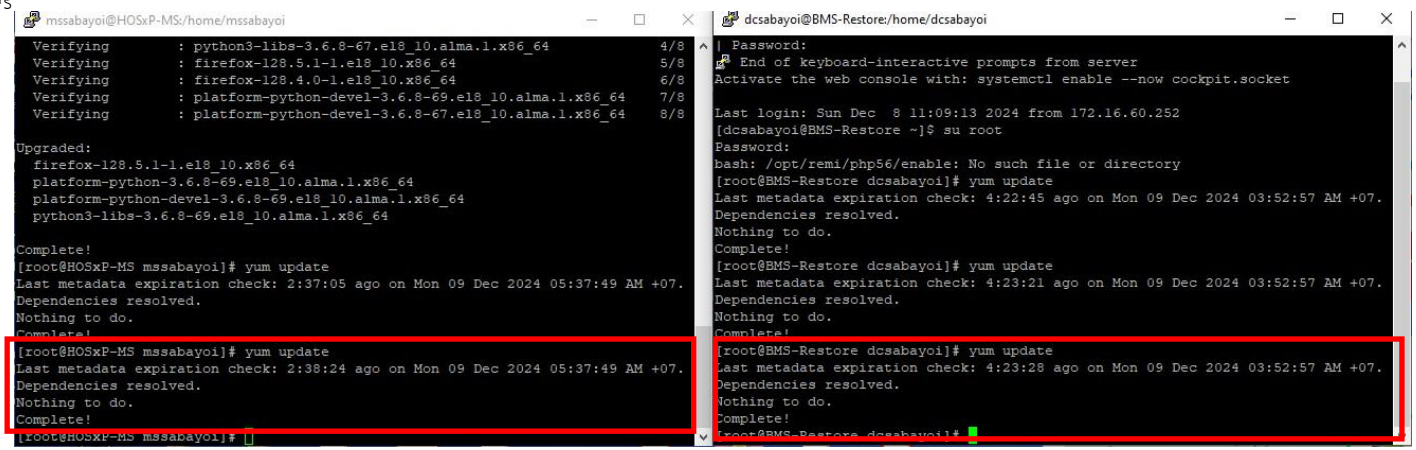
6.	OS Patching : การซ่อมแซมจุดบกพร่องของระบบปฏิบัติการ (OS) หรือปรับปรุงระบบปฏิบัติการให้ทันสมัย และเพิ่มเติมความสามารถในการใช้งานหรือประสิทธิภาพให้ดีขึ้น	มีการอัปเดต Security Patching 1. Firewall patching (Firmware) 2. Operation patching 3. Application patching	ระบบ Window OS ผ่านแล้ว (ตรวจสอบ วันที่ update) **ระบบ LINUX รอเปลี่ยน HIS**	ผ่านแล้ว √	สิทธิชัย

หลักฐาน

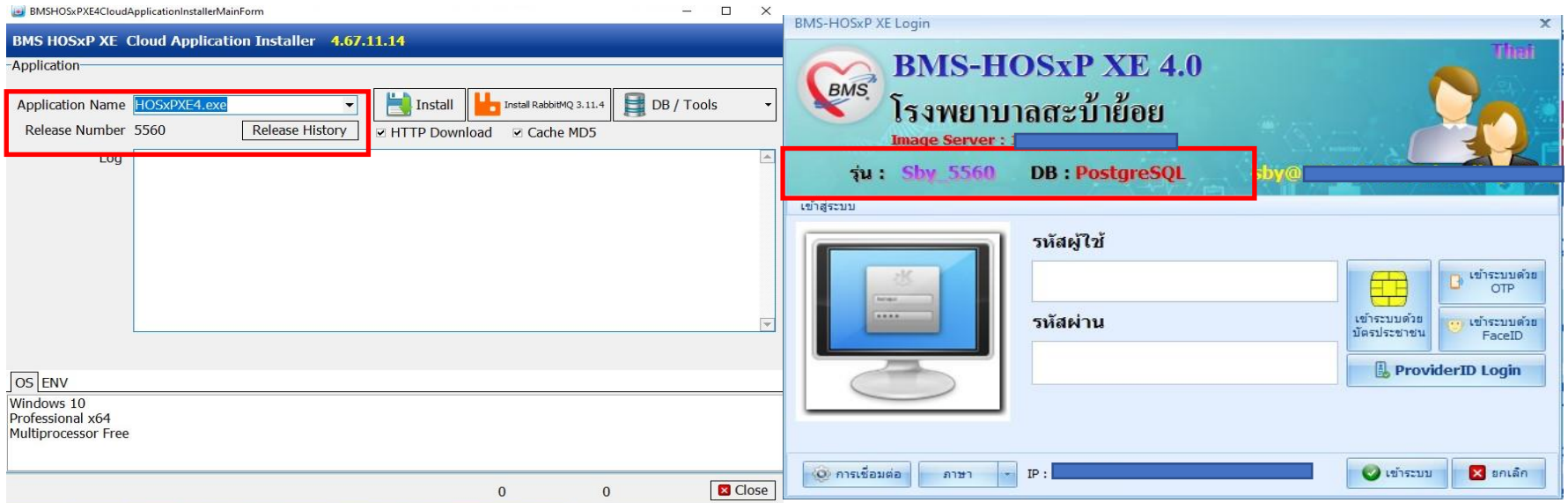
6.1 Firewall patching (Firmware)



6.2 Operation patching



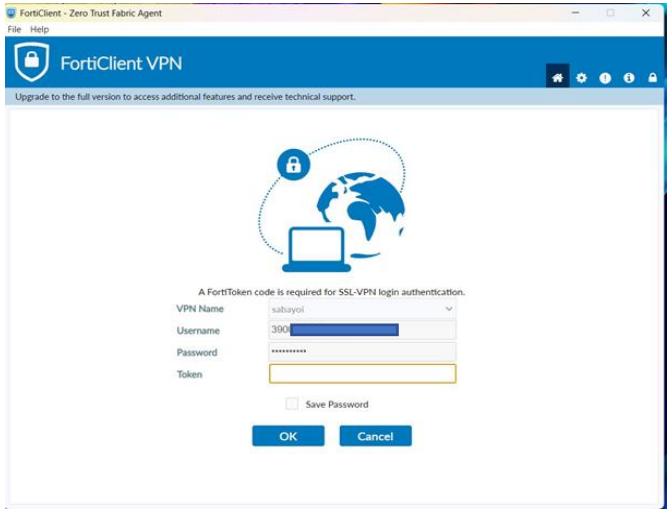
6.3 Application patching

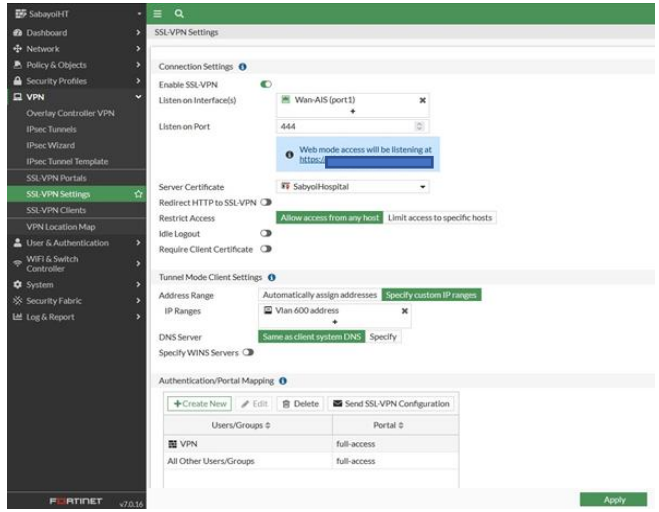


7.	Multi-Factor Authentication (2FA) : การยืนยันตัวตน 2 ชั้น เป็นการเข้าสู่ระบบบัญชีแบบหลายขั้นตอนที่กำหนดให้ผู้ใช้ป้อนข้อมูลเพิ่มเติมนอกเหนือจากรหัสผ่าน	มีการใช้งานระบบ Multi-Factor Authentication (2FA) เพื่อยืนยันตัวตน 2 ชั้นในการเข้าถึงระบบต่างๆ สำหรับ Admin ที่ใช้งานระบบอย่างน้อยดังนี้ 1. การ Login แบบ Multi-factor ไปยังระบบ VPN Access 2. การ Login แบบ Multi-factor ไปยังอุปกรณ์ Security 3. การ Login แบบ Multi-factor ไปยัง Operating system			

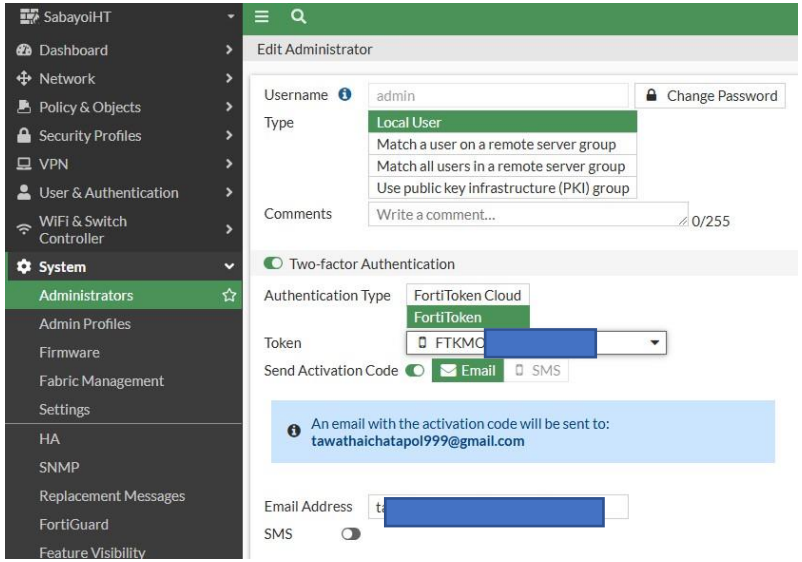
หลักฐาน

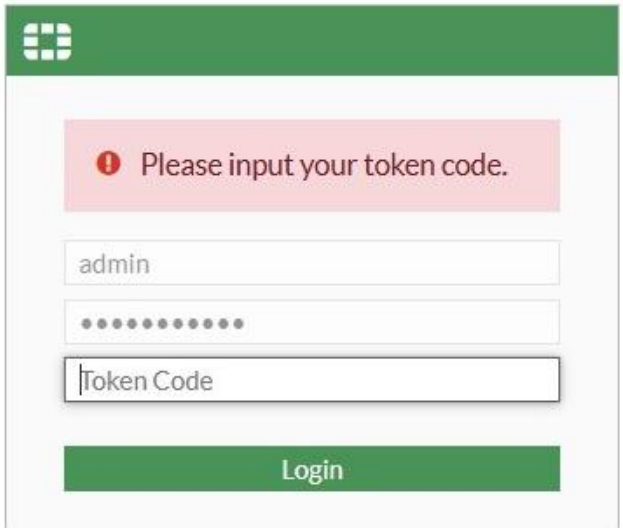
7.1 การ Login แบบ Multi-factor ไปยังระบบ VPN Access



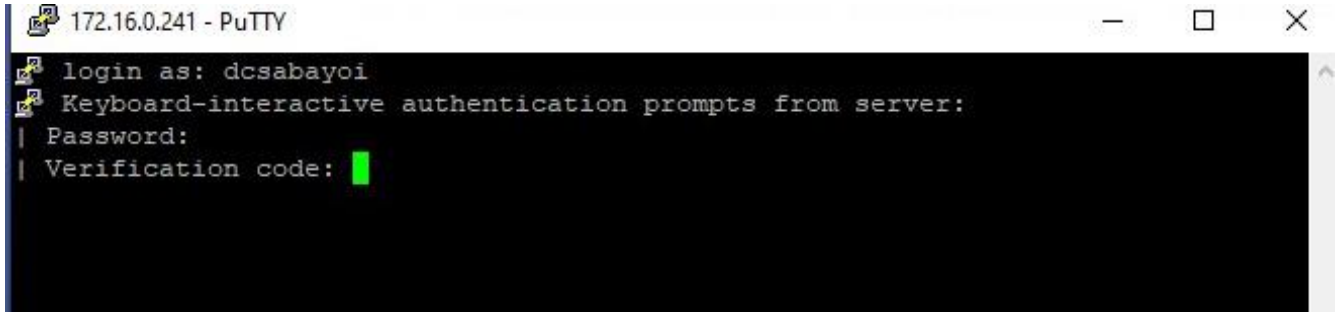


7.2 การ Login แบบ Multi-factor ไปยังอุปกรณ์ Security





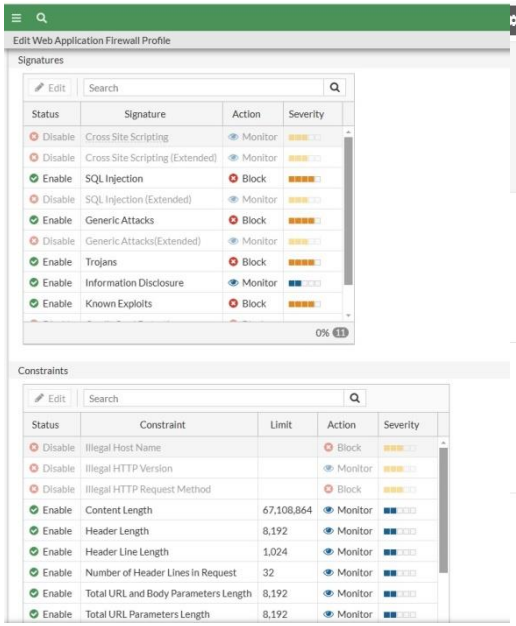
7.3 การ Login แบบ Multi-factor ไปยัง Operating system

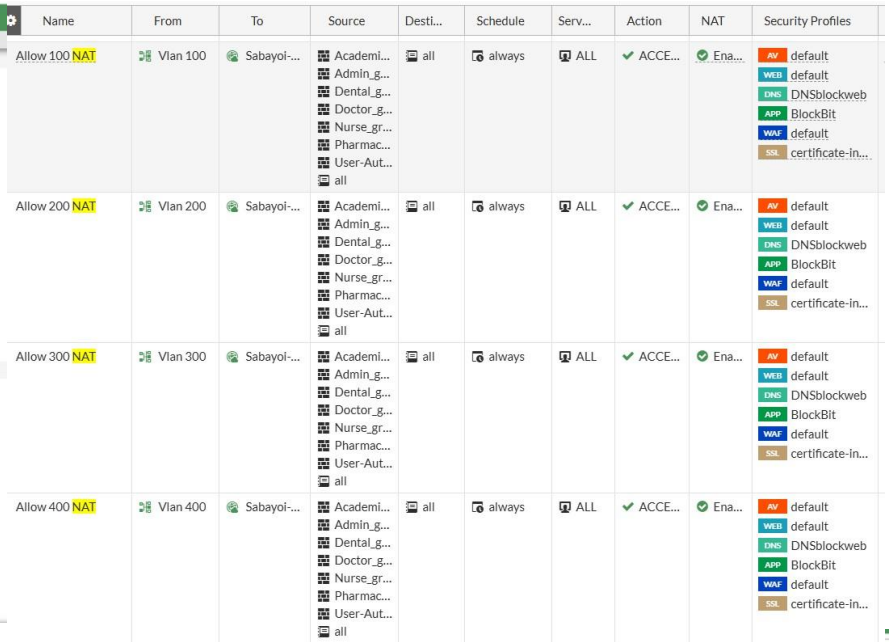


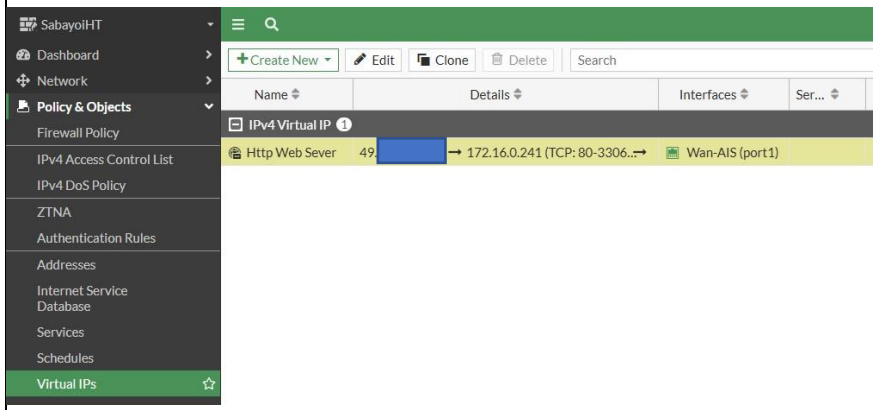
8.	Web Application Firewall (WAF) : ระบบป้องกันการโจมตีทางไซเบอร์สำหรับเว็บแอพพลิเคชั่น โดยเฉพาะเพื่อป้องกันการโจมตีไปยังระบบเว็บแอพพลิเคชั่นขององค์กร	มีการใช้งาน Web Application Firewall (WAF) กรณีที่มีระบบเป็น Web Application เพื่อป้องกันการ โจมตีตามมาตรฐาน OWASP Top 10 ได้เป็นอย่างน้อยตามรายละเอียด 1. Review Attack Report 2. Add Source IP Blocklists			

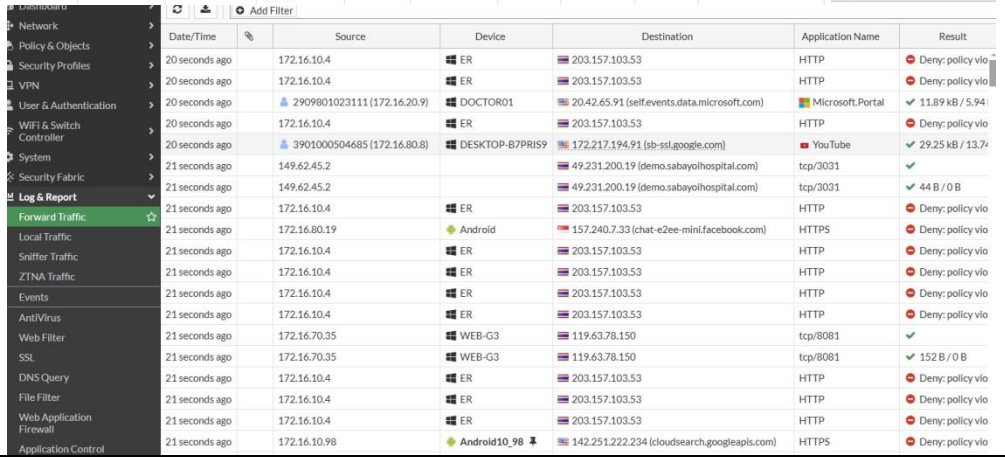
หลักฐาน

Web Application Firewall (WAF)



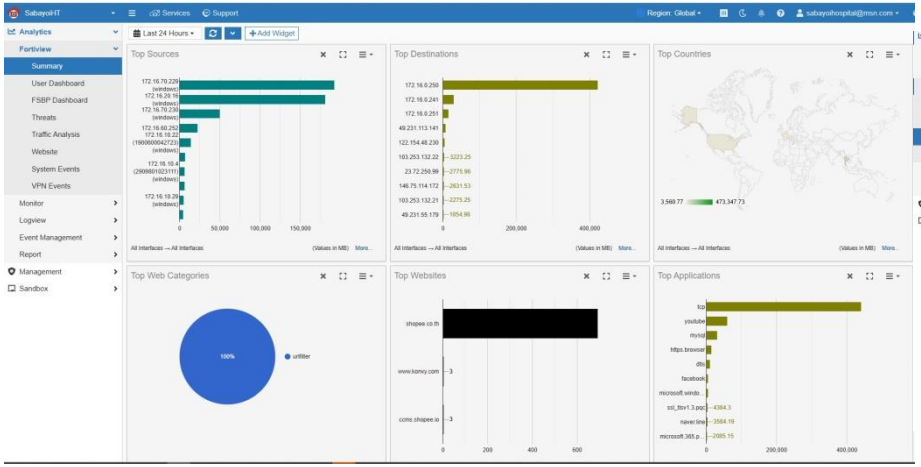


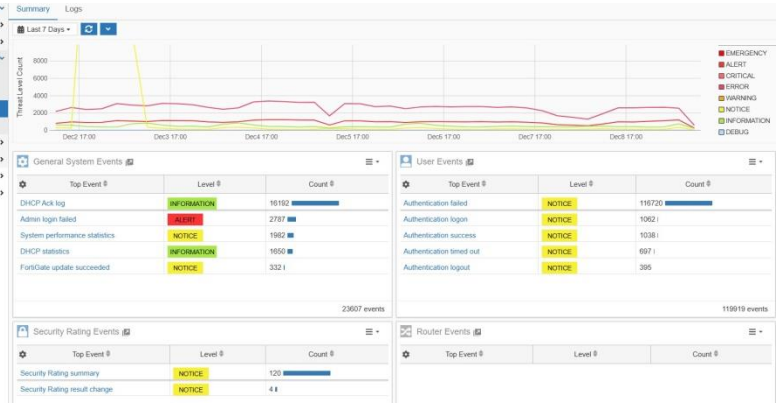


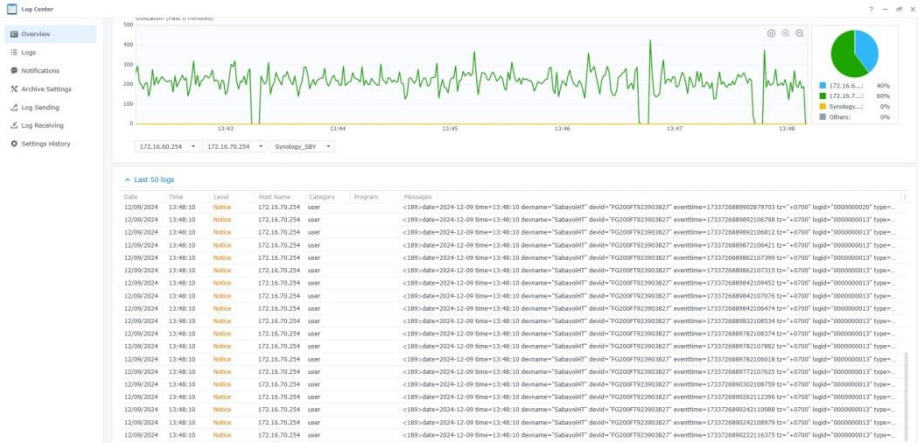


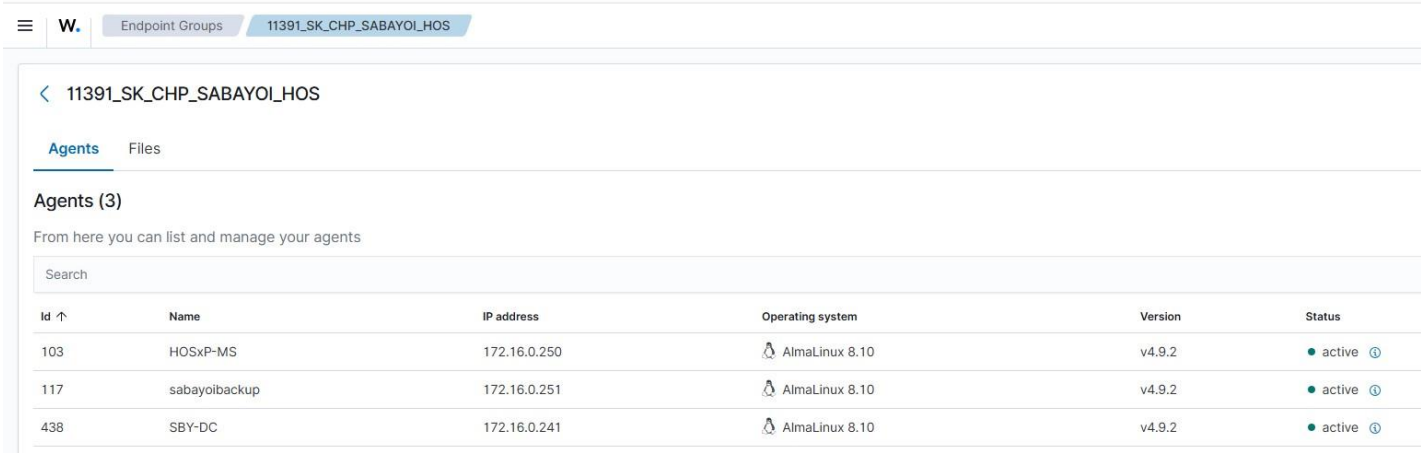
9.	Log Management : การจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์	มีระบบการจัดเก็บ Log อินเทอร์เน็ต และคอมพิวเตอร์ ตาม พ.ร.บ. คอมฯ อย่างน้อย 90 วัน 1. System Logs 2. Access Logs 3. Authentication Logs 4. Authorization Logs 5. Error Logs 6. Applications Logs	-รอการเปิดซอง เดือน ธันวาคม 2567 - โครงการศูนย์เฝ้าระวังป้องกันและรับมือภัยคุกคามทางด้านไซเบอร์สำหรับโรงพยาบาลรัฐ (Healthcare Cyber Defense Center) - ให้บริษัท ทำระบบ DEMO 2 เดือน		

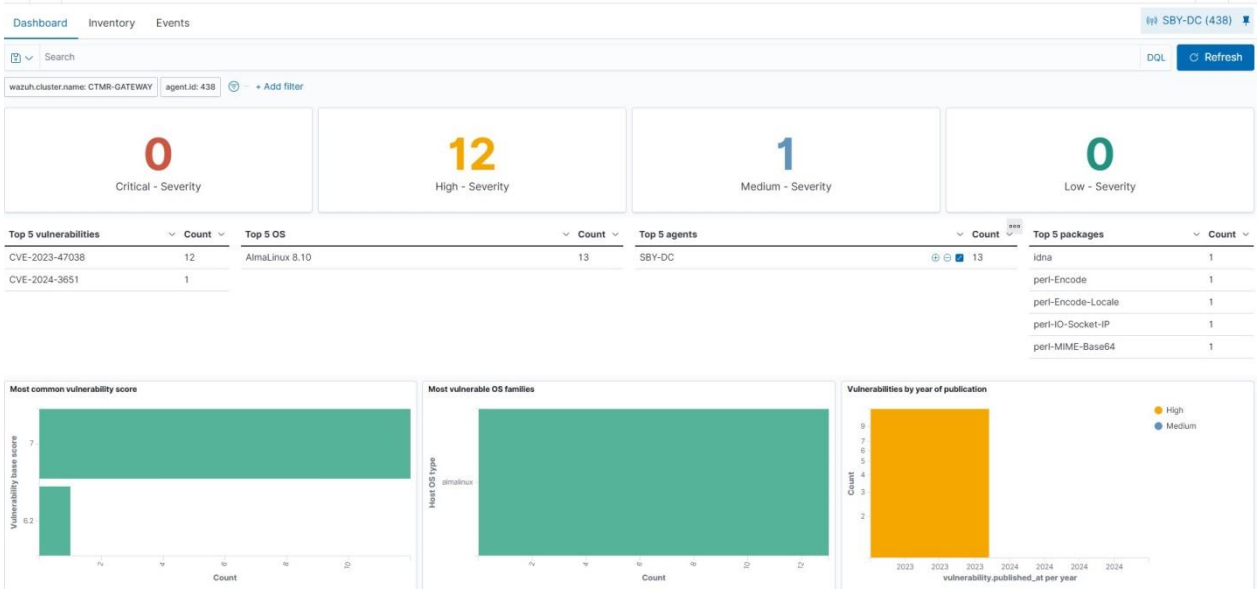
หลักฐาน

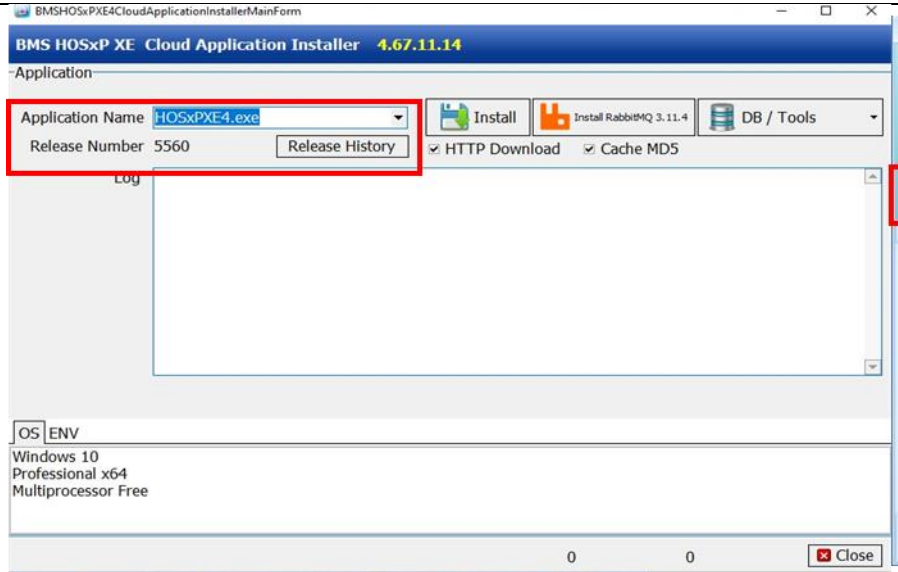






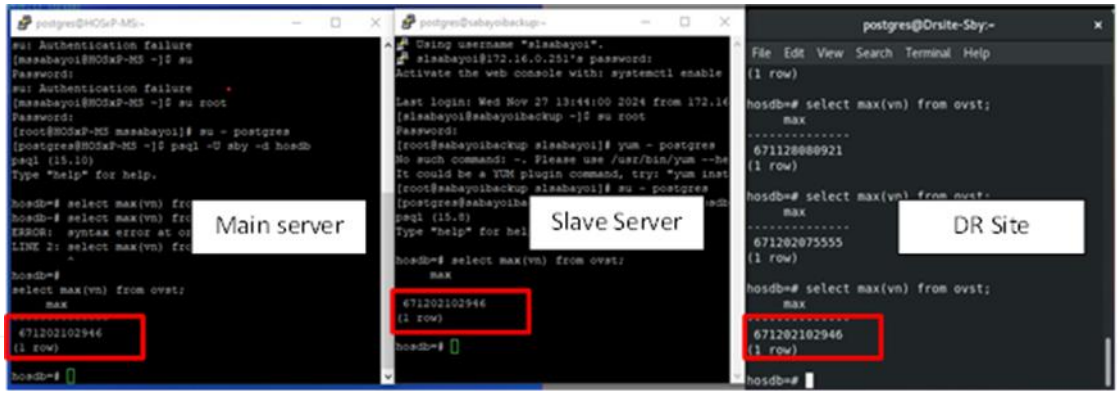
10.	Security Information & Event Management (SIEM) : ระบบที่ใช้ในการจัดการกับ Log และ Event ต่าง ๆ ที่คอยทำหน้าที่วิเคราะห์หาความเชื่อมโยงของ Event ต่าง ๆ ที่เกี่ยวข้องกับความปลอดภัยทั้งหมด ไปจนถึงการ Alert ระบุ ตำแหน่งของภัยคุกคามให้ทราบ เมื่อมี Event ที่ผิดปกติ ทำให้ สามารถป้องกัน และตอบสนอง ภัยคุกคามได้อย่างรวดเร็ว	มีระบบ SIEM เพื่อนำมาวิเคราะห์พฤติกรรมของ Cyber Attack บนระบบที่ให้บริการทั้งระดับ Infrastructure และ Operating system (OS) โดยจะต้องคลอบคลุมการตรวจจับพื้นฐาน ดังนี้ 1. ตรวจจับและแจ้งเตือนการบุกรุกที่เข้าถึงระบบเครือข่าย การพยายาม Brute force Login เข้า ระบบ และ การ Scan port (port scanning) 2. Malware-Virus Detection ตรวจจับและแจ้งเตือน Malware หรือ Virus จากพฤติกรรมต่างๆ ที่ เกิดขึ้นหรือจาก signature 3. Blacklist IP การตรวจจับและแจ้งเตือนการเข้าถึง IP Address ที่เป็น Blacklist และระบุการ เปิด connection ได้ 4. Unauthorized Access การตรวจจับการเข้าถึงข้อมูลหรือระบบที่ไม่ได้รับอนุญาต หรือไม่มีสิทธิ์เข้าถึง ระบบ 5. DDoS Attack การตรวจจับพฤติกรรมการโจมตีในรูปแบบของ DDoS ได้ ทั้งภายนอกและภายใน 6. Data Breaches การตรวจจับและแจ้งเตือนการละเมิดการเข้าถึงข้อมูลที่สำคัญของระบบที่ไม่อนุญาต ให้เข้าถึง			
หลักฐาน					
11.	Vulnerability Assessment (VA Scan) : การตรวจสอบชรองโหวรของระบบ เพื่อให้ทราบถึงความเสี่ยงจุดอ่อน และระดับความรุนแรงของผลกระทบที่อาจเกิดขึ้นจาก	มีการดำเนินการ Vulnerability Assessment (VA Scan) อย่างน้อยปีละ 1 ครั้ง โดยจะต้องดำเนินการแก้ ไข CVE และช่องโหว่ต่างๆ ที่เกิดขึ้นโดยให้ความสำคัญกับความเสี่ยงระดับ Critical, High เป็นลำดับแรก 1. Review Vulnerability Assessment Report 2. จัดลำดับความสำคัญ ความเสี่ยงระดับ Critical, High, Medium, Low กำหนดระยะเวลาในการแก้ไข ช่องโหว่	โครงการศูนย์เฝ้าระวังป้องกันและรับมือภัยคุกคามทางด้านไซเบอร์สำหรับโรงพยาบาลรัฐ (Healthcare Cyber Defense Center)		

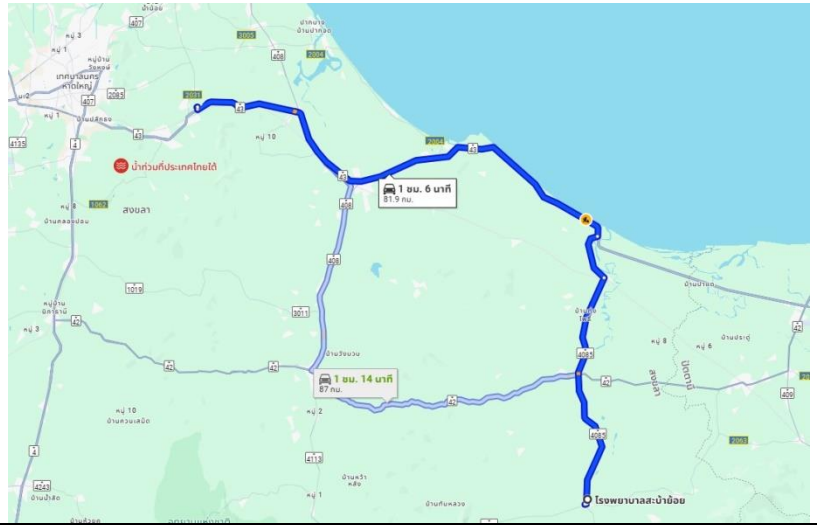
	การถูกโจรกรรมข้อมูลและการโจมตีทางไซเบอร์	3. การจัดการความเสี่ยง 3.1 ยอมรับความเสี่ยง (Risk Acceptance) 3.2 หลีกเลี่ยงความเสี่ยง (Risk Avoidance) 3.3 ลดความเสี่ยง (Risk Mitigation) 3.4 ถ่ายโอนความเสี่ยง (Risk Transfer)			
หลักฐาน 					
12.**	Penetration Testing : การทดสอบการเจาะระบบ	มีการทำ Penetration Testing ของ Web Application ในรูปแบบของ Gray box หรือ Black box อย่างน้อยปีละ 1 ครั้ง และดำเนินการแก้ไขโดยจะต้องไม่มีช่องโหว่ระดับ Severity Critical , High เกิดขึ้น และไม่มีช่องโหว่ที่เกิดขึ้นตามมาตรฐาน OWASP TOP10			
13.**	Software Update : การตรวจสอบ Version ของ Software ให้เป็น Version Update ล่าสุด เพื่อปิดช่องโหว่ที่เกิดขึ้นใน Software Version ก่อนหน้า	มีการอัปเดต Software Patching ของระบบ HIS และมีการทำ Penetration Testing อย่างน้อยปีละ 1 ครั้ง หรือมีการออก Major version โดยจะต้องดำเนินการแก้ไขช่องโหว่ในระดับ Severity Critical และ High เป็นอย่างน้อย			



14.**	Disaster Recovery site (DR) : ศูนย์สำรองข้อมูล สำหรับแก้ไขปัญหาระบบสารสนเทศที่เกิดขึ้นจากภัยพิบัติต่างๆ ให้สามารถทำงานได้อย่างต่อเนื่อง	มีระบบ Disaster Recovery site (DR) ในกรณีฉุกเฉินที่ระบบหลักมีปัญหาและไม่สามารถใช้งานได้ โดย จะต้องมี DR-Site โดยยึดจากมาตรฐาน ISO27001 และนำมาปรับใช้งานดังนี้ 1. ระยะห่างระหว่าง DC-Site กับ DR-Site ต้องไม่น้อยกว่า 60 กิโลเมตร 2. ต้องมีระบบฐานข้อมูลที่สำคัญอย่างน้อย 1 ระบบขึ้นบน DR-site 3. RTO ต้องเท่ากับหรือไม่มากกว่า = 24 ชั่วโมง หรือขึ้นอยู่กับ Solution 4. RPO ต้องเท่ากับหรือไม่มากกว่า = 24 ชั่วโมง 5. ต้องมีเอกสารสรุปผลการทดสอบการดำเนินการ DR-Site 6. ระบบต้องมีมาตรฐาน ISO ดังนี้เป็นอย่างน้อย 6.1 ISO27001 - Information Security Management System 6.2 ISO27799 - Health Informatics-Information Security Management			


DR SERVER
DC SERVER
Slave-Server
รพ.นาหม่อม
๙๐ กม.
อาคารผู้ป่วยนอก
๒๐๐ เมตร
Backup SERVER
File Backup on NAS
File Backup
อาคารผู้ป่วยนอก
๒๐๐ เมตร
อาคารอุบัติเหตุ


Main server
671202102946
(1 row)
Slave Server
671202102946
(1 row)
DR Site
671128080921
(1 row)
671202075555
(1 row)
671202102946
(1 row)


น้ำท่วมที่ประเทศไทยใต้
สงขลา
1 ชม. 6 นาที
81.9 กม.
1 ชม. 14 นาที
87 กม.
โรงพยาบาลสะบ้าย้อย