รายงานสหกิจศึกษาฉบับสมบูรณ์

การปรับปรุงประสิทธิภาพระบบเครือข่ายตามข้อปฏิบัติ ITILv3 สำหรับอุตสาหกรรมไอที

Network Infrastructure Improvement for IT Industry with ITILv3

นายสาริน จวงมุทิตา

ภาควิชาวิศวกรรมโทรคมนาคม
คณะวิศวกรรมศาสตร์
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ปีการศึกษา 2561

รายงานสหกิจศึกษาฉบับสมบูรณ์

การปรับปรุงประสิทธิภาพระบบเครือข่ายตามข้อปฏิบัติ ITILv3 สำหรับอุตสาหกรรมไอที

Network Infrastructure Improvement for IT Industry with ITILv3

นายสาริน จวงมุทิตา

ภาควิชาวิศวกรรมโทรคมนาคม

คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ปีการศึกษา 2561

ชื่อโครงงานสหกิจศึกษา การปรับปรุงประสิทธิภาพระบบเครือข่ายตามข้อปฏิบัติ ITILv3 สำหรับอุตสาหกรรมไอที

ชื่อ-สกุล นักศึกษา นายสาริน จวงมุทิตา

คณะ วิศวกรรมศาสตร์ **ภาควิชา** วิศวกรรมโทรคมนาคม

ชื่อ-สกุล อาจารย์นิเทศ ผศ.ดร. สิรภพ ตู้ประกาย

ชื่อ-สกุล ผู้นิเทศงาน นายศิริชัย กำเหนิดหล่ม

สถานประกอบการ บริษัท ซีเอส ล็อกซอินโฟ จำกัด (มหาชน)

บทคัดย่อ

โครงงานที่จัดทำขึ้นมานี้ จัดทำเพื่อทำการตรวจสอบระบบเครือข่ายขององค์กร ปรับปรุงระบบเครือข่ายให้สามารถทำงานได้อย่างราบรื่น โดยคำนึงถึงมาตรฐาน ITILv3 การตรวจสอบมีการเก็บการตั้งค่าของอุปกรณ์เครือข่าย และติดตั้งโปรแกรมมอนิเตอร์เพื่อติดตามผลการทำงานของอุปกรณ์ จากนั้นจึงนำข้อมูลมาทำการประเมินความเสี่ยงที่จะส่งผลกระทบต่อองค์กร ทำการเปลี่ยนอุปกรณ์และทดสอบผลการทำงานหลังการเปลี่ยน แล้วจึงทำเอกสารส่งมอบลูกค้าพร้อมคำแนะนำในการนำไปปรับปรุงระบบ

คำสำคัญ : การตรวจสอบระบบเครือข่าย ITILv3 ประเมินความเสี่ยง

Cooperative Title: Network Infrastructure Improvement for IT Industry with ITILv3

Student intern name: Sarin Juangmutita

Faculty: Engineering **Department:** Telecommunication Engineering

Advisor name: Assist.Prof.Dr. Siraphop Tooprakai

Mentor name: Sirichai Kamnerdlom

Company: CS LOXINFO PUBLIC COMPANY LIMITED

ABSTRACT

This project aims to investigate the network system of the organization and adjust the network systems work smoothly, By considering to ITILv3 standard, settings of network devices and installing the monitor to track the performance of a device. So, import the data to assess the risks that will impact the organization. Moreover, change the device and test the results of the work after the changes. Therefore, prepare the document send to clients with advice how to improve the system.

Keywords: Network Assessment, ITILv3, Risk Management

กิตติกรรมประกาศ

โครงงาน “การปรับปรุงประสิทธิภาพระบบเครือข่ายตามข้อปฏิบัติ ITILv3 สำหรับอุตสาหกรรมไอที” จะไม่สามารถสำเร็จลุล่วงไปได้หากขาดการสนับสนุนจากหลาย ๆ ฝ่าย ดังนี้

ผศ.ดร. สิรภพ ตู้ประกาย อาจารย์ที่ปรึกษาโครงงาน นายศิริชัย กำเหนิดหล่ม Network solution specialist นายทัดไทล์ เซโต้ Network Engineer ที่คอยให้คำปรึกษา ช่วยแนะนำแนวทางในการแก้ปัญหา รวมทั้งคอยสนับบสนุนอุปกรณ์ที่ใช้ในการดำเนินงาน สถานที่ ตลอดระยะเวลาในการดำเนินงาน

พี่ ๆ และเพื่อน ๆ ภายในบริษัท ซีเอส ล็อกซอินโฟ จำกัด (มหาชน) ทุกคนที่คอยให้ความช่วยเหลือ ให้คำปรึกษาในเรื่องต่าง ๆ และให้ความรู้เพิ่มเติมที่เป็นประโยชน์ต่อผู้จัดทำ

ผู้จัดทำขอขอบพระคุณทุก ๆ ท่านเป็นอย่างสูง ณ ที่นี้ ที่ได้มีส่วนทำให้การจัดทำโครงงานในครั้งนี้สำเร็จลุล่วงไปได้ด้วยดี

นายสาริน จวงมุทิตา

ผู้จัดทำ

สารบัญ

สารบัญ (ต่อ)

สารบัญตาราง

ตารางที่ **หน้า**

สารบัญรูป

สารบัญรูป (ต่อ)

สารบัญรูป (ต่อ)

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญ

ในปัจจุบันผู้คนมีความต้องการใช้บริการอินเทอร์เน็ตเป็นจำนวนมาก แม้แต่ทางองค์กรต่าง ๆ ก็มีความต้องการในการใช้อินเทอร์เน็ตมากขึ้นเช่นกัน โดยเฉพาะงานภายในอุตสาหกรรมไอทีที่ต้องมีการให้บริการลูกค้าเป็นจำนวนมาก เพื่อให้การทำงานขององค์กรเป็นไปอย่างราบรื่น จึงต้องมีระบบเครือข่ายที่ช่วยให้การทำงานและการติดต่อสื่อสารภายในองค์กรเป็นไปอย่างราบรื่น เพราะเมื่อระบบเครือข่ายไม่สามารถใช้งานได้อาจส่งผลให้การทำงานขององค์กรต้องหยุดลง ด้วยเหตุนี้จึงต้องมีการประเมินระบบเครือข่ายเพื่อตรวจสอบโครงสร้าง การจัดการ ความปลอดภัย และประสิทธิภาพของระบบเครือข่าย การประเมินระบบเครือข่ายยังช่วยให้สามารถวิเคราะห์ปัญหาที่เกิดขึ้น อีกทั้งยังเข้าใจโครงสร้างของระบบในปัจจุบันและช่วยให้แก้ปัญหาได้อย่างตรงจุด

โครงงานนี้มีวัตถุประสงค์เพื่อทำการตรวจสอบและประเมินความเสี่ยงระบบเครือข่ายพร้อมกับให้คำแนะนำในการปรับปรุงให้เหมาะสมกับธุรกิจตามมาตรฐานการให้บริการ IT (ITILv3) โดยการตรวจสอบจะมีการเก็บ configuration ของอุปกรณ์ Network และติดตั้งโปรแกรม Monitoring เพื่อตรวจสอบการทำงานของอุปกรณ์แล้วจึงนำข้อมูลมาทำการวิเคราะห์เพื่อหาความเสี่ยงที่อาจทำให้เกิดผลกระทบต่อธุรกิจได้ในอนาคต เมื่อวิเคราะห์ข้อมูลเสร็จแล้วจึงทำการปรับปรุงและแก้ไขความเสี่ยงด้วยการออกแบบระบบเครือข่ายใหม่ มีการเปลี่ยนอุปกรณ์และตั้งค่าอุปกรณ์ให้เหมาะสมต่อการใช้งานภายในองค์กร แล้วจึงจัดทำเอกสารส่งมอบให้ลูกค้าพร้อมกับคำแนะนำในการนำไปปรับปรุงระบบ

1.2 วัตถุประสงค์ของการวิจัย

1) เพื่อเพิ่มประสิทธิภาพในการทำงานภายในองค์กร
2) เพื่อวิเคราะห์ปัญหาที่เกิดขึ้นภายในองค์กร
3) เพื่อออกแบบระบบเครือข่ายให้เหมาะสมกับการความต้องการขององค์กร

1.3 ขอบเขตของการวิจัย

1) ตรวจสอบระบบเครือข่ายขององค์กร
2) ออกแบบระบบเครือข่ายตามความต้องการขององค์กร
3) ตรวจเช็คการทำงานของระบบเครือข่ายที่ออกแบบไว้

4) จัดทำคู่มือและสรุปผลการทำงานของระบบเครือข่าย

1.4 วิธีการดำเนินงานวิจัย

ตารางที่ 1.1 แผนการดำเนินงาน

ลำดับ	รายละเอียด	ภาคการศึกษาที่ 1 ปีการศึกษา 2561			
		เดือนที่ 1	เดือนที่ 2	เดือนที่ 3	เดือนที่ 4
1	ศึกษาการใช้งานโปรแกรม Monitoring	←	→		
2	ศึกษาวิธีการบริหารจัดการความเสี่ยงด้านสารสนเทศ	←	→		
3	ออกไปพบลูกค้าเพื่อทำสัญญาข้อตกลงในการดำเนินงาน	←	→		
4	ลงพื้นที่จริงเพื่อเก็บข้อมูลในการนำมาวิเคราะห์		←	→	
5	นำข้อมูลที่ได้มาทำการวิเคราะห์และประเมินความเสี่ยง			←	→
6	เปลี่ยนอุปกรณ์และตั้งค่าอุปกรณ์ให้เหมาะสมต่อการใช้งาน			←	→
7	ทำเอกสารส่งมอบให้ลูกค้าและจัดทำรายงานเตรียมการนำเสนอ			←	→

1.5 ผลที่คาดว่าจะได้รับ

1) ได้ประสบการณ์และความรู้ในการออกปฏิบัติงานจริง การสื่อสารกับลูกค้า การแก้ไขปัญหาระหว่างการปฏิบัติงาน

2) ได้เรียนรู้การ Configure อุปกรณ์ในระบบเครือข่ายต่าง ๆ เช่น Router, Switch, Firewall และการจัดทำเอกสารดำเนินงานต่าง ๆ

บทที่ 2
แนวคิด ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

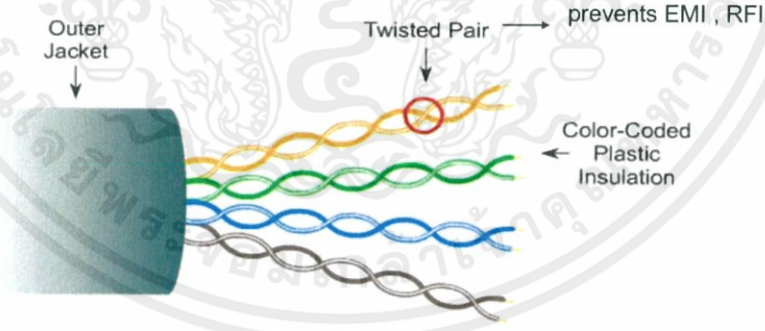
2.1 ทฤษฎีที่เกี่ยวข้อง

2.1.1 สายสัญญาณ

ในการส่งข้อมูลนั้นสิ่งที่ขาดไม่ได้เลยคือตัวกลางในการส่งข้อมูลหรือ Media ซึ่งเป็นองค์ประกอบหลักของการสื่อสารโดยจะทำหน้าที่เป็นตัวกลางในการรับส่งข้อมูลจากต้นทางไปยังปลายทาง โดยแบ่งเป็น 2 ชนิด คือการสื่อสารแบบใช้สาย และการสื่อสารแบบไร้สาย โดยในหัวข้อนี้จะกล่าวถึงสายสัญญาณที่ใช้งานในโครงงานนี้ คือสายสัญญาณแบบทองแดง และสายสัญญาณชนิดใยแก้วนำแสง

2.1.1.1 สายทองแดง

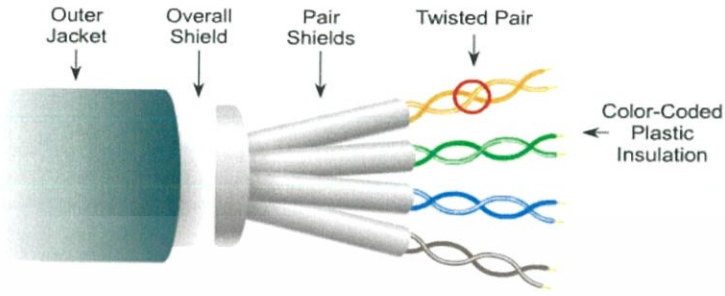
1) สายคู่บิดเกลียวแบบไม่มีฉนวนหุ้ม (UTP : Unshielded Twisted Pair) สายคู่บิดเกลียวแบบไม่มีฉนวนหุ้มหรือ UTP (Unshielded Twisted Pair) มีลักษณะเป็นสายทองแดงจำนวน 8 เส้น 4 คู่บิดเกลียวเพื่อลดขนาดของสัญญาณรบกวนแสดงในรูปที่ 2.1 เป็นสายที่ได้รับความนิยมเนื่องจากมีราคาถูกและติดตั้งได้ง่ายแต่มีข้อจำกัดเนื่องจากความยาวสายในการเชื่อมต่อได้ไม่เกิน 100 เมตร เหมาะสำหรับใช้ภายในอาคาร



รูปที่ 2.1 สายคู่บิดเกลียวแบบไม่มีฉนวนหุ้ม
(ที่มา : https://sites.google.com/a/kn.ac.th/pangboych)

2) สายคู่บิดเกลียวแบบมีฉนวนหุ้ม (STP : Shielded Twisted Pair) สายคู่บิดเกลียวแบบมีฉนวนหุ้ม หรือ STP (Shielded Twisted Pair) มีลักษณะเป็นสายทองแดงจำนวน 8 เส้น 4 คู่บิดเกลียวเพื่อลดขนาดของสัญญาณรบกวนและมีการเพิ่มฉนวนป้องกันสัญญาณรบกวนแสดงในรูปที่ 2.2 เป็นสายที่พัฒนาต่อจากสาย UTP โดยเพิ่มฉนวนป้องกันสัญญาณรบกวนทำให้คุณสมบัติ

โดยรวมของสัญญาณดีขึ้นมากแต่มีข้อจำกัดเนื่องจากความยาวสายในการเชื่อมต่อได้ไม่เกิน 100 เมตร เหมาะสำหรับใช้ภายนอกอาคาร



รูปที่ 2.2 สายคู่บิดเกลียวแบบมีฉนวนหุ้ม

(ที่มา : https://sites.google.com/a/kn.ac.th/pangboych)

2.1.1.2 เส้นใยแก้วนำแสง (Fiber Optic)

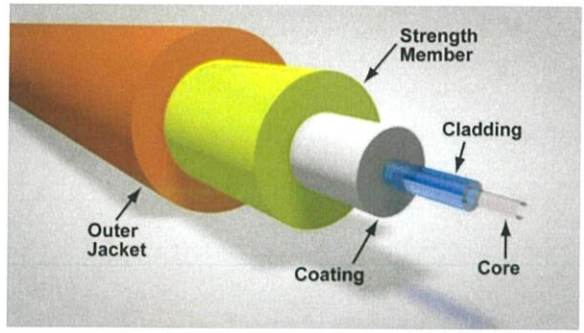
เส้นใยแก้วนำแสงเป็นสายนำสัญญาณที่ใช้แสงเป็นตัวกลางในการสื่อสารข้อมูลจากจุดหนึ่งไปยังอีกจุดหนึ่ง แสดงในรูปที่ 2.3 โดยมีโครงสร้างของเส้นใยแก้วนำแสง ดังนี้

- แกน (Core) เป็นส่วนที่อยู่ตรงกลางของเส้นใยแก้วนำแสงและเป็นส่วนที่ใช้ส่งข้อมูลสัญญาณแบบแสงจากต้นทางไปยังปลายทาง
- ส่วนห่อหุ้ม (Cladding) ทำหน้าที่เป็นตัวหักเหของแสงไม่ให้ออกไปภายนอก
- ส่วนป้องกัน (Coating) ทำหน้าที่ป้องกันส่วนที่เป็นแกนไม่ให้แตกหักหรือเสียหาย

2.1.1.3 ชนิดของเส้นใยแก้วนำแสง

1) Single Mode (SM) มีเส้นผ่าศูนย์กลางของ Core และ Cladding 9/125 μm ตามลำดับ ส่วนของแกนจะมีขนาดเล็กมากและให้แสงออกมาเพียงโหมดเดียว ซึ่งแสงที่ใช้จะต้องเป็นเส้นตรง ข้อดีคือสามารถส่งได้ระยะทางไกล

2) Multi Mode (MM) มีขนาดเส้นผ่าศูนย์กลางของ Core และ Cladding 62/125 μm และ 50/125 μm ตามลำดับ เนื่องจากมีขนาดของแกนที่ใหญ่ จึงทำให้แสงเดินทางกระจัดกระจายและเกิดการหักล้างกัน ทำให้เกิดการสูญเสียของแสงและส่งข้อมูลได้ไม่เกิน 200 เมตร



รูปที่ 2.3 เส้นใยแก้วนำแสง [1]

2.1.2 มาตรฐานของสายคู่บิดเกลียวแบบไม่มีฉนวนหุ้ม (UTP)

สมาคมอุตสาหกรรมอิเล็กทรอนิกส์ หรือ EIA (Electronics Industries Association) และสมาคมอุตสาหกรรมโทรคมนาคม หรือ TIA (Telecommunication Industries Association) ได้ร่วมกันกำหนดมาตรฐาน EIA/TIA 568 ซึ่งเป็นมาตรฐานที่ใช้ในการผลิตสายคู่บิดเกลียวแบบไม่มีฉนวนหุ้ม โดยมีมาตรฐานสองแบบคือ EIA/TIA 568A และ EIA/TIA 568B ซึ่งทั้งสองมาตรฐานนี้จะต่างกันในเรื่องของการเรียงสีของสายเท่านั้น

2.1.2.1 ประเภทของสายคู่บิดเกลียวแบบไม่มีฉนวนหุ้ม (UTP)

ในปัจจุบันสายคู่บิดเกลียวแบบไม่มีฉนวนหุ้ม (UTP) ได้แบ่งออกเป็น 7 ประเภทตามคุณสมบัติของสายดังแสดงในรูปที่ 2.4

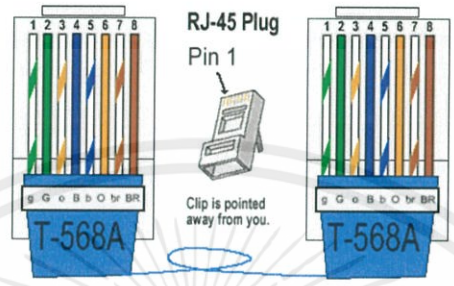
UTP Categories - Copper Cable

UTP Category	Data Rate	Max. Length	Cable Type	Application
CAT1	Up to 1Mbps	-	Twisted Pair	Old Telephone Cable
CAT2	Up to 4Mbps	-	Twisted Pair	Token Ring Networks
CAT3	Up to 10Mbps	100m	Twisted Pair	Token Rink & 10BASE-T Ethernet
CAT4	Up to 16Mbps	100m	Twisted Pair	Token Ring Networks
CAT5	Up to 100Mbps	100m	Twisted Pair	Ethernet, FastEthernet, Token Ring
CAT5e	Up to 1 Gbps	100m	Twisted Pair	Ethernet, FastEthernet, Gigabit Ethernet
CAT6	Up to 10Gbps	100m	Twisted Pair	GigabitEthernet, 10G Ethernet (55 meters)
CAT6a	Up to 10Gbps	100m	Twisted Pair	GigabitEthernet, 10G Ethernet (55 meters)
CAT7	Up to 10Gbps	100m	Twisted Pair	GigabitEthernet, 10G Ethernet (100 meters)

รูปที่ 2.4 ประเภทของสายคู่บิดเกลียวแบบไม่มีฉนวนหุ้ม [1]

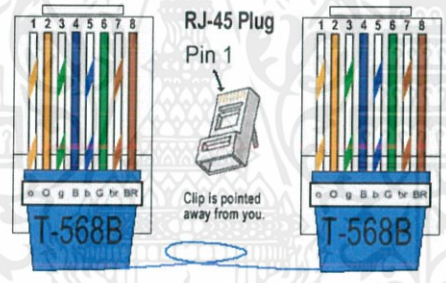
2.1.2.2 มาตรฐานการเข้าสายคู่บิดเกลียวแบบไม่มีฉนวนหุ้ม (UTP)

- สายแบบตรง (Straight-Through Cable) สายชนิดนี้มีคุณสมบัติเอาไว้ใช้งานในกรณีเชื่อมต่ออุปกรณ์ต่างชนิดกัน เช่น สวิตช์กับเครื่องคอมพิวเตอร์ โดยลักษณะของหัวสายนั้นจะต้องเหมือนกันทั้งสองฝั่ง ดังแสดงในรูปที่ 2.5 และ 2.6



รูปที่ 2.5 การเข้าหัวสายแบบตรง (A)

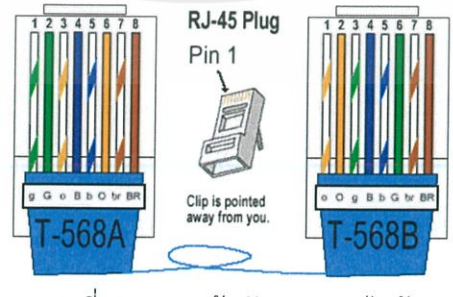
(ที่มา : http://www.similantechnology.com/news&article/connecting-the-lan.html)



รูปที่ 2.6 การเข้าหัวสายแบบตรง (B)

(ที่มา : http://www.similantechnology.com/news&article/connecting-the-lan.html)

- สายแบบไขว้ (Crossover Cable) สายชนิดนี้มีคุณสมบัติไว้ใช้งานในกรณีเชื่อมต่ออุปกรณ์ประเภทเดียวกัน เช่น เราเตอร์กับ เครื่องคอมพิวเตอร์ โดยลักษณะของหัวสายนั้นจะต้องต่างกัน ดังแสดงในรูปที่ 2.7



รูปที่ 2.7 การเข้าหัวสายแบบไขว้

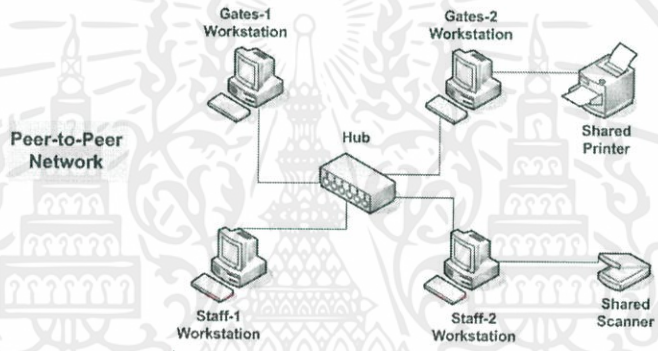
(ที่มา : http://www.similantechnology.com/news&article/connecting-the-lan.html)

2.1.3 รูปแบบการเชื่อมโยงเครือข่าย LAN

วิธีการเชื่อมต่อเครือข่ายคอมพิวเตอร์ เพื่อจัดสรรการใช้งานทรัพยากรในระบบเครือข่าย สามารถจำแนกได้เป็น 2 รูปแบบดังนี้

2.1.3.1 เครือข่ายแบบเท่าเทียม (Peer - to - Peer Network)

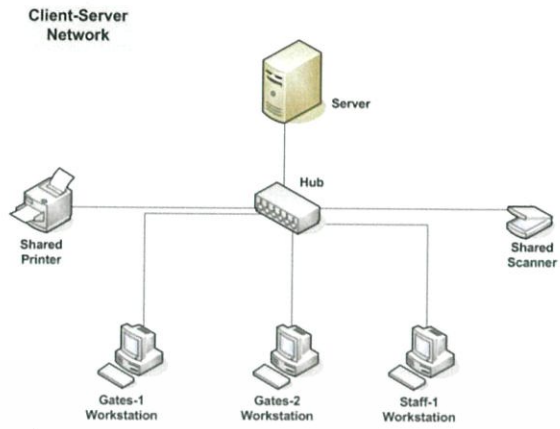
เครือข่ายแบบเท่าเทียมเป็นการเชื่อมต่อที่เครื่องทุกเครื่องในระบบเครือข่ายมีสถานะเท่าเทียมกันหมด โดยเครื่องทุกเครื่องสามารถเป็นได้ทั้งเครื่องผู้ใช้และเครื่องบริการในขณะใดขณะหนึ่งแสดงในรูปที่ 2.8 ในระบบเครือข่ายประเภทนี้การติดต่อระหว่างแต่ละเครื่องจะสามารถติดต่อกันได้โดยตรง มีข้อเสียคือประสิทธิภาพในการรับส่งข้อมูลด้อยกว่าServer base network ทำให้ไม่เหมาะกับระบบที่มีการใช้งานการรับส่งข้อมูลผ่านเครือข่ายมาก ๆ



รูปที่ 2.8 เครือข่ายแบบเท่าเทียม [2]

2.1.3.2 เครือข่ายแบบผู้ให้บริการและผู้ใช้บริการ (Client/Server Network)

เครือข่ายแบบผู้ให้บริการและผู้ใช้บริการเป็นการเชื่อมต่อโดยมีเครื่องบริการ (Server) อยู่ศูนย์กลางทำหน้าที่ในการให้บริการต่าง ๆ ที่เครื่องผู้ใช้หรือสถานีงาน (Workstation/Client) ร้องขอ แสดงในรูปที่ 2.9 รวมทั้งเป็นผู้จัดการดูแลการจราจรในระบบเครือข่ายทั้งหมด นั่นคือการติดต่อกันระหว่างเครื่องต่าง ๆ จะต้องผ่านเครื่องเซิร์ฟเวอร์ เครื่องผู้ใช้จะทำการประมวลผลในงานของตนเท่านั้น ไม่มีหน้าที่ในการให้บริการกับเครื่องอื่น ๆ ในระบบ



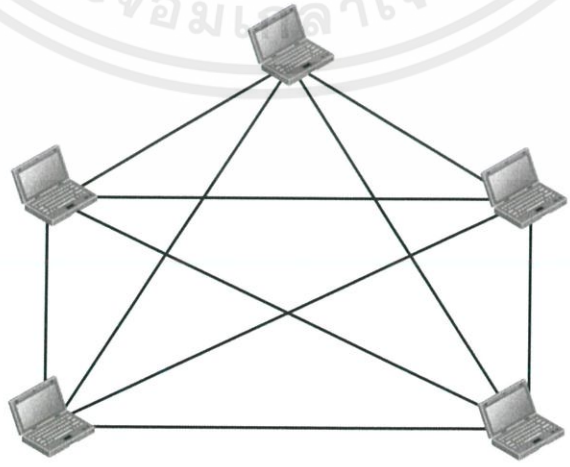
รูปที่ 2.9 เครือข่ายแบบผู้ให้บริการและผู้ใช้บริการ [2]

2.1.4 โครงสร้างเครือข่ายคอมพิวเตอร์ (Network Topology)

โครงสร้างเครือข่ายคอมพิวเตอร์ (Network Topology) คือลักษณะของการเชื่อมโยงสายสื่อสารเข้ากับอุปกรณ์ อิเล็กทรอนิกส์และเครื่องคอมพิวเตอร์ภายในเครือข่ายด้วยกัน โทโปโลยีของเครือข่าย LAN แต่ละแบบมีความเหมาะสมในการใช้งานแตกต่างกันออกไป การนำไปใช้จึงต้องทำการศึกษาลักษณะและคุณสมบัติ ข้อดีและข้อเสียของโทโปโลยีแต่ละแบบ เพื่อนำไปใช้ในการออกแบบพิจารณาเครือข่ายให้เหมาะสมกับการใช้งาน ซึ่งมีรูปแบบต่าง ๆ ดังนี้

2.1.4.1 โครงสร้างแบบตาข่าย (Mesh Topology)

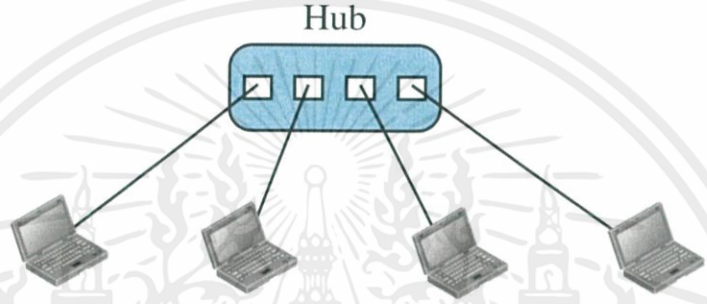
โครงสร้างแบบตาข่าย (Mesh Topology) เป็นการเชื่อมโยงแบบ point to point โดยแต่ละเครื่องจะมีการเชื่อมโยงที่เป็นของตนเองแสดงดังรูปที่ 2.10 ข้อดีของรูปแบบตาข่ายคือไม่มีการแชร์ข้อมูลกันระหว่างเครื่องใด ๆ จึงสามารถใช้แบนด์วิธ (bandwidth) ได้อย่างเต็มประสิทธิภาพ มีความปลอดภัยสูงเนื่องจากเป็นการสื่อสารกันระหว่างสองเครื่อง แต่มีข้อเสียคือเป็นรูปแบบการเชื่อมต่อเครือข่ายที่สิ้นเปลืองสายสื่อสารมากที่สุด



รูปที่ 2.10 โครงสร้างแบบตาข่าย [3]

2.1.4.2 โครงสร้างแบบดาว (Star Topology)

โครงสร้างแบบดาวเป็นรูปแบบที่เครื่องคอมพิวเตอร์ทุกเครื่องจะต่อสายเข้าไปที่อุปกรณ์ที่เรียกว่า ฮับหรือสวิตช์ แสดงในรูปที่ 2.11 โดยอุปกรณ์นี้จะทำหน้าที่รับส่งข้อมูลระหว่างเครื่องต่าง ๆ ในระบบ LAN ข้อดีของระบบแบบดาวนี้คือสามารถควบคุมดูแลได้สะดวกเนื่องจากมีจุดควบคุมอยู่ที่จุดเดียว เมื่อเครื่องใดเครื่องหนึ่งเกิดชำรุด ระบบก็จะยังคงทำงานได้ตามปรกติ การส่งข้อมูลไม่จำเป็นต้องรอคอยเครื่องใด ๆ สามารถส่งข้อมูลไปยังเครื่องคอมพิวเตอร์เป้าหมายได้เลย แต่มีข้อเสียคือ หากอุปกรณ์ที่เป็นศูนย์กลางชุดรุดระบบก็จะไม่สามารถทำงานได้ทั้งระบบ

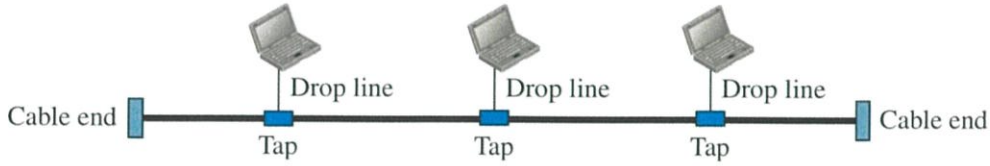


รูปที่ 2.11 โครงสร้างแบบดาว [3]

2.1.4.3 โครงสร้างแบบบัส (Bus Topology)

โครงสร้างแบบบัสจะเชื่อมต่อกันบนสายสัญญาณเส้นเดียวกัน(Backbone)โดยจำเป็นต้องมี T-Connector เป็นตัวแปลงสัญญาณข้อมูลระหว่างคอมพิวเตอร์ และจำเป็นต้องมี Terminator ปิดที่ด้านท้ายและหัวของสายสัญญาน เพื่อดูดซับไม่ให้สัญญาณสะท้อนกลับแสดงในรูปที่ 2.12 การส่งผ่านข้อมูลจะไหลผ่านไปยังปลายทั้งสองด้านที่เครื่องนั้นได้เชื่อมต่ออยู่ โดยเครื่องปลายทางจะคอยตรวจสอบแพ็คเกจว่าตรงกันกับตำแหน่งของตนเองหรือไม่ หากไม่ก็จะผ่านไป

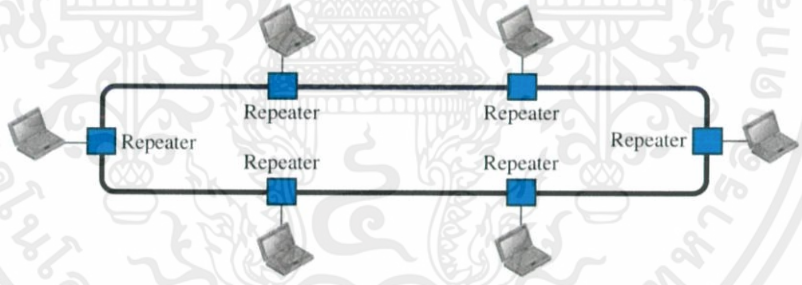
เมื่อคอมพิวเตอร์เครื่องหนึ่งที่กำลังส่งข้อมูลอยู่ เครื่องอื่น ๆ จะไม่สามารถส่งข้อมูลได้ เนื่องจากสายสัญญาณเป็นสื่อกลางที่ใช้ร่วมกัน ดังนั้นหากมีการเชื่อมต่อแบบบัสจำเป็นอย่างยิ่งที่จะต้องคำนึงถึงจำนวนเครื่องที่จะใช้ในเชื่อมต่อเครือข่าย ข้อดีของการเชื่อมต่อรูปแบบบัสนี้คือมีรูปแบบการเชื่อมต่อที่ไม่ยุ่งยากซับซ้อน ข้อเสียด้านการส่งข้อมูลอย่างที่กล่าวไปแล้วในตอนต้นคือระบบบัสจะมี backbone เพียงแค่ตัวเดียว การส่งข้อมูลจึงส่งได้ทีละเครื่องและเมื่อการส่งข้อมูลมีปัญหาจะสามารถตรวจสอบได้ยาก เนื่องจากทุกอุปกรณ์ต่างก็เชื่อมต่อเข้ากับสายแกนหลักทั้งหมด หากสายสัญญาณชำรุดระบบก็จะล่มทั้งหมด นอกจากนี้การส่งผ่านระหว่างเครื่องสู่เครื่องด้วยระบบบัสยังมีจำกัดเรื่องระยะห่างที่ไม่มาก เพราะสัญญาณข้อมูลอาจส่งไปไม่ถึง



รูปที่ 2.12 โครงสร้างแบบบัส [3]

2.1.4.4 โครงสร้างแบบวงแหวน (Ring Topology)

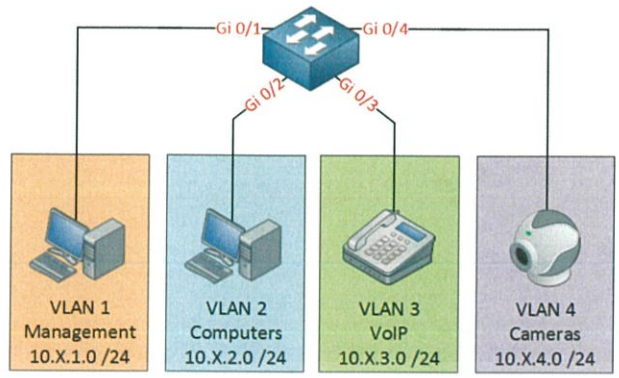
โครงสร้างแบบวงแหวนเป็นระบบที่มีการส่งข้อมูลไปในทิศทางเดียวกันโดยมีลักษณะเป็นวงกลมหรือวงแหวน (Ring Topology บางระบบสามารถส่งได้ 2 ทิศทาง) โดยจะมีเครื่อง Server ในการปล่อย Token เพื่อตรวจสอบว่ามีเครื่องคอมพิวเตอร์ใดต้องการส่งข้อมูลหรือไม่ดังรูปที่ 2.13 เครื่องใดที่ต้องการส่งข้อมูลก็จะต้องรอให้เครื่องอื่น ๆ ส่งข้อมูลให้เสร็จสิ้นเสียก่อน (เช่นเดียวกับบัส) ข้อดีของโทโปโลยีแบบวงแหวนคือการส่งข้อมูลสามารถส่งไปยังผู้รับหลาย ๆ เครื่องพร้อมกันได้ โดยกำหนดตำแหน่งปลายทางเหล่านั้นลงไปในส่วนหัวของแพ็กเกจข้อมูล ซึ่ง repeater ของแต่ละเครื่องจะคอยตรวจสอบเองว่ามีข้อมูลส่งมาให้ที่โหนดของตนหรือไม่ ข้อเสีย หากวงแหวนชำรุดหรือขาด จะส่งผลกระทบต่อระบบทั้งหมด และตรวจสอบได้ยากเช่นเดียวกันหากระบบเกิดมีปัญหา



รูปที่ 2.13 โครงสร้างแบบวงแหวน [3]

2.1.5 วีแลน (VLAN)

วีแลน (VLAN) หรือ Virtual Local Area Network เป็นการแยกกลุ่มคอมพิวเตอร์ออกเป็นกลุ่มย่อย ๆ เสมือนอยู่วง LAN เดียวกันและสื่อสารได้เฉพาะภายในวีแลนเดียวกันเท่านั้นดังในรูปที่ 2.14 ประโยชน์ที่ได้จากการสร้างและแบ่งวีแลนคือ ช่วยลดบรอดคาสต์ทราฟฟิกไม่ให้ส่งผลกระทบกับประสิทธิภาพโดยรวมของเน็ตเวิร์ก และช่วยในเรื่องของความปลอดภัย เช่น กรณีมีเครื่องคอมพิวเตอร์ติดไวรัสจะไม่แพร่กระจายไปยังวีแลนอื่น ทำให้สามารถจำกัดวงของไวรัสได้

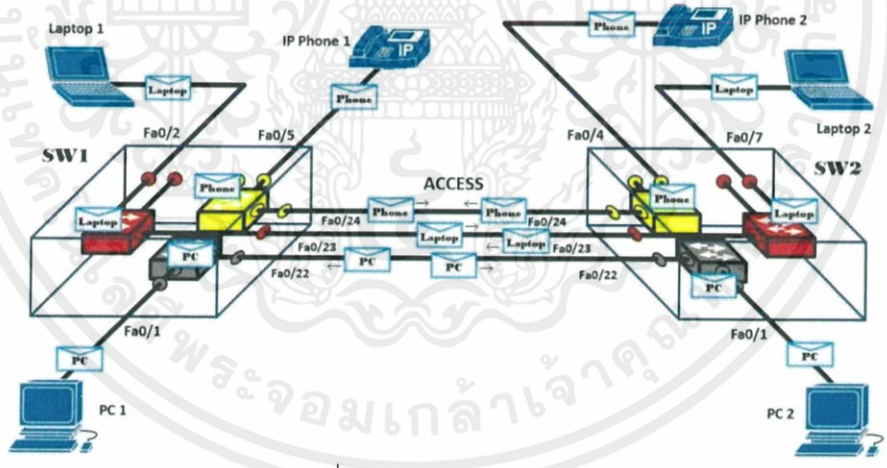


รูปที่ 2.14 Virtual Local Area Network [4]

2.1.6 ความหมายของ Access Port และ Trunk Port

2.1.6.1 Access Port

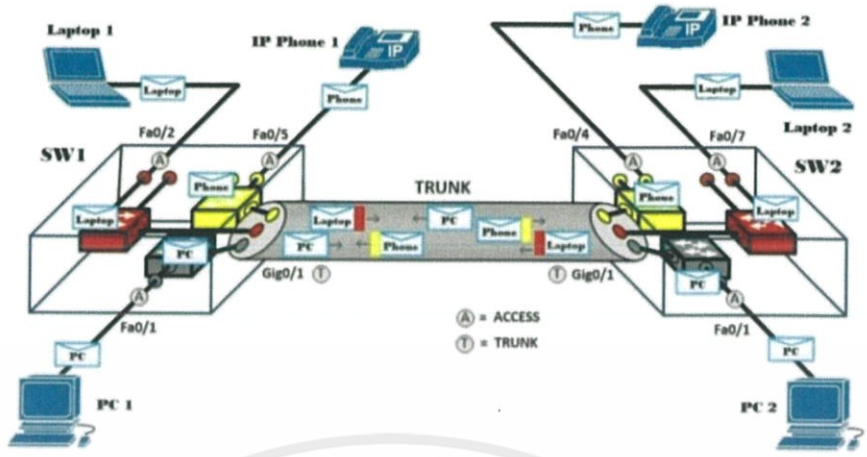
Access Port เปน Port ที่ทำหนาที่เชื่อมตอระหวางสวิตช์จาก Client ไปยังสวิตช์ ซึ่งจะใชสาย LAN แบบสายตรง (Straight Through) ในการเชื่อมตอและ Port ที่ถูกตั้งเปน Access Port นี้จะมี Traffic ของวีแลนเพียงวีแลนเดียวที่วิ่งผานออกมายัง Port นี้ ดังแสดงในรูปที่ 2.15



รูปที่ 2.15 Access Port [4]

2.1.6.2 Trunk Port

Trunk Port เปน Port ที่ทำหนาที่เชื่อมต่อสวิตช์ตัวอื่น ๆ ที่ตองการใหเปนสมาชิกของวีแลนตาง ๆ กันมาอยูดวยกันและทำหนาที่สงผาน Traffic ของหลาย ๆ วีแลนใหกระจายไปยังสวิตช์ ตัวอื่น ๆ ที่มี Port ที่ถูกกำหนดใหเปนวีแลนเดียวกันกับสวิตช์ตัวตนทางได้ หรือก็คือเป็น Port ที่สามารถมี Traffic ของหลาย ๆ วีแลนผ่านได้ ดังแสดงในรูปที่ 2.16



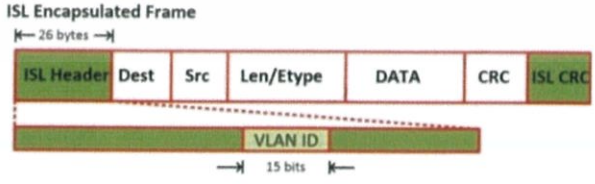
รูปที่ 2.16 Trunk Port [4]

2.1.7 ประเภทการ Encapsulation บน Trunk Port

เนื่องจากเฟรมที่วิ่งผ่าน Trunk Port ระหว่างสวิตช์เป็นเฟรมที่เป็นของวีแลนใดก็ได้ เมื่อสวิตช์ต้นทางส่งเฟรมผ่าน Port ที่เป็น Trunk Port ออกไป จึงจำเป็นต้องมีเทคนิคบางอย่างเพื่อทำให้สวิตช์ปลายทางสามารถระบุได้ว่า Traffic ที่ได้รับมาจาก Trunk Port นั้น เป็นของวีแลนใด ซึ่งเทคนิคที่ว่านั้นก็คือการเพิ่มฟิลด์ข้อมูลพิเศษเข้าไปในเฟรมมาตรฐานเพื่อไว้ระบุหมายเลขวีแลน เฟรมที่ผ่านการเพิ่มฟิลด์พิเศษนี้เข้าไปจะเรียกว่า เฟรมที่ผ่านการ “Encapsulation” แล้ว ซึ่งประเภทของการ Encapsulation บน Trunk Port มีอยู่ 2 แบบดังนี้

2.1.7.1 Inter Switch Link (ISL)

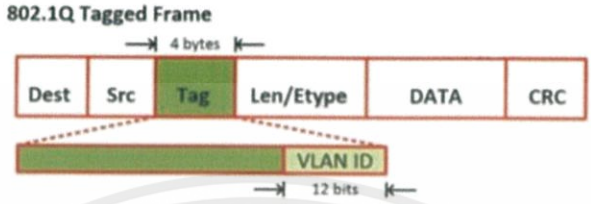
ISL จะใช้วิธีการเพิ่มฟิลด์พิเศษขนาด 26 ไบต์ที่ประกอบด้วยหมายเลขวีแลนขนาด 10 บิตเข้าไปข้างหน้าอีเธอร์เน็ตเฟรมและต่อท้ายด้วย CRC (Cyclic redundancy check) ขนาด 4 ไบต์เข้าไปที่ท้ายเฟรม โดยภายใน ISL Header ก็จะมีในส่วนของวีแลนอยู่ภายในอีกที ดังนั้นวิธีการนี้ถือได้ว่าเป็นการ Encapsulation เฟรมเดิมทั้งหมดและก็มีการสร้าง Headerใหม่ขึ้นมาแสดงในรูปที่ 2.17 โดย ISL นี้ใช้ได้กับอุปกรณของยี่ห้อ Cisco เท่านั้น



รูปที่ 2.17 Inter Switch Link [4]

2.1.7.2 802.1Q

802.1Q จะใช้วิธีการเพิ่มฟิลด์พิเศษ (Tag) ขนาด 4 ไบต์ที่ประกอบด้วยหมายเลขวีแลนขนาด 12 บิตเข้าไปในระหว่างอีเธอร์เน็ตเฟรมแสดงดังรูปที่ 2.18 โดยวิธีนี้เป็นมาตรฐานกลางของ IEEE และเป็นวิธีที่นิยมนำมาใช้งานมากที่สุดในปัจจุบัน



รูปที่ 2.18 802.1Q [4]

2.1.8 IP Address

หมายเลข IP Address เป็นแอดเดรสที่ผู้ติดตั้งระบบเครือข่ายจำเป็นต้องกำหนดให้กับเครื่องคอมพิวเตอร์ที่รัน TCP/IP เพื่อใช้บ่งบอกตำแหน่งที่อยู่ของเครื่องคอมพิวเตอร์ในระบบ เมื่อเครื่องคอมพิวเตอร์ต้องการส่งข้อมูลไปให้เครื่องปลายทางโดยอาศัยโปรโตคอล TCP/IP จำเป็นจะต้องระบุหมายเลข IP Address ของเครื่องปลายทางให้ถูกต้อง และในทางกลับกันเมื่อเครื่องปลายทางต้องการส่งข้อมูลกลับไปเครื่องต้นทาง ก็จำเป็นต้องระบุตำแหน่งเครื่องต้นทางด้วยหมายเลข IP Address ด้วยเช่นกัน ซึ่ง IP Address ประกอบด้วยตัวเลข 4 ชุด มีเครื่องหมายจุดขั้นระหว่างชุด เช่น 192.168.100.1 หรือ 172.16.10.1 เป็นต้น โดยหมายเลข IP Address ของเครื่องคอมพิวเตอร์แต่ละเครื่องจะมีค่าไม่ซ้ำกัน สิ่งที่ตัวเลข 4 ชุดนี้บอก คือ Network ID กับ Host ID ซึ่งจะบอกให้รู้ว่าเครื่อง Computer อยู่ใน Network ไหน และเป็นเครื่องไหนใน network นั้น

2.1.9 Subnet mask

Subnet mask เป็น Parameter (พารามิเตอร์) อีกตัวหนึ่งที่ต้องระบุควบคู่กับหมายเลข IP Address หน้าที่ของ Subnet mask ก็คือ การช่วยในการแยกแยะว่าส่วนใดภายในหมายเลข IP Address เป็น Network Address และส่วนใดเป็นหมายเลข Host Address ดังนั้น จะสังเกตได้ว่าเมื่อระบุ IP Address ให้กับเครื่องคอมพิวเตอร์จำเป็นต้องระบุ Subnet mask ลงไปด้วยทุกครั้ง

2.1.10 Routing Protocol

Routing Protocol คือ Protocol ที่ใช้ในการแลกเปลี่ยน routing information ระหว่างอุปกรณ์เครือข่ายต่าง ๆ ที่ทำงานในระดับ Network Layer (Layer 3) ได้แก่ เราเตอร์ สวิตช์เลเยอร์ 3 ไฟร์วอลล์ Linux Server รวมถึง OS ต่าง ๆ เป็นต้น เพื่อให้อุปกรณ์เหล่านี้สามารถส่งข้อมูล (IP packet) ไปยังคอมพิวเตอร์ปลายทางได้อย่างถูกต้อง เราเตอร์จะรู้ว่าไปยัง IP ปลายทางได้ทางอินเตอร์เฟสใด หรือไปทางเราเตอร์ตัวไหน ได้จาก routing table นั่นเอง การทำ routing Protocol นั่น มีด้วยกัน 2 แบบ ดังนี้

2.1.10.1 Static Route

Static Route คือ การกำหนดค่าแบบคงที่เข้าไปในตัวเราเตอร์ เพื่อบอกให้เราเตอร์ทราบว่าหากต้องการจะส่งแพคเกจไปยังซับเน็ตแอดเดรสต่าง ๆ จะต้องส่งไปหาเราเตอร์ตัวถัดไป (Next Hop Address) ตัวไหน หรือจะให้เราเตอร์ส่งออกไปทางอินเตอร์เฟซใด ซึ่งวิธีการนี้หากมีเราเตอร์จำนวนมากและมีซับเน็ตแอดเดรสต่าง ๆ จำนวนมาก ผู้ดูแลเน็ตเวิร์กก็จะต้องใช้เวลามากในการค่อย ๆ เพิ่ม Static Route เข้าไปในเราติ้งเทเบิลของเราเตอร์ทุกตัวด้วยตัวเอง แต่วิธีการนี้ค่า AD หรือค่าลำดับความสำคัญสูงกว่าแบบ Dynamic Route คือ จะพิจารณา Static Route ก่อนพิจารณาเส้นทางจาก Dynamic Route

2.1.10.2 Dynamic Route

Dynamic Route เป็นการสั่งให้รันเราติ้งโปรโตคอลขึ้นมา จะช่วยลดภาระของผู้ดูแลระบบเน็ตเวิร์กและทำให้การจัดการเน็ตเวิร์กเป็นไปได้อย่างง่ายดาย เมื่อรันเร้าติ้งโปรโตคอลขึ้นบนเราเตอร์แล้วก็ทำการกำหนดเราติ้งโปรโตคอลไปยังอินเตอร์เฟซใดของเราเตอร์ จากนั้นเราเตอร์แต่ละตัวจะช่วยเหลือซึ่งกันและกันในการทำให้ฐานความรู้ในเราติ้งเทเบิลมีความสมบูรณ์ และที่สำคัญเราติ้งโปรโตคอลยังสามารถตรวจจับความเปลี่ยนแปลงต่าง ๆ ในเน็ตเวิร์กโทโพโลยี และปรับปรุงเราติ้งเทเบิลให้สอดคล้องกับสภาพความเป็นจริงของเน็ตเวิร์กโทโพโลยีโดยอัติโนมัติ ซึ่งความเปลี่ยนแปลงต่าง ๆ เช่น เราเตอร์เพื่อนบ้านดาวน์ลง อินเตอร์เฟซของเราเตอร์ดาวน์ หรือ WAN Link ในเน็ตเวิร์กมีปัญหา เป็นสิ่งที่ Static Route ทำไม่ได้ การปรับเปลี่ยนเราติ้งอย่างทันทีและอัตโนมัติจึงเป็นข้อดีของ Dynamic Route

2.1.11 Access Control Lists (ACL)

Access Control Lists (ACL) เป็นฟีเจอร์หนึ่งที่ช่วยในการสร้างความปลอดภัยให้กับระบบเน็ตเวิร์กและเราเตอร์ โดยนิยามของ ACL จะทำหน้าที่กำหนดเงื่อนไขของทราฟฟิคที่ได้รับ

อนุญาต (permit) ให้เข้าถึง หรือถูกปฏิเสธ (deny) ไม่ให้เข้าถึงเน็ตเวิร์ค โดย ACL 1 ACL จะมีหมายเลขหรือชื่อกำกับอยู่เพื่อใช้อ้างอิงต่อไป และภายใน ACL หนึ่ง ๆ จะมีลิสต์บรรทัดอยู่หลาย ๆ บรรทัดซึ่งเป็นตัวกำหนดประเภทของทราฟฟิคที่ permit หรือ deny ACL ที่ถูกสร้างขึ้นมาจะยังไม่ได้ถูกนำไปใช้งานจนกว่าจะได้รับการเซตลงไปที่อินเตอร์เฟซของเร้าเตอร์

2.1.11.1 ประเภทของ ACL

- Standard ACL ACL ประเภทนี้จะตรวจเช็คได้เฉพาะหมายเลขแอดเดรสต้นทาง (Source Address) ของแพคเกจเท่านั้นว่าอยู่ในเงื่อนไขที่ต้องการหรือไม่ ACL ประเภทนี้จึงไม่สามารถแยกแยะลงไปในรายละเอียดและส่วนอื่น ๆ ของแพคเกจได้
- Extended ACL ACL ประเภทนี้สามารถประเมินค่าอื่น ๆ ของแพ็คเก็ตได้อย่างละเอียด สามารถตรวจเช็คได้ทั้งในเลเยอร์ 3 และเลเยอร์ 4 ได้แก่ การตรวจเช็กหมายเลข Source IP Address, Destination IP Address, Protocol ในส่วนเฮดเดอร์ของแพ็คเก็ต IP, หมายเลขพอร์ตของ TCP/UDP ทั้งพอร์ตต้นทางและพอร์ตปลายทาง ACL ประเภทนี้จึงให้เงื่อนไขในการตัดสินใจได้อย่างละเอียดมากยิ่งขึ้น

2.1.11.2 การทำงานของ Access List

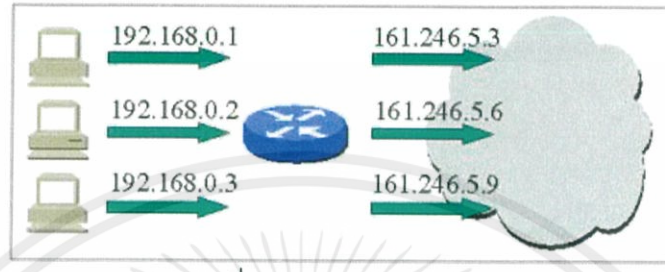
ACL จะถูกเปรียบเทียบจากบรรทัดบนลงล่างทีละบรรทัด หรือ หมายเลข Sequence Number ที่ต่ำไปยังหมายเลข Sequence Number ที่สูง จนกว่าจะพบบรรทัดที่มีเงื่อนไขที่สอดคล้องกับแพคเกจ ที่วิ่งเข้ามา เมื่อพบแล้วเราเตอร์หรือสวิตช์เลเยอร์ 3 จะดูว่าการกระทำที่ตั้งไว้ว่าเป็น Permit หรือ Deny หากเป็น Permit ตัวเราเตอร์หรือสวิตช์เลเยอร์ 3 ก็จะอนุญาตให้ทราฟฟิคนั้นวิ่งผ่านไปได้ แต่ถ้าหากเป็น Deny ทราฟฟิคนั้นจะถูกปฏิเสธ (Discard) และโยนทิ้ง (Drop) โดยทุก ๆ ACL ที่สร้างขึ้นมาจะมีเงื่อนไขสุดท้ายถูกซ่อนไว้เสมอ เรียกว่า Implicit deny all ความหมายก็คือทราฟฟิคใด ๆ ที่ไม่สอดคล้องกับเงื่อนไขในบรรทัดต่าง ๆ ทั้งหมด ทราฟฟิคประเภทนั้นจะถูกปฏิเสธ (Discard) และโยนทิ้ง (Drop) ยกเว้นถ้าใส่คำสั่งที่อนุญาตทั้งหมด (Permit all) สิ่งที่เรียกว่า Implicit deny all จะไม่มีผล

2.1.12 Network Address Translation (NAT)

Network Address Translation หรือ NAT เป็นวิธีการทางเครือข่ายที่จะเปลี่ยน Network Address จากหมายเลขหนึ่งไปเป็นอีกหมายเลขหนึ่ง ทำให้สามารถเชื่อมต่อไปยังเครื่องปลายทางได้

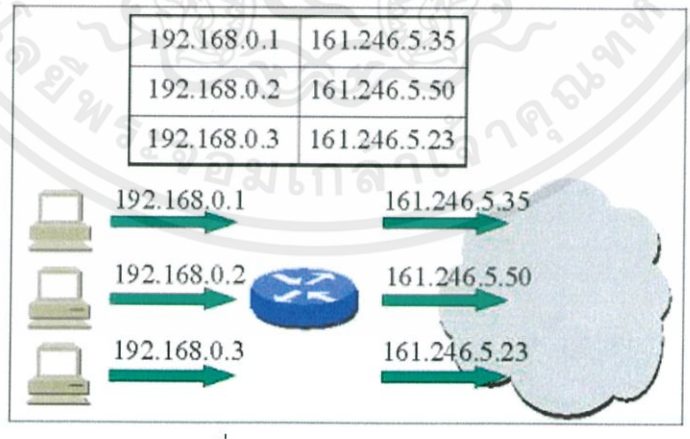
2.1.12.1 รูปแบบในการเปลี่ยนแปลงค่า IP Address

1) Static NAT (static assignment and basic NAT) เป็นการเปลี่ยนแปลงค่าหมายเลขไอพีแอดเดรสโดยมีการจับคู่กันของหมายเลขไอพีแอดเดรสตลอดการทำงานของอุปกรณ์ ซึ่งจะเปลี่ยนแปลงค่าไอพีแอดเดรสจาก Private IP เป็นหมายเลขไอพีภายนอก และเปลี่ยนจากหมายเลขไอพีแอดเดรสภายนอกเป็น Private IP แบบหนึ่งต่อหนึ่งไปตลอดแสดงในรูปที่ 2.19



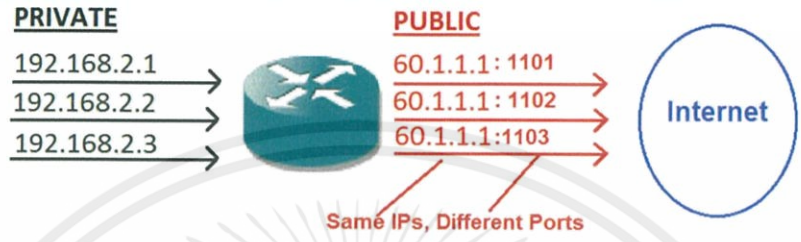
รูปที่ 2.19 Static NAT [8]

2) Dynamic NAT (dynamic assignment and basic NAT) เป็นการเปลี่ยนแปลงค่าหมายเลขไอพีแอดเดรสโดยมีการจับคู่กันของหมายเลขไอพีแอดเดรสที่เป็น Private IP กับหมายเลขไอพีแอดเดรสภายนอกเพียงชั่วคราวเท่านั้น โดยอุปกรณ์ NAT จะจับคู่หมายเลขไอพีแอดเดรสในช่วงเวลาที่ session มีการเชื่อมต่อกันอยู่เท่านั้น หลังจากที่ใช้งาน session เสร็จเรียบร้อยแล้วจะไม่เก็บข้อมูลการจับคู่นั้นไว้อีก เมื่อมีการเชื่อมต่อกับเครือข่ายภายนอกอีกครั้ง อุปกรณ์ NAT จะเลือกหมายเลขไอพีแอดเดรสภายนอกใหม่อีกครั้งหนึ่ง ซึ่งไม่จำเป็นต้องซ้ำกับหมายเลขเดิมแสดงในรูปที่ 2.20



รูปที่ 2.20 Dynamic NAT [8]

3) Overloading (NAPT) เป็นการเปลี่ยนแปลงหมายเลขไอพีแอดเดรสเพียงหมายเลขเดียว แต่มีการเปลี่ยนแปลงหมายเลขพอร์ตต้นทางในการเชื่อมต่อแทน เมื่อมีการตอบกลับจากเครื่องภายนอกเครือข่ายแล้ว ที่อุปกรณ์ NAT จะดูหมายเลขพอร์ตปลายทางในส่วนหัวของข้อมูลว่าเป็นหมายเลขอะไร แล้วจึงเปลี่ยนข้อมูลส่วนหัวให้ตรงกับเครื่องคอมพิวเตอร์ที่ทำการร้องขออีกครั้งแสดงในรูปที่ 2.21



รูปที่ 2.21 Overloading [8]

2.1.13 Virtual Private Network (VPN)

VPN หรือ Virtual Private Network คือกลุ่มของเครื่องคอมพิวเตอร์หรือเครือข่ายที่แยกออกต่างหาก ซึ่งมีการเชื่อมต่อไปยังเครือข่ายเน็ตเวิร์คสาธารณะ เช่น อินเตอร์เน็ต VPN จะช่วยทำให้การเชื่อมต่ออินเตอร์เน็ตมีความปลอดภัยโดยการเข้ารหัสข้อมูลที่ได้รับหรือส่งออกไปจากเครื่องและทำให้ข้อมูลเหล่านี้รอดพ้นจากสายตาที่ไม่หวังดี โดย VPN มีการแบ่งรูปแบบต่าง ๆ ดังนี้

2.1.13.1 Intranet VPN

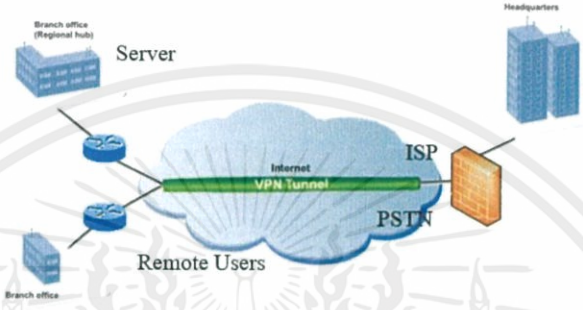
เป็นรูปแบบของ VPN ที่ใช้เฉพาะภายในองค์กรเท่านั้น เช่น การเชื่อมต่อเครือข่ายระหว่างสำนักงานใหญ่กับสำนักงานย่อยในกรุงเทพและต่างจังหวัด โดยเป็นการเชื่อมต่ออินเทอร์เน็ตผ่านผู้ให้บริการท้องถิ่นแล้วจึงเชื่อมต่อเข้ากับเครือข่ายส่วนตัวเสมือนขององค์กร จากเดิมที่ทำการเชื่อมต่อโดยใช้ Leased Line หรือ Frame relay

2.1.13.2 Extranet VPN

มีรูปแบบการเชื่อมต่อที่คล้ายกับแบบ Intranet แต่มีการขยายวงออกไปยังกลุ่มต่าง ๆ ภายนอกองค์กร เช่น ซัพพลายเออร์ ลูกค้า เป็นต้น การเชื่อมต่อแบบนี้ก็คือการเชื่อมต่อ LAN ต่าง LAN กันนั่นเอง ปัญหาก็คือการรักษาความปลอดภัยให้กับข้อมูลเพราะฉะนั้นการเลือกผู้ให้บริการที่ดีจึงเป็นสิ่งที่สำคัญมากในการรักษาความปลอดภัยของข้อมูลเพราะถ้าผู้ให้บริการดีก็สามารถรักษาความปลอดภัยให้กับข้อมูลของผู้ใช้บริการได้อย่างดี

2.1.13.3 Remote Access VPN

เป็นรูปแบบการเข้าถึงเครือข่ายระยะไกลจากอุปกรณ์เคลื่อนที่ต่าง ๆ ซึ่งสามารถเข้าถึงเครือข่ายได้ใน 2 ลักษณะ ลักษณะแรก เป็นการเข้าถึงจากไคลเอ็นต์ทั่วไป ไคลเอ็นต์จะอาศัยผู้ให้บริการอินเทอร์เน็ตเป็นตัวกลางในการติดต่อและเข้ารหัสการส่งสัญญาณจากไคลเอ็นต์ไปยังเครื่องไอเอสพีและลักษณะที่สองเป็นการเข้าถึงจากเครื่องแอ็กเซสเซิร์ฟเวอร์ (Network Access Server-Nas) แสดงดังรูปที่ 2.22



รูปที่ 2.22 Remote Access VPN
(ที่มา : http://www.wikiwand.com/th)

2.1.14 โปรแกรมที่ใช้ในการ Monitoring

2.1.14.1 PRTG Network Monitoring

Paessler Router Traffic Grapher หรือ PRTG เป็นซอฟต์แวร์สำหรับ Monitoring และเฝ้าระวังระบบเครือข่าย รวมไปถึงอุปกรณ์ปลายทางอย่าง IoT ได้อย่างครอบคลุม ไม่ว่าจะเป็นตรวจสอบความพร้อมในการให้บริการ (Availability) และปริมาณ Bandwidth ที่ใช้ของอุปกรณ์บนระบบเครือข่าย รวมไปถึงสามารถแจ้งเตือนผู้ดูแลระบบเมื่อเกิดเหตุการณ์ไม่คาดฝันขึ้นได้ เช่น อุปกรณ์หยุดให้บริการ เกิดปัญหาคอขวด หรือประสิทธิภาพเปลี่ยนไปจากค่ามาตรฐานเดิม เป็นต้น แสดงในรูปที่ 2.23

2.1.14.2 คุณสมบัติเด่นที่สำคัญของ PRTG Network Monitoring

1) สามารถมอนิเตอร์การใช้งานอุปกรณ์ IoT ระบบปฏิบัติการ Windows, Mac OS X, Linux และ Unix ผ่าน SNMP, WMI, NetFlow, sFlow, jFlow, Constrained Application Protocol (CoAP) และ RESTful HTTP โดยไม่จำเป็นต้องลง Agent แต่อย่างใด

2) มี Sensor พร้อมให้บริการมากกว่า 200 รายการสำหรับติดตามการใช้เว็บไซต์ อีเมล แอพพลิเคชัน ฐานข้อมูล อุปกรณ์ฮาร์ดแวร์ และการใช้งานแบบ Virtualization ไม่ว่าจะเป็น Bandwidth, Usage, Activity, Uptime, Downtime และ SLA ได้อย่างครอบคลุม

3) ติดตามและเฝ้าระวังการใช้ระบบเครือข่าย LAN และ WAN ของทั้งสำนักงานใหญ่และสำนักงานสาขาได้แบบรวมศูนย์ โดยไม่จำเป็นต้องเสียค่าใช้จ่ายเพิ่มเติม

4) รองรับการแจ้งเตือนผ่านแอพพลิเคชันบนอุปกรณ์ Apple iOS และ Android รวมไปถึงอีเมลและ SMS

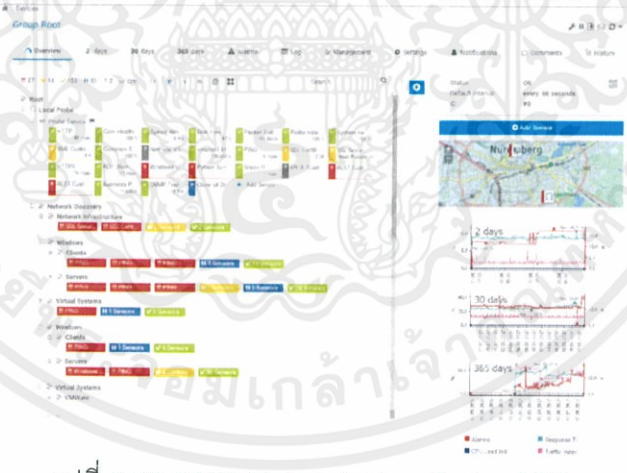
5) สามารถทำ Service Level Agreement (SLA) Monitoring ได้ โดยผูกเงื่อนไขการออก Ticket แจ้งเตือนไปยังผู้เกี่ยวข้องตามลำดับขั้น และมีกระบวนการแจ้งเตือนตามกำหนดเวลา

6) จัดทำ Network Diagram แบบ Interactive พร้อมแสดงผลข้อมูลแบบเรียลไทม์ หน้า Dashboard มีความสวยงาม ปรับแต่งได้หลากหลายรูปแบบ และสามารถเลือกดูรายละเอียดเชิงลึกได้ทันที แสดงในรูปที่ 2.24

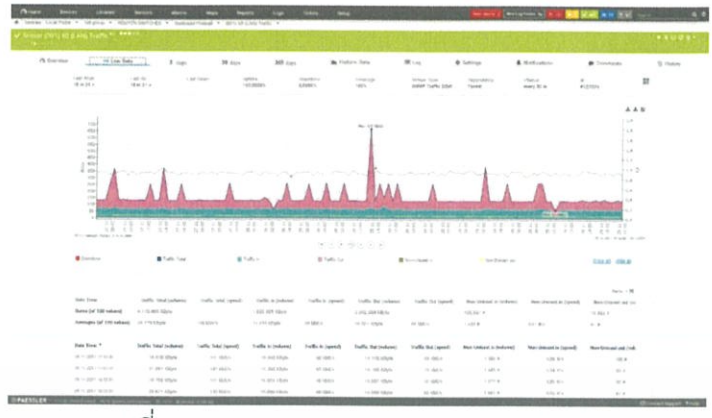
7) จัดเก็บ Log แบบ RAW ซึ่งเหมาะสำหรับนำไปวิเคราะห์ข้อมูลในอนาคตมากกว่าการเก็บข้อมูลบนฐานข้อมูล SQL

8) จัดทำรายงานได้หลากหลายรูปแบบ รวมไปถึงจัดเก็บ Event Log แล้วส่งต่อไปยังอุปกรณ์ SIEM เพื่อวิเคราะห์ข้อมูล Security Intelligence ต่อได้

9) รองรับการทำ Failover Cluster ได้ เพื่อการทำงานในระดับพร้อมใช้ขั้นสูง (High Availability)



รูปที่ 2.23 PRTG Network Mornitoring [10]



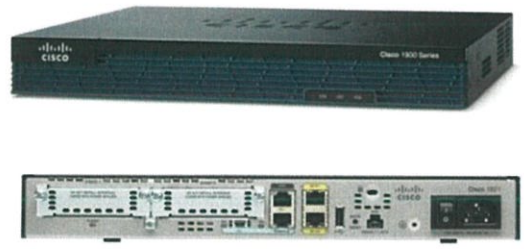
รูปที่ 2.24 Firewall traffic monitored [10]

2.1.15 อุปกรณ์ที่เก็บ Configuration

2.1.15.1 Router

เราเตอร์ (Router) คือ อุปกรณ์ที่ทำหน้าที่เชื่อมต่อระบบเครือข่ายอย่างหนึ่ง โดยการเชื่อมต่อคอมพิวเตอร์ด้วยเราเตอร์ทำให้สามารถเชื่อมต่อคอมพิวเตอร์ได้มากกว่าหนึ่งเครื่องในเวลาเดียวกัน ซึ่งเราเตอร์นั้นจะมีซอฟต์แวร์ที่ใช้ในการควบคุมการทำงานเรียกว่า Internetwork Operating System (IOS) และตัวเราเตอร์จะมีช่องที่ใช้เสียบสายสัญญาณเรียกว่า Port LAN ซึ่งโดยทั่วไปมักมี 4 Ports หรือมากกว่า ในเราเตอร์หนึ่งตัวแสดงในรูปที่ 2.25

หน้าที่หลักของเราเตอร์คือการหาเส้นทางในการส่งผ่านข้อมูลที่ดีที่สุด และเป็นตัวกลางในการส่งต่อข้อมูลไปยังเครือข่ายอื่น ทั้งนี้เราเตอร์สามารถเชื่อมโยงเครือข่ายที่ใช้สื่อสัญญาณหลายแบบแตกต่างกันได้ไม่ว่าจะเป็น Ethernet, Token Rink หรือ FDDI ทั้ง ๆ ที่ในแต่ละระบบจะมี packet เป็นรูปแบบของตนเองซึ่งแตกต่างกัน โดยโปรโตคอลที่ทำงานในระดับบนหรือ Layer 3 ขึ้นไปเช่น IP, IPX หรือ AppleTalk เมื่อมีการส่งข้อมูลก็จะบรรจุข้อมูลนั้นเป็น packet ในรูปแบบของ Layer 2 คือ Data Link Layer เมื่อเราเตอร์ได้รับข้อมูลมาก็จะตรวจดูใน packet เพื่อจะทราบว่าใช้โปรโตคอลแบบใด จากนั้นก็จะตรวจดูเส้นทางส่งข้อมูลจากตาราง Routing Table ว่าจะต้องส่งข้อมูลนี้ไปยังเครือข่ายใดจึงจะต่อไปถึงปลายทางได้ แล้วจึงบรรจุข้อมูลลงเป็น Packet ของ Data Link Layer ที่ถูกต้องอีกครั้ง เพื่อส่งต่อไปยังเครือข่ายปลายทาง



รูปที่ 2.25 เราเตอร์

(ที่มา : http://telco.ge/main/product)

2.1.15.2 Switch

สวิตช์ (Switch) เป็นอุปกรณ์ที่พัฒนาการต่อจากฮับอีกทีหนึ่งมีความสามารถมากกว่าฮับแสดงในรูปที่ 2.26 โดยการทำงานของสวิตช์จะส่งข้อมูลออกไปเฉพาะพอร์ตที่ใช้ในการติดต่อกับเครื่องคอมพิวเตอร์พีซีปลายทางเท่านั้น ไม่ส่งกระจายข้อมูลไปยังทุกพอร์ตเหมือนอย่างฮับ ทำให้ในสวิตช์ไม่มีปัญหาการชนของข้อมูล สวิตช์จะทำงานอยู่ในชั้น Data Link Layer คือจะรับผิดชอบในการเชื่อมโยงของข้อมูล ตรวจสอบความถูกต้องของการติดต่อจากโหนดหนึ่งไปอีกโหนดหนึ่งและความสมบูรณ์ของการรับส่งข้อมูล สำหรับในชั้นเชื่อมโยงข้อมูลนั่นจะทำการแบ่งข้อมูลระดับบิตที่ได้รับจากชั้น Physical Layer เป็นข้อมูลชนิดที่เรียกว่า เฟรม ก่อนจะส่งไปยังชั้นถัดไป ก็คือ Network Layer

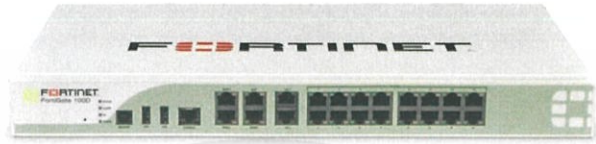
รูปที่ 2.26 สวิตช์

(ที่มา : https://www.cisco.com/c/en/us/support/switches)

2.1.15.3 Firewall

ไฟร์วอลล์ (Firewall) คือระบบรักษาความปลอดภัยของเครือข่ายคอมพิวเตอร์ ซึ่งจะทำหน้าที่เปิดและปิด การเข้าถึงจากภายนอก (เช่น จากอินเตอร์เน็ต) การเข้าถึงเครือข่ายภายใน

(เช่น เครือข่ายภายในองค์กร หรือคอมพิวเตอร์ส่วนตัว) ได้แสดงในรูปที่ 2.27 หรืออาจพูดได้ว่าไฟร์วอลล์ก็เหมือนยามหน้าประตูของคอมพิวเตอร์ ซึ่งการเข้าถึงจากภายนอกจะต้องให้ไฟร์วอลล์ตรวจสอบก่อนว่าสามารถเข้าระบบเครือข่ายภายในได้หรือไม่ โดยไฟร์วอลล์จะมีการกำหนดกฎระเบียบบังคับใช้เฉพาะเครือข่าย ซึ่งหมายความว่าหากการเข้าถึงนั้นถูกต้องตามที่ไฟร์วอลล์กำหนดไว้ ก็จะเข้าถึงเครือข่ายได้ หากไม่ตรงก็จะเข้าถึงไม่ได้



รูปที่ 2.27 ไฟร์วอลล์

(ที่มา : https://www.fortinet.com/products/next-generation-firewall/mid-range.html)

2.1.16 การบริหารจัดการความเสี่ยง

ความเสี่ยง (Risk) หมายถึง เหตุการณ์หรือการกระทำใด ๆ ที่อาจจะเกิดขึ้นภายในสถานการณ์ที่ไม่แน่นอน และจะส่งผลกระทบหรือสร้างความเสียหาย (ทั้งที่เป็นตัวเงินและไม่เป็นตัวเงิน) หรือก่อให้เกิดความล้มเหลวหรือลดโอกาสที่จะบรรลุวัตถุประสงค์ และเป้าหมายขององค์กร ทั้งในด้านยุทธศาสตร์การปฏิบัติงาน การเงิน และการบริการ ซึ่งอาจเป็นผลกระทบทางบวกด้วยก็ได้ โดยวัดจากผลกระทบ (Impact) ที่ได้รับ และโอกาสที่จะเกิด (Likelihood) ของเหตุการณ์

ปัจจัยเสี่ยง (Risk Factor) หมายถึง ต้นเหตุ หรือสาเหตุที่มาของความเสี่ยงที่จะทำให้ไม่บรรลุวัตถุประสงค์ที่กำหนดไว้ โดยต้องระบุได้ด้วยว่าเหตุการณ์นั้นจะเกิดที่ไหน เมื่อใด และเกิดขึ้นได้อย่างไร และทำไม ทั้งนี้สาเหตุของความเสี่ยงที่ระบุควรเป็นสาเหตุที่แท้จริง เพื่อจะได้วิเคราะห์และกำหนดมาตรการลดความเสี่ยงในภายหลังได้อย่างถูกต้อง

2.1.16.1 แนวทางในการบริหารความเสี่ยง

สิ่งที่จำเป็นที่สุดที่แต่ละองค์กรจะต้องทำคือ สามารถวิเคราะห์ (Risk Analysis) และกำหนดให้ได้ว่าองค์กรหรือหน่วยงานใดในองค์กรต้องเผชิญกับความเสี่ยงใดบ้าง (Risk Identification) ซึ่งความเสี่ยงที่เกิดขึ้นอาจมีขนาดและผลกระทบที่แตกต่างกัน (Risk Estimation) โดยที่ความเสี่ยงบางประเภทอาจจะมีโอกาสหรือความเป็นไปได้ที่จะเกิด (Likelihood) ตั้งแต่น้อย (Low) จนไปถึงมีความเป็นไปได้สูง (High) รวมถึงผลกระทบที่ตามมาจากความเสี่ยงที่เกิดขึ้น (Impact) อาจมีตั้งแต่ระดับน้อยมาก (Low) ในขณะที่ความเสี่ยงบางประเภทอาจมีแนวโน้มที่อาจก่อให้เกิดความเสียหายแก่องค์กรอย่างมหาศาล (High) ดังนั้นบุคคลากรในธุรกิจจึงควรที่จะวิเคราะห์และกำหนดความเสี่ยงที่ธุรกิจนั้นเผชิญให้ได้

1) ความน่าจะเป็นหรือโอกาสในการเกิดความเสี่ยง (Likelihood) ความน่าจะเป็นนี้ขึ้นอยู่กับแต่ละองค์กรณ์ในการกำหนดว่าโอกาสของการเกิดเหตุการณ์นั้น ๆ ต้องมีมากน้อยขนาดไหนถึงจะจัดว่ามีโอกาสน้อยหรือมากแสดงดังตารางที่ 2.1

ตารางที่ 2.1 โอกาสในการเกิดความเสี่ยง

ระดับ	คำอธิบาย
1	ยากที่จะเกิด
2	เป็นไปได้ที่จะเกิด
3	ค่อนข้างแน่นอน

2) ผลกระทบหรือความเสียหายที่เกิดจากความเสี่ยง (Impact) ผลกระทบหรือความเสียหายต่อองค์กรที่เกิดจากความเสี่ยงสามารถแบ่งออกเป็นด้านต่าง ๆ ได้แก่

- ผลกระทบด้านการเงิน (Financial : F)
- ผลกระทบด้านชื่อเสียงและภาพลักษณ์องค์กร (Reputation : R)
- ผลกระทบต่อการไม่ปฏิบัติตามกฎ ระเบียบ ข้อบังคับ (Rule : R2)
- ผลกระทบต่อบุคลากร (Human : H)
- ผลกระทบต่อความล่าช้าในการดำเนินงาน (Business Interruption : B)

การประเมินผลกระทบของความเสียหายสามารถแบ่งเป็นระดับต่าง ๆ ดังตารางที่ 2.2

ตารางที่ 2.2 ระดับความเสียหายที่เกิดจากความเสี่ยง

ระดับ	คำอธิบาย
1	ไม่เป็นนัยสำคัญ
2	รุนแรงปานกลาง
3	รุนแรงมาก

ความรุนแรงของเสียหายแต่ละระดับ ขึ้นอยู่กับองค์กรจะระบุว่าความเสียหายแต่ละระดับอยู่ที่เหตุการณ์แบบไหนหรือมีมูลค่าเท่าไหร่ หลังจากที่มีการประเมินความน่าจะเป็นหรือโอกาสในการเกิดของความเสี่ยงแต่ละหัวข้อ รวมถึงการประมาณการความเสียหายจากความเสี่ยงนั้น ๆ แล้ว ก็จะนำเอาทั้งสองกรณีมาพิจารณา โดยใช้ตารางประเมินความเสี่ยง (Risk Matrix) แสดงในตารางที่ 2.3

โดยสีเขียวคือระดับต่ำ (Low) ให้เป็น 1 คะแนน สีส้มคือระดับปานกลาง (Medium) ให้เป็น 2 คะแนน และสีแดงคือระดับสูง (High) 3 คะแนน เพื่อประเมินว่าความเสี่ยงใดที่ให้ความสำคัญในการบริการจัดการ (Risk Prioritization)

จากนั้นกำหนด Priority กับ Gap เพื่อประเมินว่าความเสี่ยงใดควรแก้ไขก่อน หรือมีช่องว่างในการทำงานหรือไม่ และให้แนะนำในการแก้ไขปัญหาอย่างเหมาะสม โดยการแบ่งระดับ Priority เกิดจากผลรวมของระดับความเสี่ยงในตารางประเมินความเสี่ยง (Risk Matrix) แสดงในตารางที่ 2.4 และระดับของ Gap แสดงในตารางที่ 2.5

ตารางที่ 2.3 Risk Matrix

โอกาสที่จะเกิด (Likelihood)	ความเสียหาย (Impact)			
	ระดับ (Level)	Low (1)	Medium (2)	High (3)
	High (3)	1x3	2x3	3x3
	Medium (2)	1x2	2x2	3x2
	Low (1)	1x1	2x1	3x1

ตารางที่ 2.4 การแบ่งระดับ Priority

ระดับ	คำอธิบาย
High	ระดับ “High” จำเป็นต้องแก้ไขทันที มีคะแนนระหว่าง 9 – 12 คะแนน
Medium	ระดับ “Medium” ควรแก้ไขภายใน 3 เดือน มีคะแนนระหว่าง 5 – 8 คะแนน
Low	ระดับ “ Low” ควรแก้ไขภายใน 1 ปี มีคะแนนระหว่าง 1 – 4 คะแนน

ตารางที่ 2.5 การแบ่งระดับ Gap

ระดับ	คำอธิบาย
	มีช่องว่างในการทำงานและควรแก้ไข
	ไม่มีช่องว่างในการทำงาน
	ไม่มีช่องว่างในการทำงาน แต่ควรมีการแก้ไข

การประเมินความเสี่ยงดังกล่าวเพื่อเป็นแนวทางในการตัดสินใจถึงความสำคัญของการจัดการความเสี่ยงแต่ละเรื่อง และเพื่อให้ผู้บริหารสามารถจัดลำดับความสำคัญของความเสี่ยง (Prioritization) ที่จำเป็นต้องได้รับการจัดการอย่างเป็นลำดับ รวมไปถึงใช้เป็นแนวทางในการตัดสินใจเลือกวิธีที่เหมาะสมในการจัดการกับความเสี่ยงนั้น ๆ

2.1.16.2 ความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ

1) การเปลี่ยนแปลงต่อสภาพแวดล้อมทางธุรกิจและเทคโนโลยีที่รวดเร็ว (Agility Risk) สภาพแวดล้อมการเปลี่ยนแปลงทางธุรกิจเป็นไปอย่างรวดเร็ว มีการนำนวัตกรรมและเทคโนโลยีใหม่มาใช้ในการเพิ่มประสิทธิภาพและปรับปรุงผลิตภัณฑ์/บริการแก่ลูกค้าในหลายหลายรูปแบบ จึงต้องมีการเตรียมการใช้เท่าทันกับการเปลี่ยนแปลงในมิติต่าง ๆ เพื่อพร้อมแข่งขันในตลาดธุรกิจ

2) การป้องกันภัยคุกคามทางไซเบอร์ (Cyber Risk) ภัยคุกคามทางไซเบอร์ปัจจุบันมีแนวโน้มที่เพิ่มขึ้นซับซ้อนมากขึ้นและแพร่กระจายได้อย่างรวดเร็ว จำเป็นต้องมีมาตรการความปลอดภัยที่รัดกุมและเตรียมการใช้พร้อมรับมือต่อเหตุการณ์ภัยคุกคามรูปแบบต่าง ๆ ที่อาจเกิดขึ้นเพื่อความมั่นคงปลอดภัย รวมทั้งเพื่อช่วยลดความเสี่ยงและผลกระทบเมื่อเหตุการณ์เกิดขึ้น

3) การปฏิบัติการ IT (IT Operation Risk) ที่รองรับการดำเนินการธุรกิจ ระบบ IT ถือเป็นโครงสร้างพื้นฐานหลักที่ใช้รับรองการให้บริการ ซึ่งหากมีการบริหารจัดการและควบคุมทั้งด้านบุคลากร กระบวนการ และระบบที่ไม่เพียงพอ อาจทำให้เกิดช่องโหว่ต่อการรักษาความปลอดภัย ความถูกต้องเชื่อถือได้ของระบบและข้อมูล รวมถึงความพร้อมใช้งานของระบบในการให้บริการ

4) การบริหารจัดการโครงการด้าน IT (IT Project Delivery Risk) ที่มีผลกระทบต่อการดำเนินการธุรกิจ การลงทุนโครงการทางด้าน IT ต้องใช้ทรัพยากรทั้ง เงินทุน บุคลากร และระยะเวลาในการดำเนินโครงการเพื่อบรรลุวัตถุประสงค์ ซึ่งหากไม่สามารถบริหารจัดการโครงการได้อย่างมีประสิทธิภาพ รวมถึงไม่มีการกำกับดูแลและควบคุมติดตามการบริหาร

โครงการอย่างเพียงพอ อาจทำให้โครงการไม่สำเร็จลุล่วงตามแผนและเป้าหมายที่กำหนดจนส่งผลต่อการดำเนินธุรกิจ

2.1.17 มาตรฐาน ITIL

The Information Technology Infrastructure Library (ITIL) เป็นวิธีที่จะช่วยปรับปรุงองค์กรที่ติดตั้งไอที เป็นตัวขับเคลื่อนการทำงาน จุดประสงค์คือเพื่อปรับไอทีให้สามารถเข้ากับธุรกิจ ช่วยควบคุมต้นทุนค่าใช้จ่าย เพิ่มประสิทธิภาพในการใช้งานไอที รวมทั้งสามารถใช้ทรัพยากรไอทีที่มีอยู่ได้มีคุณภาพ

2.17.1 โครงสร้างของ ITIL

ITIL v3 ประกอบขึ้นด้วยข้อมูลอันเป็นแกนหลัก 5 ประการแสดงดังรูปที่ 2.28 ได้แก่

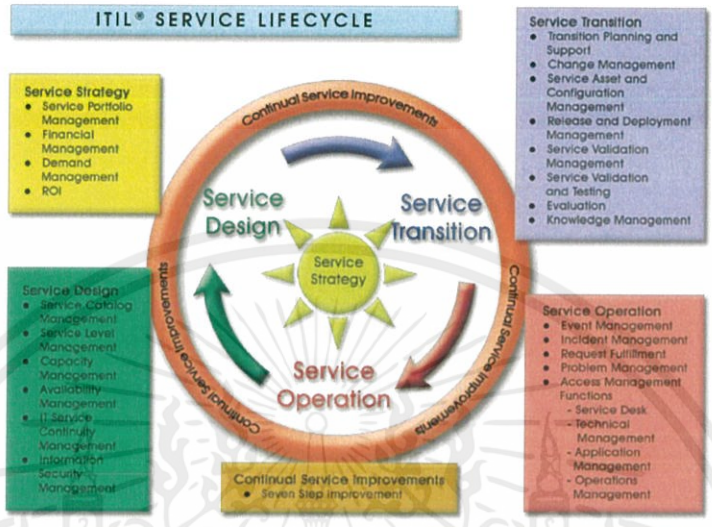
1) Service Strategy เน้นที่วิธีการพิสูจน์ทราบถึงโอกาสในการพัฒนาระบบการให้บริการแก่ตลาดธุรกิจ เพื่อให้สอดคล้องต่อ ความต้องการของผู้ใช้บริการไอทีในองค์กรและลูกค้าที่เข้ารับบริการนอกองคกร์ จุดประสงค์เพื่อให้เกิดผลลัพธ์ของวิธีการบริการที่ดีที่สุด รวมทั้งการออกแบบวิธีการนำเอาระบบให้บริการที่มีประสิทธิภาพไปใช้ตลอดจนการดูแลรักษา และการปรับปรุงแก้ไขกระบวนการบริการที่ต่อเนื่อง กุญแจหลักของ Service Strategy ได้แก่ Service Portfolio Management และ Financial Management

2) Service Design เน้นการออกแบบกิจกรรมที่จะเกิดขึ้นในการะบวนการให้บริการ รวมทั้งการพัฒนากลยุทธ์และวิธีการบริหารจัดการ ระบบบริการ โดยมีกุญแจหลักอยู่ที่ Availability Management หรือความพร้อมที่จะให้บริการ Capacity Management หรือ ขีดความสามารถในการให้บริการอย่างรวดเร็วและมีประสิทธิภาพ รวมทั้ง Continuity Management หรือความสามารถในการให้บริการที่ต่อเนื่อง และ Security Management หรือการบริหารระบบรักษาความปลอดภัย

3) Service Transition เน้นที่การดำเนินการเพื่อให้ได้ผลลัพธ์ของการบริการที่ดีที่สุด รวมทั้งการสรรค์สร้างวิธีการบริการใหม่ ๆ ขึ้น ตลอดจนการปรับปรุงวิธีการบริการที่มีอยู่แล้ว โดยมีข้อมูลบางส่วนคาบเกี่ยวกับ Service Transition และ Service Operation กุญแจสำคัญของ Service Transition ได้แก่ Change Management Configuration Management Release Management และ Service

4) Service Operation เน้นหนักไปทางด้านกิจกรรมที่จำเป็นต่อการปฏิบัติงานเพื่อให้บรรลุผลสำเร็จในการดูแลรักษาหน้าที่การทำงานหรือบริการ ที่เปนไปตามข้อตกลงว่าด้วยพันธะสัญญาบริการ (Service Level Agreement) ที่มีต่อลูกค้า กุญแจหลักของ Service Operation ได้แก่ Incident Management Problem Management และ Request Fulfillment รวมทั้ง Event Management

5) Continual Service Improvement เน้นขีดความสามารถที่จะทำให้เกิดขีดความสามารถในการปรับปรุงให้บริการที่มีคุณภาพอยู่แล้ว ให้มีความต่อเนื่อง โดยมีกุญแจหลักอยู่ที่ Service Reporting, Service Level Management และ Service Measurement



รูปที่ 2.28 โครงสร้างของ ITIL [12]

2.1.17.2 จุดประสงค์หลักของ ITIL

ITIL เป็นกระบวนการทำงานที่ควรจะต้องมีอยู่ในองค์กรเพื่อบริการโครงสร้างพื้นฐานและระบบการทำงานของไอที ให้เกิดประสิทธิภาพสูงสุดด้วยค่าใช้จ่ายที่ประหยัดที่สุด จุดประสงค์หลักของ ITIL สามารถแบ่งเป็นหัวข้อหลักได้ดังนี้

1) Cost Reduction การบริหาร ไอที อย่างเป็นระบบและมีแบบแผนจะช่วยให้สามารถนำทรัพยากรมาใช้งานได้อย่างเต็มประสิทธิภาพ สามารถลดความสูญเสีย ช่วยให้สามารถลดต้นทุนการดำเนินการบริหารจัดการได้ดียิ่งขึ้น

2) Improve Availability ITIL มีเป้าหมายเพื่อช่วยให้มีความพร้อมด้านการให้บริการ รวมทั้งช่วยให้ทรัพยากรระบบไอทีมีความพร้อมที่จะให้บริการอย่างต่อเนื่องและแม้ว่าจะมีเหตุการณ์ที่ไม่คาดคิดเกิดขึ้นก็จะสามารถนำระบบกลับคืนสู่การให้บริการได้เร็วที่สุด

3) Tune Capacity สมรรถภาพได้มาจากความพร้อม ซึ่งความพร้อมในที่นี้หมายถึงความพร้อมของทีมงานดูแล ตลอดจนทรัพยากรที่เกี่ยวข้องกับการให้บริการ การบริหารขีดความสามารถของ ITIL จะช่วยให้มีการทดสอบและการประเมินประสิทธิภาพการให้บริการของโครงสร้างพื้นฐานไอที ซึ่งจะนำไปสู่การวางแผนการปรับปรุงเพื่อรักษาประสิทธิภาพของการให้บริการ

4) Increase Throughput ITIL จะช่วยเพิ่มผลลัพธ์จากกระบวนการทำงานที่มีแบบแผน มีการใช้ทรัพยากรอย่างมีประสิทธิภาพ ช่วยเพิ่มผลลัพธ์ที่สามารถคาดหวัง

5) Optimize Resource Utilization ITIL จะช่วยให้สามารถจัดหาและบริหารจัดการทรัพยากรที่จำเป็นต่อการบริการระบบไอทีด้วยการวางแผนและควบคุมดูแลการใช้งานอย่างมีประสิทธิภาพ ช่วยให้สามารถใช้งานทรัพยากรได้อย่างเต็มที่และตรงกับงานที่ทำ ซึ่งไม่เพียงแต่เพิ่มประสิทธิภาพเท่านั้น ยังช่วยลดความสูญเสียที่ไม่จำเป็นในการใช้งานทรัพยากรด้วย

6) Improve Scalability ITIL จะช่วยเพิ่มขีดความสามารถในการให้บริการสามารถปรับแต่งลักษณะของการให้บริการที่สอดคล้องกับขนาดและความต้องการของผู้ใช้บริการ

บทที่ 3

การออกแบบและการจัดทำโครงงาน

ในขั้นตอนการดำเนินงาน ส่วนแรกจะเป็นการเก็บ configuration ของอุปกรณ์ที่ผู้จัดทำเข้าไป Assessment จากนั้นทำการติดตั้งโปรแกรมมอนิเตอร์เพื่อดูประสิทธิภาพการทำงานของอุปกรณ์ และทำการประเมินความเสี่ยงที่อาจเกิดขึ้นได้ แล้วจึงออกแบบระบบใหม่ให้สอดคล้องกับการทำงานขององค์กรมากยิ่งขึ้น

3.1 การออกแบบ

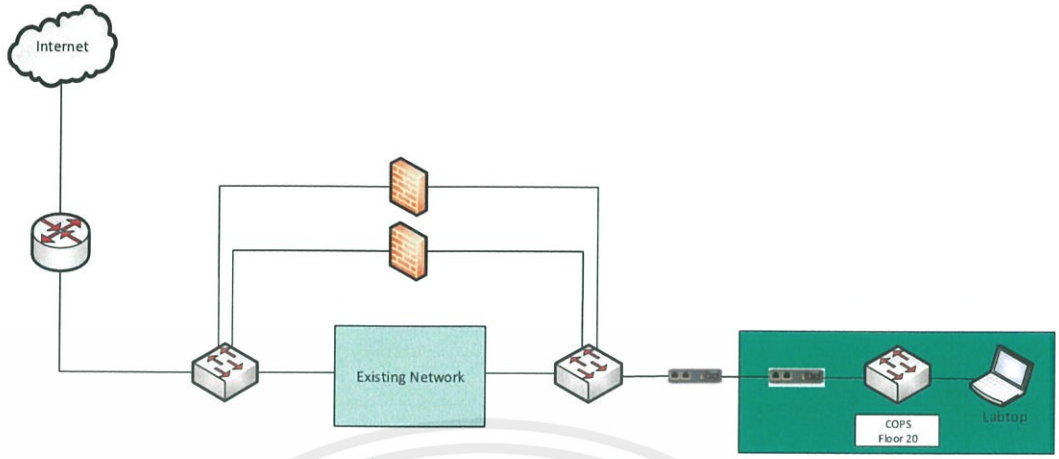
3.1.1 การออกแบบระบบ

โครงงานนี้จะเป็นการตรวจสอบระบบเครือข่ายขององค์กร ทำการเก็บข้อมูลของระบบเครือข่ายเดิม ใช้โปรแกรมมอนิเตอร์เก็บผลการทำงานของอุปกรณ์ และทำการวิเคราะห์ผล ประเมินความเสี่ยงตามมาตรฐาน ITIL แล้วจึงทำการแก้ไขความเสี่ยงด้วยการออกแบบระบบเครือข่ายใหม่ ทำการเปลี่ยนอุปกรณ์และตั้งค่าการทำงานให้เหมาะสมกับการใช้งานภายในองค์กร จากนั้นจึงจัดทำเอกสารสรุปผลพร้อมกับคำแนะนำในการปรับปรุงระบบให้กับทางองค์กร

รูปที่ 3.1 แผนภาพโครงงาน

3.1.2 การออกแบบระบบใหม่

ในการออกแบบระบบใหม่ได้ออกแบบให้สอดคล้องกับการทำงานขององค์กร จะมีการเพิ่มสวิตช์หนึ่งตัวและไฟร์วอลล์สองตัวเพื่อให้ทราฟฟิคของอุปกรณ์วิ่งผ่านไฟร์วอลล์ตัวใหม่แทน และหากมีไฟร์วอลล์ตัวไหนเกิดเสียก็สามารถเปลี่ยน Gateway ไปที่ไฟร์วอลล์อีกตัวหนึ่งเพื่อใช้งานต่อได้ โดยจะเก็บผลการทำงานด้วยโปรแกรมมอนิเตอร์ ระบบเครือข่ายใหม่ที่ออกแบบแสดงในรูปที่แสดงดังรูปที่ 3.2



รูปที่ 3.2 ระบบเครือข่ายที่ออกแบบ

3.2 เครื่องมือที่ใช้ในการทดลอง

โครงงานนี้ มีอุปกรณ์และเครื่องมือที่ใช้ในการทดลองดังนี้

1. Juniper SRX240
2. Check Point 4400
3. Fortigate 110C
4. Juniper SSG20
5. FortiAnalyzer 100C
6. Cisco 1841
7. Astaro 110/120
8. Cisco ASA5505
9. Sonic Wall APL24-08E C-11189
10. Cyberoam CR25i
11. WatchGuard XTM 330
12. Juniper MX80
13. Foundry Edgelron 2402CF
14. Juniper IDP 75
15. Cisco 3500XL
16. HP Tipping Point 2400E
17. netintact packetlogic PL7800
18. Cisco 3500XL

19. IPOQUE PRX-2G
20. Cisco 3560
21. DELL PowerEdge 860
22. DELL PowerEdge R610
23. HP Tipping Point SMS Server
24. DELL PowerEdge 860
25. DELL PowerEdge 1950
26. SUPERMICRO SUPERO
27. IBM System x3650
28. PRTG Network Monitor
29. Cisco 3560-CG Series
30. FortiWiFi 90D
31. paloalto PA-200

3.3 การจัดเก็บผลการทดลอง

3.3.1 จัดเก็บ Configuration ของอุปกรณ์

ในส่วนของการเก็บ configuration ของอุปกรณ์ จะเป็นการจัดเก็บเพื่อนำมาวิเคราะห์ระบบเครือข่ายว่ามีการใช้งานอะไรบ้าง โดยค่าที่สนใจจะมี เรื่องของ IP address, Interfaces, Routing, VLAN เป็นต้น

3.3.2 ทดสอบการใช้งานการ Ping ออกอินเตอร์เน็ต

เป็นการเก็บผลการใช้งาน Ping ออกอินเตอร์เน็ตด้วยโปรแกรม PRTG Network Monitor ของระบบเดิมและนำผลลัพธ์ที่ได้มาเปรียบเทียบกับการ Ping ออกอินเตอร์เน็ตของระบบใหม่

3.3.3 การตรวจสอบระบบเครือข่าย

ในการตรวจสอบระบบเครือข่ายทางผู้จัดทำได้ทำตารางการตรวจสอบระบบเครือข่าย เพื่อตรวจสอบว่าระบบเครือข่ายในปัจจุบันนั้นมีหรือไม่มีอะไรบ้างแสดงในตารางที่ 3.1 จากนั้นจึงประเมินความเสี่ยงในแต่ละด้านแล้วจึงนำความเสี่ยงแต่ละด้านมารวมกันและให้ระดับ GAP พร้อมกับให้คำแนะนำในการปรับปรุงระบบเครือข่ายแสดงในตารางที่ 3.2

ตารางที่ 3.1 ระบบเครือข่ายในปัจจุบัน

รายการ	คำอธิบาย
1. Network Design	
1.1 Network Overview Architecture	
Review for Modularity, scalability, and capabilities	
1.2 Traffic Flow	
Application Traffic Flow, Datacenter, Internet Edges, Client Access, WAN, Cloud	
1.3 Services and OLA's	
High Availability, OLA/SLA if defined	
1.4 MPLS/VPN Service	
Remote Office and Client Access Capabilities	
1.5 QOS Standards	
Deployment methods, OLA's	
1.6 Layer 3 Routing	

ตารางที่ 3.1 ระบบเครือข่ายในปัจจุบัน (ต่อ)

รายการ	คำอธิบาย
Dynamic, optimized, secure	
1.7 Layer 2 Optimization	
Spanning-tree security/optimization, distributed Layer 2	
2. Physical Inventory	
2.1 Hardware Inventory Spreadsheet	
Physical Hardware Inventory – Serial Numbers if Possible	
2.2 Layer 1-2 Diagrams/Documentation	
Physical interconnectivity	
2.3 Layer 3 Diagrams/Documentation	
Routing Connectivity, Gateway Management, Summarization, Route Entrances/Exits	

ตารางที่ 3.1 ระบบเครือข่ายในปัจจุบัน (ต่อ)

รายการ	คำอธิบาย
2.4 Rack Elevation Diagrams/Documentation	
Physical Rack Diagrams	
2.5 Environmental Capabilities	
Power, cooling, and cable management	
3. Infrastructure Monitoring and Management	
3.1 Central Monitoring/Alerting Capabilities	
Management Platform utilization/capabilities	
3.2 Syslog Capabilities	
Controls, retention, management	
3.3 EoL/EoS hardware and licensing	
Process for Lifecycle and licensing compliance	
4. Configuration Management	
4.1 Centralized Configuration Backup	

ตารางที่ 3.1 ระบบเครือข่ายในปัจจุบัน (ต่อ)

รายการ	คำอธิบาย
Configuration backups	
4.2 Centralized Configuration Automation	
Configuration change capabilities	
4.3 Configuration Change Management Workflow	
Change Control Management	
5. Performance Monitoring and Analysis	
5.1 Netflow Capabilities	
Bandwidth Planning Capabilities	
5.2 Client Experience Capabilities	
L4-L7 Visibility – Baseline Capabilities	

ตารางที่ 3.2 การประเมินความเสี่ยง

รายการ	ความเสี่ยง				Priority และ Gap	ข้อเสนอแนะ
	ความรวดเร็ว	ภัยคุกคาม	การปฏิบัติการ	การบริหารจัดการ		
1. Network Design						
1.1 Network Overview Architecture						
Review for Modularity, scalability, and capabilities						
1.2 Traffic Flow						
Application Traffic Flow, Datacenter, Internet Edges, Client Access, WAN, Cloud						
1.3 Services and OLA's						
High Availability, OLA/SLA if defined						

ตารางที่ 3.2 การประเมินความเสี่ยง (ต่อ)

รายการ	ความเสี่ยง				Priority และ Gap	ข้อเสนอแนะ
	ความรวดเร็ว	ภัยคุกคาม	การปฏิบัติการ	การบริหารจัดการ		
1.4 MPLS/VPN Service						
Remote Office and Client Access Capabilities						
1.5 QOS Standards						
Deployment methods, OLA's						
1.6 Layer 3 Routing						
Dynamic, optimized, secure						
1.7 Layer 2 Optimization						
Spanning-tree security/optimization, distributed Layer 2						

ตารางที่ 3.2 การประเมินความเสี่ยง (ต่อ)

รายการ	ความเสี่ยง				Priority และ Gap	ข้อเสนอแนะ
	ความรวดเร็ว	ภัยคุกคาม	การปฏิบัติการ	การบริหารจัดการ		
2. Physical Inventory						
2.1 Hardware Inventory Spreadsheet						
Physical Hardware Inventory – Serial Numbers if Possible						
2.2 Layer 1-2 Diagrams/Documentation						
Physical interconnectivity						
2.3 Layer 3 Diagrams/Documentation						
Routing Connectivity, Gateway Management, Summarization, Route Entrances/Exits						

ตารางที่ 3.2 การประเมินความเสี่ยง (ต่อ)

รายการ	ความเสี่ยง				Priority และ Gap	ข้อเสนอแนะ
	ความรวดเร็ว	ภัยคุกคาม	การปฏิบัติการ	การบริหารจัดการ		
2.4 Rack Elevation Diagrams/Documentation						
Physical Rack Diagrams						
2.5 Environmental Capabilities						
Power, cooling, and cable management						
3. Infrastructure Monitoring and Management						
3.1 Central Monitoring/Alerting Capabilities						
Management Platform utilization/capabilities						
3.2 Syslog Capabilities						
Controls, retention, management						
3.3 EoL/EoS hardware and licensing						

ตารางที่ 3.2 การประเมินความเสี่ยง (ต่อ)

รายการ	ความเสี่ยง				Priority และ Gap	ข้อเสนอแนะ
	ความรวดเร็ว	ภัยคุกคาม	การปฏิบัติการ	การบริหารจัดการ		
Process for Lifecycle and licensing compliance						
4. Configuration Management						
4.1 Centralized Configuration Backup						
Configuration backups						
4.2 Centralized Configuration Automation						
Configuration change capabilities						
4.3 Configuration Change Management Workflow						
Change Control Management						
5. Performance Monitoring and Analysis						
5.1 Netflow Capabilities						

ตารางที่ 3.2 การประเมินความเสี่ยง (ต่อ)

รายการ	ความเสี่ยง				Priority และ Gap	ข้อเสนอแนะ
	ความรวดเร็ว	ภัยคุกคาม	การปฏิบัติการ	การบริหารจัดการ		
Bandwidth Planning Capabilities						
5.2 Client Experience Capabilities						
L4-L7 Visibility – Baseline Capabilities						

3.3.4 สิ่งที่ดำเนินการแก้ไขหลังตรวจสอบระบบเครือข่าย

3.3.4.1 ออกแบบระบบเครือข่ายใหม่

ในการออกแบบระบบเครือข่ายใหม่จะออกแบบตั้งแต่ โครงสร้างระบบ หมายเลข IP การ Routing VLAN และการเปลี่ยนอุปกรณ์

3.3.4.2 การ Configuration ระบบใหม่

การตั้งค่า (config) จะตั้งค่าให้เหมาะสมกับการทำงานของทางองค์กรและตั้งค่าโปรโตคอล SNMP เพื่อใช้ในการมอนิเตอร์

3.3.4.3 มอนิเตอร์ระบบเครือข่ายใหม่

เมื่อตั้งค่าระบบเครือข่ายใหม่เสร็จเรียบร้อยแล้วจึงมอนิเตอร์ระบบเครือข่ายใหม่เพื่อเก็บผลการทำงานและนำผลมาเปรียบเทียบกับระบบเดิม

3.3.7.4 เอกสารส่งมอบลูกค้า

จัดทำเอกสารทุกอย่างที่เกี่ยวกับระบบเครือข่ายให้เป็นปัจจุบัน เอกสารการประเมินความเสี่ยงพร้อมคำแนะนำในการปรับปรุงระบบ จากนั้นจึงส่งมอบแก่ลูกค้า

บทที่ 4

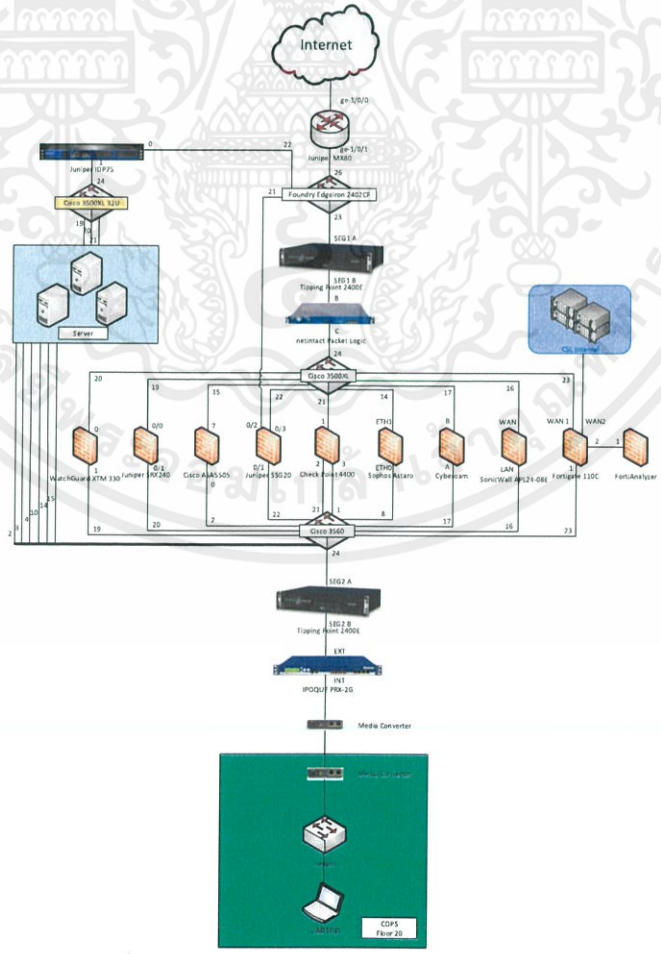
ผลการทดลอง

4.1 โครงสร้างระบบเครือข่ายเดิม

ในหัวข้อนี้จะแสดงโครงสร้างระบบเครือข่ายเดิม (Network Diagram) รายชื่ออุปกรณ์ หมายเลข IP ของอุปกรณ์ Rack Diagram และพอร์ตที่เชื่อมต่อกับอุปกรณ์ต่าง ๆ ของระบบเครือข่าย โดยจะขอยกตัวอย่างเพียงสวิตช์ Cisco 3560 และอุปกรณ์อื่นจะแสดงในภาคผนวก ข

4.1.1 Network Diagram

Network Diagram ของระบบเครือข่ายเดิมที่ผู้จัดทำได้เข้าไปสำรวจ จะแสดงในรูปที่ 4.1 และรายชื่ออุปกรณ์แสดงดังตารางที่ 4.1 โดยองค์กรที่ได้ทำการตรวจสอบนี้เป็นองค์กรที่เกี่ยวกับอุตสาหกรรมไอที จึงได้มีการใช้งานไฟร์วอลล์เป็นจำนวนมากเพื่อทดสอบระบบให้กับทางลูกค้าขององค์กร การเชื่อมต่อของระบบเครือข่ายนี้จะต้องผ่านอุปกรณ์เป็นจำนวนมากก่อนออกสู่อินเตอร์เน็ต และมีไฟร์วอลล์ที่ใช้งานหลักคือ Fortigate 110c จึงทำให้มีเพียงเส้นทางเดียวที่ใช้ออกสู่อินเตอร์เน็ต



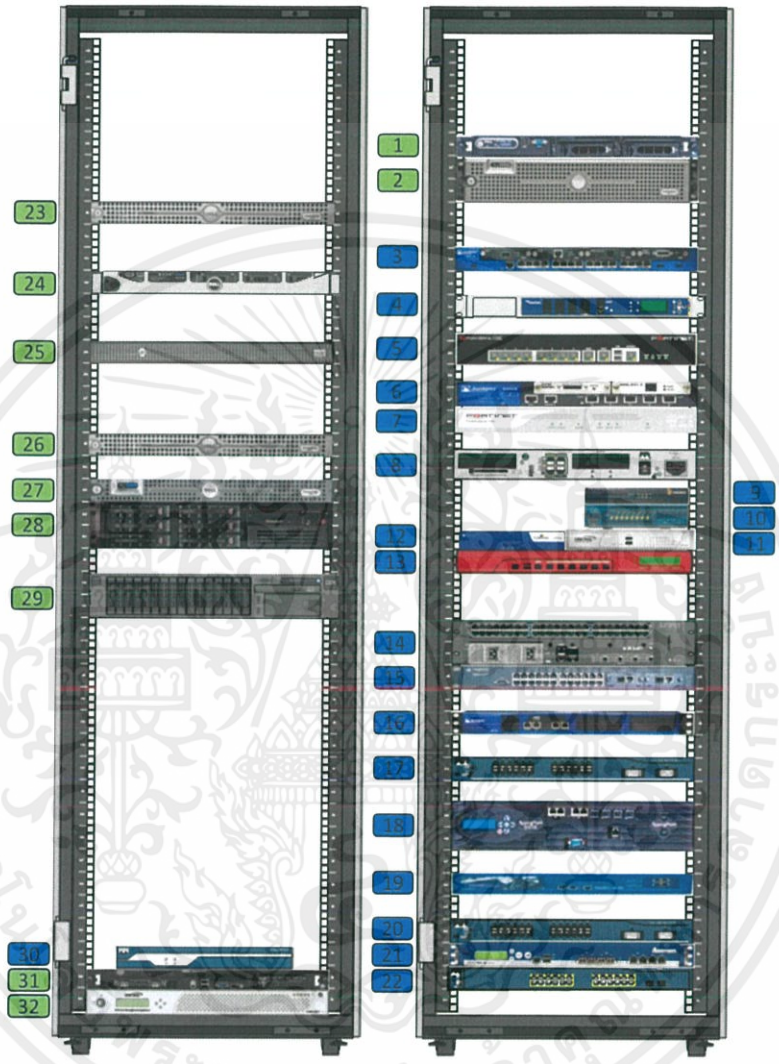
รูปที่ 4.1 Network Diagram ของระบบเดิม

ตารางที่ 4.1 รายชื่ออุปกรณ์ของระบบเครือข่ายเดิม

No.	Devices	IP Management	Access Method	Ref.
1	DELL PowerEdge 1950	-	-	2.2.2
2	DELL PowerEdge 2950	-	-	2.2.3
3	Juniper SRX240	192.168.99.15	HTTP	2.2.4
4	Check Point 4400	-	-	2.2.5
5	Fortigate 110C	202.183.152.6	HTTP	2.2.6
6	Juniper SSG20	192.168.100.1	SSH	2.2.7
7	FortiAnalyzer 100C	192.168.2.99	HTTP	2.2.8
8	Cisco 1841	-	-	2.2.9
9	Sophos Astaro 110/120	192.168.1.1	HTTP	2.2.10
10	Cisco ASA5505	58.137.180.2	console	2.2.11
11	Sonic Wall APL24-08E C-11189	-	-	2.2.12
12	Cyberoam CR25i	58.137.88.5	HTTP	2.2.13
13	WatchGuard XTM 330	192.168.99.11	HTTP	2.2.14
14	Juniper MX80	58.137.59.17	console	2.2.15
15	Foundry Edgelron 2402CF	1.1.1.2	Telnet	2.2.16
16	Juniper IDP 75	-	-	2.2.17
17	Cisco 3500XL	1.1.1.3	console, Telnet	2.2.18
18	HP Tipping Point 2400E	58.137.32.102	HTTP	2.2.19
19	netintact packetlogic PL7800	-	-	2.2.20
20	Cisco 3500XL	1.1.1.4	console,Telnet	2.2.21
21	IPOQUE PRX-2G	58.137.59.19	HTTP	2.2.22
22	Cisco 3560	192.168.100.10	console, Telnet, SSH	2.2.23
23	DELL PowerEdge 860	-	-	2.2.24
24	DELL PowerEdge R610	-	-	2.2.25
25	HP Tipping Point SMS Server	-	-	2.2.26
26	DELL PowerEdge 860	-	-	2.2.27
27	DELL PowerEdge 1950	-	-	2.2.28
28	SUPERMICRO SUPERO	-	-	2.2.29
29	IBM System x3650	-	-	2.2.30
30	Cisco 1800 Series	-	-	2.2.31
31	DELL PowerEdge R200	-	-	2.2.32
32	SonicWall UMA EM	-	-	2.2.33

4.1.2 Rack Diagram

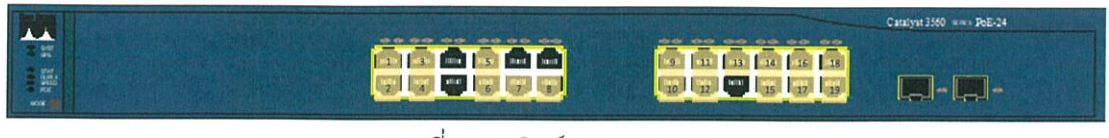
Rack Diagram ของระบบเครือข่ายเดิม แสดงในรูปที่ 4.2



รูปที่ 4.2 Rack Diagram ของระบบเครือข่ายเดิม

4.1.3 Port ที่เชื่อมต่อกับอุปกรณ์

อุปกรณ์สวิตช์ Cisco 3560 แสดงดังรูปที่ 4.3 รายละเอียดข้อมูลของอุปกรณ์แสดงดังตาราง ที่ 4.2 และ พอร์ตที่เชื่อมต่อกับอุปกรณ์ต่าง ๆ แสดงดังตารางที่ 4.3



รูปที่ 4.3 สวิตช์ Cisco 3560

ตารางที่ 4.2 รายละเอียดอุปกรณ์

Hostname	COPS_LAN_FW	IP Address	192.168.100.10
Brand	Cisco	Model	WS-C3560-24TS
Serial Number	CAT0951Z1PW	Software Version	12.2 (25) SEE2
Location	Data Center	EOL Status	EOL[3]
License Type	-	License Expire Date	-

ตารางที่ 4.3 การเชื่อมต่อของอุปกรณ์

Source Device		Destination Devices		
No.	Port	Connect to	Port	Ref.
1	Fa0/1	Check Point 4400	3	2.2.5
2	Fa0/2	DELL PowerEdge 1950	Gb1	2.2.28
3	Fa0/3	SUPERMICRO SUPERO	Eth0	2.2.29
4	Fa0/4	IBM System x3650	2	2.2.30
5	Fa0/7	Cisco ASA5505	Eth0/0	2.2.11
6	Fa0/8	Astaro 110/120	Eth0	2.2.10
7	Fa0/10	IBM System x3650	1	2.2.30
8	Fa0/12	IPOQUE PRX-2G	MGT	2.2.22
9	Fa0/13	netintact packetlogic PL7800	Admin	2.2.20
10	Fa0/14	DELL PowerEdge 1950	Gb2	2.2.28
11	Fa0/15	DELL PowerEdge R610	Gb2	2.2.25
12	Fa0/16	Sonic Wall APL24-08E C-11189	LAN	2.2.12
13	Fa0/17	Cyberoam CR25i	A	2.2.13
14	Fa0/19	WatchGuard XTM 330	1	2.2.14
15	Fa0/20	Juniper SRX240	0/1	2.2.4
16	Fa0/21	Check Point 4400	2	2.2.5
17	Fa0/22	Juniper SSG20	Eth0/1	2.2.7
18	Fa0/23	Fortigate 110C	1	2.2.6
19	Fa0/24	HP Tipping Point 2400E	SEG2 A	2.2.19

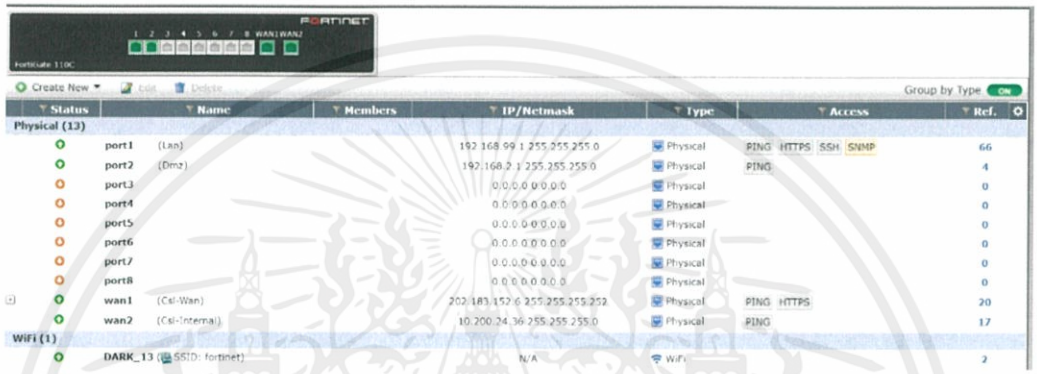
4.2 การตั้งค่าอุปกรณ์เครือข่ายเดิม

ในส่วนของการตั้งค่าระบบเครือข่ายเดิมทางผู้จัดทำจะแสดงการตั้งค่าของไฟร์วอลล์ Fortigate 110c เพียงตัวเดียว โดยการตั้งค่าของอุปกรณ์อื่นจะแสดงในภาคผนวก ก

4.2.1 Fortigate 110c

4.2.1.1 Interfaces

อินเตอร์เฟสที่ใช้ในการเชื่อมต่อแสดงในรูปที่ 4.4



รูปที่ 4.4 อินเตอร์เฟสของไฟร์วอลล์ Fortigate 110c

4.2.1.2 Routing

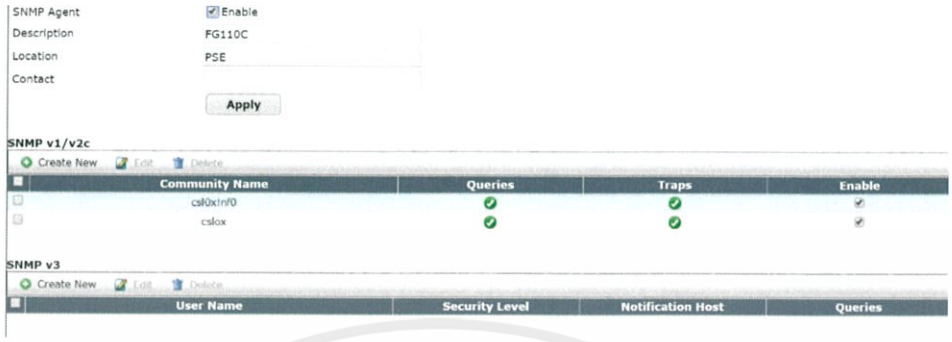
Static Route ของไฟร์วอลล์ Fortigate 110c แสดงในรูปที่ 4.5

IP/Netmask	Gateway	Device	Comment
0.0.0.0 0.0.0.0	202.183.152.5	wan1	
10.0.0.0 255.0.0.0	10.200.24.254	wan2	
10.1.1.0 255.255.255.0	192.168.99.15	port1	Juniper SRX
10.10.3.0 255.255.255.0	Test_AWN		VPN: Test_AWN (Created by VPN w...
10.15.200.0 255.255.255.0	To_Koyo		
10.212.134.0 255.255.255.0	ssl.root		
11.11.11.0 255.255.255.0	192.168.99.13	port1	CheckPoint
172.11.11.0 255.255.255.0	192.168.99.13	port1	CheckPoint DMZ
192.168.1.0 255.255.255.0	192.168.99.17	port1	Sophos
192.168.11.0 255.255.255.0	192.168.99.11	port1	WatchGuard
192.168.69.0 255.255.255.0	192.168.99.16	port1	PaloAlto
192.168.93.0 255.255.255.0	192.168.99.12	port1	Cyberoam
192.168.100.0 255.255.255.0	192.168.99.10	port1	Juniper SSG
192.168.168.0 255.255.255.0	192.168.99.14	port1	Sonicwall
203.146.4.20 255.255.255.255	10.200.24.254	wan2	
203.146.16.10 255.255.255.255	10.200.24.254	wan2	
203.146.30.0 255.255.255.0	10.200.24.254	wan2	
203.146.43.0 255.255.255.0	10.200.24.254	wan2	
203.146.64.0 255.255.255.0	10.200.24.254	wan2	
203.146.88.240 255.255.255.240	10.200.24.254	wan2	
203.146.237.222 255.255.255.255	10.200.24.254	wan2	
203.146.237.242 255.255.255.255	10.200.24.254	wan2	
203.170.160.159 255.255.255.255	10.200.24.254	wan2	

รูปที่ 4.5 Static Route ของไฟร์วอลล์ Fortigate 110c

4.2.1.3 โปรโตคอล SNMP

โปรโตคอล SNMP ของไฟร์วอลล์ Fortigate 110c แสดงในรูปที่ 4.6



รูปที่ 4.6 โปรโตคอล SNMP ของไฟร์วอลล์ Fortigate 110c

4.2.1.4 Policy

Policy ของไฟร์วอลล์ Fortigate 110c แสดงในรูปที่ 4.7 และ รูปที่ 4.8

รูปที่ 4.7 Policy ของไฟร์วอลล์ Fortigate 110c

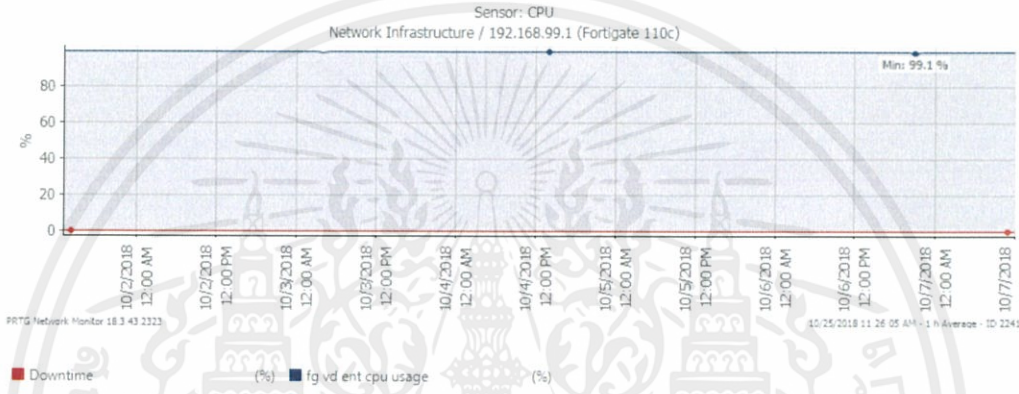
รูปที่ 4.8 Policy ของไฟร์วอลล์ Fortigate 110c (ต่อ)

4.3 ผลการมอนิเตอร์ระบบเครือข่ายเดิม

การมอนิเตอร์ระบบเครือข่ายเป็นส่วนหนึ่งของมาตรฐาน ITIL โดยในหัวข้อนี้ทางผู้จัดทำจะขอแสดงผลการมอนิเตอร์ของไฟร์วอลล์ Fortigate 110c เพียงตัวเดียวและผลมอนิเตอร์ Traffic เพียงอินเตอร์เฟสเดียว โดยจะแสดงผลมอนิเตอร์ของอุปกรณ์ที่เหลือในภาคผนวก ค

4.3.1 ผลการมอนิเตอร์ CPU

ผลการมอนิเตอร์ CPU ที่เก็บ เก็บในวันที่ 1/10/18 12:00:00 PM – 7/10/18 12:00:00 PM แสดงในรูปที่ 4.9 และแสดงค่าในตารางที่ 4.4



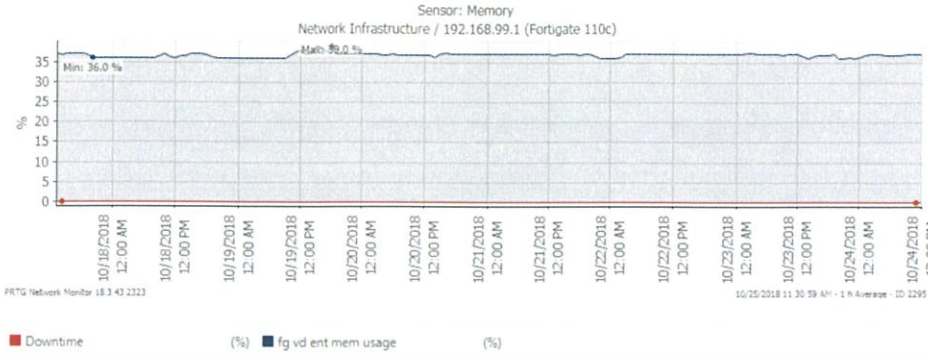
รูปที่ 4.9 ผลการมอนิเตอร์ CPU ไฟร์วอลล์ Fortigate 110c

ตารางที่ 4.4 ผลการใช้งาน CPU ไฟร์วอลล์ Fortigate 110c

	CPU Usage	Down time
Maximum	99.4 %	0 %
Average	99 %	0 %
Minimum	99.1 %	0 %

4.3.2 ผลการมอนิเตอร์ Memory

ผลการมอนิเตอร์ Memory ที่เก็บ เก็บในวันที่ 9/10/18 12:00:00 AM – 16/10/18 12:00:00 AM แสดงในรูปที่ 4.10 และแสดงค่าในตารางที่ 4.5



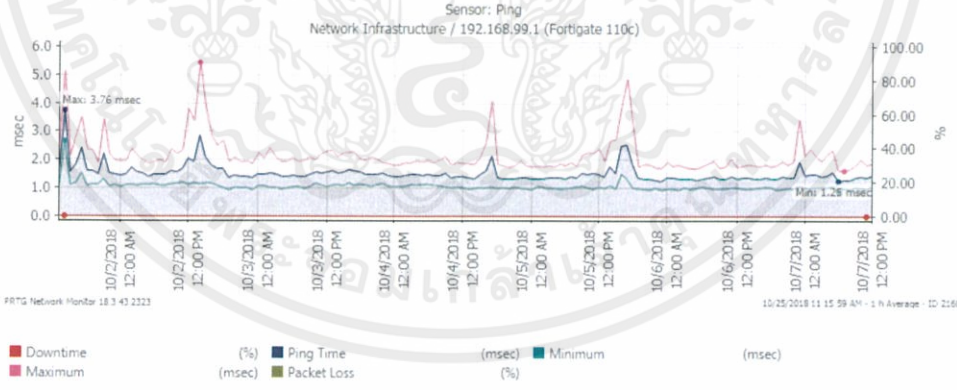
รูปที่ 4.10 ผลการมอนิเตอร์ Memory ไฟร์วอลล์ Fortigate 110c

ตารางที่ 4.5 ผลการใช้งาน Memory ไฟร์วอลล์ Fortigate 110c

	Memory Usage	Down time
Maximum	39 %	0 %
Average	37 %	0 %
Minimum	36 %	0 %

4.3.3 ผลการมอนิเตอร์ Ping

ผลการมอนิเตอร์ Ping ที่เก็บ เก็บในวันที่ 1/10/18 12:00:00 AM – 7/10/18 12:00:00 AM แสดงในรูปที่ 4.11 และแสดงค่าในตารางที่ 4.6



รูปที่ 4.11 ผลการมอนิเตอร์ ไฟร์วอลล์ Fortigate 110c

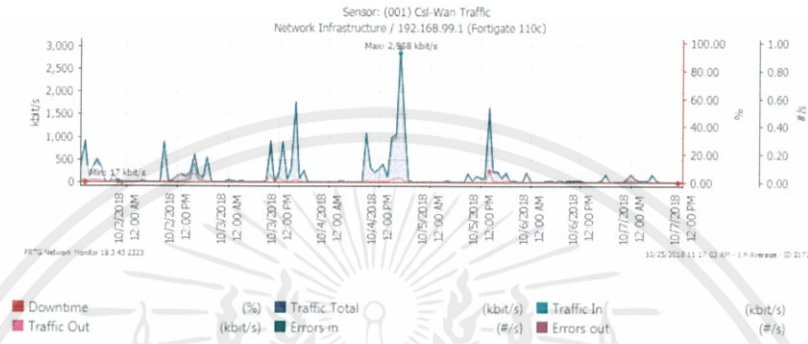
ตารางที่ 4.6 ผลการ Ping ไฟร์วอลล์ Fortigate 110c

	Ping time	Packet Loss	Downtime
Maximum	4.60 msec	0 %	0 %
Average	3 msec	0 %	0 %
Minimum	2.28 msec	0 %	0 %

4.3.4 ผลการมอนิเตอร์ Traffic

4.3.4.1 Interface WAN1

ผลการมอนิเตอร์ Traffic ที่เก็บ เก็บในวันที่ 1/10/18 12:00:00 AM – 7/10/18 12:00:00 AM แสดงในรูปที่ 4.12 และแสดงค่าในตารางที่ 4.7



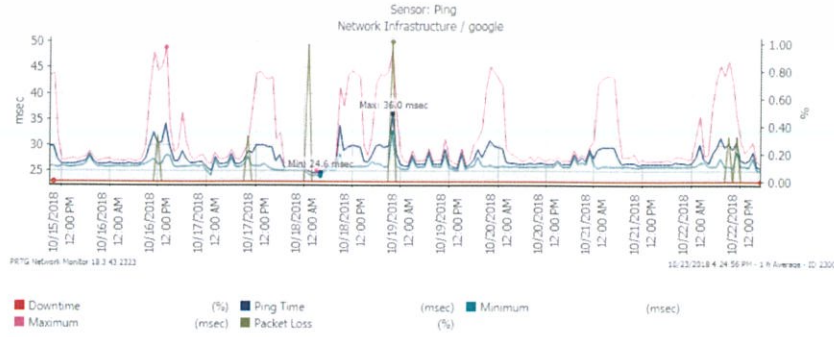
รูปที่ 4.12 ผลการมอนิเตอร์ Traffic ไฟร์วอลล์ Fortigate 110c

ตารางที่ 4.7 ผลการใช้งาน Traffic ที่อินเตอร์เฟส WAN1 ไฟร์วอลล์ Fortigate 110c

	Traffic Total	Traffic In	Traffic Out	Errors in	Errors out	Downtime
Maximum	2,958 kbit/s	2,856 kbit/s	102 kbit/s	0 kbit/s	0 kbit/s	0 %
Average	179 kbit/s	154 kbit/s	25 kbit/s	0 kbit/s	0 kbit/s	0 %
Minimum	17 kbit/s	8 kbit/s	9 kbit/s	0 kbit/s	0 kbit/s	0 %

4.3.5 ผลการมอนิเตอร์ Ping ออกอินเตอร์เน็ต

ผลการมอนิเตอร์ Ping ออกอินเตอร์เน็ตที่เก็บ โดย Ping ไปที่หมายเลข IP 8.8.8.8 ซึ่งเป็นหมายเลข IP ของ Google เก็บผลในวันที่ 15/10/18 12:00:00 PM – 22/10/18 12:00:00 PM แสดงในรูปที่ 4.13 และแสดงค่าในตารางที่ 4.8



รูปที่ 4.13 ผลการมอนิเตอร์ Ping ออกอินเตอร์เน็ตของระบบเครือข่ายเดิม

ตารางที่ 4.8 ผลการ Ping ออกอินเตอร์เน็ตของระบบเครือข่ายเดิม

	Ping time	Packet Loss	Downtime
Maximum	32 msec	0 %	0 %
Average	28 msec	0 %	0 %
Minimum	26 msec	0 %	0 %

4.4 ผลการตรวจสอบระบบเครือข่ายเดิม

จากการสอบถามผู้ใช้งานในองค์กรพบว่าการใช้งานอินเตอร์เน็ตในปัจจุบันใช้งานได้ช้ามาก ทางผู้จัดทำจึงได้นำข้อมูลที่พบเจอระหว่างการออกปฏิบัติงาน ผลที่ได้จากการมอนิเตอร์มาทำการวิเคราะห์เพื่อที่จะทราบถึงระบบเครือข่ายในปัจจุบัน โดยการตรวจสอบระบบเครือข่ายครั้งนี้ได้พบปัญหาหลักคือ ไม่มีการสร้างเส้นทางสำรองไว้เพื่อใช้ในการออกอินเตอร์เน็ต ซึ่งอาจส่งผลกระทบต่อการทำงานได้หากลิงค์เกิดความเสียหาย และปัญหาที่สำคัญอีกอย่างคือ เอกสารที่เกี่ยวข้องกับระบบเครือข่ายไม่เป็นปัจจุบัน เช่น โครงสร้างระบบเครือข่าย หมายเลข IP รหัส (Password) แผนภาพตู้บริการระบบเครือข่ายทำให้การเข้าไปตรวจสอบเป็นไปอย่างลำบาก เมื่อตรวจสอบระบบเครือข่ายเรียบร้อยแล้วผู้จัดทำจึงได้จัดทำตารางแสดงผลการตรวจสอบระบบเครือข่ายแสดงไว้ในตารางที่ 4.9

ตารางที่ 4.9 ผลการตรวจสอบระบบเครือข่ายเดิม

รายการ	คำอธิบาย
1. Network Design	
1.1 Network Overview Architecture	
Review for Modularity, scalability, and capabilities	รองรับการขยายตัวในอนาคตได้เนื่องจากอุปกรณ์อย่างเราเตอร์สามารถต่อโมดูลเพื่อเพิ่มจำนวนอินเตอร์เฟซ และอุปกรณ์อย่างสวิตช์ยังมีอินเตอร์เฟซที่ไม่ได้ใช้งาน แต่มีข้อเสียคือมีทางออกอินเตอร์เน็ตเพียงทางเดียว
1.2 Traffic Flow	
Application Traffic Flow, Datacenter, Internet Edges, Client Access, WAN, Cloud	มี Traffic วิ่งในเวลากลางคืนด้วยความเร็วสูงสุด 4Mb/s โดยเป็นเวลาหลังเลิกงานและไม่มีใครใช้งาน
1.3 Services and OLA's	
High Availability, OLA/SLA if defined	ในการใช้งานอินเตอร์เน็ตไม่มีการทำเส้นทางสำรองไว้เผื่อกรณีลิงค์เสีย อาจทำให้การทำงานต้องหยุดลง
1.4 MPLS/VPN Service	
Remote Office and Client Access Capabilities	มีการทำ VPN เพื่อให้พนักงานในแผนกสามารถเชื่อมต่อระบบเครือข่ายของบริษัทได้เมื่ออยู่นอกสถานที่
1.5 QOS Standards	
Deployment methods, OLA's	ไม่มีการสร้าง QOS เพื่อจัดลำดับความสำคัญของข้อมูล อาจส่งผลให้เมื่อมีพนักงานดู Youtube หรือโหลดบิต จะทำให้ใช้แบนด์วิธจนหมดและพนักงานคนอื่นใช้งานอินเตอร์เน็ตได้ไม่เต็มความเร็ว
1.6 Layer 3 Routing	

ตารางที่ 4.9 ผลการตรวจสอบระบบเครือข่ายเดิม (ต่อ)

รายการ	คำอธิบาย
Dynamic, optimized, secure	อุปกรณ์บางตัวมีการกำหนด Routing ไม่ครอบคลุม ส่งผลให้ต้องผ่านอุปกรณ์หลายตัวกว่าจะเจออุปกรณ์ตัวที่ต้องการ และไม่สามารถมอนิเตอร์ได้
1.7 Layer 2 Optimization	
Spanning-tree security/optimization, distributed Layer 2	อุปกรณ์บางตัวมีการปิดโปรโตคอล Spanning-tree ที่ใช้ในการป้องกันลูปและมี VLAN ที่ใช้ในการทำงานกับ VLAN ที่ใช้ในการจัดการ เป็น VLAN เดียวกัน
2. Physical Inventory	
2.1 Hardware Inventory Spreadsheet	
Physical Hardware Inventory – Serial Numbers if Possible	ไม่รายชื่ออุปกรณ์ไม่เป็นปัจจุบัน อุปกรณ์บางตัวมีหมายเลข IP กับรหัส (Password) ไม่ตรงทำให้ไม่สามารถเข้าไปดูการตั้งค่าได้ และอุปกรณ์บางตัวไม่มีการระบุ Serial Number
2.2 Layer 1-2 Diagrams/Documentation	
Physical interconnectivity	ไม่มีเอกสารระบุการใช้ VLAN และเอกสารการต่อเชื่อมไม่เป็นปัจจุบัน
2.3 Layer 3 Diagrams/Documentation	
Routing Connectivity, Gateway Management, Summarization, Route Entrances/Exits	ไม่มีเอกสารระบุการ Route มีทางออกอินเตอร์เน็ตเพียงทางเดียวและ Route ไม่ครอบคลุมทุกอุปกรณ์

ตารางที่ 4.9 ผลการตรวจสอบระบบเครือข่ายเดิม (ต่อ)

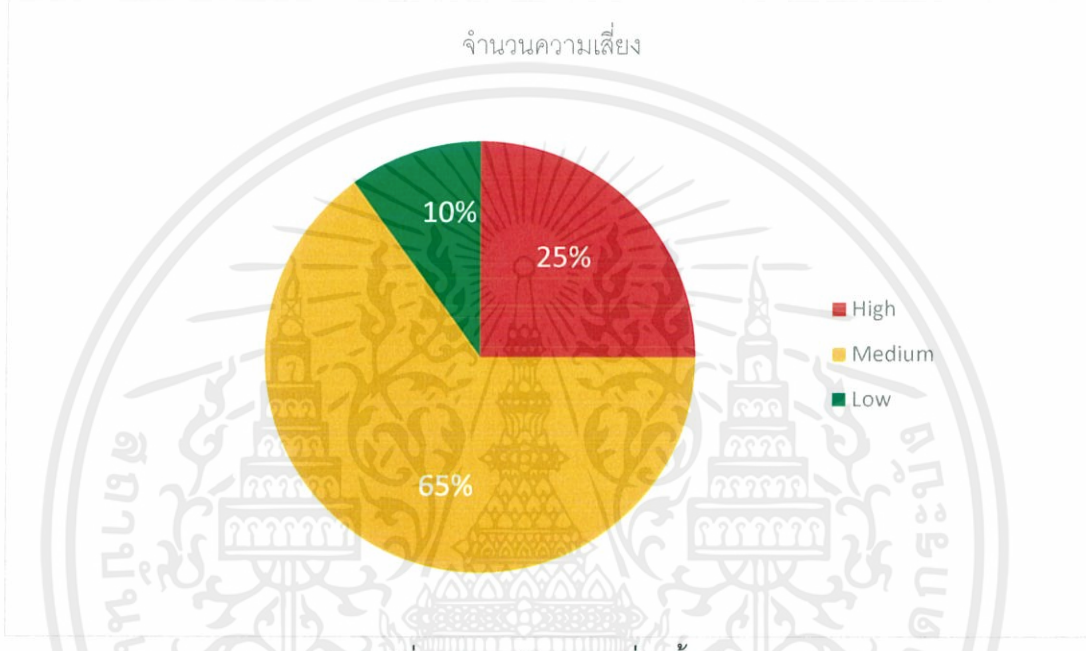
รายการ	คำอธิบาย
2.4 Rack Elevation Diagrams/Documentation	
Physical Rack Diagrams	ไม่มี Rack Diagram และภายในตู้บริการระบบเครือข่ายมีอุปกรณ์บางตัวที่ไม่ใช้และวางทับซ้อนกัน
2.5 Environmental Capabilities	
Power, cooling, and cable management	มีการระบายความเย็นที่ดีเป็นไปตามมาตรฐาน Data Center มีระบบไฟสำรอง แต่ภายในตู้บริการระบบเครือข่ายไม่มีการติดป้ายบอกปลายทางของอุปกรณ์ จัดสายไม่เป็นระเบียบและประเภทสายเป็นมาตรฐาน Cat 5e ซึ่งไม่รองรับการใช้งานในอนาคต
3. Infrastructure Monitoring and Management	
3.1 Central Monitoring/Alerting Capabilities	
Management Platform utilization/capabilities	ไม่มีการมอนิเตอร์เพื่อดูการทำงานของอุปกรณ์หรือแจ้งเตือนเมื่ออุปกรณ์เกิดการผิดปกติ ทำให้ไม่ทราบต้นเหตุของความผิดปกติที่เกิดขึ้นได้
3.2 Syslog Capabilities	
Controls, retention, management	ทางองค์กรมีอุปกรณ์ FortiAnalyzer ที่ใช้สำหรับบันทึกการใช้งาน แต่ไม่ได้บันทึกข้อมูลการใช้งาน
3.3 EoL/EoS hardware and licensing	
Process for Lifecycle and licensing compliance	อุปกรณ์หลายตัวหมดประกันและไม่ได้รับการสนับสนุนจากทางผู้ผลิต ไม่มีการต่อ license เพื่อใช้งานฟีเจอร์ต่าง ๆ เช่น Antivirus ในไฟร์วอลล์
4. Configuration Management	
4.1 Centralized Configuration Backup	

ตารางที่ 4.9 ผลการตรวจสอบระบบเครือข่ายเดิม (ต่อ)

รายการ	คำอธิบาย
Configuration backups	ไม่มีการเก็บการตั้งค่า (config) สำรองไว้เผื่อกรณีการตั้งค่า (config) เกิดเสียหาย
4.2 Centralized Configuration Automation	
Configuration change capabilities	ไม่มีอุปกรณ์ที่ใช้ในการตั้งค่าจากที่เดียว ทำให้ต้องเสียเวลาในการตั้งค่าหลายอุปกรณ์
4.3 Configuration Change Management Workflow	
Change Control Management	มีการขออนุญาติและการระบุตัวตนก่อนเข้า Data Center เพื่อเข้าไปเปลี่ยนการตั้งค่า (config)
5. Performance Monitoring and Analysis	
5.1 Netflow Capabilities	
Bandwidth Planning Capabilities	ไม่มีการมอนิเตอร์เพื่อดูการใช้งานแบนด์วิธและไม่มีการวางแผนการใช้งานแบนด์วิธเพื่อรองรับการใช้งานในอนาคต
5.2 Client Experience Capabilities	
L4-L7 Visibility – Baseline Capabilities	ไม่มีการมอนิเตอร์เพื่อดูการใช้งานในการออกอินเตอร์เน็ตและแอพพลิเคชั่น และไฟร์วอลล์ไม่มีการต่อ license ทำให้ไม่สามารถดู Application ต่าง ๆ ได้

4.5 ผลการประเมินความเสี่ยง

ในการประเมินความเสี่ยงนี้เป็นส่วนหนึ่งของมาตรฐาน ITIL หลังจากที่ทางผู้จัดทำได้ทำการตรวจสอบระบบเครือข่ายเดิมเสร็จเรียบร้อยแล้วจึงได้ทำการประเมินความเสี่ยงที่จะกระทบต่อองค์กร พร้อมกับให้คำแนะนำในการนำไปปรับปรุงระบบเครือข่ายใหม่ โดยแสดงจำนวนความเสี่ยงต่าง ๆ ที่พบเจอในแสดงรูปที่ 4.14 และแสดงผลการประเมินความเสี่ยงในตารางที่ 4.10



รูปที่ 4.14 ระดับความเสี่ยงทั้งหมด

ตารางที่ 4.10 ผลการประเมินความเสี่ยง

รายการ	ความเสี่ยง				Priority และ Gap	ข้อเสนอแนะ
	ความรวดเร็ว	ภัยคุกคาม	การปฏิบัติการ	การบริหารจัดการ		
1. Network Design						
1.1 Network Overview Architecture						
Review for Modularity, scalability, and capabilities	Medium (2x3) (B)	Medium (2x3) (B)	Medium (3x2) (RHB)	Medium (3x2) (RB)	Medium (8)	ควรมีการเพิ่มเส้นทางสำรองในการออกอินเตอร์เน็ต
1.2 Traffic Flow						
Application Traffic Flow, Datacenter, Internet Edges, Client Access, WAN, Cloud	Low (1x1)	Low (1x1)	Medium (2x3) (B)	Medium (2x3) (B)	Medium (6)	ควรมีการมอนิเตอร์และใช้ Netflow เพื่อหาสาเหตุของ Traffic ในเวลากลางคืน
1.3 Services and OLA's						

ตารางที่ 4.10 ผลการประเมินความเสี่ยง (ต่อ)

รายการ	ความเสี่ยง				Priority และ Gap	ข้อเสนอแนะ
	ความรวดเร็ว	ภัยคุกคาม	การปฏิบัติการ	การบริหารจัดการ		
High Availability, OLA/SLA if defined	Medium (2x2) (RHB)	Low (1x1)	Medium (2x2) (RHB)	Medium (2x2) (RHB)	Medium (7)	ควรมีการทำเส้นทางสำรองไว้เผื่อกรณีที่อุปกรณ์เสียจะได้ใช้งานต่อไปได้
1.4 MPLS/VPN Service						
Remote Office and Client Access Capabilities	Low (1x1)	Low (1x1)	Low (1x1)	Low (1x1)	Low (4)	
1.5 QOS Standards						
Deployment methods, OLA's	Medium (2x2) (R(2)HB)	Low (1x1)	Medium (3x2) (R(2)HB)	Medium (3x2) (R(2)HB)	Medium (7)	ควรมีการกำหนด QOS เพื่อให้ข้อมูลที่สำคัญได้ผ่านไปก่อน
1.6 Layer 3 Routing						

ตารางที่ 4.10 ผลการประเมินความเสี่ยง (ต่อ)

รายการ	ความเสี่ยง				Priority และ Gap	ข้อเสนอแนะ
	ความรวดเร็ว	ภัยคุกคาม	การปฏิบัติการ	การบริหารจัดการ		
Dynamic, optimized, secure	Medium (2x3) (B)	Low (1x1)	Low (1x1)	Medium (2x2) (B)	Medium (6)	ควรตั้ง routing ให้ครอบคลุมเพื่อที่จะได้มอนิเตอร์ได้
1.7 Layer 2 Optimization						
Spanning-tree security/optimization, distributed Layer 2	Low (1x1)	Medium (3x2) (RHB)	Medium (3x2) (RHB)	Medium (3x2) (RHB)	Medium (7)	ควรเปิดโปรโตคอล Spanning-tree เพื่อป้องกันการเกิดลูปและแบ่ง VLAN ที่ใช้ในการทำงานกับ VLAN ที่ใช้ในการจัดการออกจากกัน
2. Physical Inventory						
2.1 Hardware Inventory Spreadsheet						
Physical Hardware Inventory – Serial Numbers if Possible	Medium (2x3) (B)	Medium (2x3) (B)	High (3x3) (B)	High (3x3) (B)	High (10)	ควรมีเอกสารระบุรายชื่ออุปกรณ์ หมายเลข IP รหัส (Password) ที่เป็นปัจจุบัน และระบุ Serial Number ที่อุปกรณ์ทุกตัว
2.2 Layer 1-2 Diagrams/Documentation						

ตารางที่ 4.10 ผลการประเมินความเสี่ยง (ต่อ)

รายการ	ความเสี่ยง				Priority และ Gap	ข้อเสนอแนะ
	ความรวดเร็ว	ภัยคุกคาม	การปฏิบัติการ	การบริหารจัดการ		
Physical interconnectivity	Medium (2x3) (B)	Low (1x1)	Medium (2x3) (B)	Medium (2x3) (B)	Medium (6)	ควรมีเอกสารแสดงการใช้งาน VLAN และ Network Diagram ที่เป็นปัจจุบัน
2.3 Layer 3 Diagrams/Documentation						
Routing Connectivity, Gateway Management, Summarization, Route Entrances/Exits	Medium (2x3) (B)	Low (1x1)	High (3x3) (B)	High (3x3) (B)	High (9)	ควรตั้ง routing ให้ครอบคลุมทุกอุปกรณ์ ไม่มีเอกสารระบุ IP และ Routing
2.4 Rack Elevation Diagrams/Documentation						
Physical Rack Diagrams	Low (1x1)	Low (1x1)	Medium (2x3) (B)	Medium (2x3) (B)	Medium (6)	ควรมี Rack Diagram และภายในตู้บริการระบบเครือข่ายควรมีแต่อุปกรณ์ที่ใช้งานและไม่วางทับซ้อนกัน

ตารางที่ 4.10 ผลการประเมินความเสี่ยง (ต่อ)

รายการ	ความเสี่ยง				Priority และ Gap	ข้อเสนอแนะ
	ความรวดเร็ว	ภัยคุกคาม	การปฏิบัติการ	การบริหารจัดการ		
2.5 Environmental Capabilities						
Power, cooling, and cable management	Medium (2x3) (B)	Low (1x1)	Medium (2x3) (B)	Medium (2x3) (B)	Medium (7)	ควรมีป้ายบอกปลายทางของอุปกรณ์ติดที่สายทุกเส้น จัดสายให้เป็นระเบียบ และควรเปลี่ยนสายเป็นมาตรฐาน Cat 6 เพื่อรองรับการใช้งานในอนาคต
3. Infrastructure Monitoring and Management						
3.1 Central Monitoring/Alerting Capabilities						
Management Platform utilization/capabilities	Medium (2x3) (B)	Low (1x1)	Medium (2x3) (B)	High (3x3) (B)	Medium (B)	ควรมีการมอนิเตอร์อุปกรณ์เพื่อเก็บผลการทำงานของอุปกรณ์และแจ้งเตือนเมื่ออุปกรณ์ทำงานผิดปกติ
3.2 Syslog Capabilities						
Controls, retention, management	Low (1x1)	Low (1x1)	Medium (2x3) (B)	Medium (2x3) (B)	Medium (6)	ควรมีการเก็บ log เพื่อดูการใช้งานย้อนหลัง

ตารางที่ 4.10 ผลการประเมินความเสี่ยง (ต่อ)

รายการ	ความเสี่ยง				Priority และ Gap	ข้อเสนอแนะ
	ความรวดเร็ว	ภัยคุกคาม	การปฏิบัติการ	การบริหารจัดการ		
3.3 EoL/EoS hardware and licensing						
Process for Lifecycle and licensing compliance	Medium (2x3) (B)	High (3x3) (B)	Medium (2x3) (B)	Medium (2x3) (B)	High (9)	ควรมีอุปกรณ์ที่ยังสามารถรองรับเฟิร์มแวร์ใหม่ ๆ สำรองไว้และมีการต่อ license เพื่อใช้งานฟีเจอร์ต่าง ๆ ที่จำเป็น
4. Configuration Management						
4.1 Centralized Configuration Backup						
Configuration backups	Low (1x1)	Low (1x1)	Medium (2x3) (B)	Medium (2x3) (B)	Medium (4)	ควรมีการเก็บการตั้งค่า (config) ไว้เผื่อกรณีการตั้งค่า (config) เกิดเสียหาย
4.2 Centralized Configuration Automation						
Configuration change capabilities	Medium (2x3) (B)	Low (1x1)	Medium (2x3) (B)	Medium (2x3) (B)	Medium (4)	ควรมีศูนย์กลางการตั้งค่า (config) แบบอัตโนมัติเพื่อความรวดเร็วในการตั้งค่า (config)
4.3 Configuration Change Management Workflow						

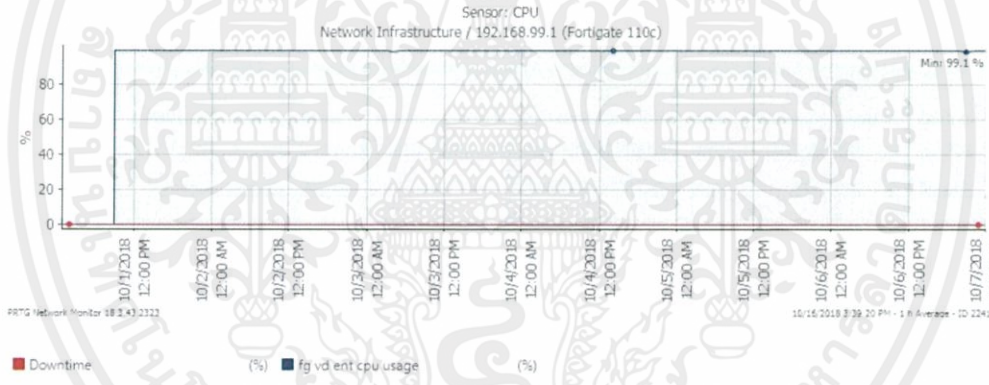
ตารางที่ 4.10 ผลการประเมินความเสี่ยง (ต่อ)

รายการ	ความเสี่ยง				Priority และ Gap	ข้อเสนอแนะ
	ความรวดเร็ว	ภัยคุกคาม	การปฏิบัติการ	การบริหารจัดการ		
Change Control Management	Low (1x1)	Low (1x1)	Low (1x1)	Medium (2x3) (R(2))	Low (4)	ควรมีการควบคุมว่าให้บุคคลใดเปลี่ยนการตั้งค่า (config) ได้บ้าง
5. Performance Monitoring and Analysis						
5.1 Netflow Capabilities						
Bandwidth Planning Capabilities	Medium (2x3) (B)	Low (1x1)	Medium (2x3) (B)	High (3x3) (B)	Medium (8)	ควรมีการมอนิเตอร์เพื่อเก็บผลของแบนด์วิธ และ Netflow และมีการวางแผนการใช้งานแบนด์วิธเผื่อในอนาคต
5.2 Client Experience Capabilities						
L4-L7 Visibility – Baseline Capabilities	Medium (2x3) (B)	High (3x3) (B)	Medium (2x3) (B)	Medium (2x3) (B)	High (9)	ควรมีการมอนิเตอร์เพื่อดูการใช้งานในการออกอินเตอร์เน็ตและแอพพลิเคชั่น

4.6 ผลสรุปหลังตรวจสอบระบบเครือข่ายเดิม

หลังจากที่ผู้จัดทำได้เข้าไปสำรวจ เก็บผลมอนิเตอร์ของระบบเครือข่ายเดิมของทางองค์กร ผู้จัดทำได้พบข้อเสียหลักดังนี้

- Fortigate มีการใช้งาน CPU 99% ตลอดเวลา แสดงดังรูปที่ 4.15 และตารางที่ 4.11
- มีการใช้งานทราฟฟิคในเวลากลางคืน แสดงดังรูปที่ 4.16
- ไม่มีเอกสารระบบเครือข่ายที่เป็นปัจจุบัน
- การจัดเรียงสายในตู้บริการระบบเครือข่ายไม่เป็นระเบียบ และไม่มีการติดป้ายบอกปลายทางของสาย แสดงดังรูปที่ 4.17
- ไม่มีการเก็บข้อมูลการใช้งาน
- อุปกรณ์หมดประกัน และไม่มีการต่อ License

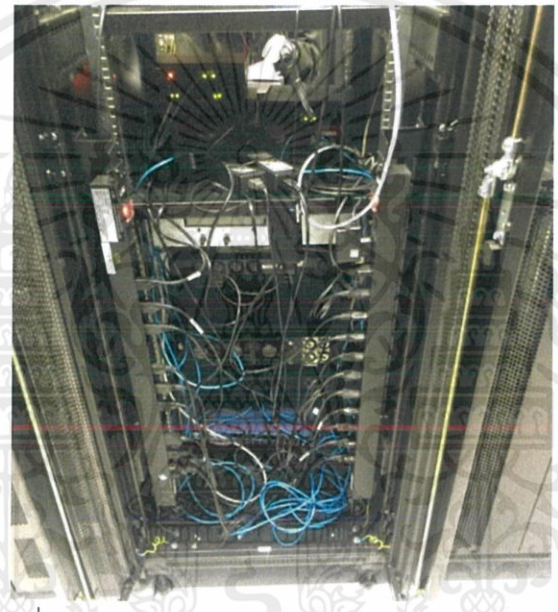


รูปที่ 4.15 ผลการมอนิเตอร์ CPU ไฟร์วอลล์ Fortigate 110c

ตารางที่ 4.11 ผลการใช้งาน CPU

	CPU Usage	Down time
Maximum	99.4 %	0 %
Average	99 %	0 %
Minimum	99.1 %	0 %

รูปที่ 4.16 ผลการมอนิเตอร์ Traffic เราเตอร์ Juniper MX80

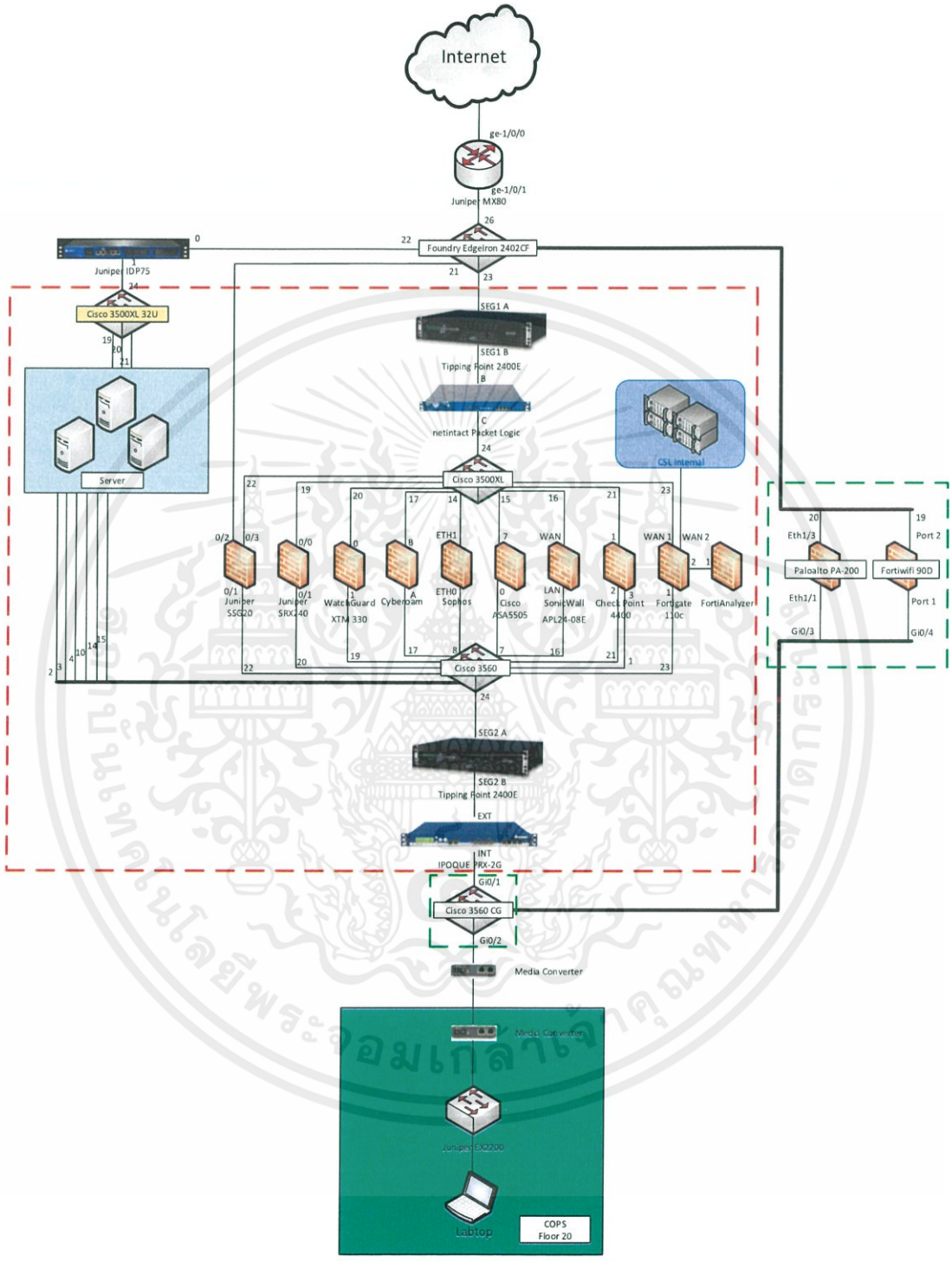


รูปที่ 4.17 การจัดสายภายในตู้บริการระบบเครือข่าย

4.7 โครงสร้างระบบเครือข่ายใหม่

ผู้จัดทำได้ทำการออกแบบระบบเครือข่ายใหม่ โดยคำนึงถึงความพร้อมในการใช้งานตามมาตรฐาน ITIL ลดจำนวนอุปกรณ์ที่ผ่านก่อนออกสู่อินเตอร์เน็ต และรองรับเทคโนโลยีใหม่ในอนาคต จึงได้แยกการใช้งานเป็นสองส่วน ส่วนแรกคืออุปกรณ์เครือข่ายเดิมที่อุปกรณ์บางตัวหมดการสนับสนุนจากทางผู้ผลิต ทำให้ไม่ได้รับการอัพเดทฟีเจอร์หรือเฟิร์มแวร์ใหม่จะอยู่ภายในเส้นประสีแดง โดยระบบเครือข่ายเดิมยังเชื่อมต่อไว้เพื่อที่จะย้ายอุปกรณ์ที่ยังไม่หมดการสนับสนุนจากผู้ผลิตมาสู่ระบบเครือข่ายใหม่ในอนาคต และอีกส่วนคืออุปกรณ์เครือข่ายใหม่ที่ยังได้รับการสนับสนุนจากทางผู้ผลิตอยู่ในเส้นประสีเขียว ในส่วนนี้จะทำการเพิ่มสวิตช์ใหม่หนึ่งตัวและไฟร์วอลล์ใหม่สองตัวเพื่อสลับการใช้งานกรณีอุปกรณ์เกิดความเสียหายไม่สามารถใช้งานได้และอุปกรณ์ทั้งสามตัวนี้เป็นอุปกรณ์ที่ทางองค์กรมีการสำรองเอาไว้ จึงไม่ได้มีค่าใช้จ่ายเพิ่มเติมเป็นการจัดสรรทรัพยากรที่มีอยู่ให้เกิดความ

คุ้มค่ามากที่สุดตามมาตรฐาน ITIL โดยผู้จัดทำรับผิดชอบการตั้งค่าไฟร์วอล์ paloalto PA-200 แสดงในรูปที่ 3.2



รูปที่ 4.18 Network Diagram ระบบเครือข่ายใหม่

4.8 การตั้งค่าระบบใหม่

ในการตั้งค่าอุปกรณ์ผู้จัดทำได้ทำการตั้งค่าตามความต้องการในการใช้งานขององค์กร โดยสิ่งที่ทางองค์กรต้องการ คือ สามารถออกอินเตอร์เน็ตได้ ห้ามไม่ให้ดาวน์โหลดบิต และสามารถ VPN แบบ Client to Site ได้ ในการตั้งค่าจะแบ่งเป็นส่วนต่าง ๆ ดังนี้

4.8.1 Interface

การตั้งค่าอินเตอร์เฟซ แสดงในรูปที่ 4.19 จากรูปอินเตอร์เฟซ eth1/1 จะอยู่ในโซน Internal และอินเตอร์เฟซ eth1/3 จะอยู่ในโซน External และอินเตอร์เฟซนี้ก็ยังใช้เป็นเกตเวย์ของการทำ VPN ด้วยเช่นกัน โดยอินเตอร์เฟซที่มีการใช้งานจะมีสถานะการใช้งานเป็นสีเขียวและมีการเปิดการใช้งานโปรโตคอล SNMP ที่ทุกอินเตอร์เฟซ

Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	Tag	VLAN / Virtual-Wire	Security Zone	Features
ethernet1/1	Layer3	Mgmt		IP_LAN	default	Untagged	none	Internal	
ethernet1/2	Layer3	Mgmt		192.168.30.1/24	default	Untagged	none	DMZ	
ethernet1/3	Layer3	Mgmt		IP_WAN	default	Untagged	none	External	
ethernet1/4	Layer3	Mgmt		IP_CSL	default	Untagged	none	CSL_Internal	

รูปที่ 4.19 การตั้งค่าอินเตอร์เฟซของไฟร์วอลล์ paloalto PA-200

4.8.2 Policy

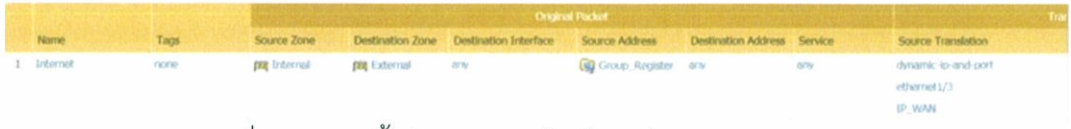
การตั้งค่า Policy นั้นจะมีลำดับการทำงานไล่จากบรรทัดบนลงมาบรรทัดล่าง โดยจะตั้งค่าให้สามารถ VPN จากภายนอกเข้ามาใช้งานระบบเครือข่ายภายในบริษัทได้ ตั้งค่าให้บล็อคการโหลดบิทและตั้งค่าให้สามารถออกอินเตอร์เน็ตได้ แสดงการตั้งค่า Policy ในรูปที่ 4.20 และ policy ที่มีการทำงานจะแสดงค่า Hit Count ดังรูป

	Name	Source Zone	Source Address	Source User	Source HIP Profile	Destination Zone	Destination Address	Rule Usage Hit Count	Application	Service
1	VPN Access	corp-VPN	any	any	any	Internal	any	16476	any	applicatic
2	Block_Bit	Internal	Group_Register	any	any	External	any	2208	bit9-parity bitbucket bitcasa bitcoin bitdefender bitrix24 bittorrent more...	applicatic
3	Internet	Internal	Group_Register	any	any	External	any	178911	any	applicatic
4	Internal	Internal	FW_Register Group_Register	any	any	CSL_Internal	any	0	any	applicatic
5	rule1	trust	any	any	any	untrust	any	0	any	any
6	Destination	External	any	any	any	Internal	192.168.20.88	8	any	applicatic
7	intrazone-default	any	any	any	any	(intrazone)	any	151990	any	any

รูปที่ 4.20 การตั้งค่า Policy ของไฟร์วอลล์ paloalto PA-200

4.8.3 NAT

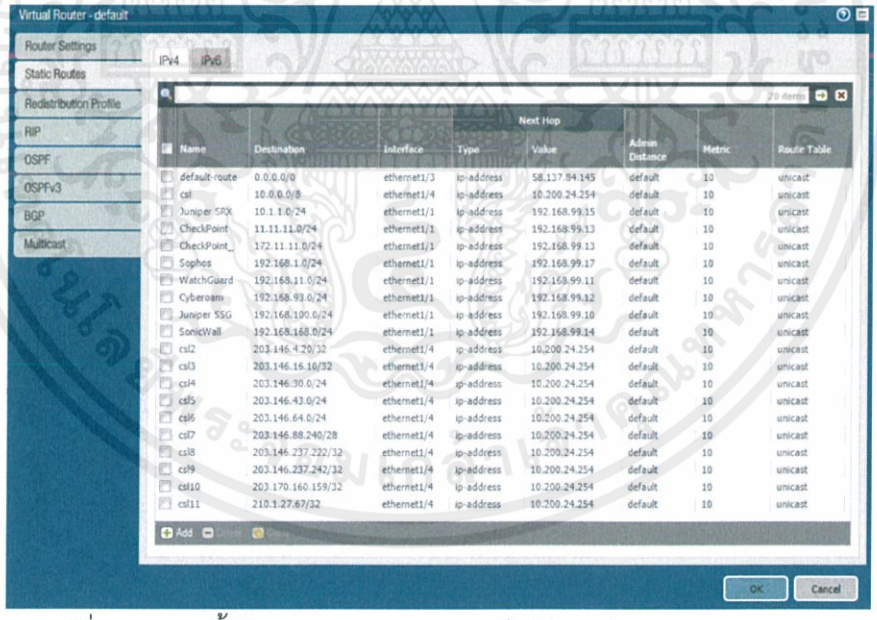
การตั้งค่า NAT เป็นการตั้งค่าเพื่อเปลี่ยนจาก IP Private เป็น IP Public เพื่อให้สามารถใช้งานอินเตอร์เน็ตได้ แสดงในรูปที่ 4.21 โดยตั้งค่าจาก IP Private คือ 192.168.88.0/24 ให้ออกอินเตอร์เน็ตด้วย IP Public ของ eth1/3 คือ IP 58.137.84.155/28



รูปที่ 4.21 การตั้งค่า NAT ของไฟร์วอลล์ paloalto PA-200

4.8.4 Routing

การตั้งค่า Static Routing จะต้องตั้งค่า IP ปลายทางที่ต้องการไป อินเตอร์เฟซที่ใช้ และ Next Hop ที่ต้องไป เพื่อที่จะได้ไปปลายทางได้อย่างถูกต้อง โดยจะตั้งค่า default route ไปที่เราเตอร์ Juniper MX80 โดยออกทางอินเตอร์เฟซ eth1/3 แสดงในรูปที่ 4.22



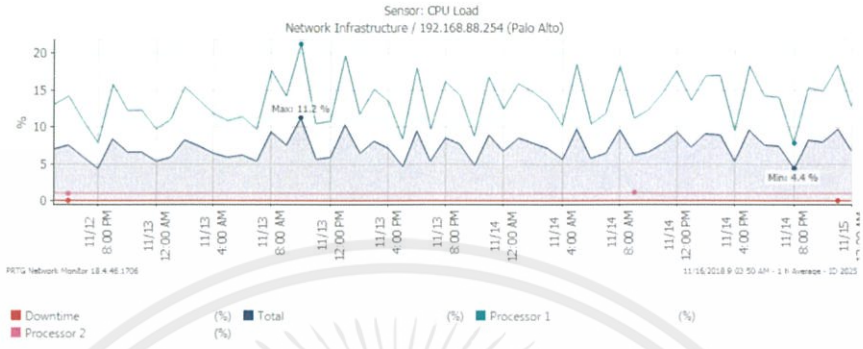
รูปที่ 4.22 การตั้งค่า Static Routing ของไฟร์วอลล์ paloalto PA-200

4.9 ผลการ Monitor ระบบเครือข่ายใหม่

ในหัวข้อนี้จะแสดงผลการมอนิเตอร์ของไฟร์วอลล์ paloalto PA-200 ที่ผู้จัดทำได้ติดตั้งเพิ่มเข้าไปในระบบเดิม โดยจะแสดงผลมอนิเตอร์ของอุปกรณ์ที่เหลือในภาคผนวก ค

4.9.1 ผลการมอนิเตอร์ CPU

ผลการมอนิเตอร์ CPU ที่เก็บ ในวันที่ 12/11/18 4:00:00 PM – 15/11/18 12:00:00 AM แสดงในรูปที่ 4.23 และแสดงค่าในตารางที่ 4.12



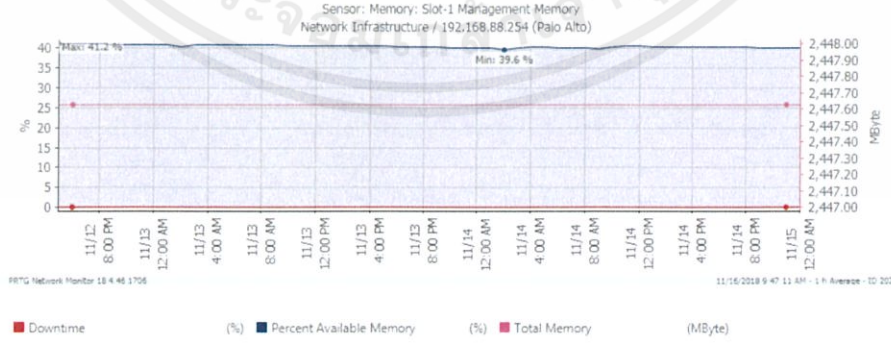
รูปที่ 4.23 ผลการมอนิเตอร์ CPU ไฟร์วอลล์ paloalto PA-200

ตารางที่ 4.12 ผลการใช้งาน CPU ไฟร์วอลล์ paloalto PA-200

	Processor 1	Processor 2	Down time
Maximum	21 %	1 %	0 %
Average	14 %	1 %	0 %
Minimum	8 %	1 %	0 %

4.9.2 ผลการมอนิเตอร์ Memory

ผลการมอนิเตอร์ Memory ที่เก็บ ในวันที่ 12/11/18 4:00:00 PM – 15/11/18 12:00:00 AM แสดงในรูปที่ 4.24 และแสดงค่าในตารางที่ 4.13



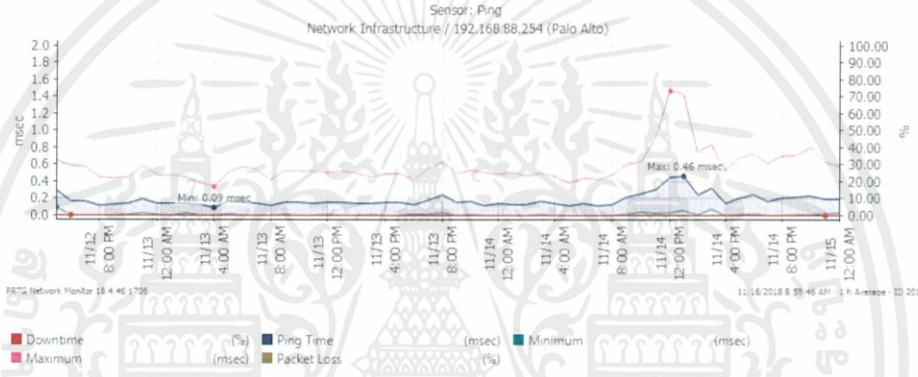
รูปที่ 4.24 ผลการมอนิเตอร์ Memory ไฟร์วอลล์ paloalto PA-200

ตารางที่ 4.13 ผลการใช้งาน Memory ไฟร์วอลล์ paloalto PA-200

	Available Memory	Down time
Maximum	41.2 %	0 %
Average	41 %	0 %
Minimum	39.6 %	0 %

4.9.3 ผลการมอนิเตอร์ Ping

ผลการมอนิเตอร์ Ping ที่เก็บ ในวันที่ 12/11/18 4:00:00 PM – 15/11/18 12:00:00 AM แสดงในรูปที่ 4.25 และแสดงค่าในตารางที่ 4.14



รูปที่ 4.25 ผลการมอนิเตอร์ Ping ไฟร์วอลล์ paloalto PA-200

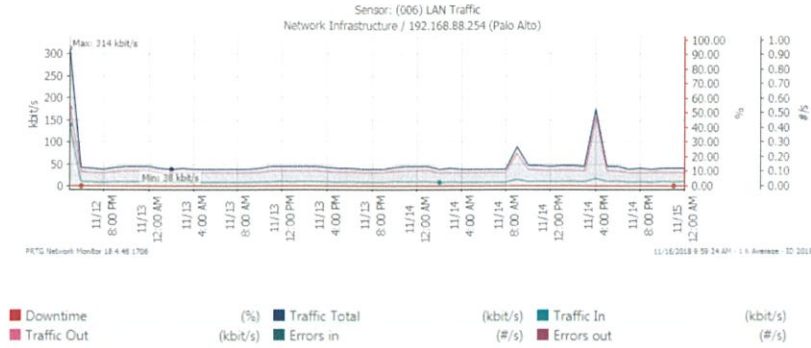
ตารางที่ 4.14 ผลการใช้งาน Ping ไฟร์วอลล์ paloalto PA-200

	Ping time	Packet Loss	Downtime
Maximum	0.46 msec	0 %	0 %
Average	0 msec	0 %	0 %
Minimum	0.09 msec	0 %	0 %

4.9.4 ผลการมอนิเตอร์ Traffic

4.9.4.1 Interface eth1/1

ผลการมอนิเตอร์ Traffic ที่เก็บ ในวันที่ 12/11/18 4:00:00 PM – 15/11/18 12:00:00 AM แสดงในรูปที่ 4.26 และแสดงค่าในตารางที่ 4.15



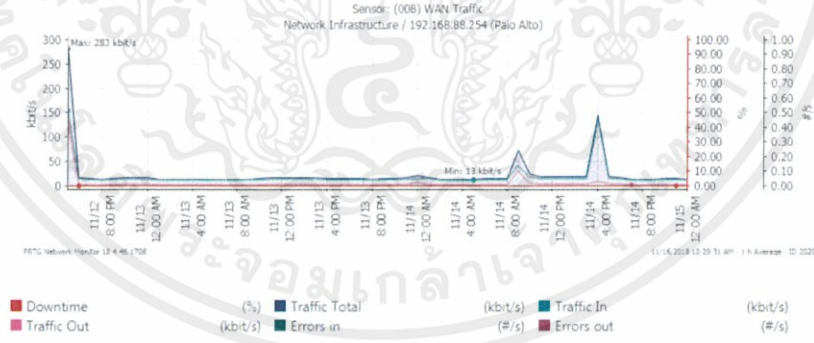
รูปที่ 4.26 ผลการมอนิเตอร์ Traffic eth1/1 ไฟร์วอลล์ paloalto PA-200

ตารางที่ 4.15 ผลการใช้งาน Traffic eth1/1 ไฟร์วอลล์ paloalto PA-200

	Traffic Total	Traffic In	Traffic Out	Errors in	Errors out	Downtime
Maximum	314 kbit/s	138 kbit/s	176 kbit/s	0 kbit/s	0 kbit/s	0 %
Average	50 kbit/s	12 kbit/s	37 kbit/s	0 kbit/s	0 kbit/s	0 %
Minimum	38 kbit/s	8.88 kbit/s	29 kbit/s	0 kbit/s	0 kbit/s	0 %

4.9.4.2 Interface eth1/3

ผลการมอนิเตอร์ Traffic ที่เก็บ ในวันที่ 12/11/18 4:00:00 PM – 15/11/18 12:00:00 AM แสดงในรูปที่ 4.27 และแสดงค่าในตารางที่ 4.16



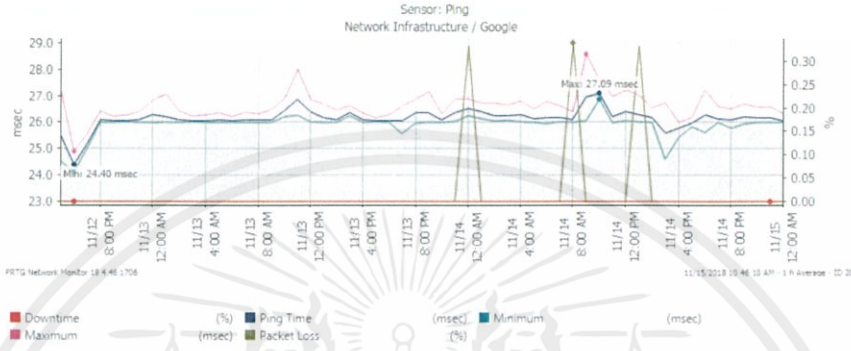
รูปที่ 4.27 ผลการมอนิเตอร์ Traffic eth1/3 ไฟร์วอลล์ paloalto PA-200

ตารางที่ 4.16 ผลการใช้งาน Traffic eth1/3 ไฟร์วอลล์ paloalto PA-200

	Traffic Total	Traffic In	Traffic Out	Errors in	Errors out	Downtime
Maximum	283 kbit/s	155 kbit/s	128 kbit/s	0 kbit/s	0 kbit/s	0 %
Average	24 kbit/s	19 kbit/s	5.19 kbit/s	0 kbit/s	0 kbit/s	0 %
Minimum	13 kbit/s	13 kbit/s	1.26 kbit/s	0 kbit/s	0 kbit/s	0 %

4.9.5 ผลการมอนิเตอร์ Ping ออกอินเตอร์เน็ต

ผลการมอนิเตอร์ Ping ออกอินเตอร์เน็ตที่เก็บ โดย Ping ไปที่หมายเลข IP 8.8.8.8 ซึ่งเป็นหมายเลข IP ของ Google เก็บผลในวันที่ 12/11/18 4:00:00 PM – 15/11/18 12:00:00 AM แสดงในรูปที่ 4.28 และแสดงค่าในตารางที่ 4.17



รูปที่ 4.28 ผลการมอนิเตอร์ Ping ออกอินเตอร์เน็ตของระบบเครือข่ายใหม่

ตารางที่ 4.17 ผลการ Ping ออกอินเตอร์เน็ตของระบบเครือข่ายใหม่

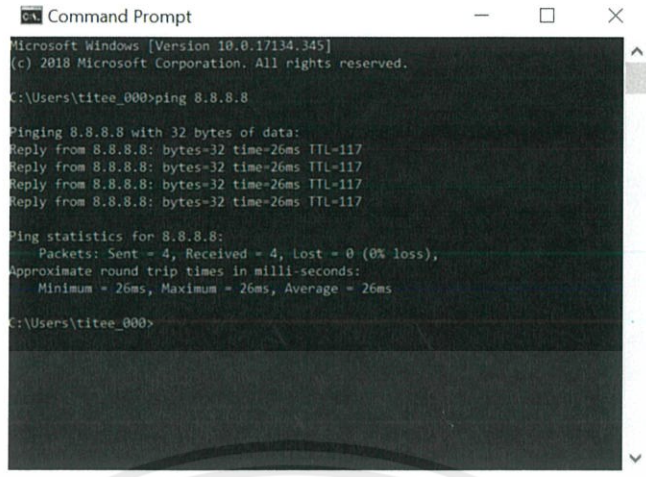
	Ping time	Packet Loss	Downtime
Maximum	27 msec	0 %	0 %
Average	26 msec	0 %	0 %
Minimum	24 msec	0 %	0 %

4.10 ผลการใช้งานระบบเครือข่ายใหม่

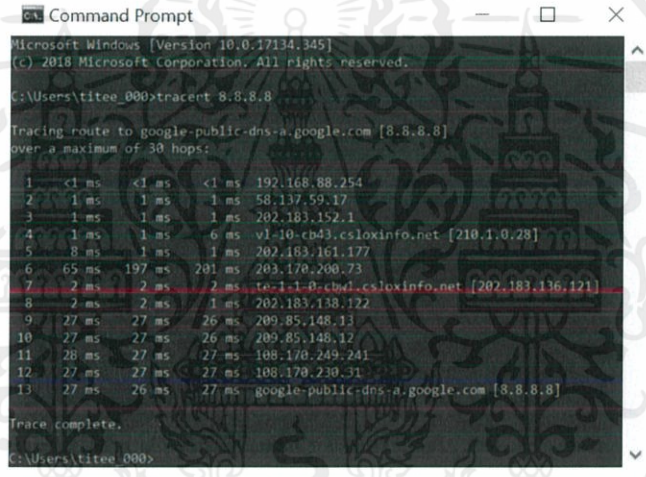
หลังจากติดตั้งระบบเครือข่ายใหม่ ผู้จัดทำได้ทดสอบการใช้งานตามที่ทางองค์กรต้องการ โดยแสดงผลดังนี้

4.10.1 การใช้งานอินเตอร์เน็ต

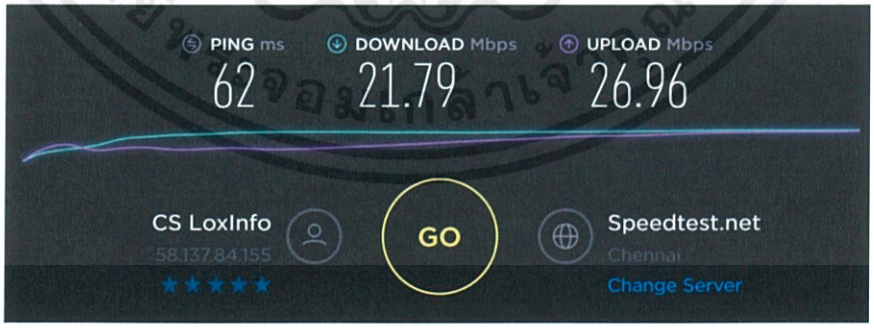
ผู้จัดทำได้ทดลองการใช้งานอินเตอร์เน็ตด้วยการ Ping ไปที่ IP 8.8.8.8 แสดงในรูปที่ 4.29 และ Traceroute เพื่อดูเส้นทางที่ผ่านของอุปกรณ์ แสดงในรูปที่ 4.30 โดยลำดับที่หนึ่งคือไฟร์วอลล์ paloalto PA-200 อินเตอร์เฟซ eth1/1 และลำดับที่สองคือเราเตอร์ Juniper MX80 อินเตอร์เฟซ ge-1/0/1 แล้วจึงออกไปที่อุปกรณ์ภายนอก โดย IP ที่ออกอินเตอร์เน็ตคือ IP ที่ทำการ NAT (58.137.84.155) แสดงในรูปที่ 4.31



รูปที่ 4.29 ทดสอบ ping ออกอินเตอร์เน็ต



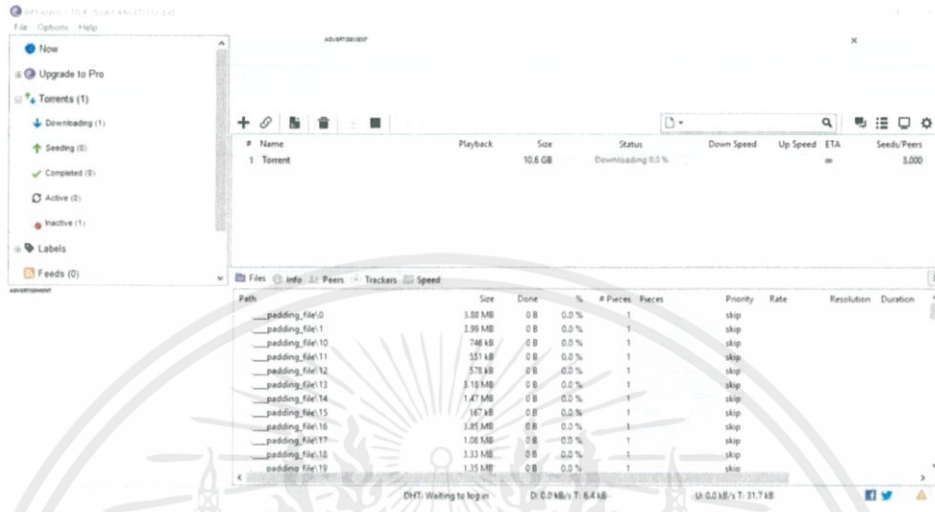
รูปที่ 4.30 ผลการ Traceroute ออกอินเตอร์เน็ต



รูปที่ 4.31 ทดสอบความเร็วในการใช้งานอินเตอร์เน็ต

4.10.2 Block Bit

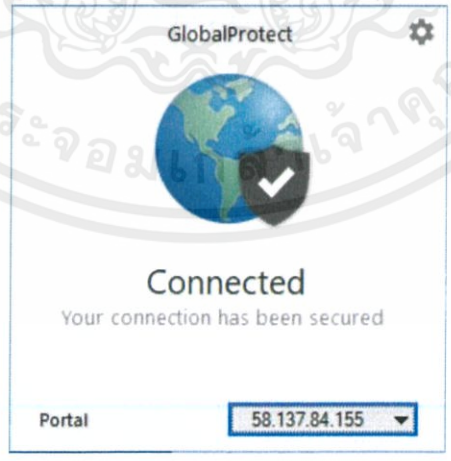
ผู้จัดทำได้ทดลองบล็อคการดาวน์โหลดบิท ด้วยการทดลองโหลด BitTorrent แสดงในรูปที่ 4.32 โดยผลที่ได้คือไม่สามารถดาวน์โหลดบิทได้ตาม Policy ที่ได้ตั้งไว้ที่ไฟร์วอลล์ paloalto PA-200



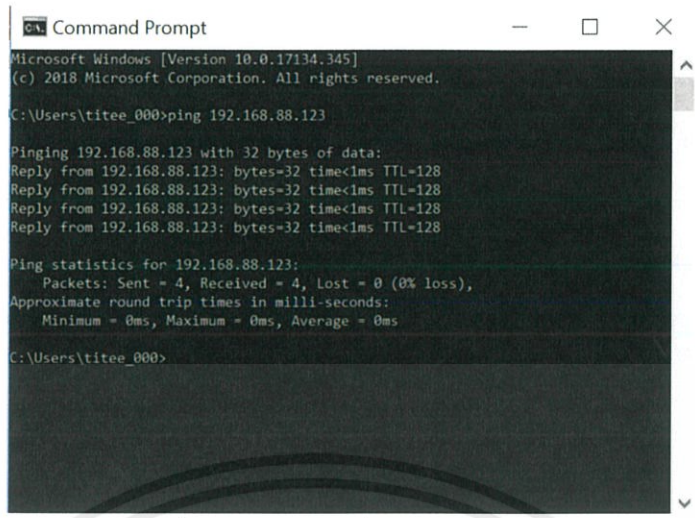
รูปที่ 4.32 Block Bit

4.10.3 VPN Client to Site

ในการทดลอง VPN ผู้จัดทำได้ใช้โปรแกรม GlobalProtect ในการเชื่อมต่อจากภายนอกเข้ามาที่อินทราเน็ตภายในองค์กรแสดงในรูปที่ 4.33 และเมื่อเชื่อมต่อสำเร็จจึงได้ ping ไปที่ IP ภายในองค์กรแสดงในรูปที่ 4.34



รูปที่ 4.33 เชื่อมต่อ VPN ด้วยโปรแกรม GlobalProtect



รูปที่ 4.34 ping ไปที่ IP ภายในองค์กร

บทที่ 5

สรุปผลและข้อเสนอแนะ

5.1 สรุปผลการดำเนินงาน

จากการสำรวจระบบเครือข่ายเดิมของทางองค์กร พบว่าเอกสารที่เกี่ยวกับระบบเครือข่ายไม่เป็นปัจจุบัน อุปกรณ์บางตัวทำงานหนัก ไม่มีการสร้างเส้นทางสำรองในการออกอินเตอร์เน็ต และมีอุปกรณ์หลายตัวที่หมดการสนับสนุนจากทางผู้ผลิต ผู้จัดทำจึงได้ทำเอกสารที่เกี่ยวกับระบบเครือข่ายให้เป็นปัจจุบัน เอกสารการประเมินความเสี่ยงและคำแนะนำในการปรับปรุงระบบ ส่งมอบให้ทางองค์กร พร้อมกับออกแบบระบบเครือข่ายใหม่ที่แยกการทำงานออกจากระบบเครือข่ายเดิม โดยเพิ่มสวิตช์และไฟร์วอลล์ใหม่สองตัวเพื่อเป็นการทำเส้นทางสำรองเผื่อกรณีอุปกรณ์เสียหายเพื่อแก้ปัญหาเรื่องความพร้อมในการใช้งานตามมาตรฐาน ITIL โดยระบบเครือข่ายใหม่สามารถใช้งานอินเตอร์เน็ตบล็อคการดาวน์โหลดบิท และ VPN แบบ Client to Site ตามที่ทางองค์กรต้องการได้

5.2 ประโยชน์ของโครงงาน

1) ช่วยให้ทราบถึงโครงสร้างและการใช้งานของระบบเครือข่ายในปัจจุบัน
2) ช่วยให้ทราบถึงสาเหตุของปัญหาในการใช้งานระบบเครือข่าย
3) ช่วยให้สามารถวางแผนรับมือผลกระทบต่าง ๆ ที่ส่งผลต่อองค์กรได้อย่างมีประสิทธิภาพ

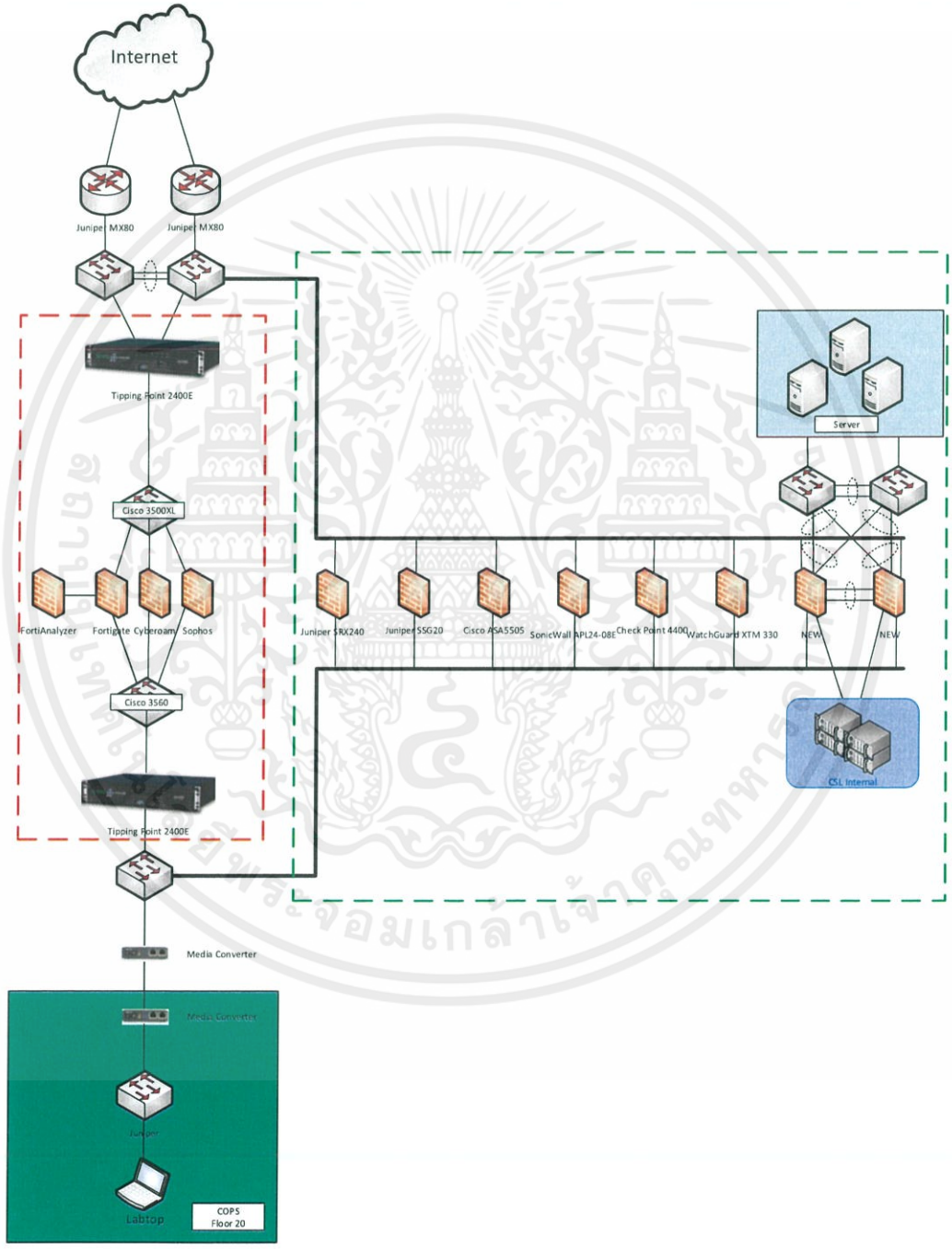
5.3 ปัญหาและอุปสรรค

การปรับปรุงประสิทธิภาพระบบเครือข่ายตามข้อปฏิบัติ ITILV3 สำหรับอุตสาหกรรมไอทีที่ได้ทำการตรวจสอบและออกแบบระบบใหม่นี้ ทางองค์กรไม่มีเอกสารเกี่ยวกับระบบเครือข่ายที่เป็นปัจจุบัน เช่น หมายเลข IP และรหัส (Password) จึงส่งผลให้ไม่สามารถเข้าไปเก็บการตั้งค่า (config) ในอุปกรณ์บางตัวได้ และไม่สามารถเข้าไปตั้งค่าโปรโตคอล SNMP เพื่อมอนิเตอร์อุปกรณ์ได้

ในการทำสหกิจศึกษาครั้งนี้มีการเปลี่ยนหัวข้อเนื่องจากทางลูกค้าขององค์กรที่ผู้จัดทำฝึกสหกิจศึกษาอยู่ไม่มีความพร้อมให้เข้าไปทำการตรวจสอบระบบเครือข่าย ทางพี่เลี้ยงจึงได้ทำการเปลี่ยนสถานที่จากอุตสาหกรรมเครื่องดื่มเป็นอุตสาหกรรมไอที โดยในช่วงที่รอทางลูกค้าเดิมยืนยันส่งผลให้เสียเวลาในการทำงานและต้องเร่งทำงานในสถานที่ใหม่ให้ทันเวลา

5.4 แนวทางในการพัฒนาต่อ

การออกแบบระบบเครือข่ายใหม่ควรออกแบบตามวิธีปฏิบัติที่ดีที่สุดในการออกแบบ คือ มีการทำเส้นทางสำรองเผื่อกรณีอุปกรณ์เสียหายที่อุปกรณ์ทุกตัว ย้ายอุปกรณ์ที่ยังไม่หมดการสนับสนุนจากทางผู้ผลิตมาอยู่ร่วมกับไฟร์วอลล์ตัวใหม่และย้ายเซิฟเวอร์มาอยู่หลังไฟร์วอลล์เพื่อป้องกันภัยคุกคามทางไซเบอร์ โดยแสดงในรูปที่ 5.1



รูปที่ 5.1 โครงสร้างระบบเครือข่ายใหม่ที่ทำการเพิ่มเส้นทางสำรอง

บรรณานุกรม

[1] นายประทิน ทับไทร. "ตัวกลางหรือสื่อกลาง (Media)."
https://sites.google.com/a/kts.ac.th/it_kts/unit3/subunit3-3.

[2] สุรชาติ ศรีอินทรสุทธิ์. "ระบบเครือข่ายคอมพิวเตอร์."
http://networkcomputer99.blogspot.com/.

[3] ดำรงศักดิ์ บุตทะปัญญา. "โครงสร้างเครือข่ายคอมพิวเตอร์ (Network Topology)."
https://sites.google.com/site/dumrongnetwork/topology.

[4] นาย พรชัย อินทร์ช่วย. "VLAN คืออะไร."
http://ninehua.com/index.php/story/menu-nw/176-vlan.

[5] มายพีเฮชพี. "IP Address คืออะไร."
http://www.mindphp.com/.

[6] เกรียงศักดิ์ นามโคตร. "Routing Protocol."
http://www.jodoi.org/router%20protocal.html.

[7] เอกสิทธ์ วิริยจารี. เรียนรู้ระบบเน็ตเวิร์กจากอุปกรณ์ของ Cisco. กรุงเทพฯ : ซีเอ็ดยูเคชั่น, 2548.

[8] ชัชวาล พร้อมมูล. "Network Address Translation (NAT)."
https://www.gotoknow.org/posts/.

[9] Thananchai Panyatavahirun. "ทำความรู้จักและตั้งค่า EtherChannel บน Cisco Catalyst Switch."
http://running-config.blogspot.com/2011/03/etherchannel-cisco-catalyst-switch.html.

[10] ทีมงาน TechTalkThai. "PRTG Network & Performance Monitoring."
https://www.techtalkthai.com/prtg-iot-monitoring/.

[11] ตลาดหลักทรัพย์แห่งประเทศไทย. "กรอบการบริหารความเสี่ยงองค์กร."
https://www.set.or.th/th/about/overview/files/ERM_Framework_2017.pdf.

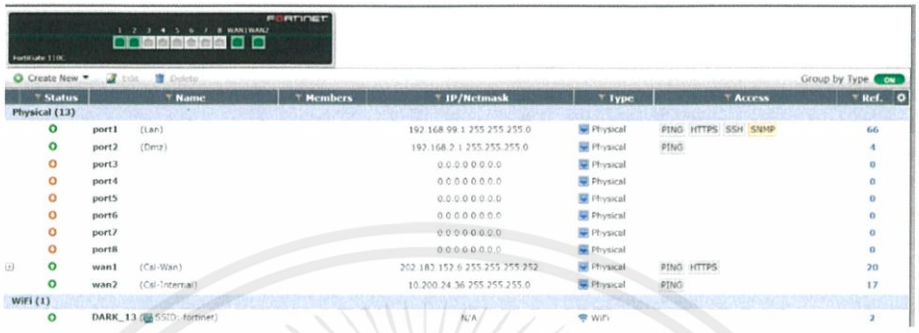
[12] ดร.วิรินทร์ เมฆประดิษฐสิน. สู่ความเป็นเลิศด้านการบริการงานไอทีด้วยมาตรฐาน ITIL v.3. กรุงเทพฯ : ซีเอ็ดยูเคชั่น, 2558.

ภาคผนวก ก

การตั้งค่าของอุปกรณ์

1. Fortigate 110c

1.1 Interfaces



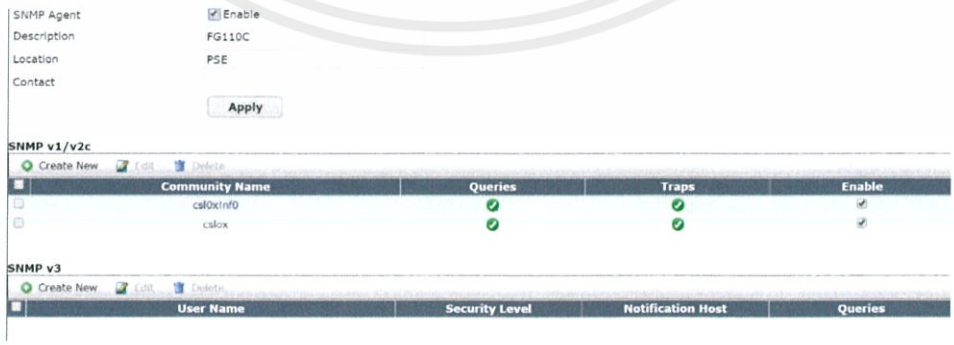
Create New | Edit | Delete | Group by Type ON

Status	Name	Members	IP/Netmask	Type	Access	Ref.
Physical (13)						
	port1 (Lan)		192.168.99.1 255.255.255.0	Physical	PING HTTPS SSH SNMP	66
	port2 (Dmz)		192.168.2.1 255.255.255.0	Physical	PING	4
	port3		0.0.0.0 0.0.0.0	Physical		0
	port4		0.0.0.0 0.0.0.0	Physical		0
	port5		0.0.0.0 0.0.0.0	Physical		0
	port6		0.0.0.0 0.0.0.0	Physical		0
	port7		0.0.0.0 0.0.0.0	Physical		0
	port8		0.0.0.0 0.0.0.0	Physical		0
	wan1 (Cal-Wan)		202.183.152.6 255.255.255.252	Physical	PING HTTPS	20
	wan2 (Cal-Internal)		10.200.24.36 255.255.255.0	Physical	PING	17
WiFi (1)						
	DARK_13 (SSID: fortinet)		N/A	WiFi		2

1.2 Static Route

IP/Netmask	Gateway	Device	Comment
0.0.0.0 0.0.0.0	202.183.152.5	wan1	
10.0.0.0 255.0.0.0	10.200.24.254	wan2	
10.1.1.0 255.255.255.0	192.168.99.15	port1	Juniper SRX
10.10.3.0 255.255.255.0	Test_AWN		VPN: Test_AWN (Created by VPN w...
10.15.200.0 255.255.255.0	To_Koyo		
10.212.134.0 255.255.255.0	ssl.root		
11.11.11.0 255.255.255.0	192.168.99.13	port1	CheckPoint
172.11.11.0 255.255.255.0	192.168.99.13	port1	CheckPoint DMZ
192.168.1.0 255.255.255.0	192.168.99.17	port1	Sophos
192.168.11.0 255.255.255.0	192.168.99.11	port1	WatchGuard
192.168.69.0 255.255.255.0	192.168.99.16	port1	PaloAlto
192.168.93.0 255.255.255.0	192.168.99.12	port1	Cyberoam
192.168.100.0 255.255.255.0	192.168.99.10	port1	Juniper SSG
192.168.168.0 255.255.255.0	192.168.99.14	port1	Sonicwall
203.146.4.20 255.255.255.255	10.200.24.254	wan2	
203.146.16.10 255.255.255.255	10.200.24.254	wan2	
203.146.30.0 255.255.255.0	10.200.24.254	wan2	
203.146.43.0 255.255.255.0	10.200.24.254	wan2	
203.146.64.0 255.255.255.0	10.200.24.254	wan2	
203.146.88.240 255.255.255.240	10.200.24.254	wan2	
203.146.237.222 255.255.255.255	10.200.24.254	wan2	
203.146.237.242 255.255.255.255	10.200.24.254	wan2	
203.170.160.159 255.255.255.255	10.200.24.254	wan2	

1.3 SNMP



SNMP Agent: Enable
Description: FG110C
Location: PSE
Contact:
Apply

SNMP v1/v2c

Create New | Edit | Delete

Community Name	Queries	Traps	Enable
cslOxInf0	✔	✔	✔
cslox	✔	✔	✔

SNMP v3

Create New | Edit | Delete

User Name	Security Level	Notification Host	Queries

1.4 Policy

Seq.#	Source	Destination	Schedule	Service	Action	NAT	AV	Web Filter	Application Control	IPS	Email Filter
IOS VPN - wan1 (Csl-Wan) (1 - 1)											
1	IOS VPN_range	all	always	ALL	✔ ACCEPT	Enable					
IOS VPN - wan2 (Csl-Internal) (2 - 2)											
2	IOS VPN_range	all	always	ALL	✔ ACCEPT	Enable					
port1 (Lan) - port1 (Lan) (3 - 3)											
3	all	all	always	ALL	✔ ACCEPT	Disable					
port1 (Lan) - port2 (Dmz) (4 - 4)											
4	NW_Internal	EQ_Fortianaly	always	ALL	✔ ACCEPT	Disable					
port1 (Lan) - Test_AWN (5 - 5)											
5	Test_AWN_local	Test_AWN_remote	always	ALL	✔ ACCEPT	Disable					
port1 (Lan) - To_Koyo (6 - 6)											
port1 (Lan) - wan1 (Csl-Wan) (7 - 9)											
9	Group_Register	all	always	ALL	✔ ACCEPT	Enable					
port1 (Lan) - wan2 (Csl-Internal) (10 - 10)											
10	Group_Register FW_Register	all	always	ALL	✔ ACCEPT	Enable					
port2 (Dmz) - wan1 (Csl-Wan) (11 - 11)											
11	EQ_Fortianaly	all	always	ALL	✔ ACCEPT	Enable					
ssl.root (sslvpn tunnel interface) - port1 (Lan) (12 - 12)											
12	SSLVPN_TUNNEL_ADDR1 SSL_Group	NW_Internal	always	ALL	✔ ACCEPT	Disable					
ssl.root (sslvpn tunnel interface) - wan1 (Csl-Wan) (13 - 13)											
13	SSLVPN_TUNNEL_ADDR1 SSL_Group	all	always	ALL	✔ ACCEPT	Enable					
ssl.root (sslvpn tunnel interface) - wan2 (Csl-Internal) (14 - 14)											
14	SSLVPN_TUNNEL_ADDR1 SSL_Group	all	always	ALL	✔ ACCEPT	Enable					
Test_AWN - port1 (Lan) (15 - 15)											
15	Test_AWN_remote	Test_AWN_local	always	ALL	✔ ACCEPT	Disable					
To_Koyo - port1 (Lan) (16 - 16)											
wan1 (Csl-Wan) - port1 (Lan) (17 - 17)											
17	all	VIP_NOX	always	RDP	✔ ACCEPT	Disable					
wan1 (Csl-Wan) - port2 (Dmz) (18 - 18)											
18	all	Fortianaly	always	TCP_4433 HTTPS	✔ ACCEPT	Disable					
Implicit (19 - 19)											
19	all	all	always	ALL	⊘ DENY						

2. Juniper SSG20

2.1 Interfaces

Name	IP/Netmask	Zone	Type	Link	PPPoE	Configure	
adsl1/0	0.0.0.0/0	Null	Unused	Down	-	Edit	
bgroup0	0.0.0.0/0	Null	Unused	Down	-	Edit	
bgroup1	0.0.0.0/0	Null	Unused	Down	-	Edit	
bgroup2	0.0.0.0/0	Null	Unused	Down	-	Edit	
bgroup3	0.0.0.0/0	Null	Unused	Down	-	Edit	
ethernet0/0	0.0.0.0/0	Untrust	Layer3	Down	-	Edit	
ethernet0/1	192.168.100.1/24	Trust	Layer3	Up	-	Edit	
ethernet0/2	1.1.1.1/24	Manage	Layer3	Up	-	Edit	
ethernet0/3	58.137.172.86/29	Untrust	Layer3	Up	-	Edit	
ethernet0/4	10.10.100.1/24	Trust	Layer3	Down	-	Edit	
serial0/0	0.0.0.0/0	Null	Unused	Down	-	Edit	
serial2/0	0.0.0.0/0	Null	WAN	Down	-	Edit	
tunnel.1	unnumbered	VPN	Tunnel	Up	-	Edit	
vlan1	0.0.0.0/0	VLAN	Layer3	Down	-	Edit	
wireless0/0	172.16.100.1/24	Trust	Layer3	Down	-	Edit	Activate
wireless0/1	0.0.0.0/0	Null	Unused	Down	-	Edit	
wireless0/2	0.0.0.0/0	Null	Unused	Down	-	Edit	
wireless0/3	0.0.0.0/0	Null	Unused	Down	-	Edit	

2.2 Routing

trust-vr

	IP/Netmask	Gateway	Interface	Protocol	Preference	Metric	Vsys	Description	Configure
*	192.168.100.0/24		ethernet0/1	C			Root		-
*	192.168.100.1/32		ethernet0/1	H			Root		-
*	192.168.99.0/24		ethernet0/1	C			Root		-
*	192.168.99.10/32		ethernet0/1	H			Root		-
*	1.1.1.0/24		ethernet0/2	C			Root		-
*	1.1.1.1/32		ethernet0/2	H			Root		-
*	58.137.172.80/29		ethernet0/3	C			Root		-
*	58.137.172.86/32		ethernet0/3	H			Root		-
	10.10.100.0/24		ethernet0/4	C			Root		-
	10.10.100.1/32		ethernet0/4	H			Root		-
	172.16.100.0/24		wireless0/0	C			Root		-
	172.16.100.1/32		wireless0/0	H			Root		-
*	0.0.0.0/0	58.137.172.81	ethernet0/3	S	5	1	Root		Remove
*	192.168.168.0/24		tunnel.1	S	10	1	Root		Remove
*	203.146.64.0/24	192.168.99.1	ethernet0/1	S	20	1	Root		Remove
*	203.146.30.0/24	192.168.99.1	ethernet0/1	S	20	1	Root		Remove
*	210.1.27.67/32	192.168.99.1	ethernet0/1	S	20	1	Root		Remove
*	203.146.43.0/24	192.168.99.1	ethernet0/1	S	20	1	Root		Remove
*	203.170.160.159/32	192.168.99.1	ethernet0/1	S	20	1	Root		Remove
*	192.168.2.99/32	192.168.99.1	ethernet0/1	S	20	1	Root		Remove

* Active route C Connected I Imported eB EBGP O OSPF E1 OSPF external type 1 H Host Route
P Permanent S Static A Auto-Exported iB IBGP R RIP E2 OSPF external type 2
D Dynamic N NHRP

2.3 Policy

From Trust To Untrust, total policy: 9

ID	Source	Destination	Service	Action	Options	Configure			Enable	Move
63	Internal_192.168.100.0_24	ASA5505_10.10.10.0	ANY			Edit	Clone	Remove	☑	
56	Internal_192.168.100.0_24	SRX240_10.1.1.0	ANY			Edit	Clone	Remove	☑	
9	Internal_192.168.100.0_24	CR25I_192.168.93.0	ANY			Edit	Clone	Remove	☑	
58	Internal_192.168.100.0_24	ASG110_192.168.1.0	ANY			Edit	Clone	Remove	☑	
61	Internal_192.168.100.0_24	CP4400_11.11.11.0	ANY			Edit	Clone	Remove	☑	
65	Internal_192.168.100.0_24	Meraki_192.168.128.0	ANY			Edit	Clone	Remove	☑	
67	Internal_192.168.100.0_24	PA200_172.16.0.0	ANY			Edit	Clone	Remove	☑	
15	Authen User	Any	ANY			Edit	Clone	Remove	☐	
1	IP_L2TP IP_Legion IP_Lex IP_Shinobu NW_10.10.100.0_24 WIFI_172.16.100.0_24	Any	ANY			Edit	Clone	Remove	☑	

From Untrust To Trust, total policy: 10

ID	Source	Destination	Service	Action	Options	Configure			Enable	Move
23	Dial-Up VPN	Any	ANY			Edit	Clone	Remove	☑	
64	ASA5505_10.10.10.0	Internal_192.168.100.0_24	ANY			Edit	Clone	Remove	☑	
57	SRX240_10.1.1.0	Internal_192.168.100.0_24	ANY			Edit	Clone	Remove	☑	
10	CR25I_192.168.93.0	Internal_192.168.100.0_24	ANY			Edit	Clone	Remove	☑	
59	ASG110_192.168.1.0	Internal_192.168.100.0_24	ANY			Edit	Clone	Remove	☑	
62	CP4400_11.11.11.0	Internal_192.168.100.0_24	ANY			Edit	Clone	Remove	☑	
66	Meraki_192.168.128.0	Internal_192.168.100.0_24	ANY			Edit	Clone	Remove	☑	
68	PA200_172.16.0.0	Internal_192.168.100.0_24	ANY			Edit	Clone	Remove	☑	
69	Any	VIP(58.137.172.82)	HTTP HTTPS SYSLOG TCP_8888			Edit	Clone	Remove	☐	
49	Any	VIP(58.137.172.82)	TCP_23000 TCP_8295			Edit	Clone	Remove	☐	

From Trust To Manage, total policy: 1

ID	Source	Destination	Service	Action	Options	Configure			Enable	Move
38	Internal_192.168.100.0_24	Any	ANY			Edit	Clone	Remove	☑	

3. Cisco ASA5505

```
ASA-COPS# sh run
: Saved
:
ASA Version 8.4(4)
!
hostname ASA-COPS
domain-name default.domain.invalid
enable password B0E4.nWAV.g9ZwlV encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface Ethernet0/0
interface Ethernet0/1
 shutdown
interface Ethernet0/2
 shutdown
interface Ethernet0/3
 shutdown
interface Ethernet0/4
 shutdown
interface Ethernet0/5
 shutdown
interface Ethernet0/6
 shutdown
interface Ethernet0/7
 switchport access vlan 100
interface Vlan1
 nameif Inside
 security-level 100
```

```
 ip address 10.10.10.1 255.255.255.0
interface Vlan100
 nameif Outside
 security-level 0
 ip address 58.137.180.2 255.255.255.248
boot system disk0:/asa844-k8.bin
ftp mode passive
clock timezone ICT 7
dns domain-lookup Outside
dns server-group DefaultDNS
 name-server 203.146.237.237
 name-server 203.146.237.222
 domain-name default.domain.invalid
same-security-traffic permit inter-interface
same-security-traffic permit intra-interface
object network NW_10.10.10.0_24
 subnet 10.10.10.0 255.255.255.0
object network NW_192.168.100.0_24
 subnet 192.168.100.0 255.255.255.0
object network NW_58.137.172.80
 subnet 58.137.172.80 255.255.255.248
object-group protocol TCPUDP
 protocol-object udp
 protocol-object tcp
access-list Inside_access_in extended permit object-group TCPUDP object NW_10.10
.10.0_24 any eq domain
access-list Inside_access_in extended permit ip object NW_10.10.10.0_24 any
access-list Outside_cryptomap extended permit ip object NW_10.10.10.0_24 object
NW_192.168.100.0_24
```

access-list Outside_access_in extended permit ip object NW_192.168.100.0_24 obje
ct NW_10.10.10.0_24

access-list Inside_authentication extended permit tcp object NW_10.10.10.0_24 an
y inactive

pager lines 24

logging enable

logging timestamp

logging buffer-size 10000

logging console notifications

logging buffered debugging

logging trap debugging

logging asdm informational

logging facility 23

logging host Outside 58.137.172.82

mtu Inside 1500

mtu Outside 1500

ip local pool VPN_Pool 10.10.10.100-10.10.10.110 mask 255.255.255.0

icmp unreachable rate-limit 1 burst-size 1

icmp permit any Inside

icmp permit any Outside

asdm image disk0:/asdm-702.bin

asdm history enable

arp timeout 14400

nat (Outside,Outside) source dynamic NW_10.10.10.0_24 interface

nat (Inside,Outside) source static NW_10.10.10.0_24 NW_10.10.10.0_24 destination
static NW_192.168.100.0_24 NW_192.168.100.0_24 unidirectional no-proxy-arp

nat (Inside,Outside) source dynamic NW_10.10.10.0_24 interface

access-group Inside_access_in in interface Inside

access-group Outside_access_in in interface Outside

route Outside 0.0.0.0 0.0.0.0 58.137.180.1 1

```
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
aaa-server AD protocol ldap
aaa-server AD (Inside) host 10.10.10.10
 ldap-base-dn dc=ians,dc=net
 ldap-scope subtree
 ldap-naming-attribute sAMAccountName
 ldap-login-password *****
 ldap-login-dn cn=administrator,cn=users,dc=ians,dc=net
 server-type microsoft
user-identity domain ians aaa-server AD
user-identity default-domain LOCAL
user-identity action domain-controller-down ians disable-user-identity-rule
no user-identity inactive-user-timer
aaa authentication ssh console LOCAL
aaa authentication enable console LOCAL
aaa authentication http console LOCAL
aaa authentication match Inside_authentication Inside AD
http server enable
http 0.0.0.0 0.0.0.0 Inside
http 0.0.0.0 0.0.0.0 Outside
snmp-server group 1 v3 priv
snmp-server group tee v3 priv
```

snmp-server user tee1 tee v3 encrypted auth md5 f0:d6:1d:ff:41:93:b2:f3:c6:22:eb :c2:75:e3:af:c1 priv 3des f0:d6:1d:ff:41:93:b2:f3:c6:22:eb:c2:75:e3:af:c1:80:52: b5:c3:fb:85:8d:38:bd:4f:3e:ba:f3:51:6b:86

snmp-server user admin 1 v3 encrypted auth md5 23:65:d7:00:cb:fb:ce:85:d9:f9:65: 48:bf:4b:ca:86 priv des 23:65:d7:00:cb:fb:ce:85:d9:f9:65:48:bf:4b:ca:86

snmp-server host Inside 192.168.99.111 version 3 admin

snmp-server host Outside 192.168.99.111 community ***** version 2c

no snmp-server location

no snmp-server contact

snmp-server community *****

snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart

snmp-server enable traps syslog

crypto ipsec ikev1 transform-set ESP-AES-128-SHA esp-aes esp-sha-hmac

crypto ipsec ikev1 transform-set ESP-AES-128-MD5 esp-aes esp-md5-hmac

crypto ipsec ikev1 transform-set ESP-AES-192-SHA esp-aes-192 esp-sha-hmac

crypto ipsec ikev1 transform-set ESP-AES-192-MD5 esp-aes-192 esp-md5-hmac

crypto ipsec ikev1 transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac

crypto ipsec ikev1 transform-set ESP-AES-256-MD5 esp-aes-256 esp-md5-hmac

crypto ipsec ikev1 transform-set ESP-AES-128-SHA-TRANS esp-aes esp-sha-hmac

crypto ipsec ikev1 transform-set ESP-AES-128-SHA-TRANS mode transport

crypto ipsec ikev1 transform-set ESP-AES-128-MD5-TRANS esp-aes esp-md5-hmac

crypto ipsec ikev1 transform-set ESP-AES-128-MD5-TRANS mode transport

crypto ipsec ikev1 transform-set ESP-AES-192-SHA-TRANS esp-aes-192 esp-sha-hmac

crypto ipsec ikev1 transform-set ESP-AES-192-SHA-TRANS mode transport

crypto ipsec ikev1 transform-set ESP-AES-192-MD5-TRANS esp-aes-192 esp-md5-hmac

crypto ipsec ikev1 transform-set ESP-AES-192-MD5-TRANS mode transport

crypto ipsec ikev1 transform-set ESP-AES-256-SHA-TRANS esp-aes-256 esp-sha-hmac

crypto ipsec ikev1 transform-set ESP-AES-256-SHA-TRANS mode transport

crypto ipsec ikev1 transform-set ESP-AES-256-MD5-TRANS esp-aes-256 esp-md5-hmac

crypto ipsec ikev1 transform-set ESP-AES-256-MD5-TRANS mode transport

```
crypto ipsec ikev1 transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-3DES-SHA-TRANS esp-3des esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-3DES-SHA-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-3DES-MD5-TRANS esp-3des esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-3DES-MD5-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-DES-SHA esp-des esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-DES-MD5 esp-des esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-DES-SHA-TRANS esp-des esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-DES-SHA-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-DES-MD5-TRANS esp-des esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-DES-MD5-TRANS mode transport
crypto ipsec security-association replay disable
crypto map Outside_map1 1 match address Outside_cryptomap
crypto map Outside_map1 1 set pfs
crypto map Outside_map1 1 set peer 58.137.172.86
crypto map Outside_map1 1 set ikev1 transform-set ESP-AES-128-SHA ESP-AES-128-MD
5 ESP-AES-192-SHA ESP-AES-192-MD5 ESP-AES-256-SHA ESP-AES-256-MD5 ESP-3DES-
SHA 3DES-MD5 ESP-DES-SHA ESP-DES-MD5
crypto map Outside_map1 1 set nat-t-disable
crypto map Outside_map1 interface Outside
crypto ca trustpoint _SmartCallHome_ServerCA
 crl configure
crypto ca trustpoint ASDM_TrustPoint0
 enrollment self
 subject-name CN=ASA-COPS
 keypair cops
 crl configure
crypto ca certificate chain ASDM_TrustPoint0
 certificate be6e1e59
```

```
 quit
crypto ikev1 enable Outside
crypto ikev1 policy 10
 authentication crack
 encryption aes-256
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 20
 authentication rsa-sig
 encryption aes-256
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 30
 authentication pre-share
 encryption aes-256
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 40
 authentication crack
 encryption aes-192
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 50
 authentication rsa-sig
 encryption aes-192
 hash sha
```

group 2
lifetime 86400
crypto ikev1 policy 60
authentication pre-share
encryption aes-192
hash sha
group 2
lifetime 86400
crypto ikev1 policy 70
authentication crack
encryption aes
hash sha
group 2
lifetime 86400
crypto ikev1 policy 80
authentication rsa-sig
encryption aes
hash sha
group 2
lifetime 86400
crypto ikev1 policy 90
authentication pre-share
encryption aes
hash sha
group 2
lifetime 86400
crypto ikev1 policy 100
authentication crack
encryption 3des
hash sha

group 2

lifetime 86400

crypto ikev1 policy 110

authentication rsa-sig

encryption 3des

hash sha

group 2

lifetime 86400

crypto ikev1 policy 120

authentication pre-share

encryption 3des

hash sha

group 2

lifetime 86400

crypto ikev1 policy 130

authentication crack

encryption des

hash sha

group 2

lifetime 86400

crypto ikev1 policy 140

authentication rsa-sig

encryption des

hash sha

group 2

lifetime 86400

crypto ikev1 policy 150

authentication pre-share

encryption des

hash sha

```
 group 2
 lifetime 86400
telnet timeout 5
ssh 0.0.0.0 0.0.0.0 Inside
ssh 58.137.172.80 255.255.255.248 Outside
ssh 202.183.152.6 255.255.255.255 Outside
ssh timeout 5
ssh key-exchange group dh-group1-sha1
console timeout 0
management-access Inside

threat-detection basic-threat
threat-detection statistics port
threat-detection statistics protocol
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
ntp server 203.146.30.185 source Outside
ssl encryption 3des-sha1
webvpn
 enable Outside
 anyconnect image disk0:/anyconnect-win-4.1.04011-k9.pkg 1
 anyconnect enable
group-policy SSLPolicy internal
group-policy SSLPolicy attributes
 wins-server none
 dns-server value 203.146.237.237
 vpn-tunnel-protocol ssl-client
 default-domain none
group-policy DfltGrpPolicy attributes
 dns-server value 203.146.237.237
```

```
 vpn-tunnel-protocol ikev1 ikev2 l2tp-ipsec ssl-client ssl-clientless
group-policy GroupPolicy1 internal
group-policy GroupPolicy1 attributes
 vpn-tunnel-protocol ikev1
username csl password Ap66Zz1WtDVyx5rG encrypted privilege 15
username copsadmin password F5bkeofjkqHBvXC4 encrypted privilege 15
tunnel-group DefaultWEBVPNGroup general-attributes
 address-pool VPN_Pool
 default-group-policy SSLPolicy
tunnel-group 58.137.172.86 type ipsec-l2l
tunnel-group 58.137.172.86 general-attributes
 default-group-policy GroupPolicy1
tunnel-group 58.137.172.86 ipsec-attributes
 ikev1 pre-shared-key *****
!
class-map inspection_default
 match default-inspection-traffic
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect ip-options
  inspect netbios
```

```
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
  inspect icmp
!
service-policy global_policy global
prompt hostname context
call-home reporting anonymous
call-home
 profile CiscoTAC-1
  no active
  destinationaddresshttp
  destination address email callhome@cisco.com
  destination transport-method http
  subscribe-to-alert-group diagnostic
  subscribe-to-alert-group environment
  subscribe-to-alert-group inventory periodic monthly
  subscribe-to-alert-group configuration periodic monthly
  subscribe-to-alert-group telemetry periodic daily
Cryptochecksum:48032645b296e32f197d995814a9894c
: end
```

4. Juniper MX80

```
root@cops# show
## Last changed: 2018-09-26 13:50:52 ICT
version 13.3R6.5;
groups {
    global {
        system {
            root-authentication {
                encrypted-password "$1$s0GiEDYB$OBajzZTHcN1/sOtUSq2VA/"; ##
SECRET-DATA
            }
        }
    }
}
apply-groups global;
system {
    host-name cops;
    domain-name csloxinfo.net;
    time-zone Asia/Bangkok;
    root-authentication {
        encrypted-password "$1$RvD2g1Mv$7LOzJZUMwZB1EECDczZGt0"; ## SECRET-
DATA
    }
    name-server {
        203.146.237.237;
        203.146.237.222;
    }

    syslog {
        user * {
```

```
            any emergency;
        }
        host 58.137.70.58 {
            any error;
        }
        file messages {
            any notice;
            authorization info;
        }
        file interactive-commands {
            interactive-commands any;
        }
        file jnpr {
            any none;
            daemon info;
            match "(.* UpDown gr-.+ .*)|(.* Add gr-.+ .*)";
        }
    }
    max-configurations-on-flash 5;
    ##
    ## Warning: statement ignored: unsupported platform (mx80)
    ##
    max-configuration-rollbacks 5;
    ntp {
        server 203.146.30.185;
    }
}
chassis {
    fpc 1 {
        pic 1 {
```

```
            tunnel-services {
                bandwidth 1g;
            }
        }
    }
}
interfaces {
    ge-1/0/0 {
        unit 0 {
            family inet {
                address 202.183.152.2/30 {
                    primary;
                }
            }
        }
    }
    ge-1/0/1 {
        unit 0 {
            family inet {
                address 58.137.59.17/29 {
                    primary;
                }
                address 203.172.32.1/29;
                address 58.137.180.1/29;
                address 202.183.246.9/29;
                address 58.137.3.113/29;
                address 202.183.152.5/30;
                address 58.137.32.97/29;
                address 58.137.88.1/28;
                address 58.137.228.41/29;
```

```
                address 58.137.70.57/29;
                address 58.137.150.145/29;
                address 58.137.164.225/29;
                address 58.137.90.49/28;
                address 58.137.84.145/28;
                address 58.137.172.81/29;
            }
        }
    }
    gr-1/1/10 {
        unit 0 {
            tunnel {
                source 202.183.152.2;
                destination 202.183.152.1;
            }
            family inet {
                unnumbered-address ge-1/0/0.0;
            }
        }
    }
    lo0 {
        unit 0 {
            family inet {
                filter {
                    input 1;
                }
            }
        }
    }
}
```

```
snmp {
    community cslox {
        authorization read-only;
    }
}
routing-options {
    static {
        route 58.137.88.2/32 next-hop 58.137.150.146;
        route 58.137.180.5/32 next-hop 58.137.150.146;
        route 58.137.180.6/32 next-hop 58.137.59.18;
        route 202.183.231.242/32 next-hop 58.137.150.146;
        route 202.183.246.10/32 next-hop 58.137.150.146;
        route 203.172.32.2/32 next-hop 58.137.150.146;
        route 58.137.164.232/29 next-hop 58.137.164.226;
        route 0.0.0.0/0 next-hop 202.183.152.1;
        route 203.146.78.85/32 next-hop 202.183.152.6;
        route 58.137.84.17/32 next-hop 58.137.150.146;
        route 58.137.228.44/30 next-hop 58.137.3.114;
        route 58.137.196.252/32 next-hop 58.137.70.58;
        route 202.183.128.10/32 next-hop 202.183.152.6;
    }
}
protocols {
    oam {
        gre-tunnel;
    }
}
firewall {
    family inet {
        filter 1 {
```

```
            term 1 {
                from {
                    address {
                        58.137.88.0/29;
                        58.137.172.80/29;
                        202.183.152.0/29;
                    }
                    destination-port ssh;
                }
                then accept;
            }
            term 2 {
                from {
                    source-address {
                        0.0.0.0/0;
                    }
                    destination-port ssh;
                }
                then {
                    discard;
                }
            }
            term 3 {
                then accept;
            }
        }
    }
}
```

[edit]

5. Foundry Edgelron 2402CF

```
Vty-0#show running-config
building running-config, please wait.....
!
hostname Core_SW
SNTP server 0.0.0.0 0.0.0.0 0.0.0.0
!
default-vlan-id 100
!
snmp-server community public ro
snmp-server community private rw
snmp-server community cslox ro
!
username csl access-level 15
username csl password 7 f71d7b86d4e68d6258b3a6f06f6a0ced
enable password level 15 7 9f1fcd483e68f07a570bf328fb6e5647
!
vlan 1 name DefaultVlan
 untagged ethernet 1/1 to 1/18
!
vlan 100 by port
 untagged ethernet 1/19 to 1/26
!
vlan 200 by port
!
spanning-tree mst configuration
interface ethernet 1/1
!
interface ethernet 1/2
!
```

interface ethernet 1/3

!

interface ethernet 1/4

!

interface ethernet 1/5

!

interface ethernet 1/6

!

interface ethernet 1/7

!

interface ethernet 1/8

!

interface ethernet 1/9

!

interface ethernet 1/10

!

interface ethernet 1/11

!

interface ethernet 1/12

!

interface ethernet 1/13

!

interface ethernet 1/14

interface ethernet 1/15

!

interface ethernet 1/16

!

interface ethernet 1/17

!

interface ethernet 1/18

```
!
interface ethernet 1/19
!
interface ethernet 1/20
!
interface ethernet 1/21
!
interface ethernet 1/22
!
interface ethernet 1/23
!
interface ethernet 1/24
!
interface ethernet 1/25
!
interface ethernet 1/26
!
interface VLAN 100
 IP address 1.1.1.2 255.255.255.0
!
IP default-gateway  1.1.1.1
!
no spanning-tree
no map IP precedence
no map IP DSCP
!
line console
!
line VTY
!
```

end

Vty-0#show version

Unit1

Serial number : AN08140811

Hardware version : R01

Module A type : Combo 1000BaseT SFP

Module B type : Combo 1000BaseT SFP

Number of ports : 26

Main power status : Up

Redundant power status : Not present

Agent (Master)

Unit ID : 1

Loader version : 2.2.0.1

Boot ROM version : 2.2.0.8

Operation code version : 2.2.7.31

6. Cisco 3500XL

COPS_Public#sh run

Building configuration...

Current configuration:

!

version 12.0

no service pad

service timestamps debug uptime

service timestamps log uptime

service password-encryption

!

hostname COPS_Public

```
!
enable password 7 0152260A485B080338
!
username csl password 7 03457B05155F2F4057
!
no spanning-tree vlan 1
no spanning-tree vlan 100
ip subnet-zero
!
interface FastEthernet0/1
!
interface FastEthernet0/2
 switchport access vlan 100
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
```

```
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
 switchport access vlan 100
!
interface FastEthernet0/17
 switchport access vlan 100
!
interface FastEthernet0/18
 switchport access vlan 100
!
interface FastEthernet0/19
 switchport access vlan 100
!
interface FastEthernet0/20
 switchport access vlan 100
!
interface FastEthernet0/21
 switchport access vlan 100
!
interface FastEthernet0/22
 switchport access vlan 100
```

```
!
interface FastEthernet0/23
 switchport access vlan 100
!
interface FastEthernet0/24
 switchport access vlan 100
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface VLAN1
 no ip address
 no ip directed-broadcast
 no ip route-cache
 shutdown
!
interface VLAN100
 ip address 1.1.1.3 255.255.255.0
 no ip directed-broadcast
 no ip route-cache
!
ip default-gateway 1.1.1.1
snmp-server engineID local 0000000902000003E3A64980
snmp-server community cslox RO
!
line con 0
 transport input none
 stopbits 1
line vty 0 4
```

```
 login local
line vty 5 15
 login
end
```

7. Cisco 3500XL

```
COPS_WAN_FW#sh run
Building configuration...

Current configuration:
!
version 12.0
no service pad
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname COPS_WAN_FW
!
enable password 7 1344371C185C0A2632
!
username csl password 7 041A2B081C71424210
!
no spanning-tree vlan 1
no spanning-tree vlan 100
ip subnet-zero
!
interface FastEthernet0/1
!
interface FastEthernet0/2
```

```
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
 switchport access vlan 100
!
interface FastEthernet0/15
 switchport access vlan 100
!
interface FastEthernet0/16
```

```
 switchport access vlan 100
!
interface FastEthernet0/17
 switchport access vlan 100
!
interface FastEthernet0/18
 switchport access vlan 100
!
interface FastEthernet0/19
 switchport access vlan 100
!
interface FastEthernet0/20
 switchport access vlan 100
!
interface FastEthernet0/21
 switchport access vlan 100
!
interface FastEthernet0/22
 switchport access vlan 100
!
interface FastEthernet0/23
 switchport access vlan 100
!
interface FastEthernet0/24
 switchport access vlan 100
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface VLAN1
```

```
 no ip address
 no ip directed-broadcast
 no ip route-cache
 shutdown
!
interface VLAN100
 ip address 1.1.1.4 255.255.255.0
 no ip directed-broadcast
 no ip route-cache
!
ip default-gateway 1.1.1.1
snmp-server engineID local 000000090200005080583240
snmp-server community cslox RO
!
line con 0
 transport input none
 stopbits 1
line vty 0 4
 login local
line vty 5 15
 login
end
```

8. Cisco 3560

```
COPS_LAN_FW#sh run
Building configuration...

Current configuration : 2411 bytes
!
version 12.2
```

```
no service pad
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname COPS_LAN_FW
!
enable password 7 15532B02177A252831
!
username csl password 7 15532B02177A252831
no aaa new-model
vtp mode transparent
ip subnet-zero
ip routing
!
no file verify auto
!
spanning-tree mode pvst
spanning-tree extend system-id
no spanning-tree vlan 1,100,888
!
vlan internal allocation policy ascending
!
vlan 11,100,888,999
!
interface FastEthernet0/1
 switchport access vlan 11
!
interface FastEthernet0/2
 switchport access vlan 11
```

```
!
interface FastEthernet0/3
 switchport access vlan 11
!
interface FastEthernet0/4
 switchport access vlan 11
!
interface FastEthernet0/5
 switchport access vlan 100
!
interface FastEthernet0/6
 switchport access vlan 100
!
interface FastEthernet0/7
 switchport access vlan 100
 switchport mode access
!
interface FastEthernet0/8
 switchport access vlan 100
!
interface FastEthernet0/9
 switchport access vlan 100
!
interface FastEthernet0/10
 switchport access vlan 100
!
interface FastEthernet0/11
 switchport access vlan 100
!
interface FastEthernet0/12
```

```
 switchport access vlan 100
!
interface FastEthernet0/13
 switchport access vlan 100
!
interface FastEthernet0/14
 switchport access vlan 100
!
interface FastEthernet0/15
 switchport access vlan 100
!
interface FastEthernet0/16
 switchport access vlan 100
interface FastEthernet0/17
 switchport access vlan 100
!
interface FastEthernet0/18
 switchport access vlan 100
!
interface FastEthernet0/19
 switchport access vlan 100
!
interface FastEthernet0/20
 switchport access vlan 100
!
interface FastEthernet0/21
 switchport access vlan 100
!
interface FastEthernet0/22
 switchport access vlan 100
```

```
!
interface FastEthernet0/23
 switchport access vlan 100
!
interface FastEthernet0/24
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 100
 switchport trunk allowed vlan 1,100,888,999
 switchport mode trunk
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 no ip mroute-cache
 shutdown
!
interface Vlan100
 ip address 192.168.100.10 255.255.255.0
 no ip mroute-cache
!
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.100.1 name Defauft_Route
ip http server
ip http secure-server
!
snmp-server community cslox RO
control-plane
```

```
!
line con 0
line vty 0 4
 login local
line vty 5 15
 no login
end
```

ภาคผนวก ข

การเชื่อมต่อของอุปกรณ์เครือข่าย

2.2.2 DELL PowerEdge 1950 (Unused)

Device Information

Hostname	-	IP Address	-
Brand	DELL	Model	PowerEdge 1950
Serial Number	-	Software Version	-
Location	Data Center	EOL Status	-
License Type	-	License Expire Date	-

Port Information

Source Device		Destination Devices		
No.	Port	Connect to	Port	Ref.
-	-	-	-	-

2.2.3 DELL PowerEdge 2950 (Unused)

Device Information

Hostname	-	IP Address	-
Brand	DELL	Model	PowerEdge 2950
Serial Number	-	Software Version	-
Location	Data Center	EOL Status	-
License Type	-	License Expire Date	-

Port Information

Source Device		Destination Devices		
No.	Port	Connect to	Port	Ref.
-	-	-	-	-

2.2.4 Juniper SRX240

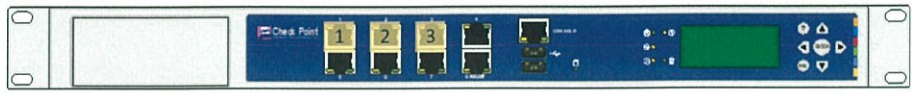
Device Information

Hostname	-	IP Address	192.168.99.15
Brand	Juniper	Model	SRX240
Serial Number	AG1512AA0005	Software Version	-
Location	Data Center	EOL Status	EOS[3]
License Type	-	License Expire Date	-

Port Information

Source Device		Destination Devices		
No.	Port	Connect to	Port	Ref.
1	0/0	Cisco 3500XL	Fa0/19	2.2.21
2	0/1	Cisco 3560	Fa0/20	2.2.23

2.2.5 Check Point 4400



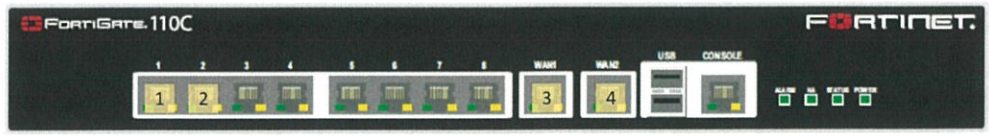
Device Information

Hostname	-	IP Address	-
Brand	Check Point	Model	4400
Serial Number	1310B02056	Software Version	-
Location	Data Center	EOL Status	EOS[3]
License Type	-	License Expire Date	-

Port Information

Source Device		Destination Devices		
No.	Port	Connect to	Port	Ref.
1	1	Cisco 3500XL	Fa0/21	2.2.21
2	2	Cisco 3560	Fa0/21	2.2.23
3	3	Cisco 3560	Fa0/1	2.2.23

2.2.6 Fortigate 110C



Device Information

Hostname	FoetiGate	IP Address	202.183.152.6
Brand	Fortinet	Model	Fortigate 110C
Serial Number	FG100C3G11614130	Software Version	v5.2.9,build736 (GA)
Location	Data Center	EOL Status	EOL[3]
License Type	-	License Expire Date	-

Port Information

Source Device		Destination Devices		
No.	Port	Connect to	Port	Ref.
1	1	Cisco 3560	Fa0/23	2.2.23
2	2	Fortinet 100C	1	2.2.8
3	WAN1	Cisco 3500XL	Fa0/23	2.2.21
4	WAN2	Juniper EX4600	-	-

2.2.7 Juniper SSG20

Device Information

Hostname	ITS_Service	IP Address	192.168.100.1
Brand	Juniper	Model	SSG20
Serial Number	0164062007000681	Software Version	6.3.0r16a.0
Location	Data Center	EOL Status	-
License Type	-	License Expire Date	-

Port Information

Source Device		Destination Devices		
No.	Port	Connect to	Port	Ref.
1	Eth0/1	Cisco 3560	Fa0/22	2.2.23
2	Eth0/2	Foundry Edgelron 2402CF	Fa21	2.2.16
3	Eth0/3	Cisco 3500XL	Fa0/22	2.2.21

2.2.8 FortiAnalyzer 100C

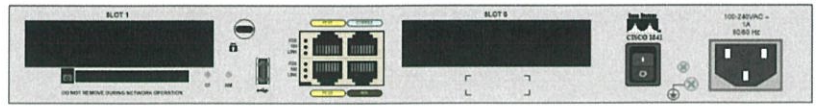
Device Information

Hostname	FAZ100C	IP Address	192.168.2.99
Brand	Fortinet	Model	Fortigate 110C
Serial Number	FL100C3910000656	Software Version	v5.2.9-build0780 160920 (GA)
Location	Data Center	EOL Status	EOL[3]
License Type	-	License Expire Date	-

Port Information

Source Device		Destination Devices		
No.	Port	Connect to	Port	Ref.
1	1	Fortigate 110C	2	2.2.6

2.2.9 Cisco 1841 (Unused)



Device Information

Hostname	-	IP Address	-
Brand	Cisco	Model	1841
Serial Number	-	Software Version	-
Location	Data Center	EOL Status	-
License Type	-	License Expire Date	-

Port Information

Source Device		Destination Devices		
No.	Port	Connect to	Port	Ref.
-	-	-	-	-

2.2.10 Sophos Astaro 110/120

Device Information

Hostname	-	IP Address	192.168.1.1
Brand	Sophos	Model	Astaro 110/120
Serial Number	A1504207E9E95B3	Software Version	-
Location	Data Center	EOL Status	-
License Type	-	License Expire Date	-

Port Information

Source Device		Destination Devices		
No.	Port	Connect to	Port	Ref.
1	Eth0	Cisco 3560	Fa0/8	2.2.23
2	Eth1	Cisco 3500XL	Fa0/14	2.2.21

2.2.11 Cisco ASA5505

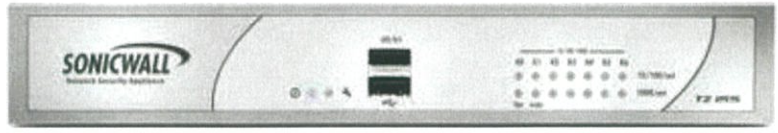
Device Information

Hostname	ASA-COPS	IP Address	58.137.180.2
Brand	Cisco	Model	ASA5505
Serial Number	JMX1123Z15J	Software Version	8.4(4)
Location	Data Center	EOL Status	EOS[3]
License Type	-	License Expire Date	-

Port Information

Source Device		Destination Devices		
No.	Port	Connect to	Port	Ref.
1	Eth0/0	Cisco 3560	Fa0/7	2.2.23
2	Eth0/7	Cisco 3500XL	Fa0/15	2.2.21

2.2.12 Sonic Wall NSA 220 APL24-08E C-11189



Device Information

Hostname	-	IP Address	-
Brand	Sonic Wall	Model	APL24-08E C-11189
Serial Number	0017C5C0434C	Software Version	-
Location	Data Center	EOL Status	One-Year Support
License Type	-	License Expire Date	-

Port Information

Source Device		Destination Devices		
No.	Port	Connect to	Port	Ref.
1	LAN	Cisco 3560	Fa0/16	2.2.23
2	WAN	Cisco 3500XL	Fa0/16	2.2.21

2.2.13 Cyberoam CR25i

Device Information

Hostname	-	IP Address	58.137.88.5
Brand	Cyberoam	Model	CR25i
Serial Number	C016200554	Software Version	-
Location	Data Center	EOL Status	EOL[4]
License Type	-	License Expire Date	-

Port Information

Source Device		Destination Devices		
No.	Port	Connect to	Port	Ref.
1	A	Cisco 3560	Fa0/17	2.2.23
2	B	Cisco 3500XL	Fa0/17	2.2.21

2.2.14 WatchGuard XTM 330

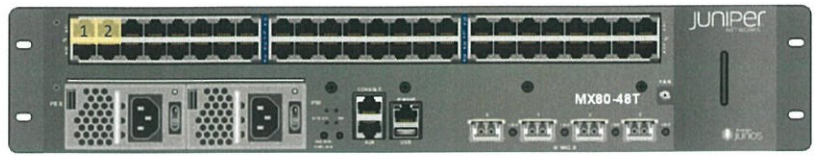
Device Information

Hostname	-	IP Address	192.168.99.11
Brand	WatchGuard	Model	XTM 330
Serial Number	80BD0042F-CDC7	Software Version	-
Location	Data Center	EOL Status	EOS[2]
License Type	-	License Expire Date	-

Port Information

Source Device		Destination Devices		
No.	Port	Connect to	Port	Ref.
1	0	Cisco 3500XL	Fa0/20	2.2.21
2	1	Cisco 3560	Fa0/19	2.2.23

2.2.15 Juniper MX80



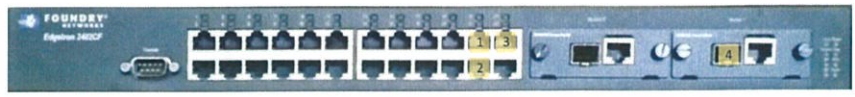
Device Information

Hostname	root@cops	IP Address	58.137.59.17
Brand	Juniper	Model	MX80
Serial Number	-	Software Version	-
Location	Data Center	EOL Status	-
License Type	-	License Expire Date	-

Port Information

Source Device		Destination Devices		
No.	Port	Connect to	Port	Ref.
1	Ge-1/0/0	internet	-	-
2	Ge-1/0/1	Foundry Edgelron 2402CF	Gi26	2.2.16

2.2.16 Foundry Edgelron 2402CF



Device Information

Hostname	Vty-0	IP Address	1.1.1.2
Brand	Foundry	Model	Edgelron 2402CF
Serial Number	AN08140811	Software Version	2.2.7.31
Location	Data Center	EOL Status	-
License Type	-	License Expire Date	-

Port Information

Source Device		Destination Devices		
No.	Port	Connect to	Port	Ref.
1	Fa21	Juniper SSG20	Fa0/2	2.2.7
2	Fa22	Juniper IDP 75	0	2.2.17
3	Fa23	HP Tipping Point 2400E	SEG1 A	2.2.19
4	Gi26	Juniper MX80	Ge-1/0/1	2.2.15

2.2.17 Juniper IDP 75

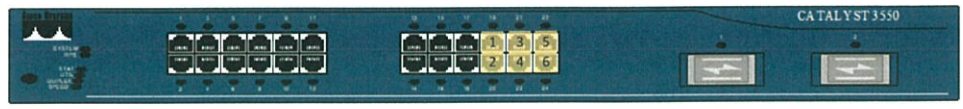
Device Information

Hostname	-	IP Address	-
Brand	Juniper	Model	IDP 75
Serial Number	-	Software Version	-
Location	Data Center	EOL Status	EOS[3]
License Type	-	License Expire Date	-

Port Information

Source Device		Destination Devices		
No.	Port	Connect to	Port	Ref.
1	MGT	Cisco 3500XL	Fa0/23	2.2.18
2	0	Foundry Edgelron 2402CF	Fa22	2.2.16
3	1	Cisco 3500XL	Fa0/24	2.2.18

2.2.18 Cisco 3500XL



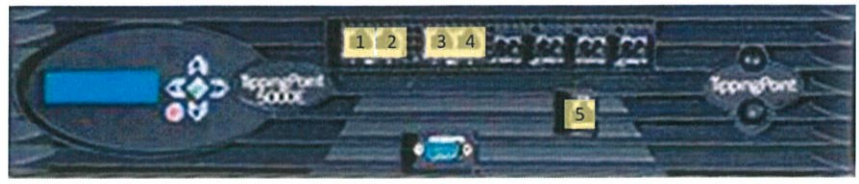
Device Information

Hostname	COPS_Public	IP Address	1.1.1.3
Brand	Cisco	Model	WS-C3524-XL-EN
Serial Number	FAB0516Q0HY	Software Version	12.0(5)WC17
Location	Data Center	EOL Status	EOL[3]
License Type	-	License Expire Date	-

Port Information

Source Device		Destination Devices		
No.	Port	Connect to	Port	Ref.
1	Fa0/19	DELL PowerEdge R610	Gb1	2.2.25
2	Fa0/20	DELL PowerEdge 860	Gb1	2.2.27
3	Fa0/21	HP Tipping Point SMS Server	Gb2	2.2.26
4	Fa0/22	HP Tipping Point 2400E	MGT	2.2.19
5	Fa0/23	Juniper IDP 75	MGT	2.2.17
6	Fa0/24	Juniper IDP 75	1	2.2.17

2.2.19 HP Tipping Point 2400E



Device Information

Hostname	COPS-IPS	IP Address	58.137.32.102
Brand	HP Tipping Point	Model	2400E
Serial Number	8VQ9A0GA19765	Software Version	-
Location	Data Center	EOL Status	EOL[3]
License Type	-	License Expire Date	-

Port Information

Source Device		Destination Devices		
No.	Port	Connect to	Port	Ref.
1	SEG1 A	Foundry Edgelron 2402CF	Fa23	2.2.16
2	SEG1 B	netintact packetlogic PL7800	B	2.2.20
3	SEG2 A	Cisco 3560	Fa0/24	2.2.23
4	SEG2 B	IPOQUE PRX-2G	EXT	2.2.22
5	MGT	Cisco 3500XL	Fa0/22	2.2.18

2.2.20 netintact packetlogic PL7800

Device Information

Hostname	-	IP Address	-
Brand	Netintact packetlogic	Model	PL7800
Serial Number	-	Software Version	-
Location	Data Center	EOL Status	-
License Type	-	License Expire Date	-

Port Information

Source Device		Destination Devices		
No.	Port	Connect to	Port	Ref.
1	Admin	Cisco 3560	Fa0/13	2.2.23
2	B	HP Tipping Point 2400E	SEG1 B	2.2.19
3	C	Cisco 3500XL	Fa0/24	2.2.21

2.2.21 Cisco 3500XL

Device Information

Hostname	COPS_WAN_FW	IP Address	1.1.1.4
Brand	Cisco	Model	WS-C3524-XL-EN
Serial Number	FAA0509I0LP	Software Version	12.0(5)WC7
Location	Data Center	EOL Status	EOL[3]
License Type	-	License Expire Date	-

Port Information

Source Device		Destination Devices		
No.	Port	Connect to	Port	Ref.
1	Fa0/14	Astaro 110/120	Eth1	2.2.10
2	Fa0/15	Cisco ASA5505	Eth0/7	2.2.11
3	Fa0/16	Sonic Wall APL24-08E C-11189	WAN	2.2.12
4	Fa0/17	Cyberoam CR25i	B	2.2.13
5	Fa0/19	Juniper SRX240	0/0	2.2.4
6	Fa0/20	WatchGuard XTM 330	0	2.2.14
7	Fa0/21	Check Point 4400	1	2.2.5
8	Fa0/22	Juniper SSG20	Eth0/3	2.2.7
9	Fa0/23	Fortigate 110C	WAN1	2.2.6
10	Fa0/24	netintact packetlogic PL7800	C	2.2.20

2.2.22 IPOQUE PRX-2G

Device Information

Hostname	-	IP Address	58.137.59.19
Brand	IPQUE	Model	PRX-2G
Serial Number	-	Software Version	-
Location	Data Center	EOL Status	-
License Type	-	License Expire Date	-

Port Information

Source Device		Destination Devices		
No.	Port	Connect to	Port	Ref.
1	EXT	HP Tipping Point 2400E	SEG2 B	2.2.19
2	INT	Media Converter	-	-
3	MGT	Cisco 3560	Fa0/12	2.2.23

2.2.23 Cisco 3560

Device Information

Hostname	COPS_LAN_FW	IP Address	192.168.100.10
Brand	Cisco	Model	WS-C3560-24TS
Serial Number	CAT0951Z1PW	Software Version	12.2 (25) SEE2
Location	Data Center	EOL Status	EOL[3]
License Type	-	License Expire Date	-

Port Information

Source Device		Destination Devices		
No.	Port	Connect to	Port	Ref.
1	Fa0/1	Check Point 4400	3	2.2.5
2	Fa0/2	DELL PowerEdge 1950	Gb1	2.2.28
3	Fa0/3	SUPERMICRO SUPERO	Eth0	2.2.29
4	Fa0/4	IBM System x3650	2	2.2.30
5	Fa0/7	Cisco ASA5505	Eth0/0	2.2.11
6	Fa0/8	Astaro 110/120	Eth0	2.2.10
7	Fa0/10	IBM System x3650	1	2.2.30
8	Fa0/12	IPOQUE PRX-2G	MGT	2.2.22
9	Fa0/13	netintact packetlogic PL7800	Admin	2.2.20
10	Fa0/14	DELL PowerEdge 1950	Gb2	2.2.28
11	Fa0/15	DELL PowerEdge R610	Gb2	2.2.25
12	Fa0/16	Sonic Wall APL24-08E C-11189	LAN	2.2.12
13	Fa0/17	Cyberoam CR25i	A	2.2.13
14	Fa0/19	WatchGuard XTM 330	1	2.2.14
15	Fa0/20	Juniper SRX240	0/1	2.2.4
16	Fa0/21	Check Point 4400	2	2.2.5

Source Device		Destination Devices		
No.	Port	Connect to	Port	Ref.
17	Fa0/22	Juniper SSG20	Eth0/1	2.2.7
18	Fa0/23	Fortigate 110C	1	2.2.6
19	Fa0/24	HP Tipping Point 2400E	SEG2 A	2.2.19

2.2.24 DELL Power Edge 860 (Unused)

Device Information

Hostname	-	IP Address	-
Brand	DELL	Model	PowerEdge 860
Serial Number	-	Software Version	-
Location	Data Center	EOL Status	-
License Type	-	License Expire Date	-

Port Information

Source Device		Destination Devices		
No.	Port	Connect to	Port	Ref.
-	-	-	-	-

2.2.25 DELL PowerEdge 1950

Device Information

Hostname	-	IP Address	-
Brand	DELL	Model	PowerEdge R610
Serial Number	-	Software Version	-
Location	Data Center	EOL Status	EOL[3]
License Type	-	License Expire Date	-

Port Information

Source Device		Destination Devices		
No.	Port	Connect to	Port	Ref.
1	Gb1	Cisco 3500XL	Fa0/19	2.2.18
2	Gb2	Cisco 3560	Fa0/15	2.2.23

2.2.26 HP Tipping Point SMS Server

Device Information

Hostname	-	IP Address	-
Brand	HP	Model	Tipping Point SMS Server
Serial Number	8VLA7X000053	Software Version	-
Location	Data Center	EOL Status	-
License Type	-	License Expire Date	-

Port Information

Source Device		Destination Devices		
No.	Port	Connect to	Port	Ref.
1	Gb2	Cisco 3500XL	Fa0/21	2.2.18

2.2.27 DELL PowerEdge 860

Device Information

Hostname	-	IP Address	-
Brand	DELL	Model	PowerEdge 860
Serial Number	5GW2N1S	Software Version	-
Location	Data Center	EOL Status	-
License Type	-	License Expire Date	-

Port Information

Source Device		Destination Devices		
No.	Port	Connect to	Port	Ref.
1	Gb1	Cisco 3500XL	Fa0/20	2.2.18

2.2.28 DELL PowerEdge 1950

Device Information

Hostname	-	IP Address	-
Brand	DELL	Model	PowerEdge 1950
Serial Number	-	Software Version	-
Location	Data Center	EOL Status	EOL[3]
License Type	-	License Expire Date	-

Port Information

Source Device		Destination Devices		
No.	Port	Connect to	Port	Ref.
1	Gb1	Cisco 3560	Fa0/2	2.2.23
2	Gb2	Cisco 3560	Fa0/14	2.2.23

2.2.29 SUPERMICRO SUPERO

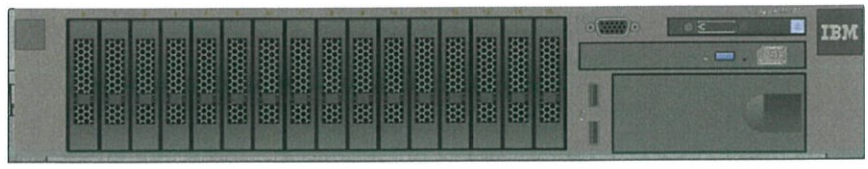
Device Information

Hostname	-	IP Address	-
Brand	SUPERMICRO	Model	SUPERO
Serial Number	-	Software Version	-
Location	Data Center	EOL Status	-
License Type	-	License Expire Date	-

Port Information

Source Device		Destination Devices		
No.	Port	Connect to	Port	Ref.
1	Eth0	Cisco 3560	Fa0/3	2.2.23

2.2.30 IBM System x3650



Device Information

Hostname	-	IP Address	-
Brand	IBM	Model	System x3650
Serial Number	99BZ648	Software Version	-
Location	Data Center	EOL Status	EOL[3]
License Type	-	License Expire Date	-

Port Information

Source Device		Destination Devices		
No.	Port	Connect to	Port	Ref.
1	1	Cisco 3560	Fa0/10	2.2.23
2	2	Cisco 3560	Fa0/4	2.2.23

2.2.31 Cisco 1800 Series (Unused)

Device Information

Hostname	-	IP Address	-
Brand	Cisco	Model	1800 Series
Serial Number	-	Software Version	-
Location	Data Center	EOL Status	-
License Type	-	License Expire Date	-

Port Information

Source Device		Destination Devices		
No.	Port	Connect to	Port	Ref.
-	-	-	-	-

2.2.32 DELL PowerEdge R200 (Unused)

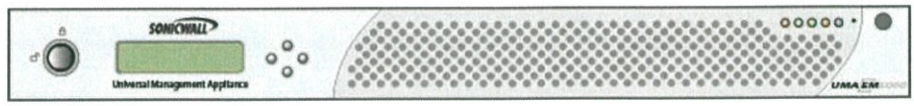
Device Information

Hostname	-	IP Address	-
Brand	DELL	Model	PowerEdge R200
Serial Number	-	Software Version	-
Location	Data Center	EOL Status	-
License Type	-	License Expire Date	-

Port Information

Source Device		Destination Devices		
No.	Port	Connect to	Port	Ref.
-	-	-	-	-

2.2.33 Sonic Wall UMA EM (Unused)



Device Information

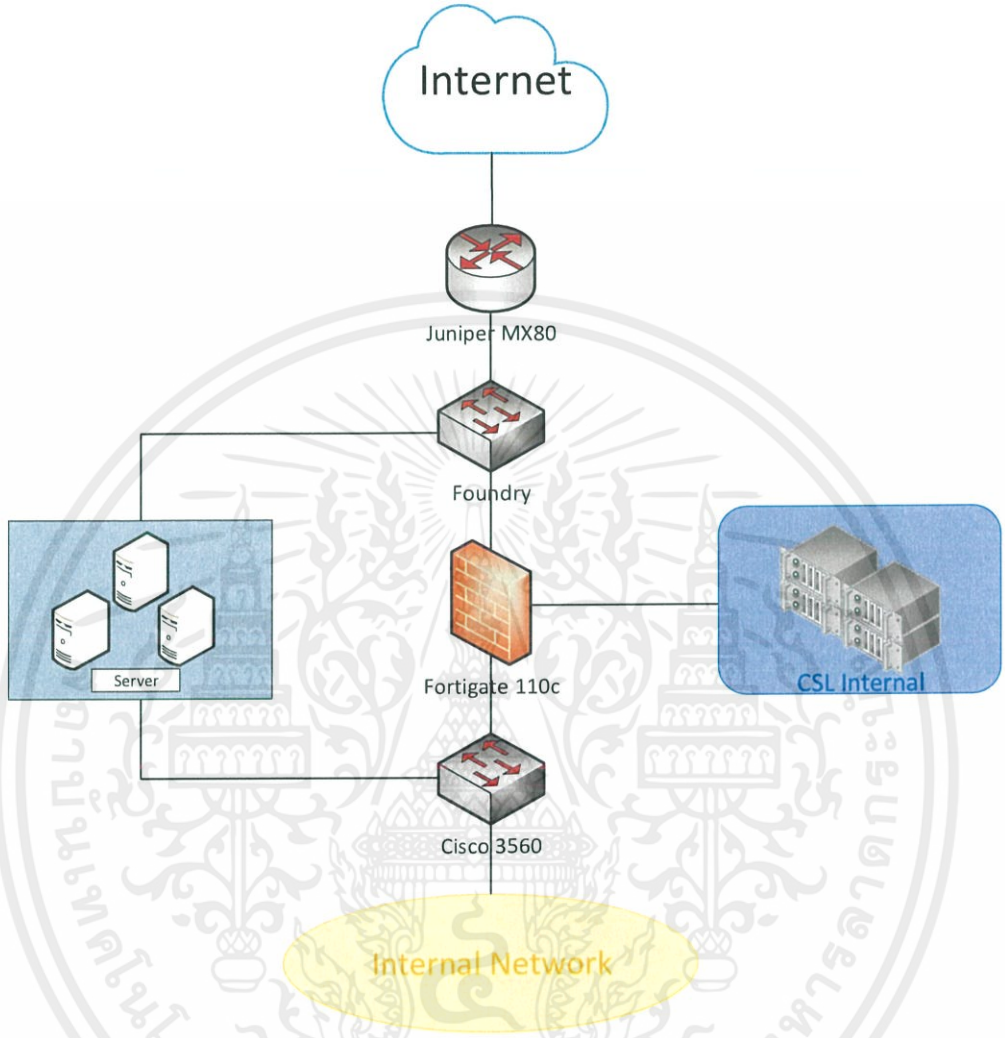
Hostname	-	IP Address	-
Brand	Sonic Wall	Model	UMA EM
Serial Number	-	Software Version	-
Location	Data Center	EOL Status	-
License Type	-	License Expire Date	-

Port Information

Source Device		Destination Devices		
No.	Port	Connect to	Port	Ref.
-	-	-	-	-

3. WAN/LAN with Logical Diagram

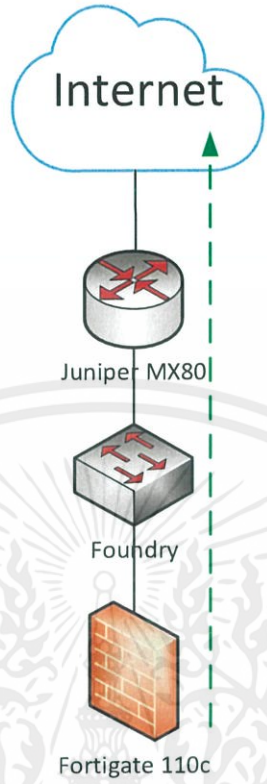
3.1 WAN/LAN Diagram Overview



Network Zone Overview

No	Zone Name	Zone Type
1	Internet	External
2	Server	Internal
3	CSL Internal	Internal
4	Internal Network	Internal

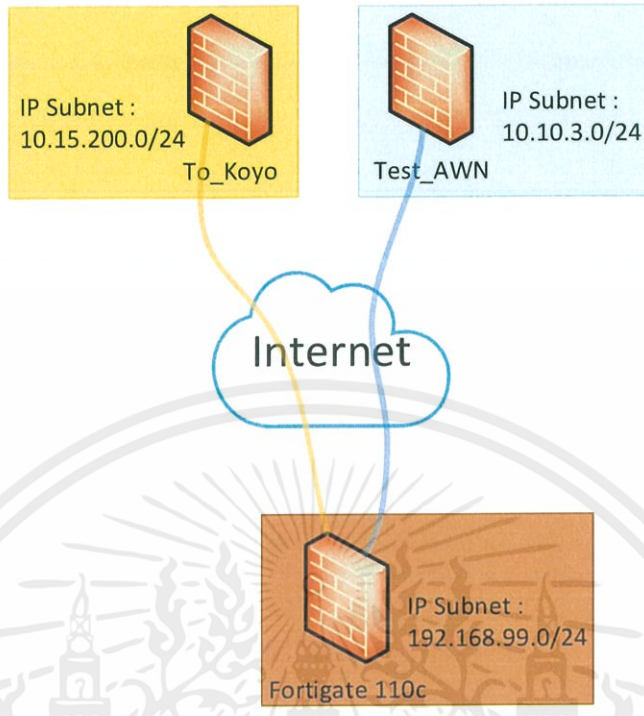
3.2 Internet Connection



Route to Internet on firewall (Fortigate 110c)

No	Destination	Interface	Gateway	Metric
1	0.0.0.0/0	WAN1	202.183.152.5	10

3.3 Virtual Private Network (VPN) Connection



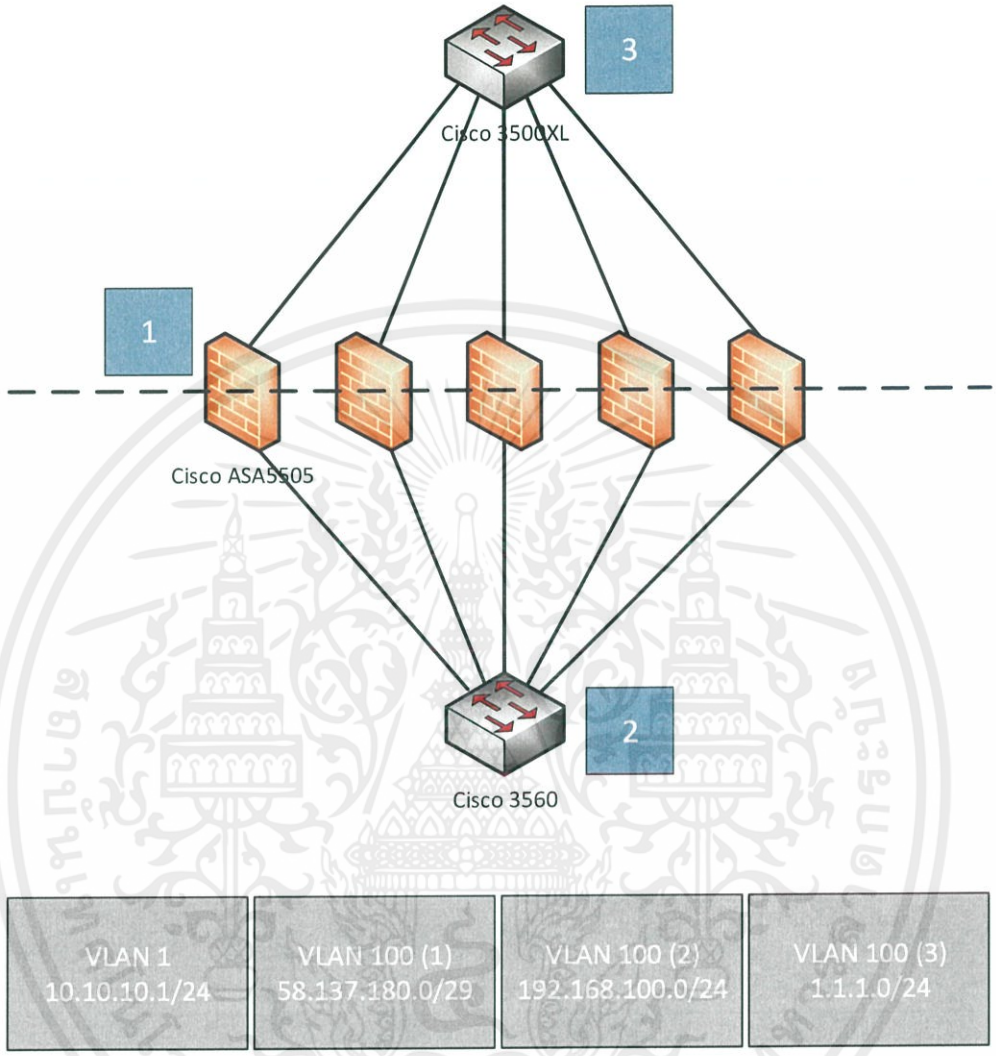
Security Algorithm of VPN Connection

No	Connection Name	Protocol	Phase 1	Phase 2	Status
1	To_Koyo	IPSec	DES SHA1 Group 1	DES SHA1	Active
2	Test_AWN	IPSec	AES256 SHA1 Group 2	AES256 SHA1	Active

Access List of VPN Connection

No	Destination	Interface		Destination	
		IP Subnet	Subnet Mask	IP Subnet	Subnet Mask
1	To_Koyo	192.168.99.0	255.255.255.0	10.15.200.0	255.255.255.0
2	Test_AWN	192.168.99.0	255.255.255.0	10.10.3.0	255.255.255.0

4. VLANs and IP Subnets Schema



VLAN ID	VLAN Name	IP Subnet	Subnet Mask	Describtion
1	VLAN 1	10.10.10.1	255.255.255.0	-
100 (1)	VLAN 100	58.137.180.0	255.255.255.248	-
100 (2)	VLAN 100	192.168.100.0	255.255.255.0	-
100 (3)	VLAN 100	1.1.1.0	255.255.255.0	-

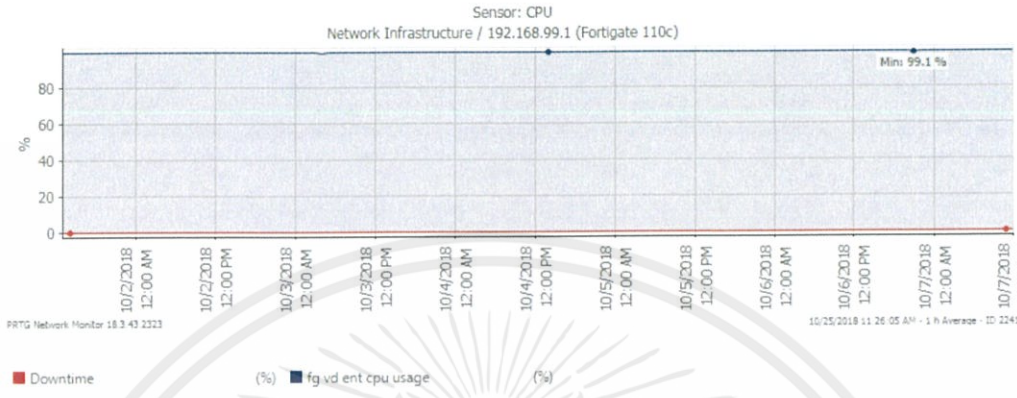
ภาคผนวก ค

ผลการมอนิเตอร์

1.ไฟร์วอลล์ Fortigate 110c

1.1 การใช้งาน CPU

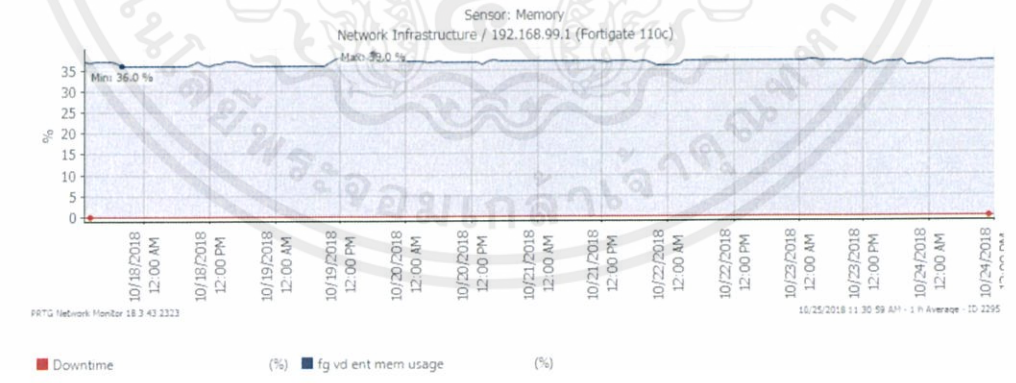
ผลการมอนิเตอร์ CPU ที่เก็บ ในวันที่ 1/10/18 12:00:00 PM – 7/10/18 12:00:00 PM



	CPU Usage	Down time
Maximum	99.4 %	0 %
Average	99 %	0 %
Minimum	99.1 %	0 %

1.2 การใช้งาน Memory

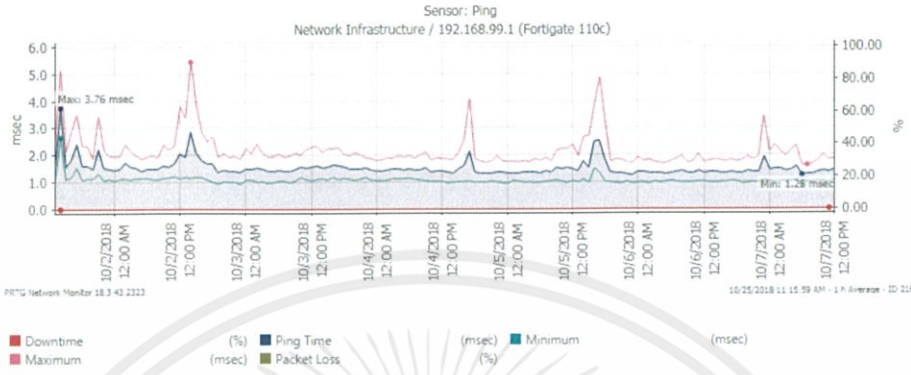
ผลการมอนิเตอร์ Memory ที่เก็บ ในวันที่ 1/10/18 12:00:00 PM – 7/10/18 12:00:00 PM



	Memory Usage	Down time
Maximum	39 %	0 %
Average	37 %	0 %
Minimum	36 %	0 %

1.3 Ping

ผลการมอนิเตอร์ Ping ที่เก็บ เก็บในวันที่ 1/10/18 12:00:00 PM – 7/10/18 12:00:00 PM

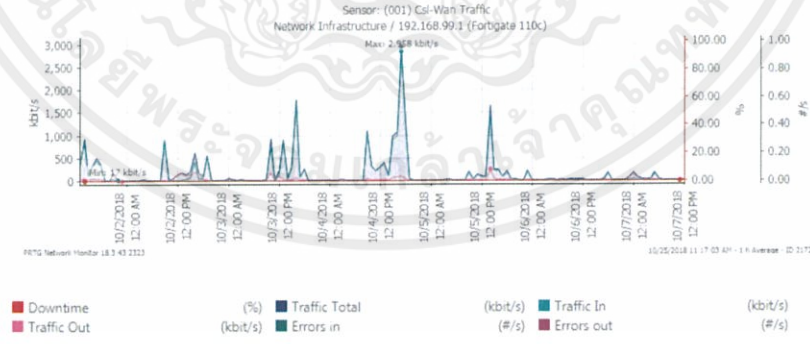


	Ping time	Packet Loss	Downtime
Maximum	4.60 msec	0 %	0 %
Average	3 msec	0 %	0 %
Minimum	2.28 msec	0 %	0 %

1.4 Traffic

1.4.1 Interface WAN1

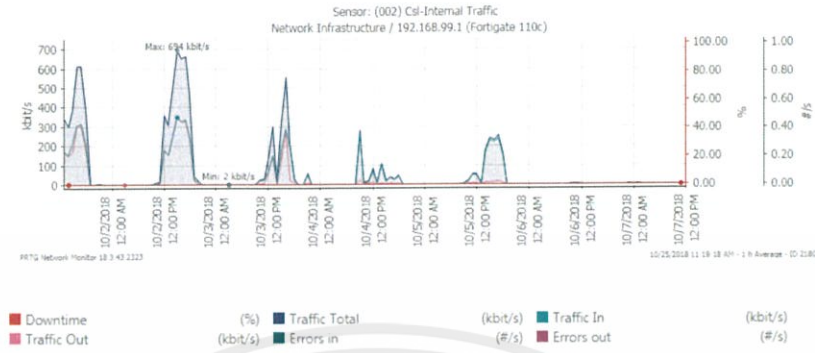
ผลการมอนิเตอร์ Traffic ที่เก็บ เก็บในวันที่ 1/10/18 12:00:00 PM – 7/10/18 12:00:00 PM



	Traffic Total	Traffic In	Traffic Out	Errors in	Errors out	Downtime
Maximum	2,958 kbit/s	2,856 kbit/s	102 kbit/s	0 kbit/s	0 kbit/s	0 %
Average	179 kbit/s	154 kbit/s	25 kbit/s	0 kbit/s	0 kbit/s	0 %
Minimum	17 kbit/s	8 kbit/s	9 kbit/s	0 kbit/s	0 kbit/s	0 %

1.4.2 Interface WAN2

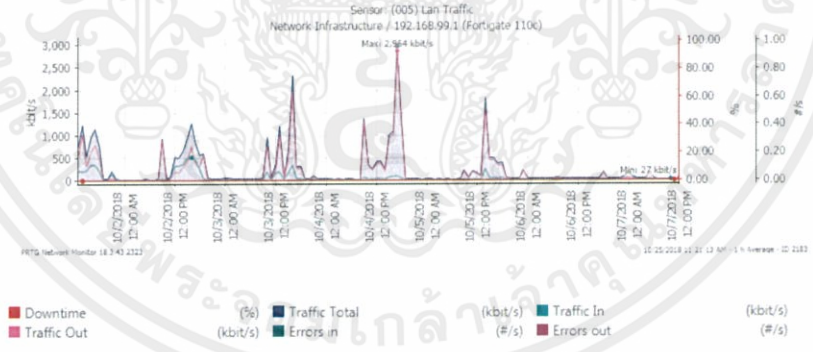
ผลการมอนิเตอร์ Traffic ที่เก็บ ในวันที่ 1/10/18 12:00:00 PM – 7/10/18 12:00:00 PM



	Traffic Total	Traffic In	Traffic Out	Errors in	Errors out	Downtime
Maximum	694 kbit/s	350 kbit/s	344 kbit/s	0 kbit/s	0 kbit/s	0 %
Average	70 kbit/s	42 kbit/s	27 kbit/s	0 kbit/s	0 kbit/s	0 %
Minimum	2 kbit/s	0 kbit/s	2 kbit/s	0 kbit/s	0 kbit/s	0 %

1.4.3 Interface Port 1

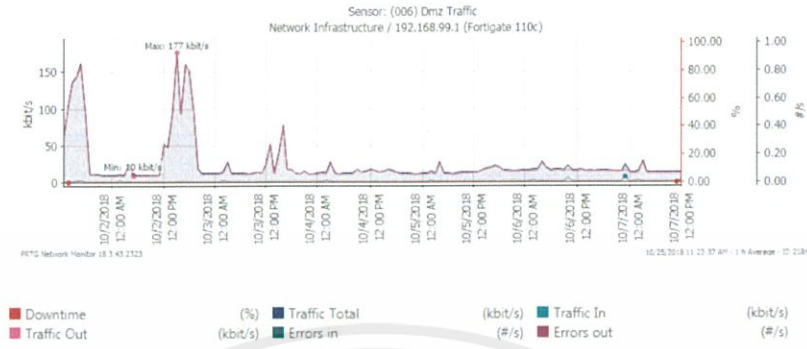
ผลการมอนิเตอร์ Traffic ที่เก็บ ในวันที่ 1/10/18 12:00:00 PM – 7/10/18 12:00:00 PM



	Traffic Total	Traffic In	Traffic Out	Errors in	Errors out	Downtime
Maximum	2,964 kbit/s	550 kbit/s	2,884 kbit/s	0 kbit/s	0 kbit/s	0 %
Average	256 kbit/s	61 kbit/s	194 kbit/s	0 kbit/s	0 kbit/s	0 %
Minimum	27 kbit/s	10 kbit/s	17 kbit/s	0 kbit/s	0 kbit/s	0 %

1.4.4 Interface Port 2

ผลการมอนิเตอร์ Traffic ที่เก็บ ในวันที่ 1/10/18 12:00:00 PM – 7/10/18 12:00:00 PM

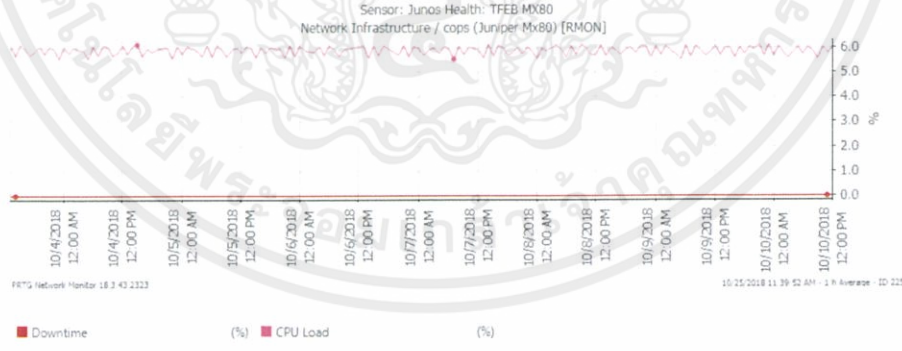


	Traffic Total	Traffic In	Traffic Out	Errors in	Errors out	Downtime
Maximum	177 kbit/s	8 kbit/s	169 kbit/s	0 kbit/s	0 kbit/s	0 %
Average	25 kbit/s	1.14 kbit/s	24 kbit/s	0 kbit/s	0 kbit/s	0 %
Minimum	10 kbit/s	2 kbit/s	8 kbit/s	0 kbit/s	0 kbit/s	0 %

2. Juniper MX80

2.1 การใช้งาน CPU

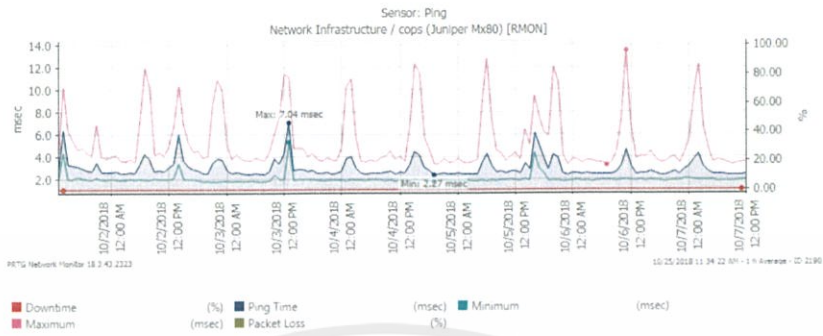
ผลการมอนิเตอร์ CPU ที่เก็บ ในวันที่ 3/10/18 12:00:00 PM – 10/10/18 12:00:00 PM



	CPU Usage	Down time
Maximum	6.2 %	0 %
Average	6 %	0 %
Minimum	5.5 %	0 %

2.2 การใช้งาน Ping

ผลการมอนิเตอร์ Ping ที่เก็บ ในวันที่ 1/10/18 12:00:00 PM – 7/10/18 12:00:00 PM

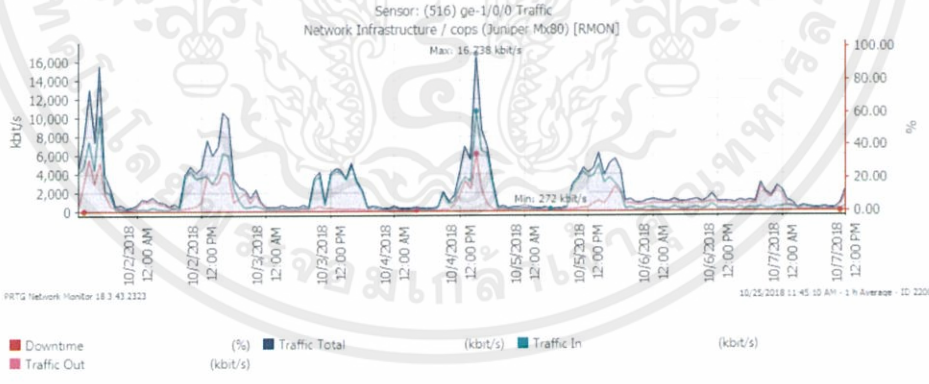


	Ping time	Packet Loss	Downtime
Maximum	7.04 msec	0 %	0 %
Average	3 msec	0 %	0 %
Minimum	2.27 msec	0 %	0 %

2.3 Traffic

2.3.1 Interface Ge 1/0/0

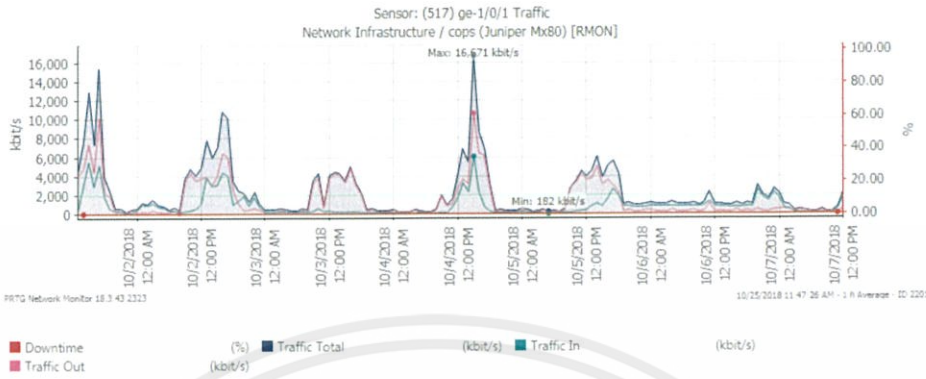
ผลการมอนิเตอร์ Traffic ที่เก็บ ในวันที่ 1/10/18 12:00:00 PM – 7/10/18 12:00:00 PM



	Traffic Total	Traffic In	Traffic Out	Downtime
Maximum	16,738 kbit/s	10,156 kbit/s	6,582 kbit/s	0 %
Average	2,378 kbit/s	1,491 kbit/s	887 kbit/s	0 %
Minimum	272 kbit/s	100 kbit/s	172 kbit/s	0 %

2.3.2 Interface Ge 1/0/1

ผลการมอนิเตอร์ Traffic ที่เก็บ ในวันที่ 1/10/18 12:00:00 PM – 7/10/18 12:00:00 PM

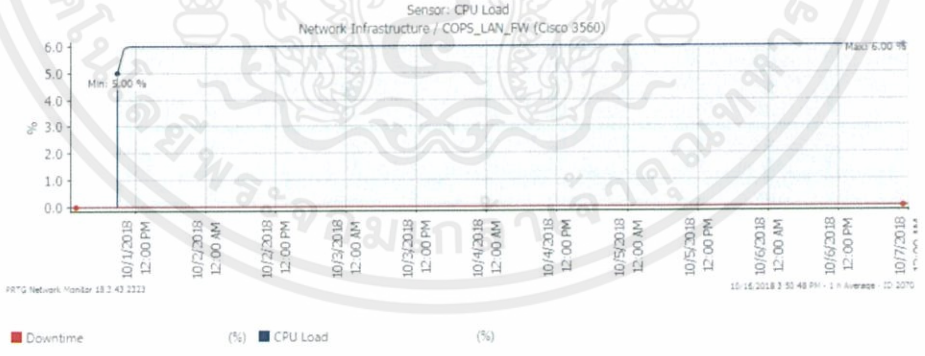


	Traffic Total	Traffic In	Traffic Out	Downtime
Maximum	16,671 kbit/s	6,582 kbit/s	10,156 kbit/s	0 %
Average	2,315 kbit/s	854 kbit/s	1,461 kbit/s	0 %
Minimum	182 kbit/s	112 kbit/s	70 kbit/s	0 %

3. Cisco 3560

3.1 การใช้งาน CPU

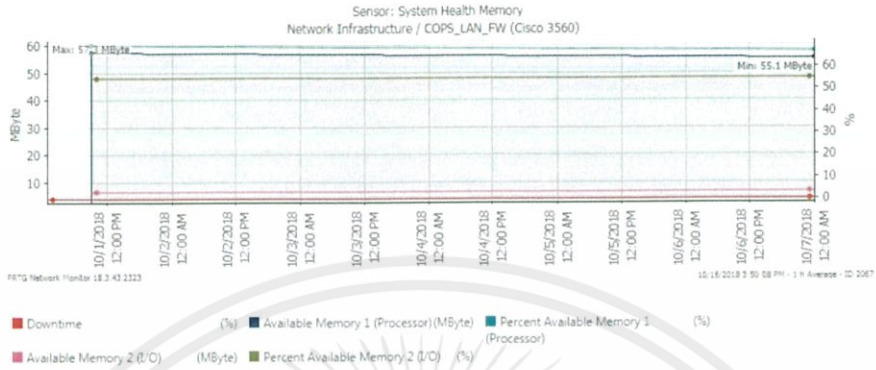
ผลการมอนิเตอร์ CPU ที่เก็บ ในวันที่ 1/10/18 12:00:00 PM – 7/10/18 12:00:00 PM



	CPU Usage	Down time
Maximum	6 %	0 %
Average	6 %	0 %
Minimum	5 %	0 %

3.2 การใช้งาน Memory

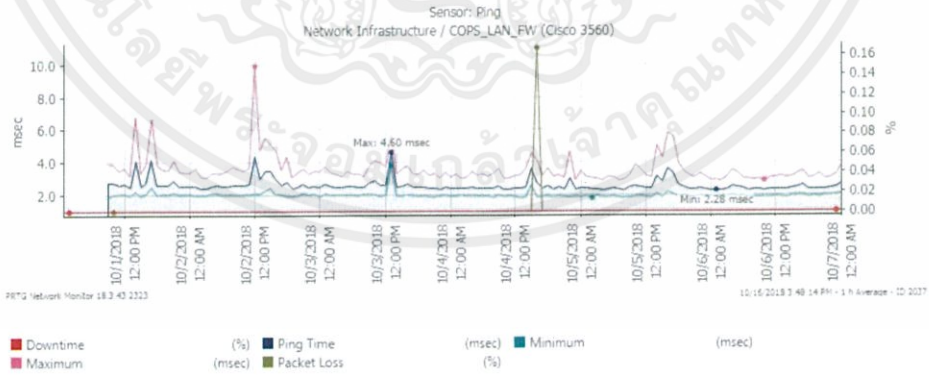
ผลการมอนิเตอร์ Memory ที่เก็บ ในวันที่ 9/10/18 12:00:00 PM – 16/10/18 12:00:00 PM



	Available Memory 1 (Processor)	Down time
Maximum	57.3 Mbyte	0 %
Average	56 Mbyte	0 %
Minimum	55.1 Mbyte	0 %

3.3 Ping

ผลการมอนิเตอร์ Ping ที่เก็บ ในวันที่ 1/10/18 12:00:00 PM – 7/10/18 12:00:00 PM

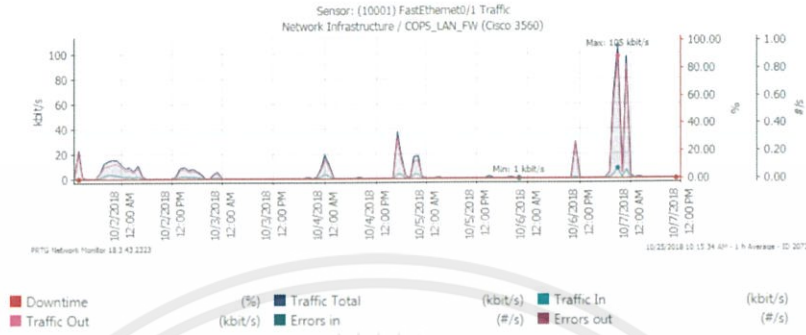


	Ping time	Packet Loss	Downtime
Maximum	4.60 msec	0 %	0 %
Average	3 msec	0 %	0 %
Minimum	2.28 msec	0 %	0 %

3.4 Traffic

3.4.1 Interface Fa0/1

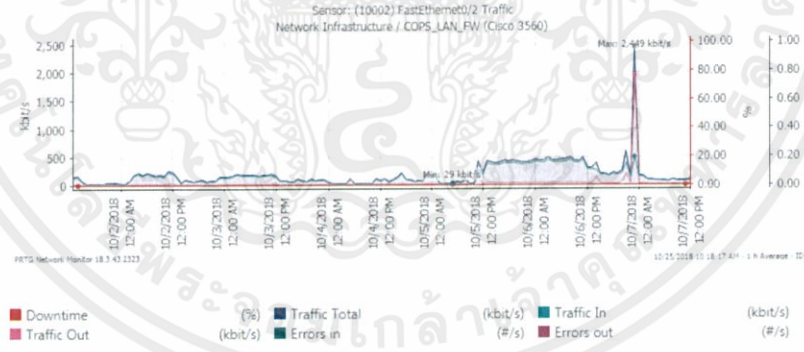
ผลการมอนิเตอร์ Traffic ที่เก็บ ในวันที่ 1/10/18 12:00:00 PM – 7/10/18 12:00:00 PM



	Traffic Total	Traffic In	Traffic Out	Errors in	Errors out	Downtime
Maximum	105 kbit/s	6 kbit/s	99 kbit/s	0 kbit/s	0 kbit/s	0 %
Average	5.07 kbit/s	0.73 kbit/s	4.34 kbit/s	0 kbit/s	0 kbit/s	0 %
Minimum	1 kbit/s	<1 kbit/s	<1 kbit/s	0 kbit/s	0 kbit/s	0 %

3.4.2 Interface Fa0/2

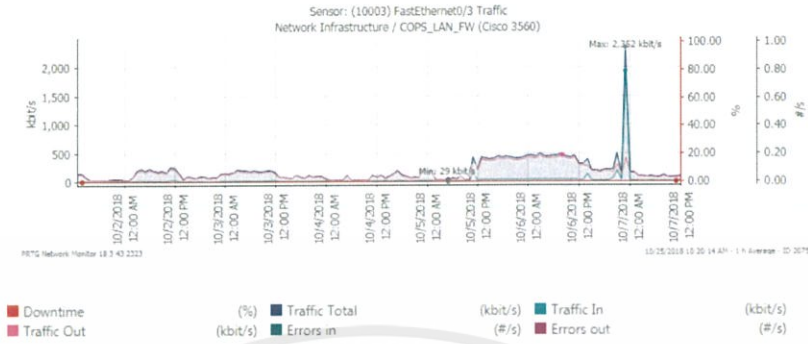
ผลการมอนิเตอร์ Traffic ที่เก็บ ในวันที่ 1/10/18 12:00:00 PM – 7/10/18 12:00:00 PM



	Traffic Total	Traffic In	Traffic Out	Errors in	Errors out	Downtime
Maximum	2,449 kbit/s	500 kbit/s	1,949 kbit/s	0 kbit/s	0 kbit/s	0 %
Average	192 kbit/s	160 kbit/s	32 kbit/s	0 kbit/s	0 kbit/s	0 %
Minimum	29 kbit/s	19 kbit/s	10 kbit/s	0 kbit/s	0 kbit/s	0 %

3.4.3 Interface Fa0/3

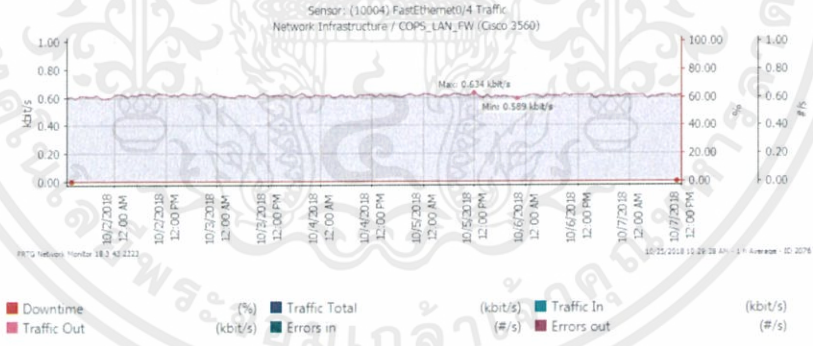
ผลการมอนิเตอร์ Traffic ที่เก็บ ในวันที่ 1/10/18 12:00:00 PM – 7/10/18 12:00:00 PM



	Traffic Total	Traffic In	Traffic Out	Errors in	Errors out	Downtime
Maximum	2,352 kbit/s	1,931 kbit/s	421 kbit/s	0 kbit/s	0 kbit/s	0 %
Average	190 kbit/s	32 kbit/s	158 kbit/s	0 kbit/s	0 kbit/s	0 %
Minimum	29 kbit/s	19 kbit/s	10 kbit/s	0 kbit/s	0 kbit/s	0 %

3.4.4 Interface Fa0/4

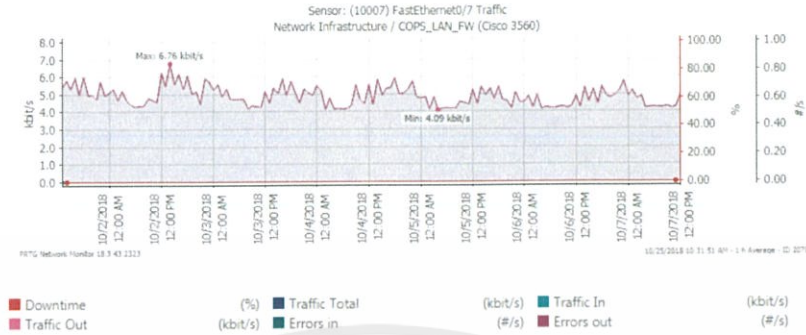
ผลการมอนิเตอร์ Traffic ที่เก็บ ในวันที่ 1/10/18 12:00:00 PM – 7/10/18 12:00:00 PM



	Traffic Total	Traffic In	Traffic Out	Errors in	Errors out	Downtime
Maximum	0.634 kbit/s	0 kbit/s	0.634 kbit/s	0 kbit/s	0 kbit/s	0 %
Average	0.61 kbit/s	0 kbit/s	0.61 kbit/s	0 kbit/s	0 kbit/s	0 %
Minimum	0.589 kbit/s	0 kbit/s	0.589 kbit/s	0 kbit/s	0 kbit/s	0 %

3.4.5 Interface Fa0/7

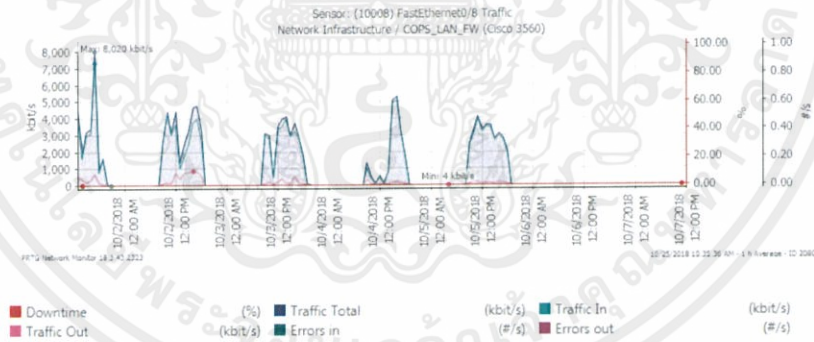
ผลการมอนิเตอร์ Traffic ที่เก็บ ในวันที่ 1/10/18 12:00:00 PM – 7/10/18 12:00:00 PM



	Traffic Total	Traffic In	Traffic Out	Errors in	Errors out	Downtime
Maximum	6.76 kbit/s	0 kbit/s	6.76 kbit/s	0 kbit/s	0 kbit/s	0 %
Average	4.88 kbit/s	0 kbit/s	4.88 kbit/s	0 kbit/s	0 kbit/s	0 %
Minimum	4.09 kbit/s	0 kbit/s	4.09 kbit/s	0 kbit/s	0 kbit/s	0 %

3.4.6 Interface Fa0/8

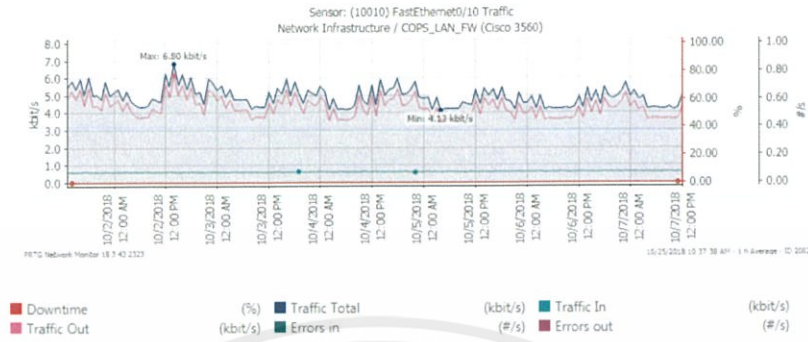
ผลการมอนิเตอร์ Traffic ที่เก็บ ในวันที่ 1/10/18 12:00:00 PM – 7/10/18 12:00:00 PM



	Traffic Total	Traffic In	Traffic Out	Errors in	Errors out	Downtime
Maximum	8,020 kbit/s	7,405 kbit/s	615 kbit/s	0 kbit/s	0 kbit/s	0 %
Average	959 kbit/s	875 kbit/s	84 kbit/s	0 kbit/s	0 kbit/s	0 %
Minimum	4 kbit/s	4 kbit/s	0 kbit/s	0 kbit/s	0 kbit/s	0 %

3.4.7 Interface Fa0/10

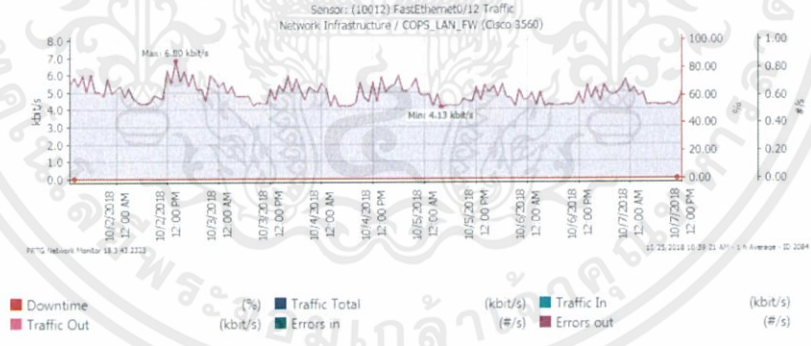
ผลการมอนิเตอร์ Traffic ที่เก็บ ในวันที่ 1/10/18 12:00:00 PM – 7/10/18 12:00:00 PM



	Traffic Total	Traffic In	Traffic Out	Errors in	Errors out	Downtime
Maximum	6.80 kbit/s	0.7 kbit/s	6.1 kbit/s	0 kbit/s	0 kbit/s	0 %
Average	4.92 kbit/s	0.62 kbit/s	4.30 kbit/s	0 kbit/s	0 kbit/s	0 %
Minimum	4.13 kbit/s	0.7 kbit/s	3.43 kbit/s	0 kbit/s	0 kbit/s	0 %

3.4.8 Interface Fa0/12

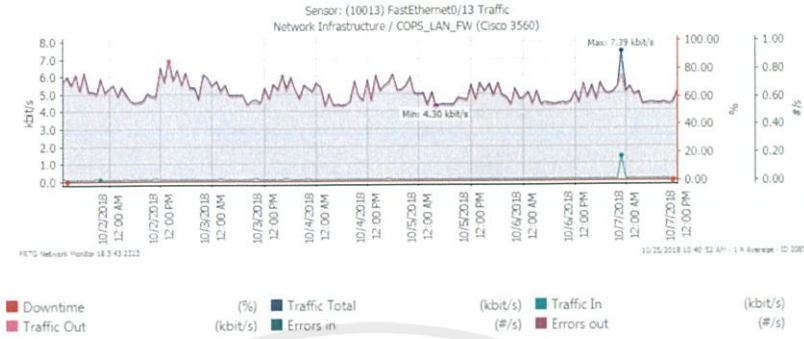
ผลการมอนิเตอร์ Traffic ที่เก็บ ในวันที่ 1/10/18 12:00:00 PM – 7/10/18 12:00:00 PM



	Traffic Total	Traffic In	Traffic Out	Errors in	Errors out	Downtime
Maximum	6.80 kbit/s	0.7 kbit/s	6.1 kbit/s	0 kbit/s	0 kbit/s	0 %
Average	4.92 kbit/s	0.62 kbit/s	4.30 kbit/s	0 kbit/s	0 kbit/s	0 %
Minimum	4.13 kbit/s	0 kbit/s	4.13 kbit/s	0 kbit/s	0 kbit/s	0 %

3.4.9 Interface Fa0/13

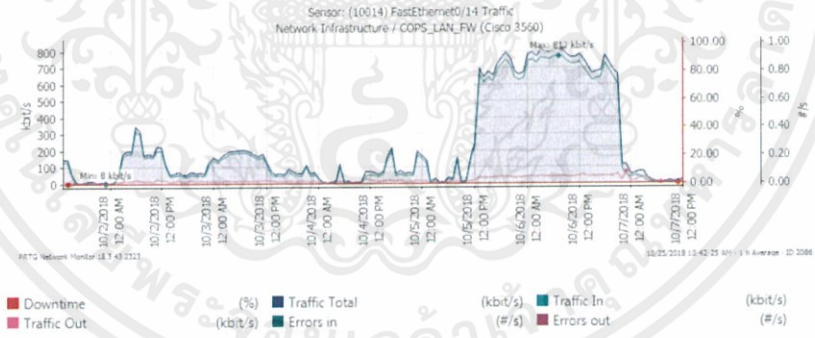
ผลการมอนิเตอร์ Traffic ที่เก็บ ในวันที่ 1/10/18 12:00:00 PM – 7/10/18 12:00:00 PM



	Traffic Total	Traffic In	Traffic Out	Errors in	Errors out	Downtime
Maximum	7.39 kbit/s	1.2 kbit/s	6.19 kbit/s	0 kbit/s	0 kbit/s	0 %
Average	5.12 kbit/s	0.12 kbit/s	5 kbit/s	0 kbit/s	0 kbit/s	0 %
Minimum	4.30 kbit/s	0.1 kbit/s	4.20 kbit/s	0 kbit/s	0 kbit/s	0 %

3.4.10 Interface Fa0/14

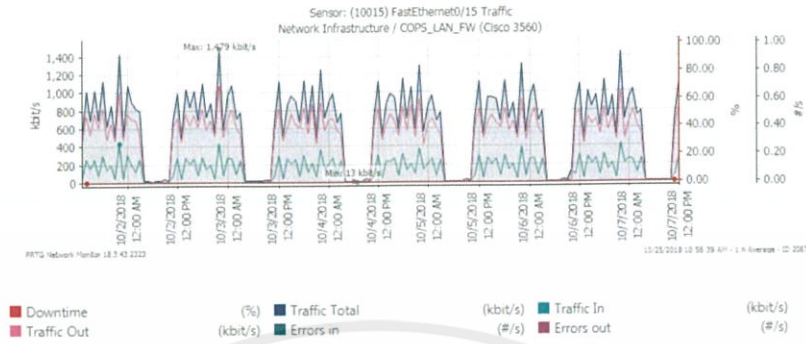
ผลการมอนิเตอร์ Traffic ที่เก็บ ในวันที่ 1/10/18 12:00:00 PM – 7/10/18 12:00:00 PM



	Traffic Total	Traffic In	Traffic Out	Errors in	Errors out	Downtime
Maximum	812 kbit/s	780 kbit/s	32 kbit/s	0 kbit/s	0 kbit/s	0 %
Average	238 kbit/s	217 kbit/s	21 kbit/s	0 kbit/s	0 kbit/s	0 %
Minimum	8 kbit/s	5 kbit/s	3 kbit/s	0 kbit/s	0 kbit/s	0 %

3.4.11 Interface Fa0/15

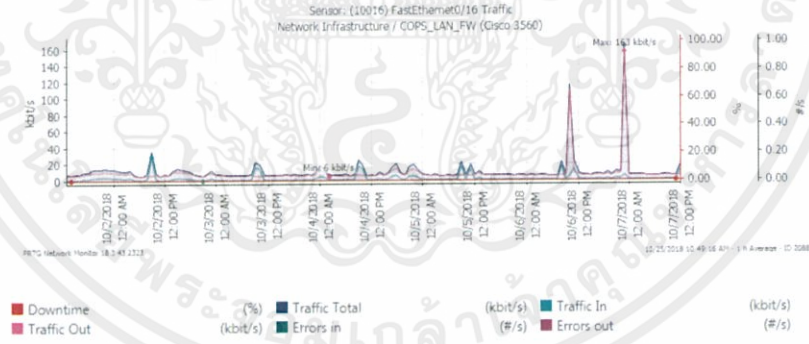
ผลการมอนิเตอร์ Traffic ที่เก็บ ในวันที่ 1/10/18 12:00:00 PM – 7/10/18 12:00:00 PM



	Traffic Total	Traffic In	Traffic Out	Errors in	Errors out	Downtime
Maximum	1,479 kbit/s	1,044 kbit/s	435 kbit/s	0 kbit/s	0 kbit/s	0 %
Average	608 kbit/s	139 kbit/s	469 kbit/s	0 kbit/s	0 kbit/s	0 %
Minimum	13 kbit/s	3 kbit/s	10 kbit/s	0 kbit/s	0 kbit/s	0 %

3.4.12 Interface Fa0/16

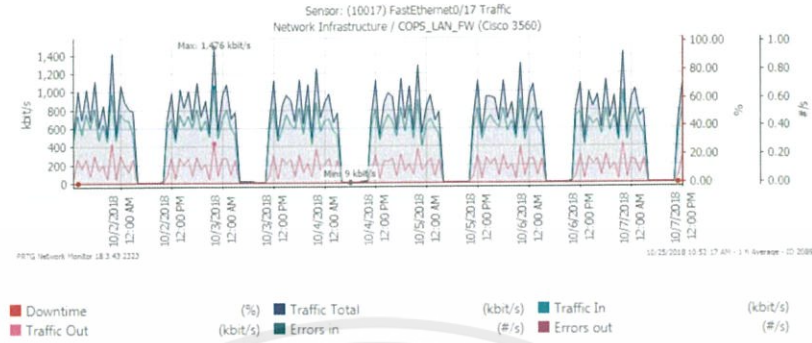
ผลการมอนิเตอร์ Traffic ที่เก็บ ในวันที่ 1/10/18 12:00:00 PM – 7/10/18 12:00:00 PM



	Traffic Total	Traffic In	Traffic Out	Errors in	Errors out	Downtime
Maximum	163 kbit/s	5 kbit/s	158 kbit/s	0 kbit/s	0 kbit/s	0 %
Average	11 kbit/s	2.66 kbit/s	8.66 kbit/s	0 kbit/s	0 kbit/s	0 %
Minimum	6 kbit/s	2 kbit/s	4 kbit/s	0 kbit/s	0 kbit/s	0 %

3.4.13 Interface Fa0/17

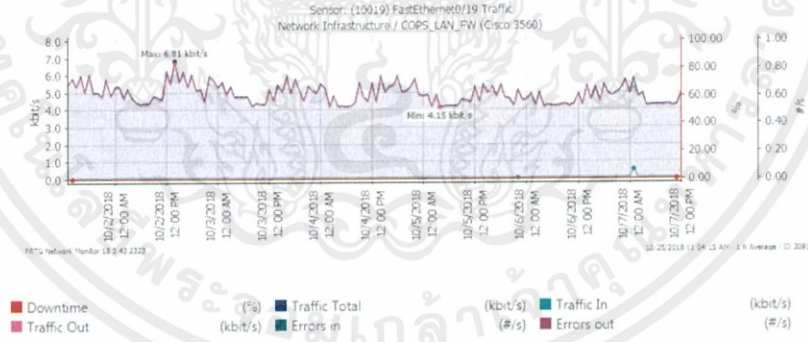
ผลการมอนิเตอร์ Traffic ที่เก็บ ในวันที่ 1/10/18 12:00:00 PM – 7/10/18 12:00:00 PM



	Traffic Total	Traffic In	Traffic Out	Errors in	Errors out	Downtime
Maximum	1,476 kbit/s	1,056 kbit/s	420 kbit/s	0 kbit/s	0 kbit/s	0 %
Average	602 kbit/s	463 kbit/s	139 kbit/s	0 kbit/s	0 kbit/s	0 %
Minimum	9 kbit/s	4 kbit/s	5 kbit/s	0 kbit/s	0 kbit/s	0 %

3.4.14 Interface Fa0/19

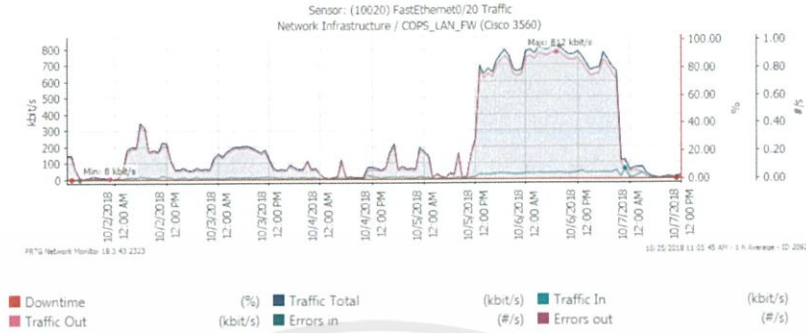
ผลการมอนิเตอร์ Traffic ที่เก็บ ในวันที่ 1/10/18 12:00:00 PM – 7/10/18 12:00:00 PM



	Traffic Total	Traffic In	Traffic Out	Errors in	Errors out	Downtime
Maximum	6.81 kbit/s	0.1 kbit/s	6.8 kbit/s	0 kbit/s	0 kbit/s	0 %
Average	4.94 kbit/s	0.08 kbit/s	4.86 kbit/s	0 kbit/s	0 kbit/s	0 %
Minimum	4.15 kbit/s	0.01 kbit/s	4.14 kbit/s	0 kbit/s	0 kbit/s	0 %

3.4.15 Interface Fa0/20

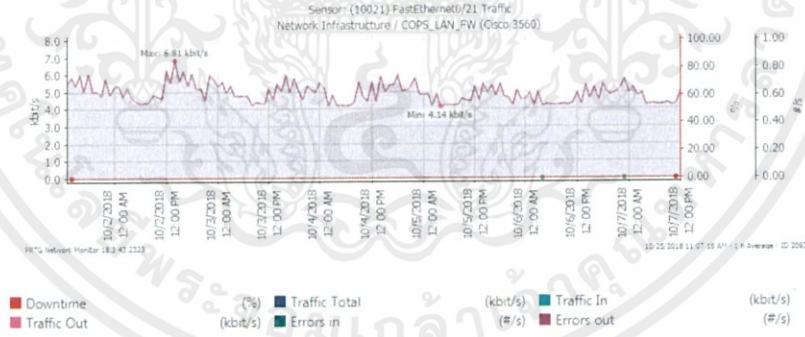
ผลการมอนิเตอร์ Traffic ที่เก็บ ในวันที่ 1/10/18 12:00:00 PM – 7/10/18 12:00:00 PM



	Traffic Total	Traffic In	Traffic Out	Errors in	Errors out	Downtime
Maximum	812 kbit/s	30 kbit/s	782 kbit/s	0 kbit/s	0 kbit/s	0 %
Average	238 kbit/s	16 kbit/s	222 kbit/s	0 kbit/s	0 kbit/s	0 %
Minimum	8 kbit/s	2 kbit/s	6 kbit/s	0 kbit/s	0 kbit/s	0 %

3.4.16 Interface Fa0/21

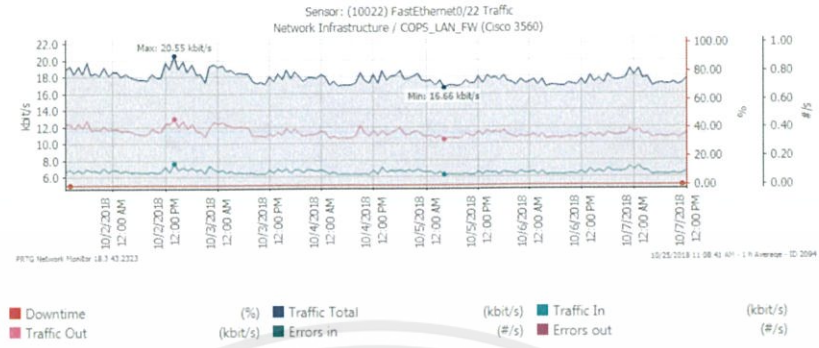
ผลการมอนิเตอร์ Traffic ที่เก็บ ในวันที่ 1/10/18 12:00:00 PM – 7/10/18 12:00:00 PM



	Traffic Total	Traffic In	Traffic Out	Errors in	Errors out	Downtime
Maximum	6.81 kbit/s	0.01 kbit/s	6.8 kbit/s	0 kbit/s	0 kbit/s	0 %
Average	4.93 kbit/s	0.01 kbit/s	4.92 kbit/s	0 kbit/s	0 kbit/s	0 %
Minimum	4.14 kbit/s	0 kbit/s	4.14 kbit/s	0 kbit/s	0 kbit/s	0 %

3.4.17 Interface Fa0/22

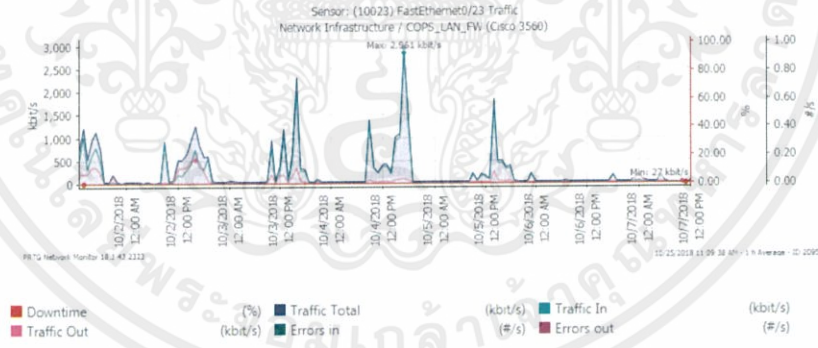
ผลการมอนิเตอร์ Traffic ที่เก็บ ในวันที่ 1/10/18 12:00:00 PM – 7/10/18 12:00:00 PM



	Traffic Total	Traffic In	Traffic Out	Errors in	Errors out	Downtime
Maximum	20.55 kbit/s	7.9 kbit/s	12.65 kbit/s	0 kbit/s	0 kbit/s	0 %
Average	18 kbit/s	6.60 kbit/s	11 kbit/s	0 kbit/s	0 kbit/s	0 %
Minimum	16.66 kbit/s	6.1 kbit/s	10.56 kbit/s	0 kbit/s	0 kbit/s	0 %

3.4.18 Interface Fa0/23

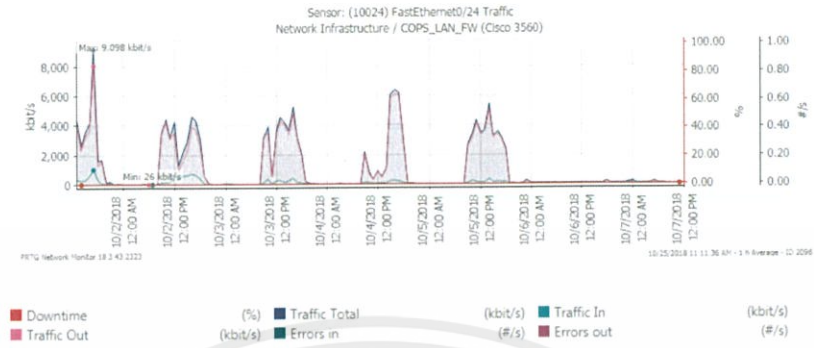
ผลการมอนิเตอร์ Traffic ที่เก็บ ในวันที่ 1/10/18 12:00:00 PM – 7/10/18 12:00:00 PM



	Traffic Total	Traffic In	Traffic Out	Errors in	Errors out	Downtime
Maximum	2,691 kbit/s	2,911 kbit/s	50 kbit/s	0 kbit/s	0 kbit/s	0 %
Average	257 kbit/s	194 kbit/s	62 kbit/s	0 kbit/s	0 kbit/s	0 %
Minimum	27 kbit/s	10 kbit/s	17 kbit/s	0 kbit/s	0 kbit/s	0 %

3.4.19 Interface Fa0/24

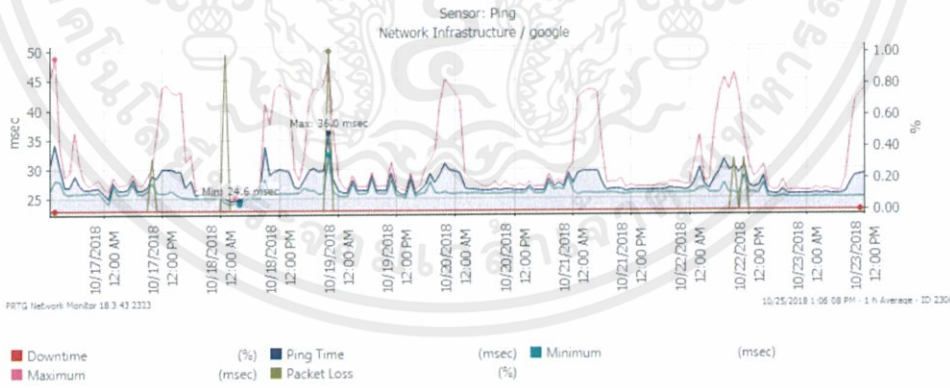
ผลการมอนิเตอร์ Traffic ที่เก็บ ในวันที่ 1/10/18 12:00:00 PM – 7/10/18 12:00:00 PM



	Traffic Total	Traffic In	Traffic Out	Errors in	Errors out	Downtime
Maximum	9,098 kbit/s	1,105 kbit/s	7,984 kbit/s	0 kbit/s	0 kbit/s	0 %
Average	1,128 kbit/s	98 kbit/s	1,030 kbit/s	0 kbit/s	0 kbit/s	0 %
Minimum	26 kbit/s	15 kbit/s	11 kbit/s	0 kbit/s	0 kbit/s	0 %

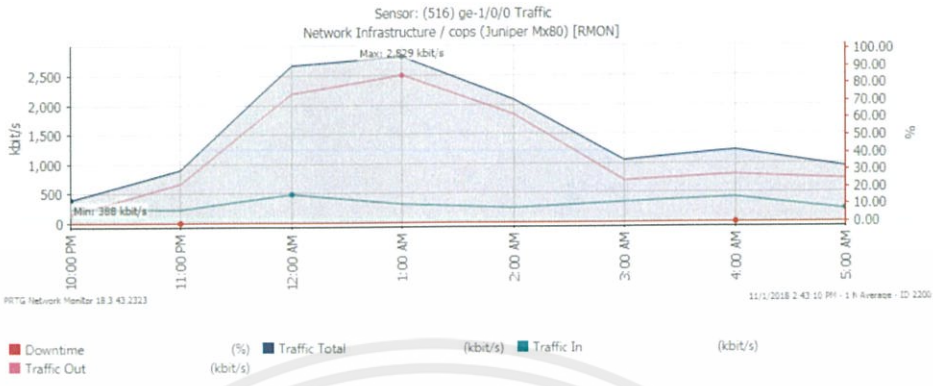
4. ผล Ping ออกอินเตอร์เน็ต

การ Ping ออกอินเตอร์เน็ต จะ Ping ไปที่หมายเลข IP 8.8.8.8 ที่เป็นหมายเลข IP ของ Google



	Ping time	Packet Loss	Downtime
Maximum	36.0 msec	0 %	0 %
Average	27 msec	0 %	0 %
Minimum	24.6 msec	0 %	0 %

5. Traffic ในเวลาหลังเลิกงาน

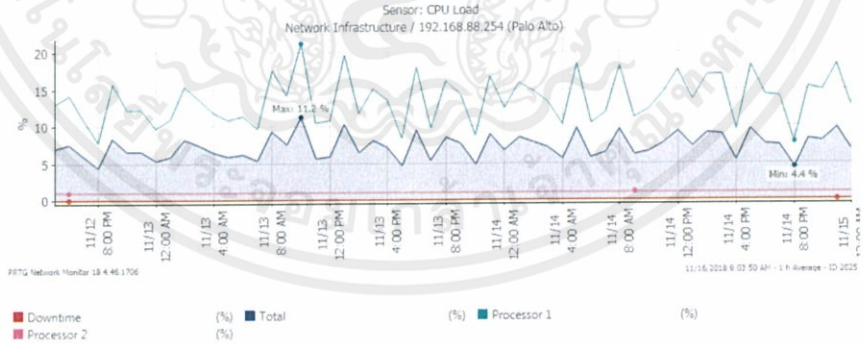


	Traffic Total	Traffic In	Traffic Out	Downtime
Maximum	2,829 kbit/s	487 kbit/s	2,512 kbit/s	0 %
Average	1,514 kbit/s	314 kbit/s	1,200 kbit/s	0 %
Minimum	388 kbit/s	217 kbit/s	147 kbit/s	0 %

6. paloalto PA-200

6.1 ผลการมอนิเตอร์ CPU

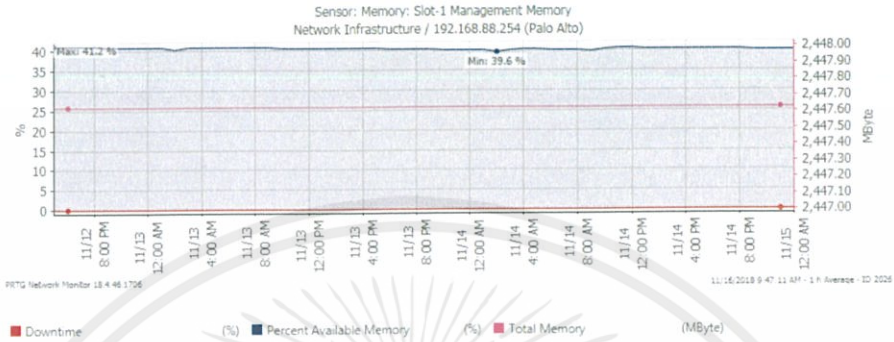
ผลการมอนิเตอร์ CPU ที่เก็บ ในวันที่ 12/11/18 4:00:00 PM – 15/11/18 12:00:00 AM



	Processor 1	Processor 2	Down time
Maximum	21 %	1 %	0 %
Average	14 %	1 %	0 %
Minimum	8 %	1 %	0 %

6.2 ผลการมอนิเตอร์ Memory

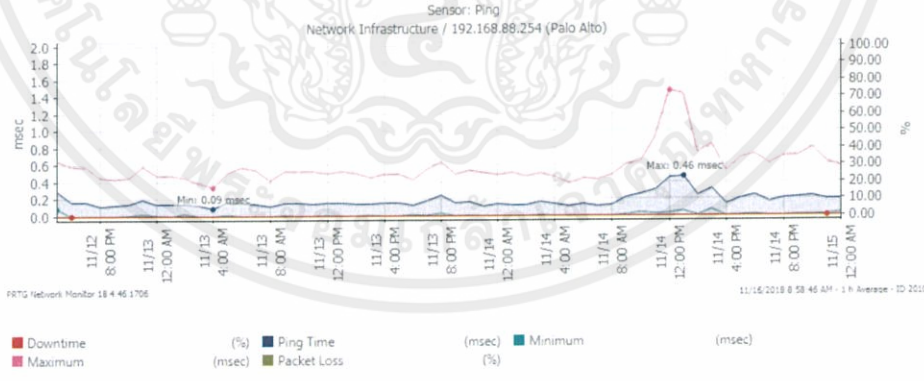
ผลการมอนิเตอร์ Memory ที่เก็บ ในวันที่ 12/11/18 4:00:00 PM – 15/11/18 12:00:00 AM



	Available Memory	Down time
Maximum	41.2 %	0 %
Average	41 %	0 %
Minimum	39.6 %	0 %

6.3 ผลการมอนิเตอร์ Ping

ผลการมอนิเตอร์ Ping ที่เก็บ ในวันที่ 12/11/18 4:00:00 PM – 15/11/18 12:00:00 AM

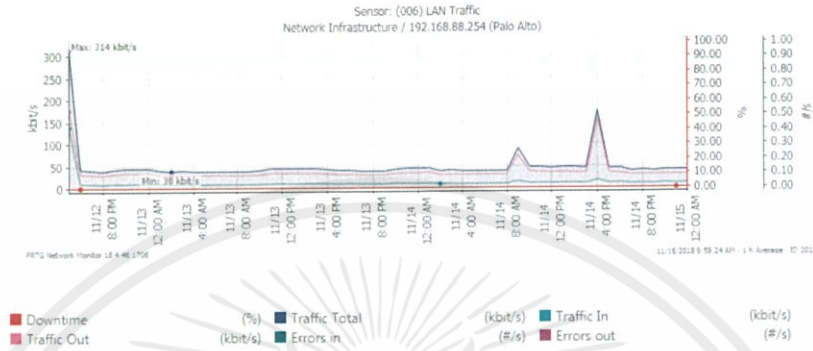


	Ping time	Packet Loss	Downtime
Maximum	0.46 msec	0 %	0 %
Average	0 msec	0 %	0 %
Minimum	0.09 msec	0 %	0 %

6.4 ผลการมอนิเตอร์ Traffic

6.4.1 Interface eth1/1

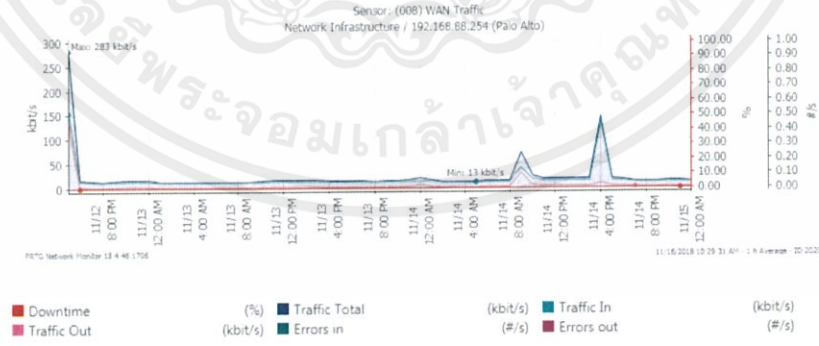
ผลการมอนิเตอร์ Traffic ที่เก็บ ในวันที่ 12/11/18 4:00:00 PM – 15/11/18 12:00:00 AM



	Traffic Total	Traffic In	Traffic Out	Errors in	Errors out	Downtime
Maximum	314 kbit/s	138 kbit/s	176 kbit/s	0 kbit/s	0 kbit/s	0 %
Average	50 kbit/s	12 kbit/s	37 kbit/s	0 kbit/s	0 kbit/s	0 %
Minimum	38 kbit/s	8.88 kbit/s	29 kbit/s	0 kbit/s	0 kbit/s	0 %

6.4.2 Interface eth1/3

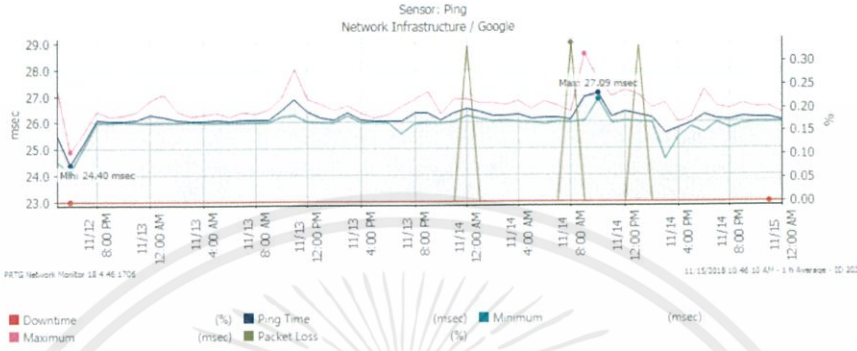
ผลการมอนิเตอร์ Traffic ที่เก็บ ในวันที่ 12/11/18 4:00:00 PM – 15/11/18 12:00:00 AM



	Traffic Total	Traffic In	Traffic Out	Errors in	Errors out	Downtime
Maximum	283 kbit/s	155 kbit/s	128 kbit/s	0 kbit/s	0 kbit/s	0 %
Average	24 kbit/s	19 kbit/s	5.19 kbit/s	0 kbit/s	0 kbit/s	0 %
Minimum	13 kbit/s	13 kbit/s	1.26 kbit/s	0 kbit/s	0 kbit/s	0 %

7. ผลการมอนิเตอร์ Ping ออกอินเตอร์เน็ตของระบบเครือข่ายใหม่

ผลการมอนิเตอร์ Ping ออกอินเตอร์เน็ตที่เก็บ โดย Ping ไปที่หมายเลข IP 8.8.8.8 ซึ่งเป็นหมายเลข IP ของ Google เก็บผลในวันที่ 12/11/18 4:00:00 PM – 15/11/18 12:00:00 AM



	Ping time	Packet Loss	Downtime
Maximum	27 msec	0 %	0 %
Average	26 msec	0 %	0 %
Minimum	24 msec	0 %	0 %

ประวัติผู้จัดทำ

ชื่อ-สกุล สาริน จวงมุทิตา

วัน เดือน ปีเกิด 29 สิงหาคม 2539

ประวัติการศึกษา

ระดับมัธยมศึกษา มัธยมศึกษาตอนปลาย
โรงเรียนไตรมิตรวิทยาลัย ปีการศึกษา 2557

ระดับปริญญาตรี วิศวกรรมศาสตรบัณฑิต สาขาวิชาวิศวกรรมโทรคมนาคม
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง ปีการศึกษา 2561