ความมั่นคงของระบบเครือข่าย

Enterprise Network Security

ธีรุตม์ ฟังเกียรติเจริญ

สิทธิชัย ศิริกิรมย์

ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรบัณฑิต

สาขาวิชาวิศวกรรมคอมพิวเตอร์

คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ปีการศึกษา ๒๕๕๘

ความมั่นคงของระบบเครือข่าย

Enterprise Network Security

ธีรุตม์ ฟุ้งเกียรติเจริญ
สิทธิธัช ศิริภิรมย์

ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรบัณฑิต
สาขาวิชาวิศวกรรมคอมพิวเตอร์
คณะวิศวกรรมศาสตร์
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ปีการศึกษา 2556

ปริญญานิพนธ์ปีการศึกษา 2556

สาขาวิชาวิศวกรรมคอมพิวเตอร์

คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

เรื่อง ความมั่นคงของระบบเครือข่าย

ENTERPRISE NETWORK SECURITY

ผู้จัดทำ

1. นายธีรุตม์	ฟุ้งเกียรติเจริญ	รหัสนักศึกษา	53010767
2. นายสิทธิธัช	ศิริภิรมย์	รหัสนักศึกษา	53011680

..... อาจารย์ที่ปรึกษา

(ดร. วรวัฒน์ ลิ้มโภคา)

ความมั่นคงของระบบเครือข่าย

นายธีรุตม์ ฟุ้งเกียรติเจริญ 53010767
นายสิทธิธัช ศิริภิรมย์ 53011680
ดร. วรวัฒน์ ลิ้มโภคา อาจารย์ที่ปรึกษา
ปีการศึกษา 2556

บทคัดย่อ

เพื่อที่จะป้องกันระบบเครือข่ายในองค์กรจากพวกภัยคุกคามต่างๆที่อาจเกิดขึ้น เพราะข้อมูลและแอพพลิเคชั่นที่ได้รับและส่งผ่านเครือข่ายโดยปราศจากการป้องกันนั้นสามารถตกเป็นเหยื่อการโจมตีได้ ซึ่งการโจมตีสามารถขัดขวางการเชื่อมต่อ ทำให้การประมวลผลของเน็ทเวิคทราฟฟิคช้าลงจนเกิดคอขวด และมีแนวโน้มที่จะเป็นสาเหตุทำให้เกิดความเสียหายที่รุนแรงและทำลายทั้งระบบ ด้วยเหตุนี้เราจึงได้ทำโครงงานความมั่นคงของระบบเครือข่ายขึ้นมา ซึ่งสามารถป้องกันเครือข่ายภายในโดยที่ไม่ให้คนภายนอกสามารถเข้าถึงเครือข่ายภายในได้ การส่งข้อมูลผ่านเครือข่ายมีประสิทธิภาพมากยิ่งขึ้น และมีการป้องกันแบบเรียลทามเพื่อที่จะรักษาระบบให้สามารถใช้งานได้อย่างสูงสุด ระบบความปลอดภัยเครือข่ายสามารถป้องกันอันตรายโดยใช้แอนตี้ไวรัสซอฟแวร์และไฟวอลล์เพื่อป้องกันการโจมตีก่อนที่จะพวกมันจะทำให้ไม่สามารถให้บริการได้ ในกรณีที่ผู้บุกรุกต้องการที่จะเข้า มีการวัดความปลอดภัยที่สามารถตรวจสอบผู้บุกรุกและกำจัดก่อนที่ผู้บุกรุกจะเป็นสาเหตุทำให้เซิฟเวอร์เกิดความเสียหาย

ENTERPRISE NETWORK SECURITY

Ms. Theerut	Foongkiatcharoen	53010767
Mr. Sittituch	Siripirom	53011680
Dr. Voravat	Limpoka	Advisor

Academic Year 2013

ABSTRACT

To protect business network against potential threats, Information and application that are retrieved and transmitted network without protection which could possibly fall victims to a variety of attacks. Attacks such as these can hinder connectivity, slow the processing of network traffic into bottlenecks, and even potentially cause serious and difficulty damage enough to crash an entire system. Therefore, we have researched the means of network protection and analysis in the Organization and we named it "Enterprise Network security". This means can prevent attackers and limit an user who connecting via internet to gain access to private network. In addition to, businesses are provided the preventative real-time protection they need to maintain a high availability, effective information transmission. With Enterprise Network security, malicious threats can be blocked using Antivirus Software and firewall to prevent these before they cause disruptions. In case of attackers gain access, security measures are able to detect the intrusion and eliminate it before it causes any server damage.

กิตติกรรมประกาศ

ปริญญานิพนธ์ฉบับนี้ได้รับคำแนะนำ และคำปรึกษาเกี่ยวกับการวิจัยและค้นคว้าเป็นอย่างดี จากอาจารย์ ดร.วรวัฒน์ ลิ้มโภคา อาจารย์ที่ปรึกษาในการจัดทำปริญญานิพนธ์ คณะผู้จัดทำรู้สึกซาบซึ้งเป็นอย่างมากในความอนุเคราะห์จากอาจารย์ที่คอยให้การสนับสนุนในการทำปริญญานิพนธ์นี้เสมอมา อีกทั้งได้รับการช่วยเหลือจากบริษัท Textile Prestige public Company Limited (TPCORP) ที่ให้ทั้งคำปรึกษาและแนะนำความรู้รวมถึงอุปกรณ์ต่างๆที่ใช้ในการทำงานในส่วนต่างๆ ของปริญญานิพนธ์ฉบับนี้

คณะผู้จัดทำขอขอบพระคุณเป็นอย่างสูง และหวังเป็นอย่างยิ่งว่าปริญญานิพนธ์ฉบับนี้จะเป็นประโยชน์ต่อทุกท่าน และสามารถให้คำแนะนำแก่นักศึกษารุ่นต่อไปในอนาคตได้

ธีรุตม์ ฟุ้งเกียรติเจริญ
สิทธิธัช ศิริภิรมย์

สารบัญ

หน้า

สารบัญรูป

รูปที่ **หน้า**

บทที่ 1
บทนำ

1.1 ความสำคัญและที่มาของโครงงาน

ในการใช้งานระบบอินเทอร์เน็ตในปัจจุบัน เราก็ยังไม่สามารถมั่นใจได้ว่าการใช้อินเทอร์เน็ตในแต่ละวันของเราแม้จะเป็นเครื่องคอมพิวเตอร์ที่อยู่ที่บ้านก็ตามนั้น ในการเข้าถึงแต่ละข้อมูลเนื้อหา หรือ แต่ละเว็บไซต์ที่เข้าไปค้นหาข้อมูล รวมถึงเวลาที่ดาวน์โหลดไฟล์จากอินเทอร์เน็ต มีความปลอดภัยหรือไม่ หรืออาจจะมีสิ่งแปลกปลอมที่เกิดจากผู้ประสงค์ร้ายไว้ในไฟล์นั้นๆ หรือ หน้าเว็บไซต์นั้นๆ หรือการถูกผู้ประสงค์ร้ายกระทำการโจมตีเน็ตเวิร์ค (Network) หรือ อาจจะล้วงข้อมูลสำคัญที่อยู่ในเครื่องคอมพิวเตอร์ของเรา โดยที่เราไม่รู้เลยว่าคอมพิวเตอร์ของเรานั้น ได้ถูกล้วงข้อมูล หรือ วางสิ่งแปลกปลอมไว้ในเครื่องแล้วเรียบร้อย

เมื่อลองดูไปถึงในระดับที่สูงขึ้นไปอีก เช่น ในองค์กรบริษัทใหญ่ๆ หรือ องค์กรบริษัททั่วไป ความเสี่ยงในการที่จะถูกโจมตีจากผู้ประสงค์ร้าย อาจจะเป็นจากบริษัทคู่แข่งหรืออะไรก็ตาม ก็ยิ่งมีมากขึ้น รวมไปถึงในเน็ตเวิร์คขององค์กรเอง ก็อาจจะมีพนักงานที่เผลอเข้าไปในเว็บไซต์ที่มีมัลแวร์ หรือ ดาวน์โหลดไฟล์ที่มีมัลแวร์ (Malware) อย่างไม่ได้ตั้งใจ และทำให้มัลแวร์นั้นทำการแพร่เชื้อในบริษัทเอง จึงต้องมีการวางระบบรักษาความปลอดภัยที่เป็นระบบที่มีความน่าเชื่อถือ และต้องมั่นใจได้ว่าจะสามารถป้องกันสิ่งแปลกปลอมไม่ให้เข้ามาภายในเน็ตเวิร์คขององค์กร หรือ ป้องกันผู้ประสงค์ร้าย ไม่ให้เข้ามาโจมตี และ ล้วงข้อมูลขององค์กรได้

1.2 วัตถุประสงค์ของโครงงาน

1) เพื่อออกแบบระบบรักษาความปลอดภัยของเครือข่ายที่ใช้ในองค์กร
2) เพื่อศึกษาการตั้งค่าไฟร์วอลล์ (Firewall)
3) เพื่อศึกษาการใช้งานโอเพ่นวีพีเอ็น (OpenVPN)
4) เพื่อศึกษาการใช้งานไอดีเอส (IDS) และ ไอพีเอส (IPS)
5) เพื่อศึกษาการใช้งานพร็อกซี่ (Proxy)
6) เพื่อศึกษาการใช้งานระบบรักษาความปลอดภัยโดยใช้เคลียร์โอเอส (ClearOS)
7) เพื่อศึกษาการเขียนโปรแกรมแสดงบันทึกเหตุการณ์ของ Snort

1.3 ขอบเขตของโครงงาน

1) การจะดาวน์โหลด เซอร์ทิฟิเคท (Certificate) มาใช้สำหรับเข้า วีพีเอ็น (VPN) สามารถทำภายในองค์กรเท่านั้น ถึงจะนำมาใช้งานเข้าระบบจากภายนอกองค์กรได้
2) มีระบบต่างๆที่รักษาความปลอดภัยสำหรับเครือข่ายในองค์กร
3) มีโปรแกรมที่สามารถวิเคราะห์บันทึกเหตุการณ์สำหรับ Snort (IDS/IPS)

1.4 วิธีการดำเนินการ

1) ศึกษาทฤษฎีของไฟร์วอลล์
2) ศึกษาทฤษฎีของไอพีเอส/ไอดีเอส (IDS)
3) ศึกษาทฤษฎีของวีพีเอ็น
4) ศึกษาทฤษฎีของเคลียร์โอเอส
5) ติดตั้งและตั้งค่าระบบเคลียร์โอเอสลงบนเน็ตเวิร์คขององค์กร
6) ตั้งค่าให้สามารถใช้งานวีพีเอ็นจากภายนอกองค์กร
7) ตั้งค่าไฟร์วอลล์ให้ทำงานตามที่ต้องการ
8) ตั้งค่าพร็อกซีให้ทำงานตามที่ต้องการ
9) เขียนโปรแกรมวิเคราะห์บันทึกเหตุการณ์ของ Snort

1.5 ประโยชน์ที่คาดว่าจะได้รับ

1) เข้าใจระบบของ เน็ตเวิร์คซีเคียวริตี้ในองค์กร
2) สามารถทำการตั้งค่าและแก้ไขระบบต่างๆของเคลียร์โอเอสได้
3) สามารถเขียนโปรแกรมแสดงบันทึกเหตุการณ์ของ Snort ได้

1.6 ส่วนประกอบของปริญญานิพนธ์

ปริญญานิพนธ์ฉบับนี้ได้แบ่งเนื้อหาออกเป็น 4 บท โดยมีรายละเอียดดังต่อไปนี้

บทที่ 1 บทนำกล่าวถึงความสำคัญและที่มาของโครงงาน วัตถุประสงค์ของโครงงาน ขอบเขตของโครงงาน วิธีการดำเนินการ ประโยชน์ที่คาดว่าจะได้รับ และส่วนประกอบของปริญญานิพนธ์

บทที่ 2 ทฤษฎีที่เกี่ยวข้อง กล่าวถึง ทฤษฎีพื้นฐาน หลักการ ความรู้ต่างๆ ที่ใช้ในโครงงาน ซึ่งประกอบด้วย รายละเอียดของโพรโทคอลเอสเอ็นเอ็มพี และรายละเอียดของเอนโทรปี ซึ่งเป็นเทคนิคที่ใช้วัดค่าความเปลี่ยนแปลงของข้อมูล

บทที่ 3 การออกแบบและการพัฒนาโปรแกรม กล่าวถึง วัตถุประสงค์ของโปรแกรม รายละเอียดการออกแบบและพัฒนาโปรแกรม บรรยายส่วนของการทำงานของระบบและโครงสร้างของระบบ

บทที่ 4 การทดสอบและผลลัพธ์จากการพัฒนาโปรแกรม กล่าวถึง การตั้งค่าโปรแกรม การทดสอบกับระบบ และผลลัพธ์ที่ได้จากการทดสอบ

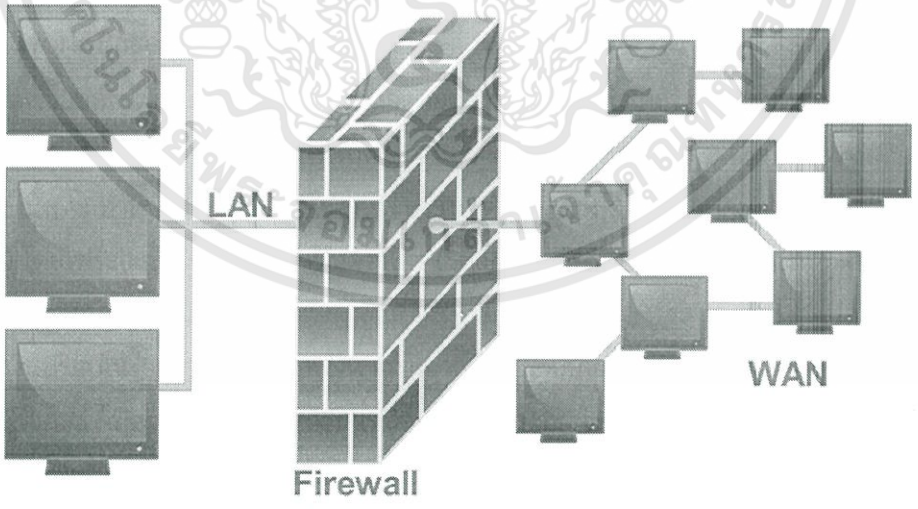
บทที่ 5 บทสรุป กล่าวถึง บทสรุปของโครงงาน วิจารณ์สิ่งที่ได้รับจากโครงงาน ข้อจำกัด รวมถึงปัญหาอุปสรรคต่างๆ ของโครงงาน และข้อเสนอแนะสำหรับเป็นแนวทางในการพัฒนาต่อ

บทที่ 2
ทฤษฎีที่เกี่ยวข้อง

2.1 Network Based Firewall

ไฟร์วอลล์ เป็นระบบรักษาความปลอดภัยของระบบคอมพิวเตอร์แบบหนึ่งที่นิยมใช้กันอย่างแพร่หลาย ซึ่งมีทั้งอุปกรณ์ ฮาร์ดแวร์ (Hardware) และ ซอร์ฟแวร์ (Software) โดยหน้าที่หลัก ๆ ของไฟร์วอลล์ นั้น จะทำหน้าที่ควบคุมการใช้งานระหว่างเน็ตเวิร์ค ต่าง ๆ การควบคุมการเข้าถึง (Access Control) โดยไฟร์วอลล์จะเป็นคนที่กำหนดว่าใคร (Source) , ไปที่ไหน (Destination) , ด้วยบริการอะไร (Service/Port)

ถ้าเปรียบให้ง่ายกว่านั้นนึกถึงพนักงานรักษาความปลอดภัย หรือที่เราเรียกกันติดปากว่า "ยาม" ไฟร์วอลล์ ก็มีหน้าที่เหมือนกับ"ยาม"เหมือนกัน ซึ่ง "ยาม" จะคอยตรวจบัตร เมื่อมีคนเข้ามา ซึ่งคนที่มีบัตร "ยาม" ก็คือว่ามี "สิทธิ์" (Authorized) ก็สามารถเข้ามาได้ ซึ่งอาจจะมีการกำหนดว่า คน ๆ นั้น สามารถไปที่ชั้นไหนบ้าง ถ้าคนที่ไม่มีบัตร ก็ถือว่า เป็นคนที่ไม่มีสิทธิ์ (Unauthorized) ก็ไม่สามารถเข้าตึกได้ หรือว่ามีบัตร แต่ไม่มีสิทธิ์ไปชั้นนั้น ก็ไม่สามารถผ่านไปได้ หน้าที่ของ ไฟร์วอลล์ ก็เช่นกัน



รูปที่ 2.1 รูปแบบของไฟร์วอลล์

โดยไฟร์วอลล์สามารถแบ่งได้เป็นหลายชนิดดังนี้

2.1.1 Packet Filtering

ลักษณะโดยพื้นฐานส่วนใหญ่ของไฟร์วอลล์ คือ แพ็คเก็ตฟิลเตอร์ (Packet Filter) ไฟร์วอลล์เก่าๆที่เป็นเพียงแค่แพ็คเก็ตฟิลเตอร์นั้นคืออุปกรณ์เราท์ติ้งที่สำคัญมากที่ให้ฟังก์ชั่นการควบคุมการเข้า (Access Control Functionality) สำหรับโฮสต์แอดเดรส (Host Address) และ เซชชั่น (Session) ในการติดต่อ อุปกรณ์เหล่านี้จะเป็นที่รู้จักกันในนามว่า สเตทเลสอินสเปคชั่น (Stateless Inspection) ไฟร์วอลล์ ซึ่งก็คือจะไม่ติดตามเส้นทางของสถานะของแต่ละการไหลของการจราจรที่ผ่าน ไฟร์วอลล์ เช่น พวกมันไม่สามารถเชื่อมต่อหลายๆรีเควส (Request) ภายในหนึ่งเซชชั่นไปยังซึ่งกันและกันได้ แพ็คเก็ตฟิลเตอริ่งอยู่ที่แก่นของไฟร์วอลล์ส่วนใหญ่สมัยนี้มีเพียงแค่ ไฟร์วอลล์บางตัวที่ทำเพียงแค่ สเตทเลสฟิลเตอริ่ง (Stateless Filtering) ขายทุกวันนี้ไม่เหมือนกับการกรองแบบใหม่ แพ็คเก็ตฟิลเตอร์ นั้นจะไม่สนใจเกี่ยวกับเนื้อหาของแพ็คเก็ต ฟังก์ชั่นการควบคุมการเข้าถูกควบคุมโดยกลุ่มของคำสั่ง ที่เรียกว่า รูลล์เซ็ต (ชุดคำสั่ง) ความสามารถของ แพ็คเก็ตฟิลเตอริ่ง ถูกสร้างในหลายๆ ระบบปฏิบัติการและอุปกรณ์ที่สามารถ เราท์ติ้ง ตัวอย่างทั่วๆไปส่วนใหญ่ของอุปกรณ์ แพ็คเก็ตฟิลเตอริ่งอย่างเดียว คือ เน็ตเวิร์คเราท์เตอร์ (Networkwork Router) ที่ใช้ การควบคุมการเข้าถึงลิสต์

บางแพ็คเก็ตฟิลเตอร์สามารถกรองแพ็คเก็ตที่ถูกแยกออกเป็นชิ้นๆได้อย่างเฉพาะเจาะจง การแบ่งแพ็คเก็ตออกเป็นชิ้นๆ (Packet Fragmentation) ถูกอนุญาตโดย ทีซีพี/ไอพี สเปซิฟิเคชั่น และถูกสนับสนุนในสถานการณ์ที่จำเป็น อย่างไรก็ตามการแบ่งแพ็คเก็ตออกเป็นชิ้นๆถูกใช้เพื่อสร้างการโจมตีให้ยากขึ้นเพื่อที่จะจรวจสอบ (โดยการวางพวกมันไว้ภายในแพ็คเก็ตที่ถูกแบ่ง(Fragmented Packet))และการแบ่งออกเป็นชิ้นๆแบบไม่ปกติจะถูกใช้ในรูปแบบของการโจมตี ตัวอย่างเช่น การโจมตีเน็ตเวิร์ค-เบสใช้แพ็คเก็ตที่ไม่ปรากฏในการติดต่อสื่อสารตามปกติ อย่างเช่น ส่งชิ้นส่วนบางส่วนที่แบ่งของแพ็คเก็ตแต่ไม่ใช้ชิ้นแรก หรือส่งชิ้นส่วนของแพ็คเก็ตที่ทับกันและกัน เพื่อที่จะป้องกันการใช้แพ็คเก็ตที่ถูกแบ่งในการโจมตี บางไฟร์วอลล์ตั้งค่าเพื่อที่จะปิดกั้นแพ็คเก็ตที่ถูกแบ่ง

2.1.2 Stateful Inspection

สเตทฟูลล์อินสเปคชั่น (Stateful Inspection) พัฒนาการทำงานของแพ็คเก็ตฟิลเตอร์ โดยติดตามสถานการณ์เชื่อมต่อและ การปิดกั้นแพ็คเก็ตที่ทำงานผิดปกติไปจากรูปแบบที่คาดไว้ โดยสิ่งนี้จะทำให้สำเร็จโดยร่วมมือการเพิ่มความรับรู้ของ ทรานสพอร์ต เลเยอร์ เมื่อเทียบกับแพ็คเก็ตฟิลเตอริ่ง สเตทฟูลล์อินสเปคชั่น สกัดแพ็คเก็ตที่เน็ตเวิร์คเลเยอร์ และ ตรวจสอบแพ็คเก็ตเพื่อที่จะเห็นว่าถ้าแพ็คเก็ตถูกอนุญาตโดยกฎของไฟร์วอลล์ที่ปรากฏแต่ไม่เหมือนแพ็คเก็ตฟิลเตอริ่ง สเตทฟูลล์อินสเปคชั่น เก็บเส้นทางของแต่ละการเชื่อมต่อในตารางสถานะ (State Table) ขณะที่รายละเอียดของข้อมูล

ตารางสถานะที่หลากหลายโดยผลิตภัณฑ์ไฟร์วอลล์ซึ่งรายละเอียดนี้ก็จะรวมถึง ไอพีต้นทาง, ไอพีปลายทาง, เลขพอร์ต, และข้อมูลสถานะการเชื่อมต่อ

สามสถานะหลักที่ปรากฏสำหรับการจราจร ทีซีพี - การสร้างการเชื่อมต่อ, การใช้การเชื่อมต่อ, การยกเลิกการเชื่อมต่อ (ซึ่งอ้างถึงทั้ง เอ็นพ็อยท์ ร้องขอการเชื่อมต่อถูกปิดและการเชื่อมต่อที่ไม่ได้ทำอะไรนานๆ สเตทฟูลล์อินสเปคชั่น ในไฟร์วอลล์ ตรวจสอบค่าที่แน่นอนใน ทีซีพีเฮดเดอร์ เพื่อที่จะตรวจดูสถานะของแต่ละการเชื่อมต่อ แต่ละแพ็คเก็ตใหม่ถูกเปรียบเทียบโดยไฟร์วอลล์ กับตารางสถานะของ ไฟร์วอลล์ เพื่อที่จะกำหนดว่าถ้าสถานะของแพ็คเก็ตขัดแย้งกับสถานะของมันที่คาดไว้ ตัวอย่างเช่น ผู้โจมตีสามารถสร้างแพ็คเก็ตกับเฮดเดอร์ที่บ่งชี้ว่ามันเป็นส่วนหนึ่งของการสร้างการเชื่อมต่อ ถ้าไฟร์วอลล์ใช้สเตทฟูลล์อินสเปคชั่นมันจะตรวจสอบแพ็คเก็ตว่า เป็นส่วนหนึ่งของรายการการสร้างการเชื่อมต่อในตารางสถานะ

Source Address	Source Port	Destination Address	Destination Port	Connection State
192.168.1.100	1030	192.0.2.71	80	Initiated
192.168.1.102	1031	10.12.18.74	80	Established
192.168.1.101	1033	10.66.32.122	25	Established
192.168.1.106	1035	10.231.32.12	79	Established

รูปที่ 2.2 ตารางสถานะของสเตทฟูลอินสเปคชั่น

2.1.3 Application Firewall

เป็นแนวทางใหม่ของสเตทฟูลล์อินสเปคชั่น โดยการเพิ่มความสามารถการวิเคราะห์ สเตทฟูลล์ โปรโตคอล

การวิเคราะห์สเตทฟูลล์โปรโตคอล พัฒนาบนมาตรฐานสเตทฟูลล์อินสเปคชั่นโดยเพิ่มเทคโนโลยีการตรวจสอบการบุกรุกแบบพื้นฐานเข้าไปซึ่งเครื่องมือตรวจสอบนี้จะวิเคราะห์ โปรโตคอลที่แอพพลิเคชั่นเลเยอร์เพื่อที่จะเปรียบเทียบโปรโตคอลแอคทิวิตี้ที่ดีกับเหตุการณ์ที่สังเกตเพื่อที่จะสามารถระบุได้ว่า โปรโตคอล ไหนทำงานผิดปกติ การเปรียบเทียบนี้จะทำให้ ไฟร์วอลล์ อัลลาวด์ หรือ ดีไนน์ ขึ้นอยู่กับ แอพพลิเคชั่น ที่กำลังทำงานอยู่บนเน็ตเวิร์คนั้นเป็นอย่างไร ตัวอย่างเช่น แอพพลิเคชั่นไฟร์วอลล์ สามารถกำหนดว่าถ้าอีเมลเมสเซจบรรจุชนิดของสิ่งที่แนบมาองค์กรจะไม่อนุญาต เช่น (ไฟล์ที่รันได้) หรือ อินสแตนท์เมซเซจจิ้ง (Instant messaging) (IM) ที่กำลังใช้อยู่บน พอร์ต 80 (ซึ่งโดยทั่วไปใช้กับ เอชทีทีพี) ฟีเจอร์อื่นๆคือสามารถปิดกั้นการเชื่อมต่อที่มีการทำงานโดยเฉพาะเจาะจง เช่น ผู้ใช้งานสามารถถูกป้องกันจากการใช้คำสั่ง พุท ในเอฟทีพี (ซึ่งคำสั่งมันจะอัลลาวด์ให้ผู้ใช้งานเขียนไฟล์ไปยัง เซิฟเวอร์) และฟีเจอร์นี้สามารถถูกใช้เพื่อ อัลลาวด์ หรือ ดีไนน์ เว็บเพจที่บรรจุชนิดของ

แอคทีฟคอนเทนท์ โดยเฉพาะ แอคทีฟคอนเทนท์ ก็อย่างเช่น จาว่า (java) หรือ แอคทีฟเอ็กซ์ (activeX) หรือมี เอสเอสแอลเซอร์ทิฟิเคทที่ ไซน์ โดยเซอร์ทิฟิเคทออทิริตี้ (CA) เช่น รีโวคซีเอ

แอพพลิเคชั่นไฟร์วอลล์สามารถระบุลำดับคำสั่งที่ไม่แน่นอน เช่น สั่งคำสั่งเดียวกันซ้ำๆ หรือ สั่งคำสั่งที่ไม่ได้มีมาก่อนโดยคำสั่งอื่นที่เกี่ยวข้องกัน โดยคำสั่งที่น่าสงสัยจะเป็นจุดเริ่มต้นของการโจมตี บัฟเฟอร์โอเวอร์โฟล์ว การโจมตีดีโอเอส, มัลแวร์ และ การโจมตีรูปแบบอื่นๆที่ประสบความสำเร็จได้ ภายในแอพพลิเคชั่นโปรโตคอล เช่น เอชทีทีพี

ไฟร์วอลล์กับทั้งสเตทฟูลล์อินสเปคชั่น และความสามารถการวิเคราะห์ สเตทฟูลล์ โปรโตคอล ไม่ได้เป็นการตรวจสอบการบุกรุก (Intrusion Detection) และระบบป้องกัน (Prevention Systems) ที่พัฒนาอย่างสมบูรณ์ ซึ่งโดยปกติจะเสนอการตรวจสอบการโจมตีและความสามารถการป้องกันได้ อย่างกว้างขวางมากยิ่งขึ้น ยกตัวอย่างเช่น ไอดีพีเอสใช้การวิเคราะห์ ซิกเนเจอร์-เบส หรือ อนอมัลลี่-เบส เพื่อที่จะตรวจสอบปัญหาภายในการจราจรเน็ตเวิร์คที่เพิ่มขึ้นด้วย

2.1.4 Application-Proxy Gateway

เป็นรูปแบบของแอดวานซ์ไฟร์วอลล์ที่ผสมระหว่าง โลเวอร์-เลเยอร์ การควบคุมการเข้าถึง กับ อัพเปอร์-เลเยอร์ฟังก์ชันแนลลิตี้ โดยไฟร์วอลล์ชนิดนี้จะมีตัวทำหน้าที่พร็อกซี่ที่เป็นตัวกลางระหว่าง โฮสต์ 2 โฮสต์ ที่จะทำการติดต่อสื่อสารกัน และไม่อนุญาตให้ทั้ง 2 โฮสต์นั้นติดต่อกันโดยตรง โดยเมื่อ มีการเชื่อมต่อสำเร็จจะแบ่งออกเป็นการเชื่อมต่อ 2 การเชื่อมต่อ คือ ระหว่างไคล์เอนท์ กับ พร็อกซี่ เซิฟเวอร์ และ ระหว่างพร็อกซี่เซิฟเวอร์ กับปลายทางจริงๆ โดยพร็อกซี่นั้นจะเหมือนล่องหนอยู่ สำหรับโฮสต์ทั้ง2 โดยจากมุมมองของโฮสต์แล้วคือเชื่อมต่อกันโดยตรง เพราะว่าโฮสต์ภายนอกนั้น สามารถติดต่อได้เพียงแต่พร็อกซี่เซิฟเวอร์ โดยที่ไอพีแอดเดรสภายในจะไม่ถูกเปิดเผยต่อเน็ตเวิร์คข้าง นอก โดยพร็อกซี่เอเจนท์อินเตอร์เฟซนั้นจะเป็นเหมือนไฟร์วอลล์รูลล์เซ็ตที่จะทำหน้าที่กำหนด เน็ตเวิร์คทราฟฟิก ว่าจะอนุญาตให้ผ่านไฟร์วอลล์หรือไม่

แอพพลิเคชั่น-พร็อกซี่เกทเวย์ นั้นค่อนข้างต่างเมื่อเทียบกับ แอพพลิเคชั่นไฟร์วอลล์ อย่างแรก แอพพลิเคชั่น-พร็อกซี่เกทเวย์ นั้นสามารถให้ความปลอดภัยในระดับที่สูงกว่าสำหรับบาง แอพพลิเคชั่น เพราะว่ามันป้องกันการเชื่อมต่อโดยตรงระหว่าง 2 โฮสต์ และ สามารถตรวจสอบ ทราฟฟิก คอนเทนท์ เพื่อแยกแยะนโยบายการละเมิด และยังมีประโยชน์อื่นอีกคือบาง แอพพลิเคชั่น-พร็อกซี่เกทเวย์ มี ความสามารถในการถอดรหัสแพ็คเก็ต(ตัวอย่างเช่น เอสเอสแอล-โพรเทค เพย์โหลด) , ตรวจสอบ , และเข้ารหัสใหม่ ก่อนที่จะส่งต่อไปยังโฮสต์ปลายทาง ส่วน ดาต้า ที่ เกทเวย์ ไม่สามารถถอดรหัสได้จะ ผ่านไปยังแอพพลิเคชั่นโดยตรง ในขณะที่เลือกชนิดของไฟร์วอลล์ที่จะใช้งาน มันเป็นสิ่งสำคัญที่จะ

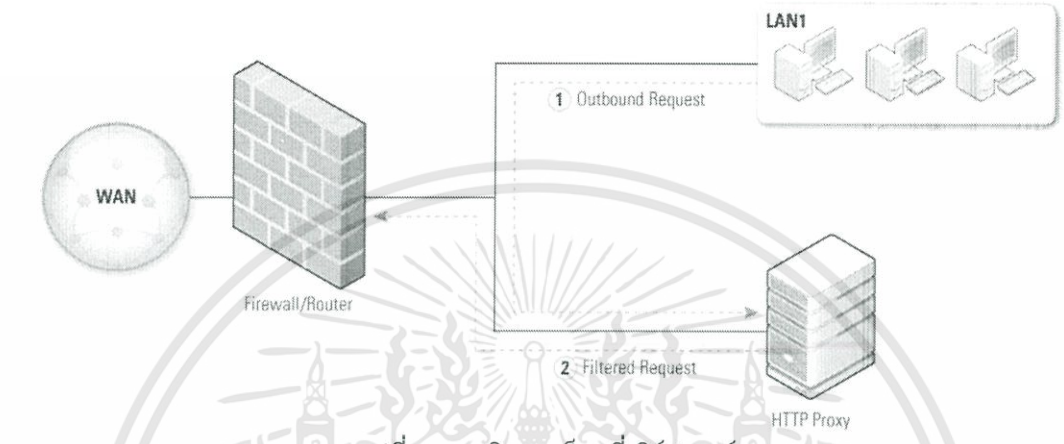
ตัดสินว่าไฟร์วอลล์แท้จริงแล้วจำเป็นที่จะต้องทำแบบ แอพพลิเคชั่นพร็อกซี่ ดังนั้นมันสามารถที่จะตรงกับนโยบายที่ต้องการขององค์กร

ไฟร์วอลล์กับแอพพลิเคชั่น-พร็อกซี่เกทเวย์ นั้นยังมีหลากหลายข้อเสียเปรียบเมื่อเปรียบเทียบกับ แพ็คเก็ตฟิลเตอริ่ง และ สเตทฟูลล์อินสเปคชั่น อย่างแรกเพราะว่า “ฟูลล์แพ็คเก็ต อแวร์เนส” ของแอพพลิเคชั่น-พร็อกซี่เกทเวย์นั้น ไฟร์วอลล์จะใช้เวลาในการอ่านแต่ละแพ็คเก็ตมากกว่าใช้เวลาในการตีความ ด้วยเหตุผลนี้บางชนิดของเกทเวย์จำพวกนี้จะทำงานได้แย่สำหรับแบนด์วิดธ์ที่สูงๆ หรือเรียลไทม์แอพพลิเคชั่น แต่ แอพพลิเคชั่น-พร็อกซี่เกทเวย์ ที่ทำงานบนแบนด์วิดธ์สูงนั้นสามารถใช้ได้ เพื่อที่จะลดโหลดบนไฟร์วอลล์นั้น เดดิเคทพร็อกซี่เซิฟเวอร์ สามารถถูกรักษาความปลอดภัยแบบ เลสไทม์เซนซิทีฟเซอร์วิซ เช่น อีเมล และ เว็บทราฟฟิกส่วนใหญ่ อีกข้อเสียหนึ่งคี แอพพลิเคชั่น-พร็อกซี่เกทเวย์ ค่อนข้างจะมีข้อจำกัดในส่วนของสนับสนุนสำหรับ เน็ตเวิร์คแอพพลิเคชั่น และ โปรโตคอลใหม่ๆ โดยแต่ละแอพพลิเคชั่น-สเปซิฟิกพร็อกซี่เอเจนท์ จะจำเป็นต้องใช้สำหรับเน็ตเวิร์คทราฟฟิก แต่ละชนิดที่จำเป็นสำหรับการผ่านไฟร์วอลล์ ผู้จำหน่าย แอพพลิเคชั่น-พร็อกซี่ เกทเวย์ ไฟร์วอลล์ จำนวนมากให้พร็อกซี่เอเจ็นท์ทั่วไปเพื่อสนับสนุน เน็ตเวิร์คโปรโตคอล หรือ แอพพลิเคชั่น ที่ไม่ได้ถูกระบุไว้โดย เอเจ็นท์ ทั่วไปเหล่านี้จะปฏิเสธจุดแข็งจำนวนมากของสถาปัตยกรรม แอพพลิเคชั่น-พร็อกซี่เกทเวย์ เพราะว่าพวกนี้จะอนุญาตให้ ทราฟฟิก เข้า “อุโมงค์” ผ่าน ไฟร์วอลล์ ไปอย่างง่ายดาย

2.1.5 Dedicated Proxy Server

เดดิเคทพร็อกซี่เซิฟเวอร์ แตกต่างจาก แอพพลิเคชั่น-พร็อกซี่เกทเวย์ ในขณะที่ เดดิเคท พร็อกซี่เซิฟเวอร์เก็บรักษาพร็อกซี่คอนโทรลของทราฟฟิกนั้น มักจะมีการจำกัดความสามารถไฟร์วอลล์มากขึ้น โดยจะถูกอธิบายในส่วนนี้เพราะว่าจะมีความสัมพันธ์ใกล้ๆกันกับ แอพพลิเคชั่น-พร็อกซี่ เกทเวย์ ไฟร์วอลล์ ตัว เดดิเคทพร็อกซี่ เซิฟเวอร์ หลายตัวเป็นแอพพลิเคชั่นโดยเฉพาะ และมีบางตัวที่จริงๆแล้วทำงานวิเคราะห์ และ ตรวจสอบคอมม่อนแอพพลิเคชั่น โปรโตคอล เช่น เอชทีทีพี เพราะว่า เซิฟเวอร์เหล่านี้มีการจำกัดความสามารถ ไฟร์วอลล์ เช่น ปิดกั้นทราฟฟิก ง่ายๆ โดยขึ้นอยู่กับต้นทาง หรือปลายทาง โดยปกติมันจะถูกสร้างข้างหลัง ไฟร์วอลล์แพลทฟอร์มเก่า ปกติแล้ว ไฟร์วอลล์หลักจะทำการรับทราฟฟิกขาเข้าขึ้นอยู่กับ แอพพลิเคชั่นใดที่เป็นเป้าหมาย และปล่อยทราฟฟิกต่อไปยังแอพพลิเคชั่น-พร็อกซี่เซิฟเวอร์ (เช่น อีเมล พร็อกซี่) เซิฟเวอร์นี้จะทำกระบวนการคัดกรองบนทราฟฟิก และส่งต่อสู่ระบบภายในโดยพร็อกซี่เซิฟเวอร์สามารถรับทราฟฟิกขาออกได้โดยตรงจากระบบภายใน คัดกรอง หรือ ปล่อยทราฟฟิกเข้าสู่ระบบ และ ส่งต่อไปยัง ไฟร์วอลล์เพื่อส่งออกไป ตัวอย่างนี้คือ เอชทีทีพี พร็อกซี่ ที่สร้างข้างหลังไฟร์วอลล์ ผู้ใช้งานจำเป็นต้องเชื่อมต่อพร็อกซี่นี้ระหว่างทางที่จะเชื่อมต่อไปยังเว็บเซิฟเวอร์ภายนอก เดดิเคทพร็อกซี่ เซิฟเวอร์ โดยทั่วไปจะใช้สำหรับลดการทำงาน

ของไฟร์วอลล์ และใช้ดำเนินการคัดกรอง และ การปล่อยเข้าสู่ระบบที่อาจจะทำงานยาก เมื่อทำงานบนตัวไฟร์วอลล์ เอง



รูปที่ 2.3 เดดิเคทพร็อกซี่เซิร์ฟเวอร์

2.1.6 Virtual Private Networking

เครื่องมือไฟร์วอลล์ที่อยู่ที่ ขอบของเน็ตเวิร์ค บางครั้งก็ต้องการความสามารถที่มากกว่าการปิดกั้นทราฟฟิกที่ไม่ต้องการ ความต้องการทั่วไปของไฟร์วอลล์เหล่านี้คือการเข้ารหัส และ การถอดรหัส โดยเฉพาะกระแสเน็ตเวิร์คทราฟฟิก ระหว่าง เน็ตเวิร์คที่ถูกป้องกัน กับ เน็ตเวิร์คภายนอก โดยนี่มักจะเกี่ยวข้องกับ เวอร์ช่วลไพรเวทเน็ตเวิร์ค (วีพีเอ็น) ที่มีโปรโตคอลเพิ่มเติมสำหรับเข้ารหัสทราฟฟิก และ การยืนยันตนของผู้ใช้ และ การตรวจสอบความสมบูรณ์ วีพีเอ็น นั้นส่วนใหญ่จะใช้ในการให้รักษาความปลอดภัยของ เน็ตเวิร์คคอมมิวนิเคชั่นผ่านเน็ตเวิร์คที่เชื่อถือไม่ได้ ตัวอย่างเช่น เทคโนโลยี วีพีเอ็น นั้นใช้อย่างเปิดกว้างสำหรับขยาย เน็ตเวิร์ค ที่ถูกป้องกัน ขององค์กรที่มีหลายสถานที่ ผ่าน อินเทอร์เน็ต และบางครั้ง ใช้สำหรับการรักษาความปลอดภัย การ รีโมท เข้ามาของผู้ใช้ที่จะเข้าสู่เน็ตเวิร์คองค์กรภายใน โดยผ่านอินเทอร์เน็ตตัวเลือกโดยทั่วไปของ วีพีเอ็น คือ ไอพีเซ็ค (IPsec) และ ซีเคียวซ็อคเก็ตเลเยอร์ (เอสเอสแอล)/ ทรานสพอร์ต เลเยอร์ ซีเคียวริตี้ (ทีแอลเอส)

สองสถาปัตยกรรมวีพีเอ็นที่ใช้กันมากที่สุดคือ เกทเวย์-ทู-เกทเวย์ (Gateway-to-Gateway) และ โฮสต์-ทู-เกทเวย์ (Host-to-Gateway) สถาปัตยกรรมเกทเวย์-ทู-เกทเวย์ จะเชื่อมต่อหลายสถานที่ผ่านเหนือเส้นทางสาธารณะโดยใช้วีพีเอ็นเกทเวย์ ตัวอย่างเช่น การเชื่อมต่อสาขาย่อยของบริษัทไปยังบริษัทใหญ่ วีพีเอ็นเกทเวย์มักจะใช้ส่วนของเครื่องมือเน็ตเวิร์คอื่นเช่น ไฟร์วอลล์ หรือ เราท์เตอร์ในขณะที่การเชื่อมต่อวีพีเอ็นถูกสร้างระหว่าง 2 เกทเวย์ ผู้ใช้ที่อยู่ที่สาขาจะไม่ต้องระมัดระวังการเชื่อมต่อ และไม่ต้องการการติดตั้งอะไรพิเศษบนคอมพิวเตอร์ของพวกเขา โฮสต์-ทู-เกทเวย์จะใช้การ

รักษาความปลอดภัยในการเชื่อมต่อสำหรับผู้ใช้แต่ละคน โดยทั่วไปเรียกว่ารีโมทผู้ใช้งานผู้ที่อยู่ข้างนอกขององค์กร เช่น อยู่บ้าน โรงแรม โดยเครื่องของผู้ใช้จะทำการติดต่อกับระบบการรักษาความปลอดภัยการเชื่อมต่อด้วย วีพีเอ็นเกทเวย์ขององค์กร สำหรับ เกทเวย์-ทู-เกทเวย์ และ โฮสต์-ทู-เกทเวย์ วีพีเอ็น ฟังก์ชั่นของวีพีเอ็นก็เป็นส่วนหนึ่งของไฟร์วอลล์ด้วยโดยการติดตั้งที่ข้างหลังไฟร์วอลล์จะต้องการวีพีเอ็นทราฟฟิกในการผ่านไฟร์วอลล์ ในขณะที่ทำการเข้ารหัสป้องกันไฟร์วอลล์ จากการตรวจสอบทราฟฟิก

การจะใช้งานวีพีเอ็นฟังก์ชั่นบนไฟร์วอลล์นั้นต้องการทรัพยากรเพิ่มเติม ขึ้นอยู่กับจำนวนของกระแสทราฟฟิกผ่านวีพีเอ็น และชนิดของการเข้ารหัสที่ใช้สำหรับบางสภาพแวดล้อมทราฟฟิกที่ถูกเพิ่มเข้ามาที่เกี่ยวข้องด้วย วีพีเอ็นอาจจำเป็นต้องวางแผนการเพิ่มความจุและทรัพยากร การวางแผนนั้นต้องการการตัดสินชนิดของ วีพีเอ็น (เกทเวย์-ทู-เกทเวย์ และหรือ โฮสต์-ทู-เกทเวย์) ที่จะถูกรวมอยู่ในไฟร์วอลล์ มีไฟร์วอลล์จำนวนมากที่รวมฮาร์ดแวร์ที่เร่งสำหรับการเข้ารหัสเพื่อลดผลกระทบของ วีพีเอ็น ซอร์วิซ

2.1.7 การควบคุมการเข้าเน็ตเวิร์ค

ความต้องการทั่วไปอื่นสำหรับไฟร์วอลล์ ที่ขอบของเน็ตเวิร์ค คือการทำงานตรวจสอบไคล์เอนท์ สำหรับการเชื่อมต่อเข้ามาจากรีโมทผู้ใช้งาน และทำการอนุญาต หรือ ไม่อนุญาตการเข้าถึงขึ้นอยู่กับการตรวจสอบเหล่านี้การตรวจสอบนี้โดยทั่วไปจะเรียกว่าการควบคุมการเข้าเน็ตเวิร์ค (NAC) หรือ เน็ตเวิร์คแอคเซซโพรเทคชั่น (NAP) โดยจะอนุญาตการเข้าถึงขึ้นอยู่กับสิ่งที่ใช้ยืนยันตนของผู้ใช้งาน และผลลัพธ์ของการทำงาน “เฮลท์เช็ค (Health Check)” บนคอมพิวเตอร์ของผู้ใช้งาน โดยทั่วไปแล้วจะประกอบด้วยการตรวจสอบอย่างหนึ่ง หรือมากกว่า ของนโยบายบริษัทตามนี้

- การอัพเดทแอนตี้มัลแวร์ และ เพอร์โซนัลไฟร์วอลล์ซอร์ฟแวร์
- การตั้งค่าแอนตี้มัลแวร์ และ เพอร์โซนัลไฟร์วอลล์ซอร์ฟแวร์
- เวลาของการสแกนมัลแวร์ครั้งที่ผ่านมา
- ระดับของส่วนเสริมของ ระบบปฏิบัติการ และ แอพพลิเคชั่ ที่เลือก
- การตั้งค่าการรักษาความปลอดภัยของ ระบบปฏิบัติการ และ แอพพลิเคชั่น ที่เลือก

การตรวจสอบสุขภาพนี้ต้องการซอร์ฟแวร์บนระบบของผู้ใช้งาน ที่สามารถควบคุมโดยไฟร์วอลล์ ถ้าผู้ใช้งานมีการผ่านการยืนยันตน แต่เครื่องมือไม่ผ่านการตรวจสุขภาพ ทั้งผู้ใช้งาน และ อุปกรณ์ จะต้องถูกจำกัดการเข้าถึงสู่เน็ตเวิร์คภายในสำหรับการแก้ไขวัตถุประสงค์

2.1.8 Unified Threat Management (ยูทีเอ็ม(UTM))

มีไฟร์วอลล์หลายตัวที่รวมการทำงานหลายอย่างลงในระบบเพียงระบบเดียว ความคิดที่ว่ามันง่ายที่จะติดตั้ง และดูแลนโยบายบนระบบเพียงระบบเดียว ง่ายกว่าบนหลายระบบที่ถูกสร้างในที่เดียวกันบนเน็ตเวิร์ค ระบบยูนิฟายเทรดเมเนจเมนท์ (ยูทีเอ็ม) ทั่วไปมี ไฟร์วอลล์การตรวจจับมัลแวร์ และ การกำจัด , ตรวจสอบ และ ปิดกั้น ของเน็ตเวิร์คที่น่าสงสัย ดังนั้นเมื่อมันมีข้อดีและข้อเสียในการหลอมรวมหลากหลายฟังก์ชั่นที่ไม่เกี่ยวข้องกันโดยสมบูรณ์ลงในระบบเพียงระบบเดียว ตัวอย่างเช่น ใช้ยูทีเอ็มลดความซับซ้อน โดยการสร้างระบบตอบสนองตัวเดียว สำหรับหลายจุดประสงค์การรักษาความปลอดภัย แต่มันก็ยังมีความต้องการที่ยูทีเอ็ม จะมีคุณสมบัติที่ต้องการในการที่จะเข้าหาทุกๆ จุดประสงค์ จุดอ่อนอื่นๆในการทำงานคือระบบระบบเดียวรับมือกับงานหลายงานจำเป็นจะต้องมีทรัพยากรเพียงพอเช่นความเร็วซีพียู และ หน่วยความจำ สำหรับรองรับงานทุกงานที่เข้ามาบางองค์กรจะค้นหาความสมดุลเพื่อสนับสนุนยูทีเอ็มในขณะที่บางองค์กร จะใช้ไฟร์วอลล์หลายตัวในที่เดียวกัน สำหรับเน็ตเวิร์คของพวกเขา

2.1.9 Web Application Firewalls

เอชทีทีพีโปรโตคอลที่ใช้สำหรับเว็บเซิฟเวอร์นั้นสามารถถูกเจาะระบบโดยผู้โจมตีได้หลากหลายทาง เช่น วางซอร์ฟแวร์ร้ายบนคอมพิวเตอร์ของใครสักคนที่ทำการเข้าเว็บ หรือเปิดเผยข้อมูลส่วนตัวที่พวกเขาอาจจะไม่มีหลากหลายการเจาะระบบเหล่านี้สามารถถูกตรวจสอบได้โดยแอพพลิเคชั่นไฟร์วอลล์เฉพาะ ที่เรียกว่าเว็บแอพพลิเคชั่นไฟร์วอลล์ที่ถูกวางไว้ที่ข้างหน้าของ เว็บเซิฟเวอร์

เว็บแอพพลิเคชั่นไฟร์วอลล์ค่อนข้างจะเป็นเทคโนโลยีใหม่ เมื่อเทียบกับเทคโนโลยีไฟร์วอลล์อื่นๆและชนิดของการโจมตีที่ได้มีการทำการแบ่งเบา ยังคงมีการเปลี่ยนแปลงอยู่บ่อยๆ เพราะว่าเขาได้ทำการวางไว้ที่ข้างหน้าของเว็บเซิฟเวอร์เพื่อป้องกันการโจมตีตัวเซิฟเวอร์จึงมีการวิเคราะห์บ่อยครั้งซึ่งจะแตกต่างกับไฟร์วอลล์แบบเก่าอย่างมาก

2.1.10 Firewalls for Virtual Infratructures

มีการจำลองมากมายที่อนุญาตให้เครื่องคอมพิวเตอร์หนึ่งเครื่องมี ระบบปฏิบัติการมากกว่าหนึ่งโดยพร้อมกันที่เห็นแต่ละอันถ้ามันเป็นคอมพิวเตอร์จริง นี่จะเป็นสิ่งที่เป็นที่นิยมที่สุดเร็วๆนี้ เพราะว่ามันอนุญาตองค์กรให้สร้างประสิทธิภาพการใช้งานของ ฮาร์ดแวร์คอมพิวเตอร์ ลักษณะส่วนใหญ่ของระบบการจำลองนี้ประกอบด้วย เวอร์ช่วลไลซ์เน็ตเวิร์คกิ้ง ที่อนุญาตให้ระบบปฏิบัติการ

หลายอย่างทำการติดต่อกัน เหมือนกับว่าอยู่บนสแตทดาดอีเทอร์เน็ต แม้จะไม่มี เน็ตเวิร์คกิ้ง ฮาร์ดแวร์จริงๆ

การทำงานของเน็ตเวิร์คที่ผ่านระหว่างระบบปฏิบัติการจำลองโดยตรงในพื้นที่ที่ไม่สามารถตรวจสอบจาก ไฟร์วอลล์ ภายนอก อย่างไรก็ตาม บางระบบการจำลอง อนุญาตให้มี บิวด์อินไฟร์วอลล์ หรือ อนุญาตเทิร์ดปาร์ตี้ ซอร์ฟแวร์ ไฟร์วอลล์ เพิ่มเข้ามาในส่วนเสริม ใช้ ไฟร์วอลล์ ในการตรวจสอบเน็ตเวิร์คจำลองนั้นค่อนข้างจะเป็นส่วนใหม่ของเทคโนโลยีไฟร์วอลล์ และมันมีโอกาสที่จะเปลี่ยนแปลงอย่างสำคัญ สำหรับการเพิ่มขึ้นของการใช้งานระบบจำลอง

2.1.11 Next Generation Firewall

คือไฟร์วอลล์ที่มีความสามารถในการมองเห็นแอพพลิเคชั่นในระดับเลเยอร์7 (แอพพลิเคชั่นเลเยอร์) ของโอเอสไอเลเยอร์ และมีความสามารถอื่น ๆ อาจมีความสามารถของไอพีเอส ในการตรวจจับการโจมตีแบบต่าง ๆ ทั้งในแบบ ระบบการตรวจสอบโดยการใช้ซิกเนเจอร์ , การตรวจสอบพฤติกรรมที่ผิดปกติ (Behavior) เป็นต้น ซึ่งความสามารถพื้นฐานที่อุปกรณ์ เน็กซ์เจนเนอเรชั่นไฟร์วอลล์ (Next Generation Firewall) นั้นจะต้องทำได้สามารถสรุปได้

จะต้องสามารถทำการระบุและกรองแอพพลิเคชั่นได้ ข้อนี้ถือได้ว่าเป็นหัวใจหลักของเน็กซ์เจนเนอเรชั่นไฟร์วอลล์ โดยสามารถกรองทราฟฟิกโดยระบุเป็นแอพพลิเคชั่นแทนที่จะสามารถเลือกกรองในรูปแบบของพอร์ต เหมือนเทรดิชันแนลสเตทฟูลล์ไฟร์วอลล์ทั่วไป

จะต้องทำงานตามมาตรฐานของอุปกรณ์ไฟร์วอลล์มาตรฐานได้เช่นเป็นสเตทฟูลล์ โปรโตคอลอินสเปคชั่น สามารถทำเราท์ติ้ง ทำเอ็นเอที และ พอร์ตแอดเดรสทรานสเลชั่น (PAT) สามารถทำ วีพีเอ็นได้

เน็กซ์เจนเนอเรชั่นไฟร์วอลล์ นั้นเป็นการรวมระบบซีเคียวริตี้หลายๆ ประเภทเข้าด้วยกัน และสามารถตรวจจับและป้องกันการโจมตีหลากหลายประเภทได้ภายในอุปกรณ์ตัวเดียวกัน ซึ่งเรียกได้ว่าเป็นเทคโนโลยีด้าน ซีเคียวริตี้ แต่สิ่งที่ต้องตรวจสอบให้แน่ชัดหากต้องการเปิดฟีเจอร์ต่างๆ ของ เน็กซ์เจนเนอเรชั่นไฟร์วอลล์ สำหรับองค์กร นั่นก็คือทรูพุตของอุปกรณ์นั้นจะลดลงด้วย ซึ่งแต่ละองค์กรควรจะทำ POC (Prove of Concept) กับอุปกรณ์เพื่อให้เห็นถึงความสามารถและ ทรูพุตให้เพียงพอต่อการใช้งาน

2.2 Firewalls for Individual Host and Home Network

แม้ว่าไฟร์วอลล์ที่ขอบของเน็ตเวิร์คจะมีตัวชี้วัดของการป้องกันสำหรับโฮสต์ภายใน ในหลายๆ กรณี การเพิ่มเติมการป้องกันเน็ตเวิร์คนั้นจำเป็นต้องใช้ เน็ตเวิร์คไฟร์วอลล์ นั้นไม่สามารถที่จะจดจำทุกรูปแบบของการโจมตีได้ โดยจะอนุญาตบางการโจมตีให้เจาะและเข้าถึงโฮสต์ภายใน และการโจมตีที่ส่งต่อจากโฮสต์ภายในโฮสต์หนึ่งไปสู่โฮสต์อื่นๆโดยไม่ผ่านเน็ตเวิร์คไฟร์วอลล์เลยเพราะว่าข้อเท็จจริงเหล่านี้เน็ตเวิร์คดีไซน์เนอร์จึงมีการรวมฟังก์ชั่นไฟร์วอลล์ที่ตำแหน่งอื่นนอกจากขอบ เน็ตเวิร์ค ที่ให้ส่วนเสริมการรักษาความปลอดภัย ในส่วนนี้จะอธิบายถึง ไฟร์วอลล์ ที่ออกแบบมาพิเศษสำหรับแต่ละโฮสต์ และเน็ตเวิร์คบ้าน

2.2.1 Host-Based Firewalls and Personal Firewalls

โฮสต์-เบสไฟร์วอลล์สำหรับเซิฟเวอร์ และ เพอร์โซนั่ลไฟร์วอลล์สำหรับเดสก์ท็อป และ แลปท็อปเพอร์โซนั่ลคอมพิวเตอร์(พีซี)จะให้เสริมส่วนของการรักษาความปลอดภัยต่อการโจมตีทาง เน็ตเวิร์ค โดย ไฟร์วอลล์ เหล่านี้จะขึ้นอยู่กับ ซอร์ฟแวร์ที่อยู่บนโฮสต์ ที่มันได้ทำการป้องกัน โดยจะแบ่งการสอดส่องและควบคุมเน็ตเวิร์คทราฟฟิกที่เข้ามา และ ออกไปสำหรับโฮสต์หนึ่ง โดยมันจะมีการป้องกันที่ค่อนข้างละเอียดมากกว่า เน็ตเวิร์ค ไฟร์วอลล์ ที่จำเป็นต้องใช้สำหรับโฮสต์เฉพาะ

โฮสต์-เบสไฟร์วอลล์ นั้นสามารถถูกใช้งานเป็นส่วนหนึ่งของเซิฟเวอร์ระบบปฏิบัติการ เช่น ลินุกซ์ (Linux) , วินโดว์ส (Windows) , โซราริส (Solaris) , บีเอสดี (BSD) และ แมคโอเอสเอ็กซ์ (Mac OS X) เซิฟเวอร์ และยังสามารถถูกติดตั้งเพื่อเป็นส่วนเสริม การตั้งค่าโฮสต์-เบส ไฟร์วอลล์ เพื่ออนุญาตแค่ทราฟฟิกที่สำคัญต่อเซิฟเวอร์ที่มีการป้องกันการทำงานที่ไม่ปลอดภัยจากทุกโฮสต์ รวมถึงที่อยู่บนซับเน็ต (subnet) เดียวกัน หรือ บนซับเน็ตเดียวกันที่ไม่ได้ถูกแยกโดย เน็ตเวิร์คไฟร์วอลล์ การจำกัดทราฟฟิก ที่ออกไปข้างนอกจากเซิฟเวอร์ ยังเป็นประโยชน์ในการป้องกันมัลแวร์ที่มีการติดเชื้อไปที่โฮสต์ และมีการแพร่กระจายไปสู่โฮสต์อื่นๆ โฮสต์-เบสไฟร์วอลล์ มักจะทำงานเข้าระบบ และสามารถถูกตั้งค่าเพื่อทำงานขึ้นกับแอดเดรส และ แอพพลิเคชั่น การควบคุมการเข้าถึงโฮสต์-เบส ไฟร์วอลล์ โดยมากจะสามารถใช้เป็นอินทรูชั่นพรีเวนชั่นซิสเตม (Intrusion Prevention System) (ไอพีเอส) โดยหลังจากตรวจสอบการโจมตีที่อยู่ในการคืบหน้าและทำการป้องกันจากผู้โจมตี และป้องกันความเสียหายต่อโฮสต์เป้าหมาย

เพอร์โซนั่ลไฟร์วอลล์ เป็นซอร์ฟแวร์ที่ทำงานบนเดสก์ท็อป หรือแลปท็อปพีซี กับระบบปฏิบัติการที่มีผู้ใช้มาก เช่น ไมโครซอร์ฟวินโดว์วิสต้า (Microsoft Windows Vista) หรือ แมคอินทอชโอเอสเอ็กซ์ (Macintosh OS X) ตัวเพอร์โซนั่ลไฟร์วอลล์นั้นแตกต่างกับ โฮสต์-เบส ไฟร์วอลล์ แต่เพราะว่าคอมพิวเตอร์ที่ถูกป้องกันนั้น ต้องหมายถึงสำหรับผู้ใช้งานที่ขอบ (End User) จึงมี

อินเตอร์เฟซที่ค่อนข้างจะแตกต่าง (และมีการใช้งานที่ง่ายต่อผู้ใช้งานที่จะทำความเข้าใจ) เพอร์โซนัล ไฟร์วอลล์ จะมีเสริมส่วนการรักษาความปลอดภัยสำหรับพีซีทั้งฝั่งข้างใน และ ข้างนอกไฟร์วอลล์ขอบ (เช่น Mobile Laptop User) เพราะว่ามันสามารถจำกัดการติดต่อสื่อสารที่เข้ามา และ สามารถจำกัดการติดต่อสื่อสารที่ออกไปได้อย่างดี นี้ไม่เพียงอนุญาตเพอร์โซนัลไฟร์วอลล์ เพื่อป้องกันพีซี จากการโจมตีที่เข้ามา แต่ยังสามารถจำกัดการแพร่กระจายของมัลแวร์ จากพีซีที่มีการติดเชื้อและสามารถใช้อันออเทอร์ไรซ์ ซอร์ฟแวร์ เช่น เครื่องมือ เพียร์ทูเพียร์ไฟล์แชร์ริ่ง (Peer-to-Peer) โดยปกติแล้ว เพอร์โซนัล ไฟร์วอลล์ จะถูกมัดรวมมากับแอนตี้มัลแวร์โปรแกรม , อินทรูชั่นดีเทคชั่นซอร์ฟแวร์ และเครื่องมือซีเคียวริตี้อื่นๆ

2.2.2 Personal Firewall Appliance

นอกจากการใช้งานเพอร์โซนัลไฟร์วอลล์ บนพีซีบางผู้ใช้งานยังใช้เครื่องมือที่เล็กราคาถูกเรียกว่า ไฟร์วอลล์แอพไพลแอนซ์ หรือ ไฟร์วอลล์เราท์เตอร์ สำหรับป้องกันคอมพิวเตอร์บนโฮมเน็ตเวิร์ค ของพวกเขา เพอร์โซนัลไฟร์วอลล์แอพไพลแอนซ์ จะมีการทำงานฟังก์ชั่นที่คล้ายกับ เพอร์โซนัล ไฟร์วอลล์ รวมถึงบางคุณสมบัติขั้นสูงโดยจะถูกลงรายละเอียดในส่วนนี้ เช่น วีพีเอ็น แม้ว่าแต่ละคอมพิวเตอร์บนโฮมเน็ตเวิร์ค นั้นจะใช้งานเพอร์โซนัลไฟร์วอลล์ แต่ ไฟร์วอลล์แอพไพลแอนซ์ก็ยังมีประโยชน์ที่จะเพิ่มในส่วนของการรักษาความปลอดภัย บนความผิดปกติของคอมพิวเตอร์นั้นที่ เพอร์โซนัลไฟร์วอลล์ถูกปิด หรือถูกตั้งค่าผิดพลาด ไฟร์วอลล์แอพไพลแอนซ์ยังสามารถป้องกันคอมพิวเตอร์จากการติดต่อสื่อสารที่จากอันออเทอร์ไรซ์เน็ตเวิร์คจากคอมพิวเตอร์ภายนอก เพอร์โซนัลไฟร์วอลล์แอพไพลแอนซ์ เหมือนกับเป็นบริษัทไฟร์วอลล์ขนาดเล็กที่นำไปใช้จากองค์กร ดังนั้นความสามารถในการทำงานจัดการส่วนกลาง และ การบริหารนั้นสำคัญสำหรับ เพอร์โซนัลไฟร์วอลล์แอพไพลแอนซ์เหมือนกับที่มันเป็นสำหรับไฟร์วอลล์องค์กร

บางเพอร์โซนัลไฟร์วอลล์แอพไพลแอนซ์สามารถถูกตั้งค่าจากยูนิเวอร์ซัลปลั๊กแอนด์เพลย์ (UPnP) ที่อนุญาตแอพพลิเคชั่นบนพีซีหลังไฟร์วอลล์ เพื่อถามไฟร์วอลล์สำหรับการเปิดพอร์ต โดยอัตโนมัติ ดังนั้น แอพพลิเคชั่นสามารถมีการติดต่อสื่อสารแบบทู-เวย์กับ ระบบภายนอกโดย เพอร์โซนัลไฟร์วอลล์ ที่สนับสนุนการตั้งค่าใหม่ผ่าน UPnP มีการทำงานนี้ที่ถูกปิดโดยพื้นฐาน เพราะว่ามันคือส่วนรักษาความปลอดภัยสำคัญที่เสี่ยงที่จะอนุญาตอันทรัสแอพพลิเคชั่น ให้ผ่านไฟร์วอลล์ ซีเคียวริตี้โพลิซี

2.3 Limitations of Firewall Inspection

ไฟร์วอลล์สามารถทำงานอย่างมีประสิทธิภาพบนทราฟฟิกที่สามารถตรวจสอบได้เท่านั้น โดยไม่คำนึงถึงไฟร์วอลล์เทคโนโลยีที่ถูกเลือก ไฟร์วอลล์ที่ไม่สามารถเข้าใจทราฟฟิกโฟล์วที่ผ่านนั้น ก็ไม่

สามารถรับมือกับทราฟฟิกนั้นเช่นกัน ตัวอย่างเช่นอนุญาตให้ทราฟฟิกที่ควรจะถูกปิดกั้นผ่านเข้ามา หลายเน็ตเวิร์คโปรโตคอลที่ใช้เข้ารหัสสำหรับซ่อนเนื้อหาของทราฟฟิก ในหัวข้อ 2.1.6 ที่คลุมเรื่อง ไอพีเซ็ค และ ทีแอลเอส โปรโตคอลการเข้ารหัสที่เหลือ รวมถึง ซีเคียวเชล (SSH) และ ซีเคียว เรียลทามทรานสพอร์ตโปรโตคอล (SRTP) ตัวไฟร์วอลล์ยังไม่สามารถอ่านแอพพลิเคชั่นดาต้า ที่ถูกเข้ารหัสไว้ เช่น อีเมล ที่ถูกเข้ารหัสโดยใช้ S/MIME หรือ โอเพ่นพีจีพี (OpenPGP) โปรโตคอล หรือไฟล์ที่ถูกเข้ารหัสโดยปกติ การจำกัดอื่นๆถูกเผชิญโดยบางไฟร์วอลล์ที่เข้าใจทราฟฟิกนั้นเป็นทันเนล ทั้งที่มันไม่ได้ถูกเข้ารหัส ตัวอย่างเช่น ไอพีวี6ทราฟฟิกสามารถเป็นทันเนลในไอพีวี4 ในหลายทางที่แตกต่าง โดยเนื้อหายังคงไม่ถูกเข้ารหัส แต่ถ้าไฟร์วอลล์ ไม่เข้าใจระบบทันเนลลิ่ง ที่ถูกใช้โดยเฉพาะ ทราฟฟิก ก็ไม่สามารถถูกตีความ

ในกรณีทั้งหมดนี้ ไฟร์วอลล์รูลล์ส จะกำหนดว่าจะทำอะไรกับ ทราฟฟิก หรือไม่ (หรือในกรณีของ ทราฟฟิก ที่ถูกเข้ารหัสนั้น ไม่สามารถทำได้) องค์กรต้องมีนโยบายเกี่ยวกับว่าจะรับมือกับทราฟฟิก ในกรณีต่างๆยังไง อย่างใดอย่างหนึ่งเช่น อนุญาตหรือปิดกั้นทราฟฟิก ที่ถูกเข้ารหัสที่ไม่มีการยืนยันตนเพื่อเข้ารหัส

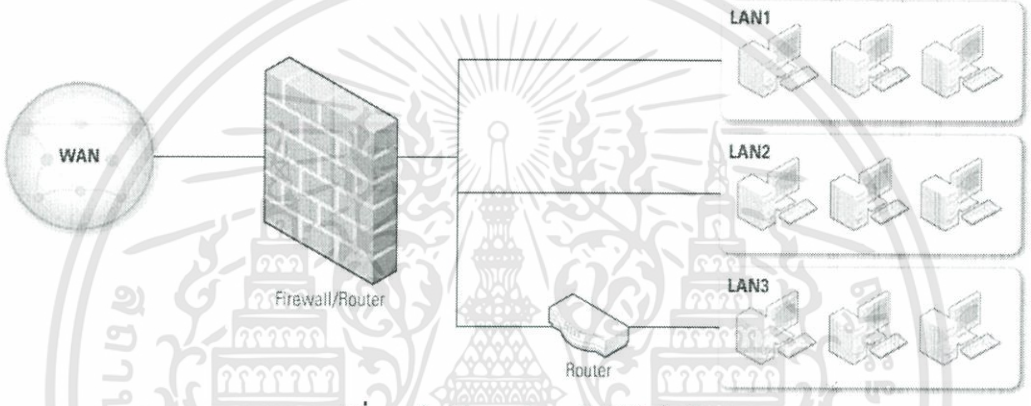
2.4 Firewall and Network Architectures

ไฟร์วอลล์ถูกใช้งานสำหรับแต่ละเน็ตเวิร์ค ด้วยความต้องการทางด้านซีเคียวริตี้ ที่แตกต่างกัน เช่น อินเทอร์เน็ต และ เน็ตเวิร์คภายในที่เซิฟเวอร์ที่บ้าน กับ ดาต้าที่อ่อนไหว องค์กรต้องมีการใช้งานไฟร์วอลล์ ไม่ว่าจะเป็นในเน็ตเวิร์คภายในของพวกเขา และ ระบบอินเตอร์เฟซ กับเน็ตเวิร์คและระบบภายนอก และ ที่ไหนที่ต้องการการรักษาความปลอดภัยระหว่างเน็ตเวิร์คภายในของพวกเขาเอง ในส่วนนี้จะตั้งใจเพื่อช่วยองค์กรในการตัดสินใจว่าที่ใดที่ควรจะวาง ไฟร์วอลล์ ไว้ และที่ไหนที่เน็ตเวิร์คและระบบอื่นนั้นจะต้องถูกตั้งในความสัมพันธ์กับ ไฟร์วอลล์

ตั้งแต่หนึ่งอย่างของฟังก์ชั่นสำคัญของไฟร์วอลล์ สำหรับป้องกัน ทราฟฟิก ที่ไม่ต้องการให้เข้าสู่เน็ตเวิร์ค (และในบางกรณีคือออกจากเน็ตเวิร์ค) ไฟร์วอลล์ ต้องมีการวางที่มุมของขอบเขตเน็ตเวิร์คนี่โดยทั่วไปแล้วหมายความว่า ไฟร์วอลล์ เป็นตำแหน่งหรือเป็น โหนด ที่เน็ตเวิร์คสามารถแยกได้เป็นหลายทาง หรือ ในสายตลอดทางหนึ่งทาง ในเส้นทางของเน็ตเวิร์ค ไฟร์วอลล์ มักจะอยู่บนเน็ตเวิร์คที่สถานที่ตั้งโดยทันทีก่อนที่ทราฟฟิกจะเข้าไปในเราท์เตอร์ (อินเกรส พ๊อยท์) และบางครั้งก็อยู่ร่วมกับเราท์เตอร์ ซึ่งหายากที่จะวางไฟร์วอลล์สำหรับ โหนดหลายทางหลัง เราท์เตอร์ เพราะว่าอุปกรณ์ ไฟร์วอลล์ นั้นต้องการที่จะดูแต่ละเส้นทางทางออก ที่ออกมาในแต่ละสถานการณ์ ส่วนใหญ่ของอุปกรณ์ฮาร์ดแวร์ไฟร์วอลล์ จะรวมความสามารถของเราท์เตอร์ด้วย และในการเปลี่ยนเน็ตเวิร์ค ไฟร์วอลล์นั้นเป็นส่วนของ สวิทช์ ด้วยตนเอง สำหรับมีการป้องกันสวิทช์หลายส่วนเท่าที่เป็นไปได้

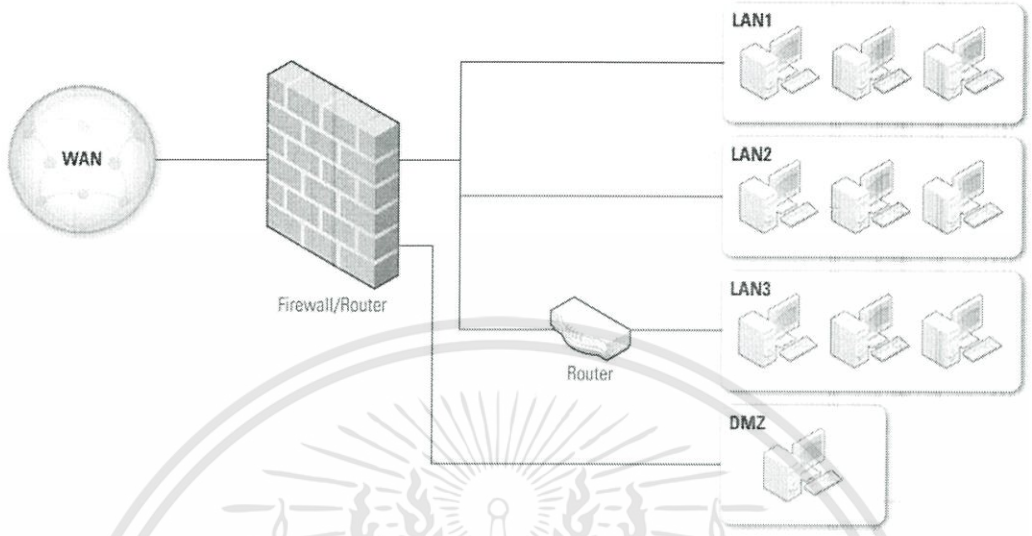
2.4.1 Network Layout with Firewalls

ในรูป2.4 แสดงตัวอย่างของ เน็ตเวิร์คเลย์เอาท์ ที่มีเครื่องมือ ฮาร์ดแวร์ไฟร์วอลล์ ที่เป็น เราท์เตอร์ ในฝั่งที่ไม่ได้ถูกป้องกันของการเชื่อมต่อไฟร์วอลล์ในทางเดียวเขียนว่า WAN และฝั่งที่ถูกป้องกันการเชื่อมต่อไปยัง 3 ทาง เขียนว่า LAN1 LAN2 LAN3 ตัว ไฟร์วอลล์ ที่ทำหน้าที่เป็นเราท์เตอร์สำหรับทราฟฟิกระหว่าง WAN กับ LAN ในรูปหนึ่งทางของ LAN ก็มี เราท์เตอร์ เหมือนกัน บางองค์กรจะใช้ มัลติเปิล เลเยอร์ สำหรับ เราท์เตอร์ สำหรับนโยบายในการหาเส้นทางภายในเน็ตเวิร์ค



รูปที่ 2.4 ไฟล์วอลล์แบบไม่มีดีเอ็มซี

มีหลายเครื่องมือฮาร์ดแวร์ไฟร์วอลล์ ที่มีคุณสมบัติที่เรียกว่า ดีเอมซี เป็นคำที่มาจากเขตปลอดทหารที่ถูกตั้งขึ้นมาระหว่างประเทศที่มีสงครามกัน ในขณะที่ไม่มีคำนิยามที่บอกถึง ไฟร์วอลล์ดีเอมซี หน้าอินเตอร์เฟซบนเราท์ติ้งไฟร์วอลล์ นั้นจะคล้ายกับ อินเตอร์เฟซ ที่เห็นบน ไฟร์วอลล์ ฝั่งที่ถูกป้องกัน ความแตกต่างหลักๆคือ ทราฟฟิกจะเคลื่อนที่ระหว่างดีเอมซี และ อินเตอร์เฟซ บนฝั่งที่ถูกป้องกันของไฟร์วอลล์ จะยังผ่านไฟร์วอลล์ และสามารถได้รับการป้องกันจากนโยบาย ไฟร์วอลล์ ตัว ดีเอมซี นี้บางครั้งประโยชน์ต่อองค์กรคือมี โฮสต์ที่ต้องการจะมีจุดหมายของทราฟฟิกสำหรับให้ โฮสต์ผ่านบางนโยบาย ไฟร์วอลล์ แต่ ทราฟฟิกมาจาก โฮสต์ ไปยังระบบอื่นบนเน็ตเวิร์คองค์กรที่ต้องการผ่านไฟร์วอลล์ มันเป็นเรื่องปกติที่จะใส่ เซิฟเวอร์ ที่หันหน้าเข้าสู่สาธารณะ อย่างเช่นเว็บ และ อีเมล เซิฟเวอร์ บนดีเอมซี ตัวอย่างจะแสดงในภาพ 2-2 แผนผังเน็ตเวิร์คอย่างง่ายของ ไฟร์วอลล์ ที่มี ดีเอมซี โดย ทราฟฟิก จาก อินเทอร์เน็ตไปยัง ไฟร์วอลล์ และมีเส้นทางไปยังระบบบน ไฟร์วอลล์ ฝั่งที่มีการป้องกัน หรือ ไปยังระบบบน ดีเอมซี กับ ทราฟฟิก ระหว่างระบบบน ดีเอมซี และ ระบบบนเน็ตเวิร์คที่ถูกป้องกันเดินทางผ่านไฟร์วอลล์และสามารถมีการรับนโยบาย ไฟร์วอลล์



รูปที่ 2.5 ไฟล์วอลล์แบบมีดีเอ็มซี

สถาปัตยกรรมเน็ตเวิร์คส่วนมากจะเป็นแบบลำดับชั้น หมายถึงว่าเส้นทางเดียวจากเน็ตเวิร์คภายนอกสามารถกระจายได้เป็นหลายเส้นทางในเน็ตเวิร์คภายใน และมันทำให้มีประสิทธิภาพมากสำหรับวาง ไฟร์วอลล์ ไว้ที่จุดที่มีการกระจายทางออก นี่เป็นประโยชน์ของการวางตำแหน่ง ไฟร์วอลล์ที่จะทำให้ไม่มีคำถามที่ว่าที่ใดคือข้างในและที่ใดคือข้างนอกเน็ตเวิร์ค

2.4.2 Firewalls Acting as Network Address Translators

โฮสต์จำนวนมากสามารถทำงานเป็นเอ็นเอที หรือบางครั้งจะถูกเรียกว่า พอร์ตแอดเดรสทรานสเลชั่น (PAT) หรือ เน็ตเวิร์คแอดเดรสแอนด์พอร์ตทรานสเลชั่น (NAPT) แม้จะมีความเข้าใจผิดๆที่ว่า เอ็นเอที ไม่ใช่ส่วนของการรักษาความปลอดภัยบน ไฟร์วอลล์ ประโยชน์ของการรักษาความปลอดภัยของ เอ็นเอที คือ จะขัดขวาง โฮสต์ ภายนอก ไฟร์วอลล์ ที่จะเริ่มทำการติดต่อกับ โฮสต์ ที่อยู่ข้างหลัง เอ็นเอที สามารถทำได้ง่ายด้วยสเตทฟูลล์ไฟร์วอลล์ กับการรบกวนโปรโตคอล ที่ไม่สามารถทำงานได้ดีข้างหลัง เอ็นเอที อย่างไรก็ตามการเปิด เอ็นเอที ของ ไฟร์วอลล์ นั้นมักจะง่ายกว่าคุณบัติที่ตั้งค่านโยบายไฟร์วอลล์ ให้มีการป้องกันที่เหมือนกัน ดังนั้นหลายคนจึงคิดว่าเอ็นเอที นั้นเป็นการรักษาความปลอดภัยเป็นหลัก

โดยปกติแล้ว เอ็นเอที ที่ใช้เป็น เราท์เตอร์ นั้นจะมีเน็ตเวิร์คกับ ไพรเวท แอดเดรส อยู่ข้างในและมีเพียงพับลิคแอดเดรสเดียวอยู่ที่ภายนอก การทำงานของเอ็นเอที จะทำงานเป็นแมนี่-ทู-วัน (many-to-one) จะมีการทำแผนงานที่แตกต่างระหว่างกัน แต่ว่าเกือบทั้งหมดจะเกี่ยวข้องกันตามนี้

- โฮสต์ ที่อยู่ฝั่งข้างในเน็ตเวิร์ค สร้างการเชื่อมต่อสู่เน็ตเวิร์คข้างนอกจะทำให้ เอ็นเอที ที่ทำพอร์ต ต้นทางของการเชื่อมต่อเปลี่ยนเป็นพอร์ตต้นทางที่แตกต่างไปที่ถูกควบคุมจากเอ็นเอที โดยเอ็นเอที จะใช้เลขพอร์ต ต้นทางนี้ในการแปลงการเชื่อมต่อจากภายนอกเมื่อกลับมาสู่โฮสต์ ที่อยู่ภายใน

- โฮสต์ ที่อยู่ข้างนอกเน็ตเวิร์คไม่สามารถสร้างการเชื่อมต่อกับโฮสต์ ที่อยู่ข้างในเน็ตเวิร์ค ในบาง ไฟร์วอลล์ เอ็นเอที นั้นสามารถตั้งค่าให้สามารถแปลง พอร์ต ปลายทางเฉพาะบนเอ็นเอทีต่อโฮสต์ เฉพาะที่อยู่ภายในเอ็นเอที ตัวอย่างเช่นเอชทีทีพี รีเควส ทั้งหมดที่ไปยังเอ็นเอที สามารถมุ่งไปยังโฮสต์ หนึ่งที่อยู่ในฝั่งที่ถูกป้องกันของ ไฟร์วอลล์ โดยลักษณะนี้บางครั้งจะถูกเรียกว่า พินโฮลลิ่ง (Pinholing)

2.4.3 Architecture with Multiple of Firewalls

ทั้งนี้ยังไม่มีข้อจำกัดว่าไฟร์วอลล์ สามารถถูกวางที่ไหนในเน็ตเวิร์ค ในขณะที่ไฟร์วอลล์ ควรจะอยู่ที่ขอบของขอบเขตเน็ตเวิร์ค และมีการสร้าง ข้างใน และ ข้างนอก ของแต่ละฝั่งของ ไฟร์วอลล์ ผู้ดูแลเน็ตเวิร์คจะมีความต้องการที่จะเพิ่มขอบเขตภายในเน็ตเวิร์ค และสร้าง ไฟร์วอลล์ เพิ่มเพื่อทำการสร้างขอบเขตดังกล่าว การใช้งานของ มัลติเปิล เลเยอร์ ขอบ ไฟร์วอลล์ นั้นค่อนข้างจะเป็นการทำเพื่อจะป้องกันลงสู่ที่ลึก ดีเฟนซ์-อิน-เดพท์ (Defense-in-Depth) ตัวอย่างของที่อธิบายเช่นที่อธิบายไว้ในหัวข้อ 2.2.1 ในที่ที่ โฮสต์-เบส ไฟร์วอลล์ สร้างขอบเขตเพียงก่อนที่ โฮสต์ จะถูกติดตั้ง และเพิ่มการตั้งค่านโยบาย ไฟร์วอลล์ อื่นๆไปยังสถาปัตยกรรมของเน็ตเวิร์ค โดยการใช้ มัลติเปิล เลเยอร์ ของไฟร์วอลล์ นั้นก็ค่อนข้างจะเป็นเทคนิคที่ธรรมดาอีกอย่างหนึ่ง

ในสถานการณ์ทั่วไปที่ต้องการใช้งาน มัลติเปิล เลเยอร์ ชอง เน็ตเวิร์ค ไฟร์วอลล์ คือการมีผู้ใช้ภายในที่มีความเชื่อถือแตกต่างระดับกัน ตัวอย่างเช่น องค์กรต้องการป้องกันฐานข้อมูลของบัญชีจากการถูกเข้าระบบโดยผู้ใช้ที่ไม่ใช่ส่วนหนึ่งของแผนกบัญชี นี่จะทำได้โดยการวาง ไฟร์วอลล์ อันหนึ่งไว้ที่ขอบ ของเน็ตเวิร์ค (สำหรับป้องกันการเข้าถึงทั่วไปสู่เน็ตเวิร์คจาก อินเทอร์เน็ต) และอีกสวนหนึ่งที่ขอบ ของเน็ตเวิร์คภายในที่เป็นขอบเขตของแผนกบัญชี ไฟร์วอลล์ ข้างในจะมีหน้าที่ปิดกั้นการเข้าถึงฐานข้อมูลจากใครบางคนที่อยู่ภายนอกเน็ตเวิร์คของบัญชีในขณะที่อนุญาตจำกัดการเข้าถึงสู่ทรัพยากรอื่นบนเน็ตเวิร์คบัญชี การใช้งานทั่วไปอื่นใช้สำหรับ ไฟร์วอลล์ ภายในเน็ตเวิร์คกับ ไฟร์วอลล์ที่ ขอบ ของตัวเองเกี่ยวข้องกับผู้เยี่ยมชมที่ต้องการเข้าสู่ อินเทอร์เน็ต หลายองค์กรสร้าง ไวร์เลส แอคเซซ พ๊อยท์ ขึ้นมากับเน็ตเวิร์คของเขาสำหรับผู้เยี่ยมชมใช้งาน ไฟร์วอลล์ ระหว่าง แอคเซซ พ๊อยท์ และเน็ตเวิร์คภายในทั้งหมด สามารถป้องกันไม่ให้ผู้เยี่ยมชมเข้าถึง โลคอล เน็ตเวิร์ค โดยมีสิทธิ์เหมือนกันกับพนักงาน

2.5 Firewalls Policy

นโยบายไฟร์วอลล์จะเป็นตัวสั่งการว่าไฟร์วอลล์ จะทำการรับมือเน็ตเวิร์คทราฟฟิกอย่างไร สำหรับเฉพาะ ไอพีแอดเดรส และ แอดเดรส เรนจ์ , โปรโตคอล , แอพพลิเคชั่น ,และ คอนเทนท์ ไทป์ ขึ้นอยู่กับนโยบายการรักษาความปลอดภัยข้อมูลขององค์กร ก่อนที่นโยบาย ไฟร์วอลล์ จะถูกสร้าง บางรูปแบบของการวิเคราะห์ความเสี่ยงต้องมีการทำการสร้างรายการของชนิดของ ทราฟฟิก ที่ต้องการจากองค์กรและแบ่งหมวดหมู่ว่าจะทำการรักษาความปลอดภัยอย่างไร รวมถึงว่าชนิดของทราฟฟิก ไหนสามารถข้าม ไฟร์วอลล์ ภายใต้สถานการณ์นั้น การวิเคราะห์ความเสี่ยงต้องมีการวิเคราะห์ตามพื้นฐานบนการประเมินผลของภัยคุกคาม ช่องโหว่ของระบบ และทำการอุดช่องโหว่ของระบบ และมีการทำงานถ้าระบบหรือข้อมูลตกอยู่ในอันตราย นโยบายไฟร์วอลล์ควรจะมีเอกสารในแผนการรักษาความปลอดภัยของระบบ และ มีการดูแลรักษาและอัพเดทอย่างบ่อยครั้งเหมือนกันที่มีรูปแบบของการโจมตีและหรือช่องโหว่ใหม่เพิ่มขึ้นมา มาว่าองค์กรต้องการเกี่ยวกับการเปลี่ยนแปลงเน็ตเวิร์คแอพพลิเคชั่นนโยบายยังต้องรวมถึงการแนะนำว่าจะเปลี่ยนแปลง แอดเดรสไปสู่รูลล์เซ็ตอย่างไร

2.5.1 Policies Bases on IP address and Protocol

นโยบายไฟร์วอลล์ ควรจะอนุญาตเพียงแค่ไอพีโปรโตคอลที่จำเป็นเท่านั้นที่จะผ่านได้ ตัวอย่างเช่น ไอพีโปรโตคอลที่ใช้กันทั่วไปกับเลขของไอพีโปรโตคอล นั้น คือ ไอซีเอ็มพี (1) ,ทีซีพี (6) และ ยูดีพี (17) และ ไอพี โปรโตคอล อื่นๆ อย่างเช่น ไอพีเซ็ค ที่มีส่วนประกอบของ เอ็นแคปซูเลติ้ง ซีเคียวริตี้ เพย์โหลด (อีเอสพี) (50) และ ออเทนทิเคชั่น เฮดเดอร์ (เอเอช) (51) และ เราท์ติ้ง โปรโตคอล อาจจำเป็นต้องผ่าน ไฟร์วอลล์ ตัว โปรโตคอล สำคัญเหล่านี้ต้องมีการจำกัดเมื่อไรก็ตามที่เป็นไปได้ต่อโฮสต์ เฉพาะ และ เน็ตเวิร์คภายในองค์กรด้วยความต้องการที่จะใช้มัน ด้วยการอนุญาตเพียงโปรโตคอลสำคัญ และ ไอพีโปรโตคอลที่ไม่สำคัญทั้งหมดนั้นถูกปฏิเสธโดยพื้นฐาน

2.5.1.1 IP address and Other IP Characteristics

นโยบายไฟร์วอลล์ควรจะอนุญาตเพียงไอพีต้นทาง และ ปลายทางที่เหมาะสม ที่จะใช้งานโดยเฉพาะแนะนำสำหรับ ไอพีแอดเดรส ที่มีลักษณะดังนี้

- ทราฟฟิกที่เป็นอินแวลิซอร์ส และ เดสทิเนชั่นแอดเดรส จะต้องถูกปิดกั้นเสมอโดยไม่คำนึงถึงตำแหน่งของ ไฟร์วอลล์ ตัวอย่างเช่น อินแวลิด ไอพีวี4 แอดเดรส คือ 127.0.0.0 ถึง 127.255.255.255 (อย่างที่รู้คือเป็นโลคอลโฮสต์แอดเดรส และ 0.0.0.0 ตีความโดยบาง

ระบบปฏิบัติการ เป็น โลคอลโฮสต์ หรือ บอร์ดแคส แอดเดรส) ไอพี เหล่านี้จะไม่มีการใช้งานบนเน็ตเวิร์ค รวมถึง ทราฟฟิก ที่ใช้ ลิงค์-โลคอล แอดเดรส (169.254.0.0 ถึง 169.254.255.255) จะถูกปิดกั้นด้วยเช่นกัน

- ทราฟฟิกที่มี อินแวลิด ซอร์สแอดเดรส สำหรับเข้าสู่ ทราฟฟิก หรือ เดสทิเนชั่นแอดเดรส สำหรับออกจาก ทราฟฟิก (อินแวลิด เอ็กซ์เทอนอล แอดเดรส) ควรจะถูกปิดกั้นที่ระบบเน็ตเวิร์ค ทราฟฟิก นี้มักจะเป็น มัลแวร์, สปูฟฟิ่ง, เดเนียลออฟ เซอร์วิซ แอทแทค หรือ ส่วนที่มีการตั้งค่าผิดพลาดชนิดปกติของ อินแวลิด เอ็กซ์เทอนอล แอดเดรส คือ ไอพีวี4 แอดเดรส ที่อยู่ในช่วง อาร์เอฟซี 1918. แอดเดรสออลโลเคชั่นฟอร์ไพรเวทอินเทอร์เน็ต, ที่สามารถรองรับ ไพรเวทเน็ตเวิร์ค ช่วงนี้คือ 10.0.0.0 ถึง 10.255.255.255 , 172.16.0.0 ถึง 172.31.255.255 และ 192.168.0.0 ถึง 192.168.255.255

- ทราฟฟิกที่มีไพรเวทเฟสติเนชั่นแอดเดรส สำหรับเข้าสู่ทราฟฟิก หรือ ซอร์สแอดเดรส สำหรับออกจาก ทราฟฟิก (อินเทอร์นอล แอดเดรส) ต้องถูกปิดกั้นที่ระบบเน็ตเวิร์ค เครื่องมือของระบบสามารถทำงานแปลงแอดเดรสเพื่ออนุญาตโฮสต์ภายในกับ ไพรเวทแอดเดรส เพื่อติดต่อสื่อสารผ่านขอบ แต่ไพรเวทแอดเดรสควรจะไม่ส่งผ่านถึงขอบของเน็ตเวิร์ค

- ทราฟฟิกขาออกที่มีอินแวลิดซอร์สแอดเดรส ต้องถูกปิดกั้น (นี่มักจะถูกเรียกว่า อีเกรสฟิลเตอร์ริ่ง) ระบบที่มีการตกอยู่ในอันตรายจากผู้โจมตีสามารถถูกใช้โจมตีระบบอื่นใน อินเทอร์เน็ต การใช้งานอินแวลิดซอร์สแอดเดรส จะทำให้การโจมตีประเภทนี้ยากที่จะหยุดได้ การปิดกั้นชนิดของทราฟฟิก นี้ในองค์กร ไฟร์วอลล์ จะช่วยลดประสิทธิภาพของการโจมตีนี้

- ทราฟฟิกขาเข้าที่มีเดสทิเนชั่นแอดเดรสของ ไฟร์วอลล์เองจะถูกปิดกั้นเว้นแต่ว่า ไฟร์วอลล์นั้นเสนอบริการเพื่อ ทราฟฟิก ขาเข้าที่ต้องการการเชื่อมต่อโดยตรง ตัวอย่างเช่น แอพพลิเคชั่น พร็อกซี่

องค์กรควรจะปิดกั้นชนิดของ ทราฟฟิก ดังนี้ที่ขอบเน็ตเวิร์ค

- ทราฟฟิกที่บรรจุข้อมูลการเราท์ติ้งของไอพีซอร์ส ที่จะอนุญาตระบบเพื่อระบุเส้นทางที่แพ็คเก็ตจะถูกใช้ในขณะที่เดินทางจากต้นทางไปจนถึงปลายทาง นี่สามารถเกิดการอนุญาตผู้โจมตีในการสร้างแพ็คเก็ตที่ผ่าน เน็ตเวิร์คซีเคียวริตี้คอนโทรล โดยการ เราท์ติ้งไอพีซอร์ส นั้นหายากที่จะใช้งานบนเน็ตเวิร์คสมัยใหม่ และ แอพพลิเคชั่น ที่ใช้งานได้ก็น้อยบน อินเทอร์เน็ต

- ทราฟฟิกจากภายนอกเน็ตเวิร์คที่บรรจุ บอร์ดแคส แอดเดรส ที่มีการเชื่อมต่อโดยตรงสู่เน็ตเวิร์คภายใน ระบบใดที่ตอบสนองต่อการ บอร์ดแคส โดยตรงจะมีการส่งการตอบสนองนั้นไปสู่ระบบโดยเฉพาะจากต้นทาง มากกว่าที่จะไปยังระบบต้นทางด้วยตัวเองแพ็คเก็ตนี้สามารถถูกใช้ในการสร้าง “สตอร์ม” ขนาดใหญ่ของเน็ตเวิร์คทราฟฟิก สำหรับ เดเนียลออฟเซอร์วิซแอทแทค ,บอร์ดแคส แอดเดรสปกติ ตลอดจนแอดเดรสที่ใช้เป็น มัลติแคสไอพี อาจจะมีหรือไม่มีความเหมาะสมสำหรับปิด

กั้นที่ไฟร์วอลล์ขององค์กร มัลติแคส และ บอร์ดแคส เน็ตเวิร์คจะไม่ค่อยใช้ในสภาพแวดล้อม เน็ตเวิร์คปกติ แต่เมื่อมันใช้ทั้งข้างในและข้างนอกขององค์กร มันจะได้รับการอนุญาตให้ผ่านไฟร์วอลล์

2.5.1.2 IPV6

ไอพีวี6คือเวอร์ชันใหม่ของไอพีที่ถูกใช้งานกันอย่างเพิ่มมากขึ้น ถึงแม้ว่ารูปแบบภายในของไอพีวี6และขนาดของแอดเดรสแตกต่างจากพวกไอพีวี4 หลายๆลักษณะอื่นๆยังคงเหมือนเดิม และพวกนี้เองก็เชื่อมต่อกับไฟวอลล์

สำหรับลักษณะที่เหมือนกันระหว่างไอพีวี4และไอพีวี6 ไฟวอลล์ควรจะทำงานเหมือนกัน ยกตัวอย่างเช่น การปิดกั้นทราฟฟิคขาเข้าและขาออกทั้งหมดที่ไม่ได้อนุญาตโดยไฟวอลล์โพลีซีควรจะทำให้เสร็จโดยปราศจากทราฟฟิคมีไอพีวี4หรือไอพีวี6หรือไม่

2.5.1.3 TCP and UDP

แอพพลิเคชั่นโปรโตคอลสามารถใช้ทีซีพีหรือยูดีพีหรือทั้งสองขึ้นอยู่กับการออกแบบของโปรโตคอล โดยทั่วไปแอพพลิเคชั่นเซิฟเวอร์เปิดพอร์ททีซีพีหรือยูดีพีพอร์ทเดียวบางเซิฟเวอร์ก็เฉพาะพอร์ทหลายๆพอร์ท บางแอพพลิเคชั่นใช้พอร์ทเดียว บางแอพพลิเคชั่นก็ใช้หลายพอร์ท ยกตัวอย่างเช่น ถึงแม้ว่าเอสเอ็มทีพีใช้ทีซีพีพอร์ท 25 สำหรับส่งเมลล์ แต่มันใช้ทีซีพีพอร์ท 587 สำหรับเมลล์ซับมิชชั่น เอฟทีพีก็คล้ายๆกันใช้อย่างน้อยสองพอร์ท อันแรกไม่สามารถเดาได้ และในขณะที่เว็บเซิฟเวอร์ส่วนใหญ่ใช้เพียงแค่ทีซีพีพอร์ท 80 มันก็มีอีกพอร์ทเพิ่มขึ้นมาคือ พอร์ท 8080บางแอพพลิเคชั่นใช้ทั้งพอร์ททีซีพีและยูดีพี ยกตัวอย่างเช่น ดีเอนเอสลุ๊คอัพสามารถเกิดขึ้นบนยูดีพีพอร์ท 53 และทีซีพีพอร์ท 53 แอพพลิเคชั่นของไคล์เอนต์โดยทั่วไปใช้หลายพอร์ท

2.5.1.4 ICMP

ผู้บุกรุกสามารถใช้ไอซีเอ็มพีและโค๊ดได้หลายชนิดเพื่อที่จะสอดแนมหรือบังคับการเคลื่อนไหวของทราฟฟิค อย่างไรก็ตามไอซีเอ็มพีจำเป็นสำหรับสิ่งที่มีประโยชน์หลายสิ่ง เช่นดูการทำงานผ่านอินเทอเน็ท บางนโยบายไฟวอลล์ระงับไอซีเอมพีทราฟฟิคทั้งหมดแต่เป็นหนทางสู่ปัญหาการวินิฉัยและการทำงานอยู่บ่อยๆ บางนโยบายทั่วๆไปจะอนุญาตไอซีเอมพีทราฟฟิคขาออกทั้งหมดแต่จำกัดไอซีเอมพีขาเข้าทั้งหมดที่ชนิดและโค๊ดที่จำเป็นสำหรับการค้นพบพีเอ็มทียู(ไอซีเอ็มพี โค๊ด3) และจำกัดความสามารถการมาถึงปลายทาง

2.5.2 Policies Based on Applications

ไฟวอลล์ส่วนใหญ่ก่อนหน้านี้ทำงานเกี่ยวข้องกับการระงับทราฟฟิคที่ไม่ต้องการและน่าสงสัยที่ขอบเขตเน็ทเวิร์คแอลลพิเคชั่นไฟวอลล์ขาเข้าหรือแอพพลิเคชั่นพร็อกซี่จะใช้วิธีที่ต่างกัน พวกมันจะปล่อยทราฟฟิคที่ส่งไปยังเซิฟเวอร์โดยเฉพาะไปในเน็ทเวิคแต่จับการจราจรในเซิฟเวอร์ที่ทำงานกับทราฟฟิคเหมือนกับพอร์ทเบดไฟวอลล์ วิธีแอพพลิเคชั่นเบดตัดให้เพิ่มเลเยอร์ของความปลอดภัยสำหรับทราฟฟิคที่เข้ามาโดยตรวจสอบบางทราฟิคก่อนที่มันจะไปถึงเซิฟเวอร์ที่ต้องการ ทฤษฎีคือแอลลพิเคชั่นไฟวอลล์ขาเข้าหรือพร็อกซี่ที่เพิ่มแอพพลิเคชั่นเลเยอร์เพิ่มขึ้นมาสามารถป้องกันเซิฟเวอร์ได้ดีกว่าเซิฟเวอร์จะสามารถปกป้องตัวมันเอง และสามารถเอาทราฟฟิคที่เป็นอันตรายออหไปได้ก่อนที่มันจะมาถึงเซิฟเวอร์เพื่อที่จะช่วยลดเซิฟเวอร์โหลด ในบางกรณีแอพพลิเคชั่นหรือพร็อกซี่สามารถเอาทราฟฟิคที่เซิฟเวอร์อาจจะไม่สามารถเอาออกโดยตัวของมันเองออกได้เพราะมันมีความสามารถการกรองที่ดีกว่า แอพพลิเคชั่นไฟวอลล์หรือพร็อกซี่ป้องกันเซิฟเวอร์ที่มีการเชื่อมต่อโดยตรงจากเน็ทเวิคภายนอกด้วย

2.5.3 Policies Based on User Identity

แพ็คเกตฟิวเตอริ่งดั้งเดิมไม่สามารถระบบว่ายุเซอร์คนไหนกำลังติดต่อในทราฟฟิคที่ผ่านไฟวอลล์ ดั่งนั้นเทคโนโลยีไฟวอลล์โดยปราศจากความสามารถขั้นสูงไม่สามารถมีนโยบายที่อนุญาตหรือปฏิเสธการเข้าสู่โดยขึ้นอยู่กับการระบุตัวตน อย่างไรก็ตามเทคโนโลยีไฟวอลล์อื่นๆสามารถเห็นการระบุเหล่านี้และออกนโยบายที่ไฟวอลล์โดยใช้วีพีเอ็น ทั้งไอพีเซค วีพีเอ็น และ เอสเอสแอลวีพีเอ็นมีหลายวิธีที่จะระบุผู้ใช้ เช่น ความลับที่ถูกจัดหาให้โดยพื้นฐานของยูเซอร์บายยูเซอร์กับการยืนยันตัวตนแบบมัลติแฟ็กเตอร์ หรือกับดิจิตอลเซอร์ทิพิเขทที่ถูกควบคุมโดยแต่ละยูเซอร์ เอ็นเอซี(แนค)กลายมาเป็นวิธีที่นิยมสำหรับไฟวอลล์ที่จะอนุญาตหรือปฏิเสธยูเซอร์เข้าสู่ทรัพยากรเนทเวิคโดยเฉพาะ ยิ่งไปกว่านั้นแอพพลิเคชั่นไฟวอลล์และพร็อกซี่สามารถอนุญาตหรือปฏิเสธการเข้าของยูเซอร์ขึ้นอยู่กับการยืนยันตัวตนของยูเซอร์ขึ้นภายในแอพพลิเคชั่นของพวกมันเอง

2.5.4 Policies Based on Network Activity

หลายๆไฟวอลล์อนุญาตผู้ดูแลระบบเพื่อที่จะระงับการสร้างการเชื่อมต่อหลังจากช่วงเวลาที่ไม่ได้ทำงาน ยกตัวอย่างเช่น ถ้ายูเซอร์ที่อยู่ข้างนอกไฟวอลล์ล๊อคอินเข้าไปที่ไฟล์เซิฟเวอร์แต่ไม่สามารถร้องขอในช่วง 15 นาทีผ่านไป นโยบายอาจจะระงับการจราจรที่จะทำต่ไปในการเชื่อมต่อนั้น นโยบายทามเบดมีประโยชน์ในการหยุดการโจมตีซึ่งเป็นสาเหตุจากยูเซอร์ที่ล๊อคอินเดินออกไปจากคอมพิวเตอร์ลีคนอื่นมานั่งและสร้างการเชื่อมต่อแทน อย่างไรก้ตามนโยบายเหล่านี้สามารถรบกวนยู

เซอร์ผู้ที่สร้างการเชื่อมต่อแต่ไม่ได้ใช้บ่อยๆ ยกตัวอย่างเช่น ยูเซอร์อาจจะเชื่อมต่อไปที่ไฟล์เซิฟเวอร์เพื่อที่จะอ่านไฟล์และใช้เวลานานๆในการแก้ไขไฟล์ ถ้ายูเซอร์ไม่ได้บนทึกไฟล์กลับไปที่เซิฟเวอร์ก่อนที่ไฟล์วอลล์ที่ตั้งไว้ว่าหมดเวลา การหมดเวลานี้สามารถเป็นสาเหตุการเปลี่ยนแปลงไฟล์ให้สุญหาย

2.6 Intrusion Detection and Prevention Systems

การตรวจสอบผู้บุกรุกคือการตรวจสอบการจราจรที่ไม่ต้องการบนเน็ตเวิร์คหรืออุปกรณ์ ไอดีเอส สามารถเป็นส่วนของการติดตั้งซอร์ฟแวร์ หรือ ฟิสิคอลแอพไพลแอนซ์ ที่ ตรวจดู การจราจรเน็ตเวิร์คเพื่อที่จะตรวจสอบกิจกรรมและเหตุการณ์ที่ไม่ต้องการ เช่น การจราจรที่ผิดก็หรือเป็นอันตราย, ละเมิดนโยบายความปลอดภัยและการจราจรที่ละเมิดนโยบายการใช้ที่ยอมรับได้ เครื่องมือไอดีเอส หลายๆเครื่องมือจะเก็บเหตุการณ์ที่ตรวจสอบไว้ใน ล็อก เพื่อที่จะได้มาดูใหม่ในภายหลัง หรือจะรวบรวมเหตุการณ์ไว้กับข้อมูลอื่นเพื่อที่จะตัดสินใจเกี่ยวกับนโยบายหรือการควบคุมความเสียหาย ไอพีเอส คือชนิดของ ไอพีเอส ที่สามารถป้องกันหรือหยุดการจราจรที่ไม่ต้องการได้ ไอพีเอส โดยปกติแล้วบันทึกเหตุการณ์และข้อมูลที่สัมพันธ์กัน

ไอพีเอส เทคโนโลยีหลายๆชนิดปรากฏเพราะความแตกต่างของการคอนฟิคเน็ตเวิร์ค แต่ละชนิดมีข้อดีและข้อเสียในการตรวจสอบ, การคอนฟิคและราคา

2.6.1 Network-Based Intrusion Detection System

ระบบการตรวจสอบการบุกรุกทางเน็ตเวิร์ค (เอ็นไอดีเอส) คือชนิดของ ไอดีเอส โดยทั่วไปที่วิเคราะห์การจราจรเน็ตเวิร์คทุกเลเยอร์ ของโอเอสไอโมเดล และตัดสินใจเกี่ยวกับวัตถุประสงค์ของการจราจร, การวิเคราะห์กิจกรรมที่น่าสงสัย เอ็นไอดีเอส ส่วนใหญ่นั้นง่ายที่จะใช้บนเน็ตเวิร์คและสามารถมองการจราจรบ่อยๆจากหลายๆระบบได้ในครั้งเดียว
เอ็นไอดีเอสถูกวางบนเน็ตเวิร์คเพื่อวิเคราะห์การจราจรในการค้นหาเหตุการณ์ที่ไม่ต้องการและเป็นอันตราย การจราจรเน็ตเวิร์คถูกสร้างบนหลายๆ เลเยอร์ ซึ่งแต่ละเลเยอร์ส่งข้อมูลจากจุดหนึ่งไปอีกจุดหนึ่ง

สองชนิดองค์ประกอบหลักประกอบด้วยอุปกรณ์ เอ็นไอดีเอส และ ซอร์ฟแวร์เท่านั้น อุปกรณ์เอ็นไอดีเอส คือส่วนเฉพาะของฮาร์ดแวร์ ฟังก์ชั่นของมันทำแค่เป็นไอดีเอส ซึ่งมีโอเอส (OS), ซอร์ฟแวร์ และ เน็ตเวิร์คอินเตอร์เฟซการ์ดรวมอยู่ในอุปกรณ์นั้นด้วยชนิดองค์ประกอบที่สอง คือ ซอร์ฟแวร์เท่านั้น ซึ่งบรรจุไอดีเอสซอร์ฟแวร์ ทั้งหมดและบางครั้งโอเอสด้วย อย่างไรก็ตาม ผู้ใช้งานจัดหาฮาร์ดแวร์ ซอร์ฟแวร์-โอนลี่ เอ็นไอดีเอส แพงน้อยกว่าอุปกรณ์ -เบส เอ็นไอดีเอส เพราะ

ซอร์ฟแวร์-โอนลี่ เอ็นไอดีเอส ไม่จัดหาฮาร์ดแวร์อย่างไรก็ตามมีความต้องการการคอนฟิคเพิ่มมากยิ่งขึ้น และความสามารถทางฮาร์ดแวร์ เพิ่มมากขึ้นด้วย

องค์ประกอบระบบสำคัญต่อระบบมากกับไอดีเอส เอ็นไอดีเอส ไม่ได้ประกอบด้วยอุปกรณ์เดียวแต่ประกอบด้วยหลายๆองค์ประกอบแยกกัน ถึงแม้ว่าใน เอ็นไอดีเอส ที่มีความซับซ้อนน้อยๆ องค์ประกอบทั้งหมดอาจจะปรากฏแต่จะถูกบรรจุอยู่ในอุปกรณ์เดียว โดยองค์ประกอบที่เห็นๆกันอยู่ รวมถึง เซ็นเซอร์ (sensor) , เมเนจเมนท์เซิฟเวอร์, ดาต้าเบสเซิฟเวอร์ และ คอนโซล

เซ็นเซอร์ หรือ เอเจนท์ คือ องค์ประกอบของเอ็นไอดีเอสที่เห็นการจราจรเน็ตเวิร์คและสามารถตัดสินใจเกี่ยวกับว่าการจราจรนั้นเป็นอันตรายหรือไม่ เซ็นเซอร์หลายๆตัวถูกวางเฉพาะจุดรอบๆเน็ตเวิร์คและตำแหน่งของเซ็นเซอร์ นั้นสำคัญมาก การเชื่อมต่อไปที่เน็ตเวิร์คสามารถเป็นที่ ไฟร์วอลล์, สวิทช์, เราท์เตอร์, หรือที่อื่นที่เน็ตเวิร์คนั้นแบ่ง

เมเนจเมนท์เซิฟเวอร์ อยู่ที่ศูนย์กลางสำหรับเซ็นเซอร์ทั้งหมดเพื่อที่จะส่งผลลัพธ์ของเซ็นเซอร์ เหล่านั้น เมเนจเมนท์เซิฟเวอร์ เชื่อมต่อกั เซ็นเซอร์ ผ่าน เมเนจเมนท์เน็ตเวิร์ค เพราะเหตุผลทางความปลอดภัย เมเนจเมนท์ เซิฟเวอร์ แยกออกจากส่วนที่เหลือของเน็ตเวิร์ค เมเนจเมนท์ เซิฟเวอร์ จะตัดสินใจขึ้นอยู่กับว่า เซ็นเซอร์ รายงานอะไร มันสามารถรวมข้อมูลที่มีความสัมพันธ์ร่วมกันจากหลายๆ เซ็นเซอร์ และตัดสินใจขึ้นอยู่กับเฉพาะการจราจรในตำแหน่งต่างๆกันบนเน็ตเวิร์ค

ดาต้าเบส เซิฟเวอร์ คือที่เก็บข้อมูลองค์ประกอบของ เอ็นไอดีเอส เหตุการณ์จากหลายๆ เซิฟเวอร์ และข้อมูลที่สัมพันธ์กันจาก เมเนจเมนท์ เซิฟเวอร์ สามารถถูกบันทึกจาก ดาต้าเบส เซิฟเวอร์เหล่านี้ ดาต้าเบส ถูกใช้เพราะพื้นที่ที่เก็บข้อมูลขนาดใหญ่และคุณสมบัติการทำงาน

คอนโซล คือส่วนของเอ็นไอดีเอส ซึ่งผู้ดูแลระบบสามารถเข้าไปคอนฟิค เอ็นไอดีเอส หรือตรวจดูสถานะของเอ็นไอดีเอส คอนโซล สามารถถูกติดตั้งเป็น โปรแกรมบนคอมพิวเตอร์ ของผู้ดูแลระบบ หรือ เว็บแอพพลิเคชั่น

การวางเซ็นเซอร์ของเอ็นไอดีเอส

เพราะว่า เซ็นเซอร์ คือส่วนของ เอ็นไอดีเอส ที่มองเห็นการจราจรของเน็ตเวิร์ค ซึ่งการวางของ เซ็นเซอร์ นั้นสำคัญต่อการตรวจสอบการจราจรมาก

อินไลน์

อินไลน์ เอ็นไอดีเอส เซ็นเซอร์จะถูกวางระหว่าง 2 อุปกรณ์เน็ตเวิร์ค เช่น เราท์เตอร์ และไฟร์วอลล์ ซึ่งการจราจรทั้งหมดระหว่าง 2 อุปกรณ์จะต้องเคลื่อนที่ผ่าน เซ็นเซอร์ ซึ่งรับประกันว่าเซ็นเซอร์ สามารถวิเคราะห์การจราจรได้ เซ็นเซอร์ ของ ไอดีเอส ที่อยู่ภายในสามารถถูกใช้เพื่อที่จะไม่อนุญาตให้การจราจรผ่าน เซ็นเซอร์ ที่ถูกพิจารณาว่าเป็นอันตราย อินไลน์ เซ็นเซอร์ ถูกวาง

ระหว่างฝั่งของไฟร์วอลล์ที่ปลอดภัย และส่วนที่เหลือของเน็ตเวิร์คภายในเพื่อที่จะทำให้วิเคราะห์การจราจรได้น้อยลง

พาสซิฟ – พาสซิฟเซ็นเซอร์ วิเคราะห์การจราจรที่ถูกคัดลอกจากเน็ตเวิร์คต่อสู้กับการจราจรที่ผ่านมัน ซึ่งการจราจรที่คัดลอกมานั้นสามารถมาได้จากหลายๆที่

สแปนนิ่งพอร์ต – สวิทช์ อนุญาตให้การจราจรทั้งหมดบน สวิทช์ถูกคัดลอกไปที่ พอร์ต เดียว ระหว่างเวลาของ โลว์ เน็ตเวิร์ค โหลด นี้คือวิธีที่ง่ายที่จะมองการจราจรทั้งหมดบน สวิทช์ อย่างไรก็ตาม ถ้า โหลด เพิ่มขึ้น สวิทช์ อาจจะไม่สามารถคัดลอกการจราจรทั้งหมด ถ้า สวิทช์ พิจารณาว่าการจราจรมันผิดรูปแบบของมันจะไม่คัดลอกการจราจรทั้งหมดด้วย การจราจรที่ผิดรูปแบบเป็นชนิดที่ เซ็นเซอร์ ของ เอ็นไอดีเอส ต้องวิเคราะห์

เน็ตเวิร์คแท็บ

เน็ตเวิร์คแท็บคัดลอกการจราจรที่ฟิสิคอลเลเยอร์ ส่วนใหญ่ใช้ในไฟเบอร์ออปติคเคเบิ้ล ซึ่งเน็ตเวิร์คแท็บ อยู่ภายใน (อินไลน์) และคัดลอกสัญญาณโดยปราศจากการลดจำนวนของแสงไฟไประดับที่ใช้ไม่ได้ เพราะ เน็ตเวิร์คแท็บสามารถเชื่อมต่อโดยตรงไปที่มีเดีย แต่ปัญหาของเน็ตเวิร์คแท็บคือสามารถยกเลิกการเชื่อมต่อทั้งหมดได้

ชนิดของเหตุการณ์

เอ็นไอดีเอส สามารถตรวจสอบชนิดของเหตุการณ์ได้หลายชนิด จากดีไปยังอันตราย

เหตุการณ์ที่สอดแนมเพียงตัวเดียวนั้นไม่เป็นอันตรายแต่สามารถนำไปสู่การโจมตีที่เป็นอันตรายได้ เหตุการณ์สอดแนมนี้สามารถเริ่มที่ ทีซีพีเลเยอร์ เช่น พอร์ตสแกนรันบริการที่มี พอร์ตเปิดอยู่เพื่อที่จะอนุญาตให้มีการเชื่อมต่อที่ถูกต้อง ระหว่างการ สแกนพอร์ต ผู้โจมตีพยายามที่จะเปิดการเชื่อมต่อทุกๆพอร์ตของเซิฟเวอร์เพื่อที่จะกำหนดว่าบริการไหนกำลังรันอยู่

การโจมตีแบบสอดแนมรวมถึงการเปิดการเชื่อมต่อของแอพพลิเคชั่น ที่รู้จักด้วย เช่น เว็บเซิฟเวอร์ เพื่อที่จะรวบรวมข้อมูลเกี่ยวกับโอเอส และ เวอร์ชั่นของเซิฟเวอร์ เอ็นไอดีเอสสามารถตรวจสอบการโจมตีที่ เน็ตเวิร์คเลเยอร์, ทรานสพอร์ต เลเยอร์ และ แอพพลิเคชั่น เลเยอร์ การโจมตีเหล่านี้รวมถึงโค้ดที่เป็นอันตรายซึ่งสามารถถูกใช้เป็น ดีโอเอสแอทแทค และสำหรับการขโมยข้อมูลล่าสุด เอ็นไอดีเอส สามารถถูกใช้เพื่อตรวจสอบการจราจรอันตรายที่เป็นอันตรายน้อยๆ แต่อย่างไรก็ตามเป็นการจราจรที่ไม่ต้องการ เช่น บริการที่ไม่ได้คาดหวัง ตัวอย่างแบ็คดอร์ และ การละเมิดกฎ

การป้องกัน

เมื่อไอดีเอสถูกวางในการคอนฟิคภายในการจราจรทั้งหมดจะต้องเคลื่อนที่ผ่าน เซ็นเซอร์ของไอดีเอส เมื่อการจราจรทั้งหมดถูกกำหนดว่าไม่ต้องการ ไอดีเอสจะไม่ฟอร์เวิร์ดการจราจรไปส่วนที่เหลือของเน็ตเวิร์ค เพื่อที่จะได้ผล อย่างไรก็ตามความพยายามนี้ต้องการให้การจราจรทั้งหมดผ่านเซ็นเซอร์ เมื่อไอดีเอสไม่ได้ถูกคอนฟิคในการคอนฟิคภายใน มันจะต้องจบมัลลิเชียสเซชชั่น โดยการส่ง รีเซ็ตแพ็คเก็ตไปที่เน็ตเวิร์ค บางครั้งการโจมตีสามารถเกิดขึ้นก่อนที่ ไอดีเอส สามารถ รีเซ็ต การเชื่อมต่อ ยิ่งกว่านั้นการจบการเชื่อมต่อทำงานเพียงแค่บนการเชื่อมต่อแบบ ทีซีพี ไม่ใช่บน ยูดีพี หรือ ไอซีเอ็มพี วิธีที่ทำให้ง่ายขึ้นกับ ไอพีเอส โดยการคอนฟิคอุปกรณ์เน็ตเวิร์คใหม่ ตัวอย่าง ไฟร์วอลล์, สวิทช์ และ เราท์เตอร์ เพื่อให้ตอบกลับการจราจรวีแลน สามารถถูกคอนฟิคเพื่อที่จะกักการจราจรไว้และจำกัดการเชื่อมต่อของจราจรนั้นไปยังรีซอร์ส อื่นๆ

2.6.2 Host-Based Intrusion Detection System

ระบบการตรวจสอบการบุกรุกระดับโฮส (Host-Based Intrusion Detection System(เอชไอดีเอส)) วิเคราะห์การจราจรเน็ตเวิร์คและ การเซ็ทค่าระบบโดยเฉพาะ เช่น ซอร์ฟแวร์ คอลล์, โลคอล ซีเคียวริตี้ โพลิซี, โลคอลล็อกออดิท และอื่นๆ

เอชไอดีเอส ประกอบด้วยหลาย เซ็นเซอร์ ที่ตั้งอยู่บน เซิฟเวอร์, เวิร์คสเตชั่น เพื่อที่จะป้องกันการโจมตีที่เครื่องโดยเฉพาะ เอชไอดีเอส สามารถมองเห็นได้มากกว่าการจราจรเน็ตเวิร์คและสามารถตัดสินใจขึ้นอยู่กับ โลคอล เซ็ตติ้ง, การเซ็ตค่าไปที่ โอเอส และ ล็อก ดาต้า

เอชไอดีเอส มีอุปกรณ์หลายๆชนิดเซ็นเซอร์ หรือ เอเจนท์ตั้งอยู่บนโฮสต์ หรือใกล้ๆ เช่น เซิฟเวอร์, เวิร์คสเตชั่น หรือ แอพพลิเคชั่นเซอร์วิซ เหมือนกับการคอนฟิคไอดีเอส อื่นๆ ข้อมูลเหตุการณ์ถูกส่งไปที่ ล็อกกิ้ง เซอร์วิซ เพื่อที่จะบันทึกเหตุการณ์และรวมรวมสิ่งที่สัมพันธ์กันกับข้อมูลอื่นๆ

เอเจนท์ ของเอชไอดีเอสสามารถวางบนโฮสต์ ได้หลายชนิด เซ็นเซอร์ของเอชไอดีเอสสามารถ ตรวจดูเซิฟเวอร์, ไคล์เอนท์, โฮสต์ และ แอพพลิเคชั่นเซิฟเวอร์ เซิฟเวอร์ คือ คอมพิวเตอร์ที่รันเซอร์วิซให้ไคล์เอนท์มาเชื่อมต่อ, ส่ง, หรือรับข้อมูล เช่น เว็บ, อีเมล หรือ เอฟทีพี เซิฟเวอร์

โฮสต์ ของไคล์เอนท์ คือ เวิร์คสเตชั่น เช่น เดสก์ท็อป หรือ แลปท็อป ซึ่งผู้ใช้งานสามารถเชื่อมต่อไปยังเครื่องอื่นๆ

แอพพลิเคชั่นเซอร์วิซ คือ ซอร์ฟแวร์ที่รันบนเซิฟเวอร์ เช่น เว็บเซอร์วิซ หรือ ดาต้าเบสแอพพลิเคชั่น เพราะแต่ละโฮสต์ทำงานบนระบบปฏิบัติการหรือการบริการที่ต่างกัน ชนิดของการโจมตีที่จะมีผลต่อเครื่อง คือ ชนิดที่เฉพาะเจาะจงกับเครื่องเหล่านั้น

เพราะเอชไอดีเอสเซ็นเซอร์ ตรวจดูเครื่องไม่เพียงแค่การจราจรเน็ตเวิร์คเอเจนท์จะต้องถูกวางบนโฮสต์ซึ่งเป็นส่วนหนึ่งของซอร์ฟแวร์ตามเหตุและผล มันถูกวางในวิธีเดียวกับเซ็นเซอร์ ของเอ็นไอดีเอส ระหว่างแอซเซ็ท และ เน็ตเวิร์คภายนอก อย่างไรก็ตามแทนที่จะเป็นอุปกรณ์เน็ตเวิร์คเอชไอดีเอสเซ็นเซอร์ เป็น ซอร์ฟแวร์เลเยอร์ ที่การจราจรจะต้องผ่านเพื่อที่จะได้รับบริการ

ชนิดของเหตุการณ์

โฮสต์-เบส ไอดีเอส เช่น เอ็นไอดีเอสเซ็นเซอร์ สามารถตรวจดูระบบสำหรับการโจมตีเน็ตเวิร์ค-เบส และสามารถตรวจสอบเหตุการณ์ที่เกิดเฉพาะ โฮสต์ ซึ่งเหตุการณ์เฉพาะ โฮสต์ รวมถึงการวิเคราะห์โค้ด เช่น การรันโค้ดที่เป็นอันตรายและ บัฟเฟอร์โอเวอร์โฟล์ว, ไฟล์ซิสเต็มมอนิเตอริ่ง, รวมถึงความถูกต้องและการเข้าถึง, การวิเคราะห์ล็อก และ ระหว่างว่าโฮสต์ล็อกไหนถูกเอามาดูใหม่ และ เน็ตเวิร์คคอนฟิกกูเรชั่นมอนิเตอร์ระหว่างการคอนฟิคของการเซ็ตค่าเน็ตเวิร์ค ตัวอย่าง ไวร์เลส, วีพีเอ็น, และการคอนฟิคที่ทันสมัยถูกดูใหม่อีกครั้งสำหรับการเปลี่ยนแปลงและการเซ็ตค่าที่ไม่เหมาะสม

การป้องกัน

เอชไอดีเอส ตรวจดูหลายๆเหตุการณ์เฉพาะ โฮสต์ และในทางกลับกันสามารถป้องกันระบบจากการโจมตีของชนิดนี้ได้ เมื่อเหตุการณ์โค้ด ที่เป็นอันตรายถูกตรวจสอบ เช่นบัฟเฟอร์โอเวอร์โฟล์ว

เอชไอดีเอสสามารถมั่นใจว่าโค้ดที่เป็นอันตรายไม่ถูกรันเพราะ บัฟเฟอร์โอเวอร์โฟล์ว เมื่อการเข้าถึง ไฟล์ ซิสเต็ม เกิดขึ้น เอชไอดีเอส เซ็นเซอร์ จะปฏิเสธการเข้าถึงด้วย เพราะ เอชไอดีเอส เซ็นเซอร์ ไม่ได้พึ่งการจราจรของเน็ตเวิร์คเพื่อที่จะตัดสินใจบนการจราจรที่เป็นอันตรายหรือหยุดการจราจรเน็ตเวิร์คเทคนิคเอชไอดีเอสไอพีเอส สามารถทำงานได้อย่างรวดเร็วและประสบความสำเร็จ

2.7 ชนิดของการตรวจสอบของ ไอดีเอส

2.7.1 Signature-Based Detection

ไอดีเอสสามารถใช้ ซิกเนเจอร์-เบสดีเทคชั่น ขึ้นอยู่กับข้อมูลการจราจรที่รู้จักเพื่อที่จะวิเคราะห์การจราจรที่ไม่ต้องการที่เป็นไปได้ การตรวจสอบชนิดนี้เร็วและง่ายที่จะคอนฟิค อย่างไรก็ตามผู้โจมตีสามารถดัดแปลงการโจมตีเล็กน้อยเพื่อที่จะคัดลอกการโจมตีให้ไม่สามารถตรวจสอบได้ ถึงแม้ว่า ซิกเนเจอร์-เบสดีเทคชั่น จะมีขีดจำกัดความสามารถในการตรวจสอบ แต่มันก็สามารถตรวจสอบได้อย่างแม่นยำ

2.7.2 Anomaly-Based Detection

ไอดีเอส ที่มองการจราจรเน็ตเวิร์คและตรวจสอบข้อมูลว่าไม่ถูกต้อง หรือผิดปกติเรียกว่า อนอมัลลี่-เบส ดีเทคชั่น (Anomaly-Based Detection)
วิธีนี้มีประโยชน์สำหรับการตรวจสอบการจราจรที่ไม่ต้องการและไม่เป็นที่รู้จักโดยเฉพาะ ยกตัวอย่าง เช่น อนอมัลลี่-เบส (Anomaly-Based) จะตรวจสอบไอพีแพ็คเก็ตว่าผิดรูปแบบ มันไม่สามารถตรวจสอบว่ามันผิดรูปแบบโดยเฉพาะทาง แต่มันสามารถระบุได้ว่าผิดปกติ

2.7.3 Stateful Protocol Inspection

สเตทฟูลล์โปรโตคอลอินสเปคชั่น คล้ายกับ อนอมัลลี่-เบสดีเทคชั่น แต่มันจะวิเคราะห์การจราจรที่เน็ตเวิร์ค และ ทรานสพอร์ตเลเยอร์ และผู้ใช้งานโดยเฉพาะ อาจตรวจได้ถึงแอพพลิเคชั่นเลเยอร์ ซึ่ง อนอมัลลี่-เบสดีเทคชั่นไม่สามารถตรวจได้

2.8 Intrusion Prevention System

หรือ ไอพีเอสคืออุปกรณ์หรือโปรแกรมที่ใช้เพื่อตรวจสอบสัญญาณของการบุกรุกเข้าไปในระบบหรือเน็ตเวิร์คและทำงาน การทำงานนั้นประกอบด้วยการสร้างอลาร์ม และ การปิดกั้นการบุกรุก

บางไอพีเอสเซ็นเซอร์ มี โหมดการเรียนรู้หรือการจำลองที่หยุดยั้งการทำการป้องกันทั้งหมดและชี้ให้เห็นเมื่อการทำการป้องกันจะถูกทำแทน สิ่งนี้เป็นการอนุญาตให้ผู้ดูแลระบบเพื่อที่จะ ตรวจดูและ ไฟน์-จูน (fine-tune) การคอนฟิคของความสามารถการป้องกันก่อนที่จะให้ทำการป้องกันซึ่งลดเป็นการลดความเสี่ยงของการปิดกั้นแอคทิวิตี้ที่เป็นปกติโดยไม่ได้ตั้งใจ

การระบุแอคทิวิตี้ ที่ปกติว่าเป็นอันตราย เราเรียกว่า ฟอลซ์โพซิทีฟ และการที่เราไม่สามารถระบุ แอคทิวิตี้ที่เป็นอันตรายได้ นั้นคือ ฟอลซ์ เนกาทีฟ

2.9 ความแตกต่างของ ไอดีเอส กับ ไอพีเอส

กุญแจที่สำคัญที่ทำให้ไอดีเอส แตกต่างจากไอพีเอส คือ ไอพีเอส ตอบสนองทันทีทันใดและไม่อนุญาตให้การจราจรที่เป็นอันตรายผ่าน ในขณะที่ไอดีเอส อนุญาตให้การจราจรที่เป็นอันตรายผ่านก่อนที่มันจะสามารถตอบสนอง
ไอดีเอส

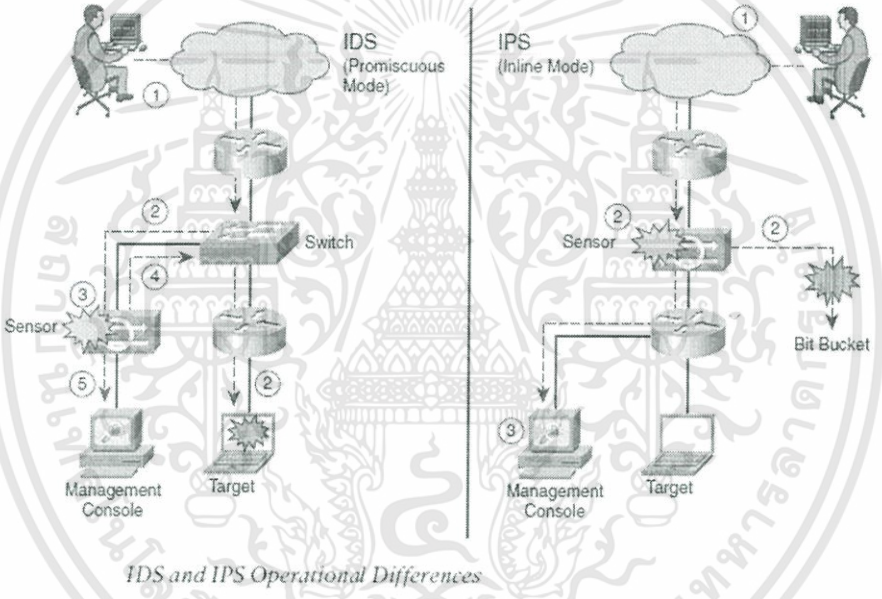
- วิเคราะห์การคัดลอกของการไหลของจราจร
- ไม่ทำให้การจราจรเน็ตเวิร์คช้า

- อนุญาตให้บางการจราจรที่เป็นอันตรายเข้าสู่เน็ตเวิร์ค

ไอพีเอส

- ทำงานภายในในเวลาจริงเพื่อที่จะ ตรวจดู การจราจรของ เลเยอร์ 2 ถึง เลเยอร์ 7 และเนื้อหา
- จำเป็นที่สามารถที่จะรับมือกับการจราจรเน็ตเวิร์ค
- ป้องกันการจราจรที่เป็นอันตรายจากการเข้าสู่เน็ตเวิร์ค

รูปที่ 2.6 แสดงถึงความแตกต่างในการทำงานระหว่าง ไอดีเอส กับ ไอพีเอส



รูปที่ 2.6 ความแตกต่างระหว่างไอดีเอสกับไอพีเอส

จากรูปฝั่งซ้ายขั้นตอนที่เกิดขึ้นเมื่อการโจมตีถูกสั่งในสภาพแวดล้อมที่ ตรวจดู โดย ไอดีเอส

1. การโจมตีเกิดขึ้นบนเน็ตเวิร์คที่มีเซ็นเซอร์ใช้ในไอดีเอสโหมด
2. สวิทช์ส่งการคัดลองของแพ็คเก็ตทั้งหมดไปที่ ไอดีเอสเซ็นเซอร์ (คอนฟิคในโพรมิคูอัสโหมด ซึ่งการคอนฟิคในโพรมิคูอัสโหมด คือ เซ็นเซอร์รับการคัดลอกของข้อมูลสำหรับการวิเคราะห์ ขณะที่การจราจรธรรมดายังคงสร้างทางของมันไปสู่ปลายทางของมันในท้ายที่สุด)
3. ไอดีเอสเซ็นเซอร์ ใช้ ซิกเนเจอร์แมทช์ กับการจราจรที่เป็นอันตรายเพื่อที่จะ ซิกเนเจอร์
4. ไอดีเอสเซ็นเซอร์ ส่ง สวิทช์คอมมานด์ เพื่อที่จะปฏิเสธการเข้าถึงไปที่การจราจรที่เป็นอันตราย

5. ไอดีเอสส่งอลาร์ม ไปที่ เมเนจเมนท์คอนโซลสำหรับล็อกกิ้ง และจุดประสงค์การบริหารจัดการอื่นๆ

จากรูปฝั่งขวาคือขั้นตอนที่เกิดขึ้นเมื่อการโจมตีถูกสั่งในสภาพแวดล้อมที่ ตรวจดู โดย ไอพีเอส

1. การโจมตีเกิดขึ้นบนเน็ตเวิร์คที่มีเซ็นเซอร์ใช้ใน ไอพีเอสโหมด (คอนฟิคในอินไลน์โหมด ซึ่งการคอนฟิคใน อินไลน์โหมด คือ เซ็นเซอร์ที่ทำงานอินไลน์วิเคราะห์การจราจรปรากฏอยู่และสามารถปิดกั้นแพ็คเก็ตก่อนที่จะไปถึงปลายทางของพวกมัน)
2. ไอพีเอสเซ็นเซอร์ วิเคราะห์แพ็คเก็ตทันทีที่แพ็คเก็ตมาถึง ไอพีเอสเซ็นเซอร์อินเตอร์เฟซ ไอพีเอสเซ็นเซอร์ ใช้ ซิกเนเจอร์แมทช์ กับการจราจรที่เป็นอันตรายเพื่อที่จะ ซิกเนเจอร์ และการโจมตีจะถูกหยุดทันทีไอพีเอสเซ็นเซอร์ สามารถทิ้งการจราจรที่ละเมิดนโยบาย
3. ไอพีเอสเซ็นเซอร์ สามารถส่งอลาร์ม ไปที่ เมเนจเมนท์คอนโซล สำหรับล็อกกิ้ง และจุดประสงค์การบริหารจัดการอื่นๆ

2.10 ความแตกต่างของ ไฟร์วอลล์ กับ ไอดีเอส/ไอพีเอส

ไฟร์วอลล์ และ ไอพีเอส เป็นเครื่องมือที่สำคัญทั้งคู่สำหรับการป้องกันองค์กรจากการบุกรุก ซึ่งทั้งคู่จำเป็นอย่างยิ่ง

ไฟร์วอลล์ ถูกออกแบบเพื่อที่จะปิดกั้นการจราจรเน็ตเวิร์คทั้งหมดยกเว้นว่าอันไหนอัลลาวด์อย่างเห็นได้ชัด

อินทรูชั่นพรีเวนชั่นซิสเต็ม ถูกออกแบบเพื่อที่จะอนุญาตทุกๆสิ่งยกเว้นว่าสิ่งไหนที่ ดิสอัลลาวด์อย่างเห็นได้ชัด

ไฟร์วอลล์ ถูกออกแบบเพื่อที่จะอนุญาต(หรือปิดกั้น) เน็ตเวิร์คแพ็คเก็ตขึ้นอยู่กับต้นทาง, ปลายทาง, และ พอร์ตนัมเบอร์ ของเน็ตเวิร์คแพ็คเก็ตโดยไม่คำนึงถึงเนื้อหาของแต่ละ แพ็คเก็ตเพย์โหลด (เนื้อหาของเมสเซจ)

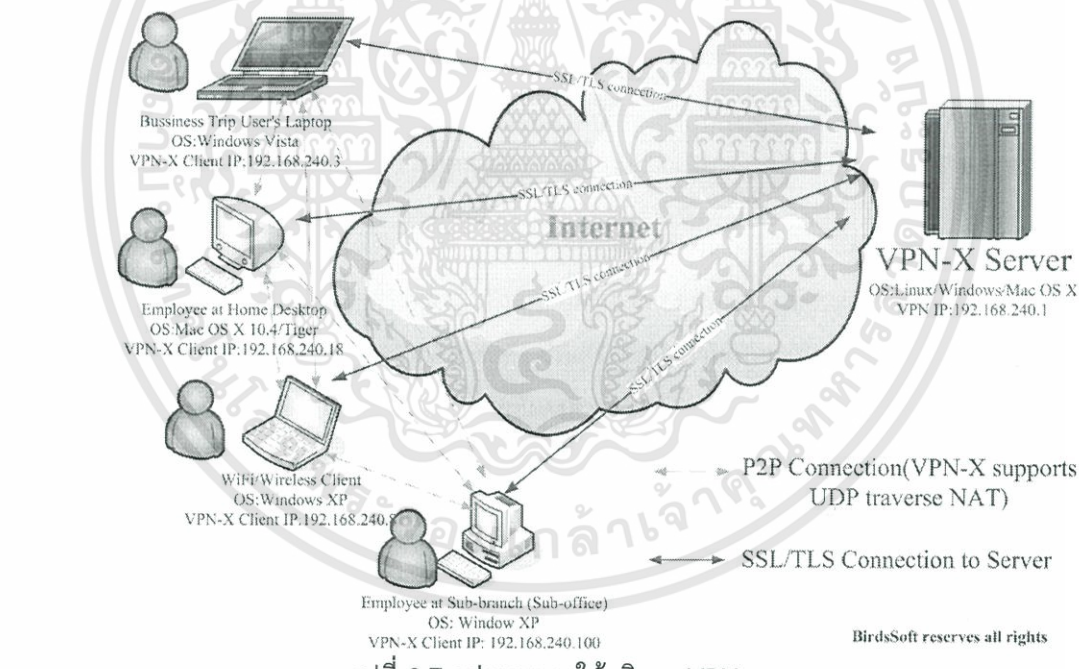
อินทรูชั่นพรีเวนชั่นซิสเต็ม ถูกออกแบบเพื่ออนุญาต เน็ตเวิร์ค แพ็คเก็ต(หรือ ปิดกั้น) เน็ตเวิร์คแพ็คเก็ตขึ้นอยู่กับ แพ็คเก็ตเพย์โหลด

2.11 วีพีเอ็น (VPN)

วีพีเอ็น หรือ เวอช่วลไพรเวทเน็ตเวิร์ค (Virtual Private Network) หมายถึง เครือข่ายเสมือนส่วนตัวที่ทำงานโดยใช้โครงสร้างของเครือข่ายสาธารณะหรืออาจจะวิ่งบนเครือข่ายไอพีก็ได้แต่ยังสามารถคงความเป็นเครือข่ายเฉพาะขององค์กรได้ด้วยการเข้ารหัสแพ็กเก็ตก่อนส่งเพื่อให้ข้อมูลมี

ความปลอดภัยมากขึ้น อย่างไรก็ดีคำว่า วีพีเอ็นจะครอบคลุมทั้งอุปกรณ์ฮาร์ดแวร์ (เช่น เกทเวย์ และเราท์เตอร์), ซอฟต์แวร์ และส่วนที่เป็นไฟร์วอลล์

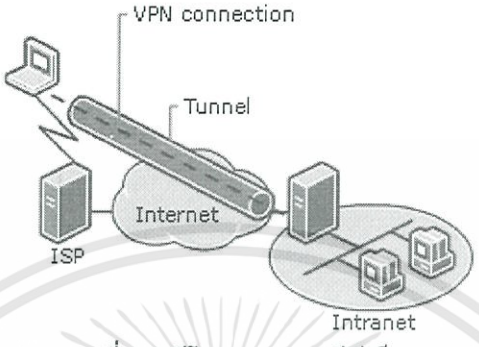
การเข้ารหัสแพ็กเก็ตเพื่อทำให้ข้อมูลมีความปลอดภัยนั้นก็มีอยู่หลายกลไกด้วยกันซึ่งวิธีเข้ารหัสข้อมูลจะทำกันที่เลเยอร์ 2 คือ ดาต้าลิงค์เลเยอร์ แต่ปัจจุบันมีการเข้ารหัสใน ไอพีเลเยอร์ โดยมักใช้เทคโนโลยี ไอพีเซค (IP Security) ปกติแล้ว วีพีเอ็น ถูกนำมาใช้กับองค์กรขนาดใหญ่ที่มีสาขาอยู่ตามที่ต่างๆ และต้องการต่อเชื่อมเข้าหากันโดยยังคงสามารถรักษาเครือข่ายให้ใช้ได้เฉพาะคนภายในองค์กรหรือคนที่เกี่ยวข้องด้วย เช่น ลูกค้า เป็นต้น นอกจากนี้แล้วกลไกในการสร้างโครงข่าย วีพีเอ็นอีกประเภทหนึ่ง คือ มัลติโปรโตคอลลาเบลสวิทช์ (Multiprotocal Label Switch) เป็นวิธีในการส่งแพ็กเก็ตโดยการใส่ ลาเบล ที่ส่วนหัวของข้อความและค่อยเข้ารหัสข้อมูล จากนั้นจึงส่งไปยังจุดหมายปลายทาง เมื่อถึงปลายทาง ก็จะถอดรหัสที่ส่วนหัวออก วิธีการนี้ ช่วยให้ผู้วางระบบเครือข่าย สามารถแบ่ง เวอช่วลแลน (Virtual LAN) เป็นวงย่อย ให้เป็น เครือข่ายเดียวกันได้



รูปที่ 2.7 รูปแบบการให้บริการ VPN

บริการ วีพีเอ็น แบ่งออกเป็น 3 รูปแบบ

2.11.1 รีโมทแอคเซส วีพีเอ็น (remote access VPN)



รูปที่ 2.8 รีโมทแอคเซส วีพีเอ็น

เป็นรูปแบบในการเข้าถึงเครือข่ายวีพีเอ็น จากอุปกรณ์เคลื่อนที่ต่างๆ ซึ่งสามารถเข้าถึงเครือข่ายได้ใน 2 ลักษณะ โดยลักษณะแรก เป็นการเข้าถึงจากไคลเอ็นต์ใดๆ ก็ได้โดยอาศัย ผู้ให้บริการอินเทอร์เน็ต เป็นตัวกลาง ในการติดต่อซึ่งจะมีการเข้ารหัสในการส่งสัญญาณจากเครื่องไคลเอ็นต์ไปยัง วีพีเอ็น เซิร์ฟเวอร์ และลักษณะที่สองเป็นการเข้าถึงจากเครื่องแอ็กเซสเซิร์ฟเวอร์ (เน็ตเวิร์คแอคเซส Server-เอ็นเอเอส) โดยเริ่มต้นจาก ผู้ใช้หมุนโมเด็ม ติดต่อมายังไอเอสพี และจากนั้น จะมีการเข้ารหัสข้อมูล และส่งต่อไปยังปลายทาง ในกรณีของ รีโมทแอคเซส วีพีเอ็น นั้นเครื่องลูกข่ายสามารถที่จะสร้างท่อรับส่งข้อมูล หรือ ทันเน่ล ได้ใน 2 ลักษณะตามการใช้งาน ได้แก่

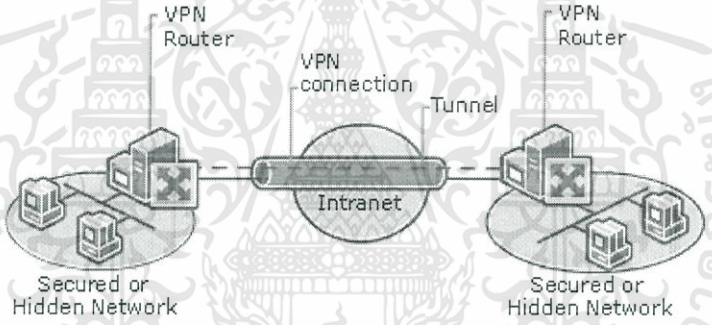
2.11.1.1. Compulsory Tunnel (หรือ mandatory Tunnel)

คือการเชื่อมต่อรีโมทแอคเซสวีพีเอ็น โดยวิธีการหมุนโมเด็มผ่านสายโทรศัพท์จากเครื่องลูกข่ายไปยังอุปกรณ์ รีโมทแอคเซส เซิร์ฟเวอร์ (RAS) ที่มักจะตั้งอยู่ในที่ทำงานของผู้ให้บริการอินเตอร์เน็ต การสร้างท่อรับส่งข้อมูลหรือ ทันเน่ล จะเกิดขึ้นระหว่างอุปกรณ์อาร์เอเอส และวีพีเอ็น เซิร์ฟเวอร์เท่านั้น ระหว่างเครื่องลูกข่ายและ อาร์เอเอสจะเป็นการเชื่อมต่อด้วยวิธีหมุนโมเด็มตามปกติ นอกจากนี้เครื่องลูกข่ายจะไม่จำเป็นต้องติดตั้งซอฟต์แวร์หรือตั้งค่าใดๆที่เกี่ยวกับวีพีเอ็นเพิ่มเลย อย่างไรก็ตามอุปกรณ์ อาร์เอเอส นั้นจะต้องมีความสามารถในการเชื่อมต่อแบบวีพีเอ็น กับ วีพีเอ็น เซิร์ฟเวอร์ ด้วย การใช้งานวีพีเอ็นในลักษณะนี้มักจะเป็นบริการพิเศษของผู้ให้บริการอินเตอร์เน็ต แต่จำเป็นต้องต้องเสียค่าบริการเพิ่ม

2.11.1.2 Voluntary Tunnel

คือการเชื่อมต่อรีโมทแอคเซสวีพีเอ็น โดยที่การสร้างท่อรับส่งข้อมูลหรือ ทันเน่ล เกิดขึ้นตั้งแต่เครื่องลูกข่ายจนถึงตัววีพีเอ็นเซิร์ฟเวอร์เลย เครื่องลูกข่ายสามารถเชื่อมต่ออินเตอร์เน็ตโดยการหมุนโมเด็ม,เอดีเอสแอล หรือแชร์อินเตอร์เน็ตจากระบบแลน ภายในองค์กรก็ได้การใช้งานรีโมทแอคเซส วีพีเอ็น ในปัจจุบันส่วนใหญ่ จะเป็นแบบนี้เนื่องจากไม่ต้องสนใจว่าอุปกรณ์อาร์เอเอส ของผู้ให้บริการอินเตอร์เน็ตจะสนับสนุนการเชื่อมต่อกับวีพีเอ็นเซิร์ฟเวอร์ได้หรือไม่ อย่างไรก็ตามเครื่องลูกข่ายจะได้รับการติดตั้งซอฟต์แวร์เพื่อเพิ่มความสามารถในการเชื่อมต่อ วีพีเอ็น กับวีพีเอ็น เซิร์ฟเวอร์ ด้วย แต่ในกรณีของระบบปฏิบัติการวินโดวส์ นั้นจะมีความสามารถในตัวอยู่แล้ว ขอเพียงตั้งค่าให้ถูกต้องก็ใช้ได้แล้ว

2.11.2 Intranet VPN



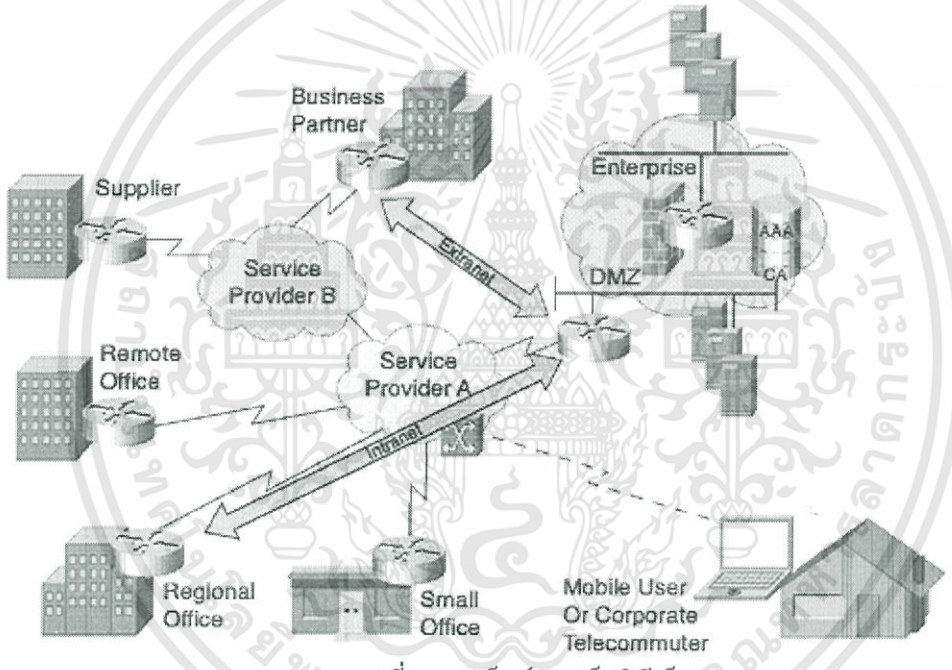
รูปที่ 2.9 อินทราเน็ตวิพีเอ็น

เป็นรูปแบบในการเข้าถึงเครือข่ายวีพีเอ็น ที่ใช้เฉพาะภายในองค์กรเท่านั้น อาทิการต่อเชื่อมเครือข่าย ระหว่างสำนักงานใหญ่ในกรุงเทพฯ และสาขาย่อยในต่างจังหวัด เสมือนกับการทดแทน การเช่าวงจรลีสไลน์ ระหว่างกรุงเทพกับต่างจังหวัด โดยที่แต่ละสาขาสามารถต่อเชื่อมเข้ากับผู้ให้บริการอินเทอร์เน็ตในท้องถิ่นของตน เพื่อเชื่อมเข้าโครงข่ายวีพีเอ็น ขององค์กรอีกทีหนึ่งหรือสรุปก็คือ ต้องให้เราท์เตอร์ หรืออุปกรณ์ 2 ฝั่ง ทำ วีพีเอ็น แบบ ไซท์-ทู-ไซท์ถึงกัน โดย เครื่องของไคลเอนท์ ไม่ต้องทำอะไร ปัจจุบันเป็นที่นิยมมาก ยกตัวอย่าง มีบริษัทที่มีเอดีเอสแอลในพื้นที่เช่น เชียงใหม่กับกรุงเทพฯ และ เอดีเอสแอล เราท์เตอร์เป็นรุ่นที่มีฟังก์ชัน วีพีเอ็น ไซท์-ทู-ไซท์ ทำให้ทั้ง 2 สาขาใช้งานภายในได้แบบประหยัดค่าใช้จ่ายมากๆ ไม่ว่าจะเป็น ข้อมูล, เสียง หรือ วิดีโอ เป็นต้น

ไซท์-ทู-ไซท์ วีพีเอ็น คือการเชื่อมต่อ วีพีเอ็น ระหว่างระบบ แลน 2 ระบบเข้าด้วยกัน โดยอาศัยอุปกรณ์ที่เรียกว่า วีพีเอ็น เกทเวย์ ที่ติดตั้งไว้ในระบบ แลน ทั้ง 2 ฝั่งเป็นตัวเชื่อมต่อ อุปกรณ์ไฟร์วอลล์ โดยทั่วๆไปจะมีความสามารถในการทำตัวเป็น วีพีเอ็น เกทเวย์ ได้ ตัวอย่างเช่น การ

เชื่อมต่อระบบ แลน ระหว่างสาขาและสำนักงานใหญ่เข้าด้วยกันโดยอาศัยการทำ ไซท์-ทู-ไซท์ วีพีเอ็น ถ้าสร้างท่อรับส่งข้อมูล หรือ ทันเน่ล จะเกิดขึ้นระหว่าง วีพีเอ็น เกทเวย์ เท่านั้น เครื่องลูกข่ายภายในระบบ แลน แต่ละฝั่ง จะสามารถติดต่อสื่อสารากอีกฝั่งได้ โดยไม่ต้องติดตั้งซอฟแวร์หรือตั้งค่าใดๆในเครื่องเพิ่ม อธิบายง่ายๆคือ เครื่องลูกค่าจะไม่สามารถรับรู้ว่ามีการเชื่อมต่อระหว่างระบบ แลนทั้งสองฝั่งด้วยวีพีเอ็น กันอยู่ สำหรับโปรโคอลที่สามารถใช้ในการทำ ไซท์-ทู-ไซท์ วีพีเอ็น โดยมาตรฐานทั่วไปนิยมใช้ไอพีเซค ในการเชื่อมต่อ

2.11.3 Extranet VPN



รูปที่ 2.10 เอ็กซ์ทราเน็ตวิพีเอ็น

เป็นรูปแบบในการเข้าถึงเครือข่าย ที่คล้ายกับอินทราเน็ตวีพีเอ็น แต่มีการขยายวงออกไป ยังกลุ่มลูกค้า ซัพพลายเออร์ และพาร์ตเนอร์ เพื่อให้ใช้เครือข่ายได้ จุดสำคัญอย่างหนึ่งในการเลือกติดตั้ง วีพีเอ็น คือการเลือก ผู้ให้บริการอินเทอร์เน็ตที่วางระบบรักษาความปลอดภัยเป็นอย่างดี มีส่วนอย่างมากในการส่งข้อมูลบน วีพีเอ็น ให้ปลอดภัยมากยิ่งขึ้น เพราะถ้า ไอเอสพี มีระบบรักษาความปลอดภัยที่รัดกุมก็จะช่วยให้ข้อมูลที่ส่งมามีความปลอดภัยมากขึ้น เอ็กซ์ทราเน็ต วีพีเอ็น อาจจะเปิดให้ใช้งานได้แค่บางเมนูเท่านั้น ต้องเน้นเรื่องของความเป็นส่วนตัว

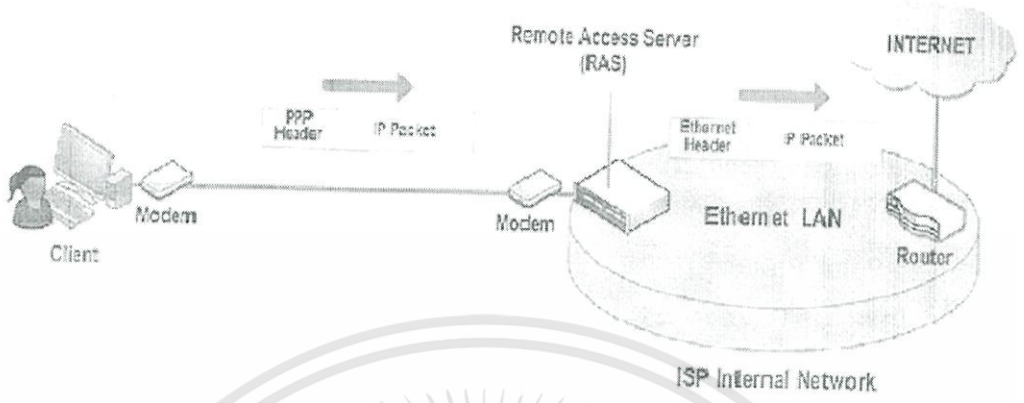
2.12 Protocol PPP

พีพีพี (PPP) คือโปรโตคอลที่เอื้ออำนวยให้เครื่องลูกข่ายสามารถเชื่อมต่อหรือเข้าถึงระบบเครือข่ายภายในองค์กรได้จากระยะไกล (รีโมทแอคเซส) ด้วยวิธีหมุนโมเด็มผ่านสายโทรศัพท์ (Dial-up) ภายในตัวโปรโตคอล พีพีพี นั้นจะมีกลไกการรักษาความปลอดภัยของข้อมูลพร้อมสรรพในตัวมันเอง เช่น การตรวจยืนยันตัวผู้ใช้ (User authentication) และการเข้ารหัสข้อมูล (การเข้ารหัสลับ) เป็นต้น

โดยทั่วไปจะใช้ พีพีพี สำหรับการเชื่อมต่ออินเตอร์เน็ตโดยผ่านการหมุนโมเด็มจากเครื่องของผู้ใช้ไปยังอุปกรณ์ที่เรียกว่า รีโมทแอคเซสเซิร์ฟเวอร์ (อาร์เอเอส) ที่ตั้งอยู่ในที่ทำงานของผู้ให้บริการอินเตอร์เน็ต ซึ่งในกรณีนี้โปรโตคอล พีพีพี จะรับผิดชอบในการขนถ่ายข้อมูลผ่านโมเด็มและสายโทรศัพท์ระหว่างเครื่องของผู้ใช้และอุปกรณ์อาร์เอเอส นั่นเอง

รูปที่ 2.11 พีพีพีเฟรม

โครงสร้างของโปรโตคอล พีพีพี นั้นสามารถบรรจุแพ็คเก็ตของโปรโตคอลในระดับที่สูงกว่าไว้ภายในตัวได้เช่น ไอพี,ไอพีเอ็กซ์ และ เน็ทบีอียูไอ เป็นต้นซึ่งในกรณีนี้พีพีพี จะทำหน้าที่ขนถ่ายแพ็คเก็ตของโปรโตคอลระดับสูงเหล่านั้นให้ไปถึงอุปกรณ์ อาร์เอเอส จากนั้นอุปกรณ์ อาร์เอเอสจะทำการถอดโครงสร้างส่วนหัว (เฮดเดอร์) ของพีพีพีออกให้เหลือเฉพาะเนื้อข้อมูล (ดาต้า) ซึ่งก็คือแพ็กเก็ตของโปรโตคอลในระดับสูงที่บรรจุอยู่ข้างใน จากนั้นจึงส่งต่อไปยังระบบแลน ภายในองค์กรเพื่อให้แพ็กเก็ตนั้นไปถึงปลายทางได้



รูปที่ 2.12 การเชื่อมต่อโดยใช้พีพีพี

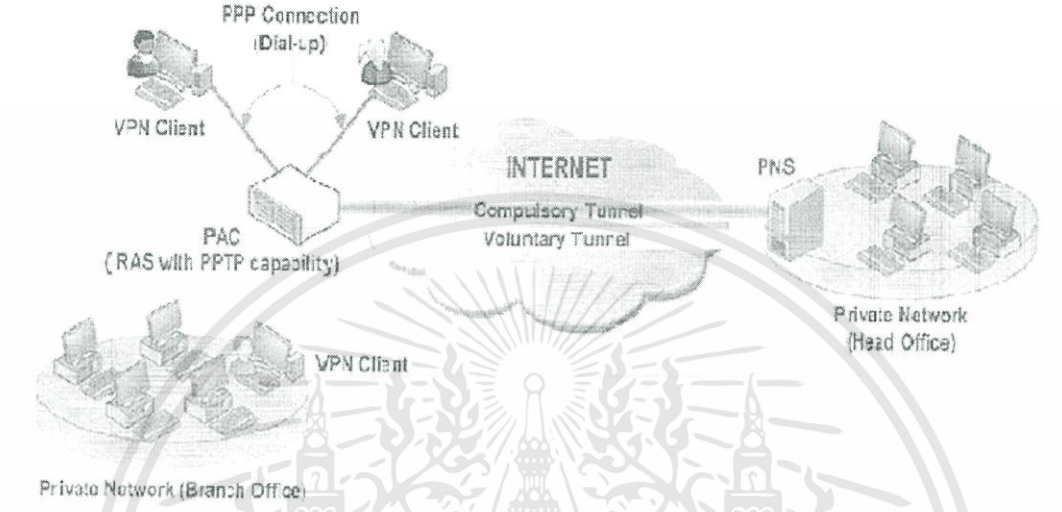
สำหรับกลไกการรักษาความปลอดภัยของข้อมูลของ พีพีพีนั้นจะประกอบด้วยการตรวจยืนยันตัวผู้ใช้ (User Authentication) ที่กระทำโดยฝั่งที่เป็นอุปกรณ์ อาร์เอเอส และเข้ารหัสข้อมูล (การเข้ารหัสลับ) ระหว่างต้นทางและปลายทาง โดยที่การตรวจยืนยันตัวผู้ใช้สามารถใช้เทคนิคต่างๆ เช่น พีเอพี (PAP) (Password Authentication Protocol) เอสพีเอพี (SPAP) ซีเอชเอพี (CHAP) (Challenge Handshake Authentication Protocol), เอ็มเอส-ซีเอชเอพี (MS-CHAP) (Microsoft CHAP) เวอร์ชั่น1 และ 2 และอีเอพี (Extensible Authentication Protocol) เป็นต้นในขณะที่การเข้ารหัสข้อมูลระหว่างกันนั้นใช้เทคนิคที่เรียกว่า อีซีพี (ECP) (Encryption Control Protocol) หรือถ้าเป็นในกรณีของระบบปฏิบัติการ วินโดวส์ จะสามารถใช้เทคนิค เอ็มพีพีอี (MPPE) (Microsoft Point-to-Point Encryption)

2.12.1 พีพีพี และหลักการทำงานของวีพีเอ็น

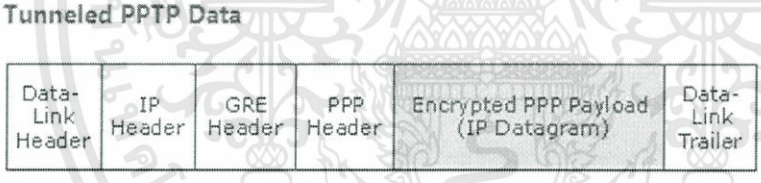
พีพีพี คือโปรโตคอลที่มีกลไกรักษาความปลอดภัยของข้อมูลพร้อมสรรพในตัวมันเอง เช่น การตรวจยืนยันตัวผู้ใช้ และการเข้ารหัสข้อมูลดังนั้นจึงเหมาะที่จะนำมาใช้ในการขนถ่ายข้อมูลผ่านอินเตอร์เน็ตหรือเครือข่าย ไอพี แต่เนื่องจากพีพีพี ถูกออกแบบมาให้ทำงานเฉพาะการเชื่อมต่อผ่านโมเด็มและสายโทรศัพท์เท่านั้น หากสามารถทำให้พีพีพี เดินเข้าเครือข่ายอินเตอร์เน็ตหรือเครือข่าย IP ประเภทต่างๆเช่นระบบLANได้ก็จะเป็นการเพิ่มขอบเขตการทำงานของพีพีพีออกไปได้ ดังนั้น วิธีการก็คือการนำโปรโตคอลอื่นๆมาช่วยขนถ่ายโปรโตคอล พีพีพี อีกทีหนึ่ง ซึ่งมีอยู่ด้วยกันหลายตัว ได้แก่ พีพีทีพี,แอลทูเอฟ,แอลทูทีพี เป็นต้นโปรโตคอลดังกล่าวนี้ก็คือโปรโตคอลที่ใช้ในการทำวีพีเอ็น และเป็นหลักการทำงานของวีพีเอ็นนั่นเอง

2.13 รูปแบบโปรโตคอลของการทำ ทันเน่ล

2.13.1 พีพีทีพี (PPTP)



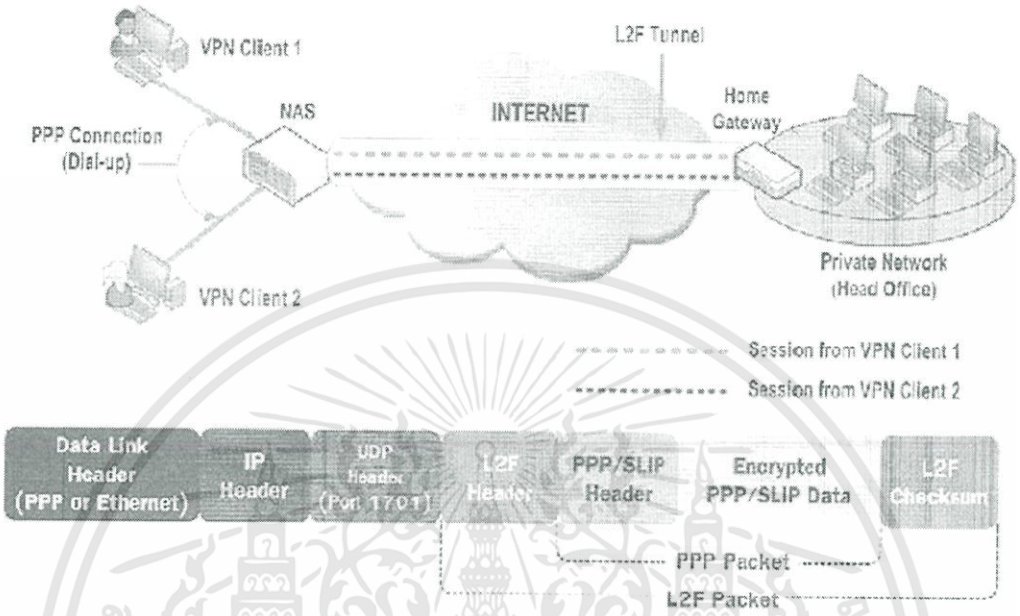
รูปที่ 2.13 การเชื่อมต่อโดยใช้พีพีทีพี



รูปที่ 2.14 พีพีทีพีแพ็คเก็ต

พีพีทีพี ย่อมาจาก พ็อยท์-ทู-พ็อยท์ (point-to-point) ทันเน่ลลิ่ง โปรโตคอล เป็นโพรโทคอลที่ผลิตและ ติดมากับระบบปฏิบัติการของ Microsoft ซึ่งร่วมกับบริษัทอื่นๆ 3 บริษัทพัฒนาขึ้น พีพีทีพีใช้คอนโทรลแชนเน่ล บนการทำงานทีซีพี และ จีอาร์อีทันเน่ล เพื่อที่จะเอนแคปซูเลทพีพีพี แพ็คเก็ตพีพีทีพี เป็นส่วนต่อเติมของโพรโทคอล พีพีพี ดังนั้นจึงสนับสนุนเฉพาะการเชื่อมต่อแบบพ็อยท์-ทู-พ็อยท์ แต่ไม่สนับสนุนการเชื่อมต่อแบบ พ็อยท์-ทู-มัลติพ็อยท์ พีพีทีพี มีข้อได้เปรียบตรงที่สนับสนุนทั้งไคลเอ็นต์ และทันแนลเซิร์ฟเวอร์และยังได้รับการพัฒนาเพื่อให้เพิ่มประสิทธิภาพในด้านต่างๆขึ้นมาอีก ข้อดีคือสามารถใช้ได้กับทุกระบบปฏิบัติการ ใช้งานผ่าน เอ็นเอที ได้ สะดวกในการติดตั้ง

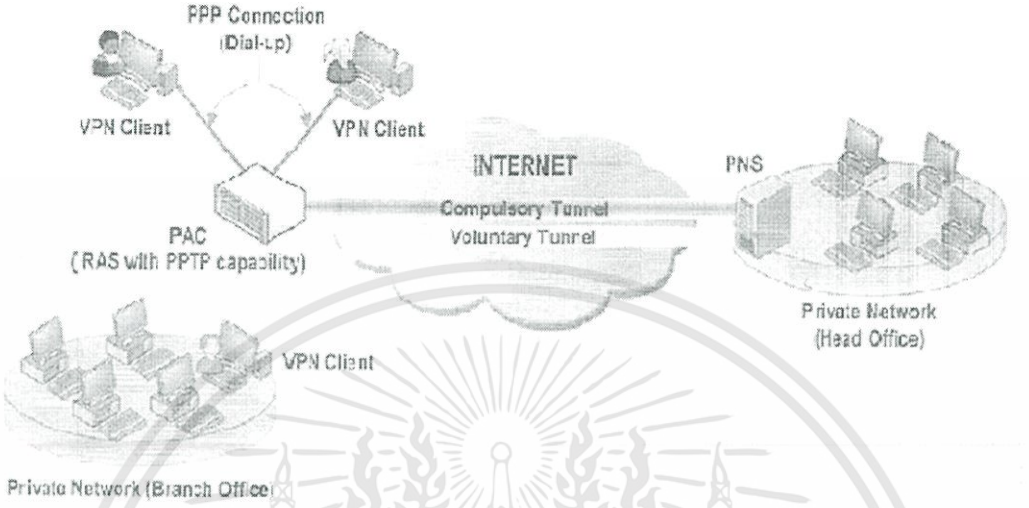
2.13.2 แอลทูเอฟ (L2F)



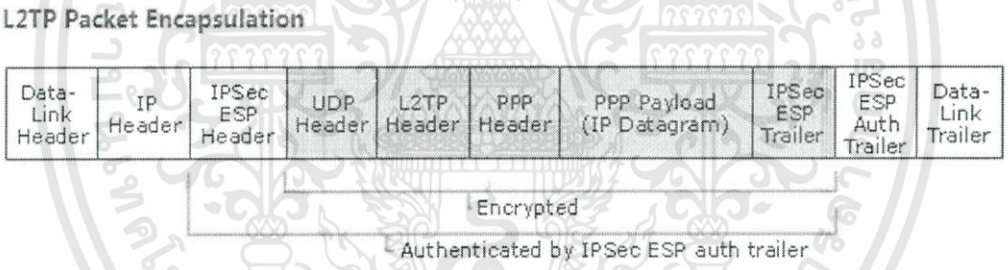
รูปที่ 2.15 การเชื่อมต่อโดยใช้แอลทูเอฟ

แอลทูเอฟ (เลเยอร์ 2 Forwarding) คือโปรโตคอลที่พัฒนาโดยบริษัทซิสโกซิสเทม เพื่อใช้ทำรีโมทแอคเซสวีพีเอ็นในอุปกรณ์ยี่ห้อ ซิสโก เช่นเราท์เตอร์ หรือ ไฟร์วอลล์เป็นหลัก ทันเน่ล ที่สร้างขึ้นจะอยู่ระหว่างอุปกรณ์ เน็ตเวิร์คแอคเซสเซิร์ฟเวอร์ (เอ็นเอเอส) ซึ่งก็คืออุปกรณ์อาร์เอเอสที่มีความสามารถในการเชื่อมต่อกับอุปกรณ์ของ ซิสโกโปรโตคอลแอลทูเอฟ ซึ่งมักตั้งอยู่ในที่ทำการของไอเอสพี สำหรับอุปกรณ์ของซิสโก ที่ทำหน้าที่เป็นวีพีเอ็นเซิร์ฟเวอร์ จะเรียกว่า โฮมเกทเวย์

2.13.3 แอลทูทีพี (L2TP)



รูปที่ 2.16 การเชื่อมต่อโดยใช้แอลทูทีพี

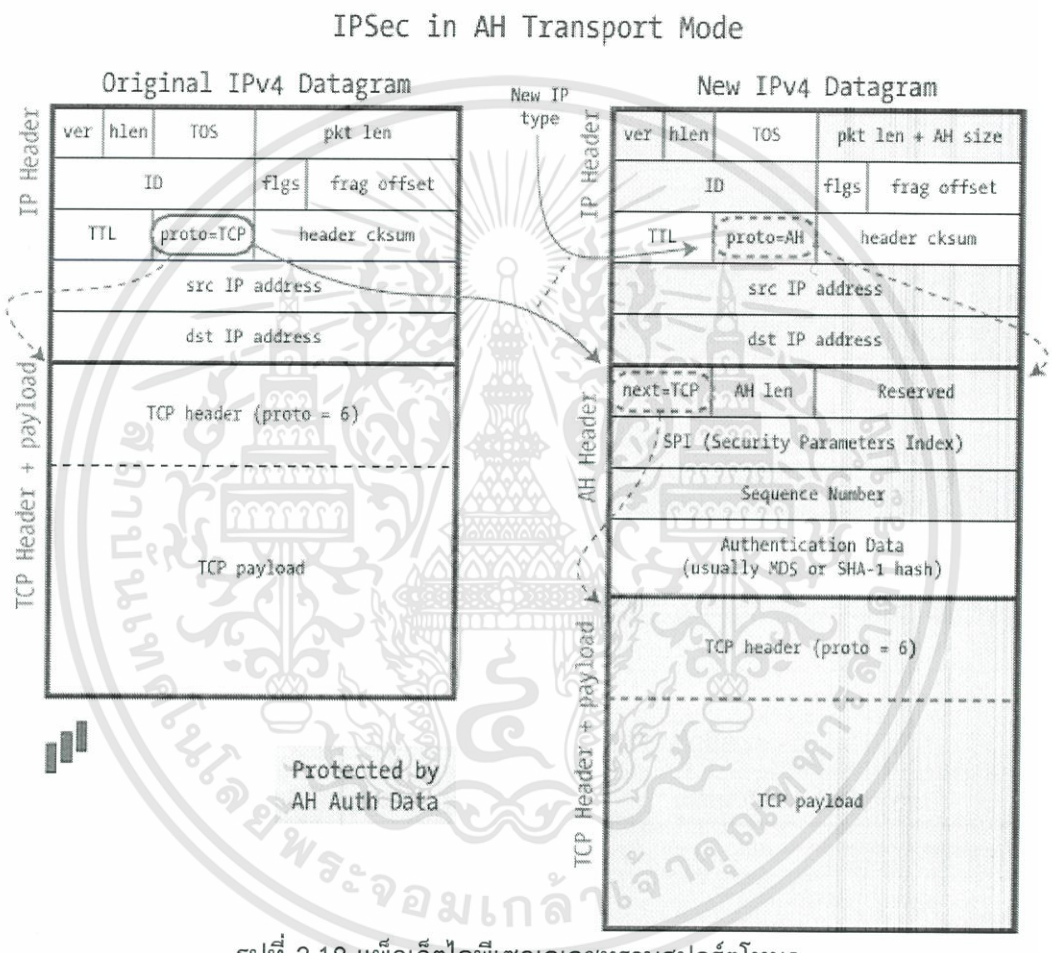


รูปที่ 2.17 แอลทูทีพีแพ็คเก็ต

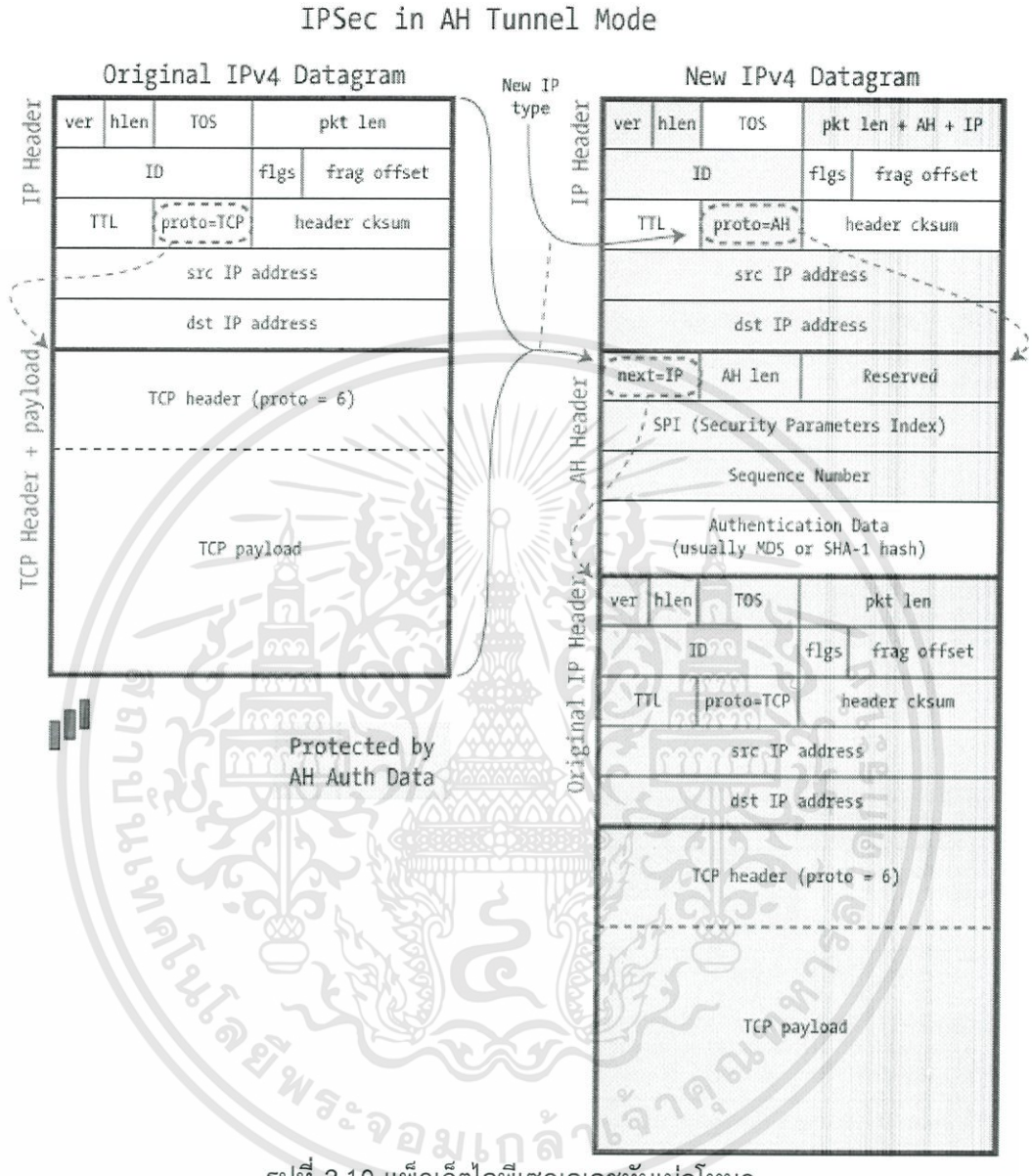
แอลทูทีพี ย่อมาจาก เลเยอร์ 2 ทันเน่ลลิ่ง โปรโตคอล การทำงานคล้ายๆกับพีพีทีพี ต่างกันตรงแอลทูทีพี จะใช้ ยูเซอร์ดาต้าแกรม โปรโตคอล (ยูดีพี) ในการตกลงรายละเอียดในการรับส่งข้อมูลและสร้าง ทันเน่ล ซึ่งเป็นการนำเอาข้อดีของทั้งสองโพรโทคอลมารวมไว้ด้วยกัน โดยนำโพรโทคอลในระดับ เลเยอร์ 2 หรือ พีพีพี มาหุ้มแพ็กเก็ตใน เลเยอร์ 3 ก่อนที่จะหุ้มด้วยไอพีแพ็คเก็ตอีกชั้น ดังนั้นจึงใช้วิธีพิสูจน์แบบพีพีพี แอลทูทีพี ยังสนับสนุนการทำทันเน่ลพร้อมกันหลายๆ อันบนไคลเอ็นต์เพียงตัวเดียว และ แอลทูทีพี ยังคงใช้หลักการเดิมคือการขนถ่ายแพ็กเก็ตของพีพีพีให้สามารถเดินผ่านเครือข่ายอินเตอร์เน็ตหรือระบบเครือข่ายแบบไอพี นั่นเอง ดังนั้นการเข้ารหัสข้อมูลและการตรวจยืนยันตัวผู้ใช้ยังคงใช้กลไกภายในตัว พีพีพีเองอยู่ ใน แอลทูทีพี นั้นนิยมเรียกอุปกรณ์วีพีเอ็นเซิร์ฟเวอร์ ว่า แอลเอ็นเอส (LNS)และสามารถเรียกอุปกรณ์หรือเครื่องที่เชื่อมต่อกับ วีพีเอ็นเซิร์ฟเวอร์ ว่า แอลเอซี (แอลเอซี) (L2TP Access Concentrator)โดยที่ แอลเอซี นั้นจะสามารถถึง

อุปกรณ์รีโมทแอคเซสเซิร์ฟเวอร์ ที่มีความสามารถในการติดต่อกับ แอลเอ็นเอส ด้วยโปรโตคอล แอลทูทีพี หรืออาจหมายถึงเครื่องลูกข่ายที่มีความสามารถในการเชื่อมต่อกับ แอลเอ็นเอส ด้วยโปรโตคอล แอลทูทีพี ได้โดยตรงนั่นเอง

2.13.4 ไอพีเซค (IPsec)



รูปที่ 2.18 แพ็คเก็ตไอพีเซคเอเอชทรานสปอร์ตโหมด



รูปที่ 2.19 แพ็คเก็ตไอพีเซคเอเอชทันเน่ลโหมด

ไอพีเซค หรือ ไอพีซีเคียวริตี้เป็นการรวมโปรโตคอลหลายๆอันมาไว้ด้วยกัน ประกอบด้วยการรักษาความปลอดภัยในการเข้ารหัส การตรวจสอบตัวตนและความถูกต้องของข้อมูล โดยมีการเข้ารหัส 2 แบบด้วยกัน คือ การเข้ารหัสแบบทรานสปอร์ทโหมด และ ทันเน่ลโหมดซึ่งวิธีนี้จะทำให้ข้อมูลมีความปลอดภัยขึ้น ทรานสปอร์ท โหมด ใช้เพื่อป้องกัน เอ็น-ทู-เอ็นคอนเวอร์เซชั่น ระหว่างโฮสต์-ทู-โฮสต์ การป้องกันนี้คือการออเทนทิเคชั่น หรือ การเข้ารหัสลับ หรือเป็นทั้งสองแต่ไม่ได้เป็นทันเน่ลลิ่ง โปรโตคอล ไม่เกี่ยวกับวีพีเอ็นแค่ทำให้ ไอพีคอนเนคชั่น ปลอดภัยอย่างง่าย เอเอช

ในทรานสปอร์ทโหมด ไอพีแพ็คเก็ตจะถูกดัดแปลงเพียงเล็กน้อยรวมถึงเอเอช เฮดเดอร์ ใหม่ระหว่าง ไอพีเฮดเดอร์ และ โปรโตคอลเพย์โหลด (ทีซีพี, ยูดีพี, ฯลฯ) ถูกเก็บกลับไปในไอพีเฮดเดอร์ เราจะดู เน็กซ์ เฮดเดอร์ ฟิลด์ อีกครั้งตอนเราตรวจสอบ ไอพีเซค เมื่อแพ็คเก็ตมาถึงที่ปลายทางของมันและส่ง ออเทนทิเคชั่นเซ็คเอเอช เฮดเดอร์ ถูกถอดออกและ โปรโต=เอเอช ฟิลด์ ใน ไอพีเฮดเดอร์ ถูกแทนที่ กับ เน็กซ์ โปรโตคอล ที่บันทึกไว้ ซึ่งนี่ก็คือการใส่ ไอพี ดาต้าแกรม กลับไปที่สเตทดั้งเดิมของมัน และ มันสามารถถูกส่งไปที่เวทติ้งโปรเซสทันเน่ลโหมดสร้างฟังก์ชันการทำงานของ วีพีเอ็น ที่คล้ายกว่า ที่ ซึ่งไอพีแพ็คเก็ตทั้งหมดถูกห่อหุ้มภายใน ไอพีแพ็คเก็ตอื่นๆ และ ถูกส่งไปที่ปลายทาง

2.13.4.1 ส่วนประกอบของ ไอพีเซค

ไอพีเซค ประกอบด้วยโปรโตคอลย่อยอื่นๆ อีกหลายตัวที่ทำงานร่วมกัน แต่ที่สำคัญและขาด ไม่ได้ในการทำงานมีดังต่อไปนี้

- เอนแคปซูเลท ซีเคียวริตี้ เพย์โหลด (encapsulated security payload) อีเอสพี (ESP) คือ โปรโตคอลที่ใช้ในการเข้ารหัสข้อมูลโดยใช้หลักการของซิมเมตริคคริปโตกราฟฟี (Symmetric Cryptography) หรือการใช้กุญแจการเข้าและถอดรหัสร่วมกันทั้งต้นทางและปลายทาง แพ็กเก็ตของ ไอพี ที่ต้องการความปลอดภัยของข้อมูลสามารถใช้ อีเอสพี ในการเข้ารหัสข้อมูลก่อนส่งได้ แต่ ขอบเขตการป้องกันข้อมูลในแพ็กเก็ตนั้นจะมีผลเฉพาะในส่วนของเนื้อข้อมูล (IP ดาต้า) ของแพ็กเก็ต

รูปที่ 2.20 รูปแบบของแพ็คเก็ตอีเอสพี

แพ็กเก็ตของ IP ที่ผ่านการเข้ารหัสข้อมูลโดยอีเอสพี แล้วจะได้รับการเพิ่มข้อมูลใหม่เข้าไปใน โครงสร้างของแพ็กเก็ต 2 ส่วนคือ ไอพีเซคอีเอสพีเฮดเดอร์ ที่จะแทรกอยู่ระหว่างโครงสร้างส่วนหัว (IP เฮดเดอร์) และเนื้อข้อมูลของแพ็กเก็ต และ ไอพีเซคอีเอสพีเทรลเลอร์ ที่จะอยู่ต่อท้ายแพ็กเก็ต อย่างไร ก็ตาม อีเอสพี ไม่ได้มีเฉพาะกลไกการเข้ารหัสข้อมูลเท่านั้น เนื่องจาก ในปัจจุบันได้มีการเพิ่มกลไกการ ตรวจสอบการแก้ไขหรือปลอมแปลงแพ็กเก็ตหรือที่เรียกว่า อีเอสพีออเทนทิเคชั่น ดาต้า อีกด้วย

ออเทนทิเคชั่นเฮดเดอร์ (เอเอช) คือโปรโตคอลที่ใช้ในการป้องกันการแก้ไขหรือปลอมแปลง แพ็กเก็ต โดยอาศัยการคำนวณค่า เช็คซัมซึ่งได้จากการนำเอาข้อมูลจากโครงสร้างส่วนหัวและเนื้อ ข้อมูลของแพ็กเก็ตพร้อมด้วยกุญแจการเข้ารหัสมาเข้าสูตรการคำนวณค่าทางคณิตศาสตร์ ปละนำ

ค่าที่ได้ไปบันทึกไว้ในโครงสร้างส่วนหัวของแพ็กเก็ตเพื่อให้ทั้งต้นทางและปลายทางสามารถใช้ในการตรวจสอบว่าแพ็กเก็ตที่ได้รับมานั้นไม่ได้ผ่านการปลอมแปลงมา และเนื่องจากเอเอชใช้ทั้งข้อมูลในโครงสร้างส่วนหัวและเนื้อข้อมูลของแพ็กเก็ตมาคำนวณค่า เช็คซัม ดังนั้นขอบเขตการปกป้องข้อมูลจะมีผลครอบคลุมทุกส่วนของแพ็กเก็ตด้วย

รูปที่ 2.21 รูปแบบของแพ็คเก็ตเอเอช

- อินเทอร์เน็ตคีย์เอ็กซ์เชนจ์ (อินเทอร์เน็ต Key Exchange) ไอเคอี (ไอเคอี) โปรโตคอล คือโปรโตคอลที่ใช้ในการตกลงรายละเอียดหรือวิธีการที่จะใช้ในการสร้างช่องทางการสื่อสารที่ปลอดภัยขึ้นระหว่างต้นทางและปลายทาง การทำงานของ ไอเคอี จะแบ่งออกเป็น 2 ขั้นตอนหรือ 2 เฟส ดังนี้

เฟส 1 เป็นการตกลงรายละเอียดหรือวิธีการที่จะใช้ในการสร้างช่องทางการสื่อสารที่ปลอดภัยขึ้นระหว่างต้นทางและปลายทาง เช่น วิธีการเข้ารหัสข้อมูล วิธีการป้องกันการแก้ไขหรือปลอมแปลงแพ็กเก็ต การสร้างกุญแจการเข้ารหัสข้อมูลที่จะใช้ร่วมกัน และ วิธีการตรวจยืนยันตัว (ออเทนทิเคชั่น) ระหว่างกันนั้นแบ่งออกได้เป็น 3 วิธีหลักๆคือ

- พรีแชร์คีย์ (Pre-shared Key) คือการกำหนดรหัสลับซึ่งคล้ายๆกับรหัสผ่านเพื่อให้ต้นทางและปลายทางใช้ในการยืนยันระหว่างกัน หรืออีกนัยหนึ่งคือเป็นการตรวจสอบเพื่อยืนยันว่าฝ่ายตรงข้ามที่กำลังติดต่อสื่อสารกันอยู่นั้นเป็นตัวจริงที่ไม่ได้สวมรอยมา Pre-shared Key จะกำหนดโดยผู้ดูแลระบบและต้องเก็บเป็นความลับไว้และรู้กันเฉพาะต้นทางและปลายทางเท่านั้น

- ดิจิตอลซิกเนเจอร์ (ดิจิตอล Signature) คือการที่ฝั่งต้นทางใช้ไพรเวทคีย์ของตัวเองซึ่งถูกเก็บเป็นความลับไว้มาทดลองเข้ารหัสข้อมูลเพื่อส่งไปให้ปลายทางทดลองถอดรหัสด้วย พับลิค ที่เผยแพร่ไว้ โดยฝั่งต้นทางเพื่อให้ใช้คู่กัน หากปลายทางสามารถถอดรหัสได้ก็แสดงว่าข้อมูลที่ได้รับมานั้นมาจากต้นทางที่แท้จริง ในทางกลับกันฝั่งปลายทางก็จะมีไพรเวทคีย์ และ พับลิค ของตัวเองอีกชุดหนึ่งเพื่อให้ต้นทางใช้ตรวจสอบปลายทางได้ด้วยวิธีเดียวกัน ดังนั้นดิจิตอลซิกเนเจอร์จึงใช้สำหรับการตรวจสอบยืนยันตัวระหว่างกันได้เช่นเดียวกันกับการใช้ Pre-shared Key อย่างไรก็ตามการที่จะเลือกใช้ ดิจิตอลซิกเนเจอร์ ได้นั้นทั้งต้นทางและปลายทางจะต้องไปขอจดทะเบียนเพื่อขอมี ดิจิตอล เซอร์ทิฟิเคท จากตัวแทน ซีเอ (CA) (Certificated Authority) ด้วย

- เซลฟ์ไซน์ (Self Signed) เซอร์ทิฟิเคท คือการใช้เทคนิคและวิธีการของ ดิจิตอลเซอร์ทิฟิเคท นั่นเอง แต่ที่ต่างกันคือ เซลฟ์ไซน์เซอร์ทิฟิเคท นั้นจะออกโดยผู้ดูแลระบบเพื่อใช้ภายในองค์กรเอง ทำให้ประหยัดค่าใช้จ่ายในการขอมี ดิจิตอลเซอร์ทิฟิเคท จากซีเอและยังสะดวกในการบริการจัดการอีกด้วย ในระบบปฏิบัติการ วินโดวส์ เซิร์ฟเวอร์ นั้นจะมีเครื่องมือที่ช่วยอำนวยความสะดวกในการออก ดิจิตอลเซอร์ทิฟิเคทเองได้ นอกจากนี้ก็ยังสามารถเลือกใช้เครื่องมือต่างๆอีกหลายตัวได้เช่นกัน

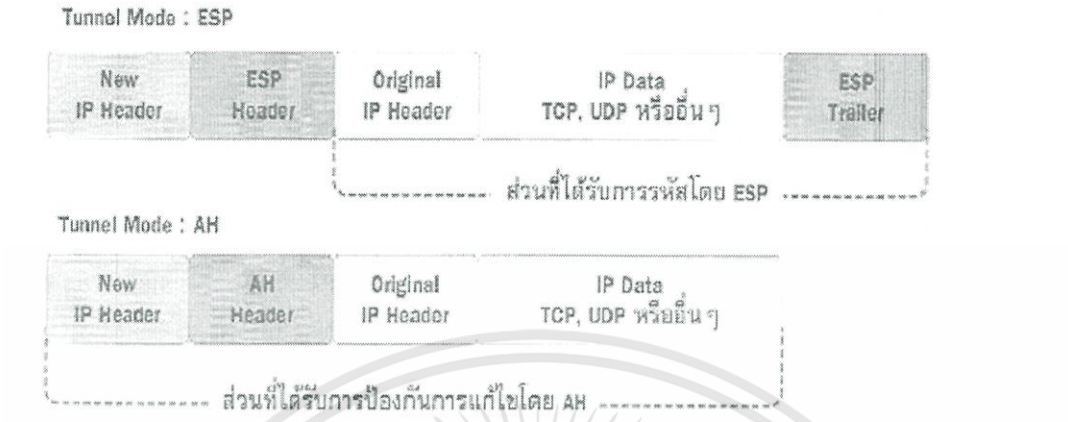
เฟส 2 เป็นการตกลงรายละเอียดหรือวิธีการที่จะใช้ในการปกป้องระหว่างข้อมูลต้นทางและปลายทาง เพื่อใช้ในการทำงานของโปรโตคอล อีเอสพี และ เอเอช โดยอาศัยช่องทางการสื่อสารที่สร้างขึ้นในเฟส 1 ในขั้นตอนนี้จะมีการตกลงระหว่างต้นทางและปลายทางเพื่อสร้างกุญแจการเข้ารหัสข้อมูลสำหรับ อีเอสพี และ เอเอช ที่จะใช้ร่วมกันทั้งสองฝ่ายขึ้นใหม่จำนวน 2 ชุด โดยชุดที่ 1 ใช้สำหรับการส่งข้อมูล (Inbound) กุญแจการเข้ารหัสดังกล่าวนี้จะหมดอายุภายในเวลาสั้นๆและต้องมีการสร้างจึ้นใหม่อยู่เป็นระยะๆ ตลอดการสื่อสาร ทั้งนี้ก็เพื่อเป็นการเพิ่มความปลอดภัยของข้อมูลที่มากยิ่งขึ้นนั่นเอง การทำงานของ ไอเคอี นั้นจะทำงานผ่านโปรโตคอล ยูดีพี โดยใช้พอร์ตหมายเลข 500 ดังนั้นหากเป็นการใช้งานผ่าน ไฟร์วอลล์ ก็ต้องเปิดพอร์ตดังกล่าวด้วย

2.13.4.2 ไอพีเซค ทรานสปอร์ท โหมด และ ทันเน่ล โหมด

การใช้งาน ไอพีเซค ไม่ว่าจะผ่านโปรโตคอล อีเอสพี หรือ เอเอช ก็ตามสามารถแบ่งได้เป็น 2 โหมดดังนี้

ทรานสปอร์ท โหมด

ในทรานสปอร์ทโหมด นั้นการเข้ารหัสข้อมูลโดยใช้อีเอสพี จะมีผลเฉพาะกับส่วนของเนื้อข้อมูลหรือ ดาต้าในแพ็กเก็ตของไอพีเท่านั้น ซึ่งโดยทั่วไปเนื้อข้อมูลในแต่ละแพ็กเก็ตของไอพี มักจะเป็นโปรโตคอลในระดับที่สูงขึ้นไป เช่น ในระดับของทรานสปอร์ทเลเยอร์ ซึ่งได้แก่ ทีซีพี และ ยูดีพี เป็นต้น ในขณะที่การใช้วิธีคำนวณค่า เช็คซัม เพื่อป้องกันการแก้ไขหรือปลอมแปลงแพ็กเก็ตโดยใช้เอเอชนั้น จะมีผลในการปกป้องทั้งแพ็กเก็ต ซึ่งได้แก่ข้อมูลทั้งในโครงสร้างส่วนหัวและเนื้อข้อมูลด้วย ในกรณีของ เอเอชนั้นข้อมูลในส่วนหัว (เฮดเดอร์) ของแพ็กเก็ตไอพีซึ่งได้แก่ ไอพีแอดเดรส จะไม่สามารถเปลี่ยนแปลงแก้ไขได้เนื่องจากมันจะมีผลต่อการคำนวณค่า เช็คซัม ดังรูปที่ 13 และไม่ว่าจะเป็น อีเอสพี หรือ เอเอช ก็ตามเนื้อข้อมูลภายในแพ็กเก็ตของไอพี ซึ่งประกอบด้วยหมายเลขพอร์ตที่ใช้ของ ทีซีพี หรือ ยูดีพี จะไม่สามารถถูกเปลี่ยนแปลงแก้ไขได้ เช่นกัน ดังนั้นมันจึงไม่สามารถทำงานผ่านอุปกรณ์เอ็นเอที ได้



รูปที่ 2.22 รูปแบบของแพ็คเก็ตทรานสปอร์ตทั้งหมด

ทันเน่ล โหมด

ในกรณีของทันเน่ลโหมดนั้นจะเป็นการนำเอาแพ็กเก็ตของไอพี มาบรรจุไว้ภายในแพ็กเก็ตของไอพี ใหม่อีกทีหนึ่ง อธิบายง่ายๆคือเป็นไอพีซ้อนไอพี นั่นเอง จากนั้น ถึงจะนำแพ็กเก็ตที่ได้ไปเข้ารหัสโดย อีเอสพี หรือป้องกันการแก้ไขแพ็กเก็ตโดยเอเอชต่อไป ซึ่ง หากเป็นการเข้ารหัสโดย อีเอสพี จะมีผลครอบคลุมเฉพาะแพ็กเก็ตของไอพี ที่บรรจุอยู่ข้างในแต่ในกรณีของเอเอช นั้นจะมีผลครอบคลุมทั้งแพ็กเก็ตของไอพี ที่ครอบอยู่ข้างนอก

รูปที่ 2.23 รูปแบบของแพ็คเก็ตทันเน่ลโหมดทั้งหมด

ทันเน่ลโหมด จะใช้สำหรับเชื่อมต่อระหว่างระบบแลน 2 วง (ไซท์-ทู-ไซท์) หรือใช้ในกรณีของรีโมทแอคเซสวีพีเอ็นก็ได้ โดยทั่วไปผู้ผลิตอุปกรณ์ ไฟร์วอลล์ หรือ วีพีเอ็นเกทเวย์จะให้การสนับสนุนไอพีเซค ในโหมดทันเน่ลโหมดกันเป็นหลัก

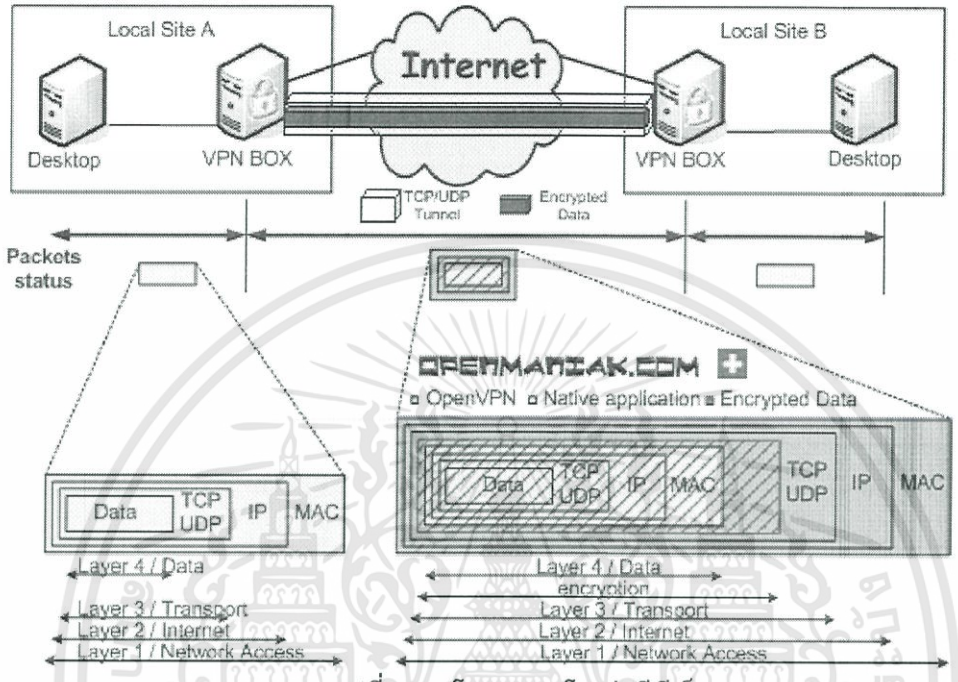
อีเอสพี ออเทนทิเคชั่น ดาต้า

ในขณะที่เอเอช จะใช้ในการป้องกันการแก้ไขหรือปลอมแปลงแพ็กเก็ต อย่างไรก็ตามแพ็กเก็ตที่อาศัย อีเอสพี ในการเข้ารหัสข้อมูลเพียงอย่างเดียวอาจจะถูกแก้ไขหรือปลอมแปลงในส่วนที่ไม่ได้ถูกเข้ารหัสไว้ เช่น ข้อมูลในโครงสร้างส่วนหัวของแพ็กเก็ตไอพี เป็นต้น ในขณะที่แพ็กเก็ตที่อาศัย เอเอช เพียงอย่างเดียว ก็ไม่สามารถซ่อนเนื้อหาในส่วนของเนื้อข้อมูลในแพ็กเก็ตได้หากถูกดักจับแพ็กเก็ตระหว่างทางดังนั้นเพื่อให้เกิดความปลอดภัยของข้อมูลสูงสุดจึงนิยมใช้อีเอสพี ควบคู่กับ เอเอช เสมอ โดยการนำเอาแพ็กเก็ตที่ผ่านขบวนการเข้ารหัสของอีเอสพี ไปผ่านการคำนวณค่า เช็คซัม โดยใช้ เอเอช อีก ซึ่งจะได้แพ็กเก็ต

2.13.4.3 ข้อดี-ข้อเสียของ ไอพีเซค

คุณสมบัติของไอพีเซค เป็นจุดเด่นก็คือเรื่องของการเข้ารหัสข้อมูล การป้องกันการปลอมแปลงแพ็กเก็ตและการตรวจสอบยืนยันแหล่งที่มาของแพ็กเก็ตได้ สามารถป้องกันการรีเพลย์ ได้ (การรีเพลย์ หมายถึงการแอบเก็บบันทึกแพ็กเก็ตที่เกิดจากการสื่อสารระหว่างเครื่อง 2 เครื่องไว้จากนั้นอาจจะมีการเปลี่ยนแปลงหรือแก้ไขแพ็กเก็ตที่เก็บไว้แล้วจึงปล่อยกลับเข้าสู่เครือข่ายเดิม ตามจังหวะและเวลาที่เหมาะสม เพื่อใช้ในการหลอกเครื่องให้เข้าใจผิดคิดว่าแพ็กเก็ตเหล่านั้นมาจากเครื่องจริงๆ) แต่จุดอ่อนของ ไอพีเซค ก็มีคือ ไม่สามารถทำงานผ่านอุปกรณ์ เอ็นเอที แบบธรรมดาได้ และ ใช้งานได้เฉพาะเครือข่ายไอพี เท่านั้น

2.13.5 โอเพ่นวีพีเอ็น (OpenVPN)



รูปที่ 2.24 โมเดลของโอเพ่นวีพีเอ็น

โอเพ่นวีพีเอ็นพัฒนาจากเอสเอสแอล หรือ เอชทีทีพีเอส ซึ่ง มีความปลอดภัยสูงมาก โดยการทำงานจะทำงานที่ โอเอสไอ เลเยอร์ 2 หรือ 3 เพื่อทำให้การขยายเครือข่ายปลอดภัย โดยใช้ เอสเอสแอล/ทีแอลเอส โปรโตคอลสนับสนุนวิธีการออเทนทิเคชั่น ของไคลเอนท์ อย่างยืดหยุ่นโอเพ่นวีพีเอ็นไม่ได้เป็น เว็บแอพพลิเคชั่น พร็อกซีและไม่ทำงานผ่าน เว็บบราวเซอร์

โอเพ่นวีพีเอ็นสามารถทันเน่ลไอพีซับเน็ตเวิร์คใดๆ หรือ เวอช่วลอีเทอร์เน็ตอแดปเตอร์บนยูดีพี หรือ ทีซีพีพอร์ท ก็ได้ และสามารถคอนฟิกเกอร์สเกเลเบิล และ โหลดบาลานซ์ วีพีเอ็น เซิร์ฟเวอร์ และ โดยใช้เครื่องเดียวหรือมากกว่าหนึ่งเครื่องซึ่งสามารถรับมือกับหลายๆการเชื่อมต่อได้จาก วีพีเอ็นไคลเอนท์ที่เข้ามาได้ โอเพ่นวีพีเอ็นสามารถใช้ทั้งการเข้ารหัสลับ , ออเทนทิเคชั่น และ เซอร์ทิฟิเคชั่น ของ โอเพ่นเอสเอสแอล ไลบรารี่ เพื่อที่จะป้องกัน ไพรเวทเน็ตเวิร์ค ทราฟฟิค ของคุณที่มันส่งบนอินเทอร์เน็ตใช้ ไซเฟอร์, คีย์ไซส์ หรือ เอชเอ็มเอซี ไดเกสท์ สำหรับ ดาต้าแกรม อินทริกิตี้ เช็คกิ้ง สนับสนุนโดย โอเพ่นเอสเอสแอลไลบรารี่ โอเพ่นวีพีเอ็นสามารถเลือกระหว่างการเข้ารหัสแบบ สเตติค-คีย์ เบส คอนเวนชันแน่ล (static-key based conventional) หรือ การเข้ารหัสแบบเซอร์ทิฟิเคท-เบส พับลิค (certificated-based พับลิค) และสามารถใช้สเตติคคีย์ (static keys), พรีแชร์คีย์ (pre-shared keys) หรือ ทีแอลเอส-เบสไดนามิคคีย์เอ็กเชนจ์ (TLS-based dynamic key

exchange) การทำงานของโอเพ่นวีพีเอ็นอนุญาตให้ทำงานข้ามระบบปฏิบัติการและสถาปัตยกรรมโพรเซสเซอร์ ข้อดีที่สำคัญของการติดต่อสื่อสารแบบ โอเพ่นวีพีเอ็น คือ สามารถที่จะใช้กับระบบที่ต่างกัน ลดการคอนฟิกกูเรชั่นและสามารถเข้ากันได้กับเอ็นเอที และ ไดนามิคแอดเดรส

2.13.5.1 ข้อดีและข้อเสียของระบบ วีพีเอ็น

ข้อดีของระบบ วีพีเอ็น

- สามารถขยายการเชื่อมต่อเครือข่ายได้แม้ว่าเครือข่ายนั้นจะอยู่สถานที่ต่างกัน
- มีความยืดหยุ่นสูงเพราะสามารถใช้ วีพีเอ็น ที่ใดก็ได้ และยังสามารถขยาย แบนด์วิดธ์ในการใช้งานได้ง่ายดาย โดยเฉพาะในการทำ รีโมทแอคเซส ให้ผู้ใช้ติดต่อเข้ามาใช้งานเครือข่ายได้จากสถานที่อื่น
- สามารถเชื่อมโยงเครือข่ายและแลกเปลี่ยนข้อมูลออกภายนอกองค์กรได้อย่างปลอดภัย โดยใช้มาตรการระบบเปิดและมีการเข้ารหัสข้อมูลก่อนการส่งข้อมูลทุกครั้ง
- สามารถลดค่าใช้จ่ายในการเชื่อมต่อ ง่ายต่อการดูแลรักษาการใช้งานและการเชื่อมต่อ

ข้อเสียของระบบ วีพีเอ็น

- ไม่สามารถที่จะควบคุมความเร็ว การเข้าถึงและคุณภาพของ วีพีเอ็น ได้ เนื่องจากวีพีเอ็นทำงานอยู่บนเครือข่ายอินเทอร์เน็ตซึ่งเป็นเรื่องที่อยู่เหนือการควบคุมของผู้ดูแล
- วีพีเอ็น ยังถือว่าเป็นเทคโนโลยีที่ค่อนข้างใหม่สำหรับประเทศไทยและมีความหลากหลายต่างกันตามผู้ผลิตแต่ละราย ฉะนั้นจึงยังไม่มีมาตรฐานที่สามารถใช้ร่วมกันได้แพร่หลาย
- วีพีเอ็น บางประเภทต้องอาศัยความสามารถของอุปกรณ์เสริมเพื่อช่วยในการเข้ารหัสและต้องมีการอัพเกรดประสิทธิภาพ

2.14 เคลียร์โอเอส (ClearOS)

เป็นซอฟท์แวร์ที่เป็นโอเพ่นซอร์ส ที่มีความสามารถในการบริการเกทเวย์, ไดเรคทอรี่เซอร์วิส อย่างครบถ้วน ด้วยการที่เป็น โอเพ่นซอร์ส นั้นการติดตั้งและบริหารระบบ จึงสามารถทำเองโดยยูสเซอร์ส่วนการซัพพอร์ทโดยตรงจาก เคลียร์โอเอส จะสามารถทำได้โดยซื้อซัพพอร์ท, ไลเซนซ์ เพิ่มเติมได้ เคลียร์โอเอส สามารถทำไฟร์วอลล์, พร็อกซี, ไอดีพี, เว็บฟิลเตอร์ริ่ง, มัลติแวน, แบนด์วิดธ์เชปปิ้ง, แอลดีเอพี, เมลเซิร์ฟเวอร์, เว็บ เซิร์ฟเวอร์, วินโดวส์ ไฟล์แชร์ริ่ง และยังมีคุณสมบัติอื่นๆ ในการทำให้เป็น เกทเวย์ เซิร์ฟเวอร์ อย่างดีเยี่ยม โดยในที่นี้จะอธิบายแค่ที่ใช้ในงานนี้เท่านั้น

2.14.1 IP Setting

1.) เอ็กซ์เทอร์น่อล เป็นการตั้งค่าตัวที่เป็นการเชื่อมต่อสู่อินเทอร์เน็ต โดยมีการตั้งค่า ไอพีแอดเดรสโฮสต์ และ เกทเวย์

2.) แลน เป็นการตั้งค่า ไอพีแอดเดรสของเครื่องตามปกติ

3.) ฮอทแลน (Hot LAN) จะอนุญาตให้มีการแยกเน็ตเวิร์คสำหรับ untrusted system โดยทั่วไปแล้วฮอตแลนจะใช้สำหรับ

- เซิร์ฟเวอร์ ที่ต้องมีการเชื่อมต่อกับอินเทอร์เน็ต (เว็บเซิร์ฟเวอร์, เมลเซิร์ฟเวอร์)
- เครื่องข่ายของแขก
- ไวร์เลสเน็ตเวิร์ค

ฮอตแลนนั้นจะสามารถเข้าสู่อินเทอร์เน็ตแต่ไม่สามารถเข้าสู่ระบบใดๆที่อยู่บน แลนได้ ตัวอย่างเช่น ฮอตแลนที่ถูกตั้งค่าในห้องมีตติ้งของบริษัท ซึ่งจะสามารถถูกใช้งานจากผู้ที่ไม่ได้เป็นพนักงานได้ ผู้ใช้ที่อยู่ในมีตติ้งรูมจะสามารถเข้าสู่ อินเทอร์เน็ตได้ แต่ไม่สามารถเข้าสู่ แลนเน็ตเวิร์ค ได้

4.) ดีเอ็มซี (ดีเอ็มซี) ในเคลียร์โอเอสดีเอ็มซีนั้นจะถูกใช้จัดการปิดกั้น พับลิคอินเทอร์เน็ต ไอพีแอดเดรส ถ้าไม่ต้องการที่จะปิดกั้นพับลิคไอพีแอดเดรส ก็จะต้องใช้ฮอตแลน

2.14.2 ไฟร์วอลล์

1.) 1 to 1 เอ็นเอที เพื่อทำการแมพพับลิคไอพี กับ ไอพีที่อยู่ในวงแลนของเรา การอินสตอลสามารถทำที่ มาร์เก็ตเพลซ (market place)

การตั้งค่า

เราสามารถตั้งค่า 1 to 1 เอ็นเอที ได้ 2 แบบ คือ

- แบบไม่มีไฟร์วอลล์
- แบบเลือกเปิดพอร์ต

แบบไม่มี ไฟร์วอลล์

บาง โปรโตคอลที่อยู่หลังไฟร์วอลล์ จะมีความละเอียดอ่อนเป็นอย่างมาก ในการที่จะทำการตั้งค่า 1 to 1 เอ็นเอทีแบบไม่มีไฟร์วอลล์ (ต้องมีความมั่นใจว่าได้ทำการรักษาความปลอดภัยระบบแลนที่ต้องการในทางอื่นด้วย)

แบบเลือกเปิดพอร์ต

ถ้าต้องการจะทำการแมพเฉพาะพอร์ตที่เลือก ตัวอย่างเช่น ทีซีพีพอร์ต80 เว็บเซิร์ฟเวอร์พอร์ตจะสามารถตั้งค่าพอร์ตได้จากการ map 1 to 1 เอ็นเอที

2.) ดีเอ็มซี ไฟร์วอลล์ ใช้สำหรับป้องกันเครือข่ายที่แยกกันของ พับลิคไอพีแอดเดรส โดยทั่วไปเน็ตเวิร์คการ์ด ที่3จะใช้เป็น ดีเอ็มซี เน็ตเวิร์ค โดยเฉพาะ

การจัดการกับเน็ตเวิร์คขาเข้า

โดยปกติแล้วการเชื่อมต่อที่เข้ามาจาก อินเทอร์เน็ต ทั้งหมดสู่ ดีเอ็มซี จะถูกปิดกั้น (มีข้อยกเว้นสำหรับ ping โปรโตคอล) โดยจะสามารถอนุญาตการเชื่อมต่อสู่ระบบบน ดีเอ็มซี โดยอนุญาต

- ทุกพอร์ต และ ทุกโปรโตคอล บนไอพีแอดเดรสหนึ่ง
- ทุกพอร์ต และ ทุกโปรโตคอล บนทั้งเครือข่ายของพับลิค IP
- บางพอร์ต และ บางโปรโตคอล บนไอพีแอดเดรสหนึ่ง

Pinhole Connection (DMZ to LAN)

ในบางสถานการณ์ที่ต้องการจะอนุญาตเฉพาะบางเครือข่ายจากดีเอ็มซีไปสู่แลน สามารถใช้กฎพินโฮลล์ ตัวอย่าง เรามีระบบการจัดการเอกสารที่ทำงานบน พอร์ต 2401 ที่อยู่บน แลน เราต้องการอนุญาตเว็บเซิร์ฟเวอร์ที่อยู่ในดีเอ็มซีของเรา ให้เข้าถึงระบบการจัดการเอกสารเราจึงทำพินโฮลล์ เพื่อใช้งาน

3.) อีเกรสไฟร์วอลล์ (egress firewall) เป็น ไฟร์วอลล์ขาออก ที่อนุญาตให้ทำการปิดกั้น หรือ อนุญาตการออกไปสู่เน็ตเวิร์คภายนอก

ประโยชน์ของเอาท์โกอิ้งไฟร์วอลล์ คือการปิดกั้น หรือ อนุญาตการส่งข้อความ , แชท , การดาวน์โหลด และอื่นๆ โดยสามารถใช้การปิดกั้นโดย โปรโตคอลฟิลเตอร์ โดยจะสามารถปิดกั้นได้2ทาง คือ จากเดสทิเนชั่นพอร์ต และ เดสทิเนชั่นไอพีแอดเดรส

โดยจะมีเอาท์โกอิ้ง โหมด อยู่ 2 โหมด คือ 1. อนุญาตทุกทราฟฟิคที่ออกสู่ข้างนอก และปิดกั้นบางทราฟฟิค เฉพาะ ที่ออกสู่ข้างนอก 2. ปิดกั้นทุกทราฟฟิคที่ออกสู่ข้างนอก และ อนุญาตบางทราฟฟิคที่ออกสู่ข้างนอก

4.) อินคัมมิ่ง ไฟร์วอลล์ (Incoming Firewall) จะใช้สำหรับ 2 วัตถุประสงค์หลักคือ

- เพื่ออนุญาตการเชื่อมต่อจากภายนอก (อินเทอร์เน็ต) สู่ระบบ เคลียร์โอเอส
- สำหรับปิดกั้น ไอพีแอดเดรส เฉพาะ หรือ ทั้งเครือข่ายจากการเข้าสู่ระบบ อย่างถาวร

การตั้งค่า

Incoming connections

เมื่อไฟร์วอลล์ทำงานบนเคลียร์โอเอสซิสเทม โดยพื้นฐานแล้วจะทำการปิดกั้น ทราฟฟิคภายนอก (อินเทอร์เน็ต) ทั้งหมด แต่ถ้ามีการวางแผนที่จะทำการใช้งานบริการของระบบ เคลียร์โอเอส ที่สามารถเข้าใช้งานจากอินเทอร์เน็ตได้ จะต้องทำการเพิ่มนโยบายไฟร์วอลล์ เพื่อให้ทำงานด้วย ตัวอย่างเช่น โอเพ่นวีพีเอ็นเซิร์ฟเวอร์ที่ต้องการให้เปิดยูดีพีพอร์ต 1194 บน ไฟร์วอลล์

2.14.3 Intrusion Protection

1.) อินทรูชั่นดีเทคชั่น เป็นซอร์ฟแวร์ที่มีเพื่อทำให้ผู้ใช้มีการระวังบางทราฟฟิคที่มุ่งร้าย ที่สามารถผ่านโดยการเชื่อมต่ออินเทอร์เน็ต โดยตัวซอร์ฟแวร์นี้สามารถตรวจจับ และ รายงานเครือข่ายที่ผิดปกติ รวมถึงที่พยายามจะพังเข้ามา และ โทรจัน , ไวรัส บนเครือข่าย และการสแกนพอร์ต

จะมีกฎ 2 ชนิดสำหรับอินทรูชั่นดีเทคชั่น คือ ซีเคียวริตี้รูลล์ จะทำการตรวจจับปัญหาที่เกี่ยวกับทั้งระบบรักษาความปลอดภัย และ โพลิซีรูลล์ จะทำการตรวจจับปัญหาที่เกี่ยวกับนโยบายการใช้งานอินเทอร์เน็ตขององค์กร

2.) อินทรูชั่นโพรเทคชั่น จะทำการปิดกั้นผู้โจมตีจากเครือข่าย และ ระบบ

2.15 Proxy

เป็นบ่อเก็บข้อมูลตรงกลาง เวลาที่จะโหลดข้อมูลจากอินเทอร์เน็ต จะต้องมาที่พร็อกซี่ก่อนแล้วเราก็จะไปโหลดมาจากพร็อกซี่อีกทีโดยจะมีประโยชน์คือ ถ้าคนที่ต่ออินเทอร์เน็ตในที่เดียวกันใช้พร็อกซี่เดียวกัน สมมติว่าคนที่ใช้พร็อกซี่เดียวกันเข้าเว็บไซต์เดียวกัน เมื่อมีผู้ใช้มาโหลดทีหลังจะมีการโหลดได้เร็วขึ้น ประหยัดสายข้อมูล ทำให้ไม่ต้องโหลด ข้อมูลซ้ำซ้อนครับ

พร็อกซี่มี 3 ประเภทใหญ่ๆ

2.15.1 Transparent

เมื่อมีการรีเควสข้อมูลจากต้นทางซึ่งโดยปกติต้องมีการกำหนดพร็อกซี่ที่เราต้องการจะใช้งานถึงจะ รีเควสข้อมูลที่เราต้องการผ่านทางพร็อกซี่ที่เรากำหนด แต่ในปัจจุบันทางฝ่ายไอทีทั้งหลายได้นำไฟร์วอลล์ หรือ เราท์เตอร์มาขวางก่อนที่จะเข้าสู่เกทเวย์ทำให้ข้อมูลที่จะถูกส่งไปยังต้นทาง ที่เรารีเควส นั้น ต้องมาผ่านพร็อกซี่เซิฟเวอร์ก่อน ซึ่งผู้ใช้งานส่วนมากจะไม่จำเป็นต้องทำการตั้งค่า อะไรเพิ่มเติม เนื่องจากเราท์เตอร์ และ ไฟร์วอลล์ เป็นตัวจัดการตรงนี้ให้แทนแล้ว โดยมีการทำรีไดเรคชั่นของ แพคเกจ ทั้งหมดไปยัง พร็อกซี่เซิฟเวอร์

2.15.2 Anonymous

จะซ่อนไอพีแอดเดรสของเครื่องต้นทางจริง ๆ โดยการใช้งานจะเหมือนกับการใช้งานโดยใช้พร็อกซี่เอง และทำการซ่อนข้อมูลอื่นๆ (เฮดเดอร์) แต่ซ่อนไม่ทั้งหมด เพราะว่าตัวเฮดเดอร์จริงๆ ของเรายังอยู่ ประโยชน์ของการใช้พร็อกซี่แบบนี้ เช่น เราต้องการจะอ้างว่าเราอยู่ประเทศใดๆ ถ้าหากรา

ใช้งานตัวพร็อกซี่ของประเทศนั้น ๆ ก็เสมือนว่าใช้งานจากประเทศนั้นเลย แน่นอนมันก็จะช้ากว่าแบบแรก

2.15.3 High Anonimity

จะไม่เปิดเผยข้อมูลอะไรของเราเลย การทำงานคือตัวพร็อกซี่จะไปเรียกใช้งานที่ปลายทางให้เอง และได้ข้อมูลมาก็จะส่งมาให้เครื่องที่เรียกใช้งาน ดังนั้นการใช้งานก็จะเปรียบได้ว่าเครื่องพร็อกซี่ได้ทำการรีเควสไปเองเลย จะไม่มีข้อมูลอะไรของเราออกไปเลยประโยชน์ ใช้หลบซ่อนการโจมตีต่างๆ เพราะจะไม่รู้ที่มาของเครื่อง

2.15.4 Proxy Server

คือ การนำเครื่องคอมพิวเตอร์มาตั้งเพื่อให้บริการแก่กลุ่มผู้ใช้ที่อยู่ในบริเวณเดียวกัน และกำหนดให้ผู้ใช้ทุกคนเรียกใช้ข้อมูลเว็บไซต์ผ่านเครื่องคอมพิวเตอร์นี้ โดยเครื่องดังกล่าวจะมีการติดตั้งโปรแกรมเพื่อทำหน้าที่เรียกข้อมูลเว็บไซต์มาให้บริการแก่ผู้ใช้ และจัดเก็บข้อมูลที่เคยถูกเรียกนั้นไว้ในเครื่อง เพื่อให้บริการแก่ผู้ใช้ข้อมูลนั้นซ้ำ ได้ทันที โดยไม่ต้องเสียเวลาไปเรียกข้อมูลมาจากแหล่งข้อมูลใหม่อีก ซึ่งเทคนิคดังกล่าว จะทำให้ผู้ใช้สามารถเรียกใช้ข้อมูลที่(ส่วนใหญ่)เคยมีผู้เรียกใช้มาก่อนได้รวดเร็วขึ้นเป็นอย่างมาก เนื่องจากไม่ต้องเสียเวลาไปเรียกข้อมูลจากแหล่งข้อมูลใหม่ อันจะทำให้ประสิทธิภาพในการใช้งานระบบเครือข่ายอินเทอร์เน็ต เพิ่มขึ้นเป็นอย่างมาก

2.16 Configuration On ClearOS

จะบอกถึงวิธีการตั้งค่าส่วนของระบบต่างๆในเคลียร์โอเอสเพื่อให้ใช้งานได้ตามที่ต้องการ หรือเป็นไปตามนโยบายขององค์กร

2.16.1 OpenVPN

การตั้งค่า

Internet domain โดยปกติจะถูกใช้ตามค่าเริ่มต้นของชื่อเซิฟเวอร์โดเมนที่ถูกตั้งค่าใน ไอพี เซตติ้ง

DNS server คือ ดีเอนเอสเซิฟเวอร์ ที่จะใช้ในขณะที่เชื่อมต่อผ่านวีพีเอ็น การตั้งค่านี้จะมีประโยชน์มากถ้ามีการใช้เข้าถึง แอดเดรส/โฮสต์เนม ภายใน

WINS server (windows internet name service) คือ บริการชื่อ เน็ตไบออส (NetBIOS) ที่อนุญาตให้เครื่องคอมพิวเตอร์โคลเอนท์สามารถใช้งานชื่อเน็ตไบออส และ ไอพีแอดเดรส ใน ไดนามิค, ดิสทริบิวท์ดาต้าเบส (Distributed Database) และเพื่อแก้ไขชื่อเน็ตไบออส ของทรัพยากรเครือข่าย สำหรับไอพีแอดเดรสนั้น ถ้าหากมีไมโครซอร์ฟเซิฟเวอร์ (หรือเซิฟเวอร์ อื่นๆที่มีการทำงาน Samba) บน LAN โดยมีการใช้ WINS จะต้องทำการแก้ไข auto-configuration setting และเปลี่ยนเป็นไอพีที่มีการทำงานบริการนี้ แต่ถ้าหากมีการทำงาน Samba เป็นโลคอล ก็สามารถตั้งค่าเป็น auto-configuration ได้ และ ถ้าไม่ได้ใช้งาน Samba การตั้งค่านี้ก็จะไม่เกี่ยวข้องและถูกข้ามไป

2.16.2 Incoming Firewall

เมื่อมีการตั้งค่าไฟร์วอลล์บนระบบเคลียร์โอเอส โดยปกติแล้วจะทำงานโดยการปิดกั้นทุกการเชื่อมต่อที่มาจากภายนอก (internet) แต่ถ้ามีแผนการที่จะทำให้ระบบเคลียร์โอเอส นี้มีการเชื่อมต่อจากภายนอกได้ก็จะต้องมีการเพิ่มนโยบายที่ใช้ เช่น โอเพนวีพีเอ็นเซิฟเวอร์ ต้องมีการเปิด พอร์ต 1194 บนไฟร์วอลล์

มี 3 ทางที่จะเพิ่มกฎ incoming firewall

เลือกจากบริการทั่วไป

ใส่โปรโตคอล และ เลขพอร์ต

ใส่โปรโตคอล และ ช่วงพอร์ต

การปิดกั้นโฮสต์ภายนอก

ในบางสถานการณ์ต้องมีการป้องกันการรบกวนระบบที่เชื่อมต่อมายังระบบเคลียร์โอเอส ตัวอย่างเช่น มีการสังเกตเห็นทราฟฟิคไวรัสที่รบกวนจำนวนมาก จะทำการปิดกั้นทราฟฟิคนี้ได้โดยการระบุไอพีแอดเดรส หรือ เครือข่าย ลงใน Block External Hosts

2.16.3 Port Forwarding

ถ้ามีการใช้งานเซิฟเวอร์ ที่อยู่ข้างหลังเคลียร์โอเอสเกตเวย์เราสามารถใช้ port Forwarding สำหรับฟอร์เวิร์ดพอร์ตไปยังระบบที่อยู่บนโลคอลโดยจะสามารถทำได้ 3 ทาง

เลือกจากบริการทั่วไป

ใส่โปรโตคอล และ เลขพอร์ต

ใส่โปรโตคอล และ ช่วงพอร์ต

2.16.4 Web Proxy

Web Proxy ของเคลียร์โอเอส จะใช้งานsquid ซึ่งเป็น พร็อกซี่แคชชิ่งเซิฟเวอร์ (Proxy Caching Server) ที่มีประสิทธิภาพสูง สำหรับเว็บไคลเอนท์สนับสนุนโปรโตคอล เอชทีทีพี เอฟทีพี และ บางโปรโตคอลอื่นๆที่เป็นที่รู้จักน้อยลงมา ตัวซอร์ฟแวร์ไม่แค่ประหยัดแบนด์วิดธ์และเพิ่มเวลาการแอคเซซ แต่ยังให้ผู้ดูแลมีความสามารถในการแกะรอยการใช้งานเว็บผ่านรายงาน

การตั้งค่า

User Authentication ใช้สำหรับผู้ที่ต้องการใช้ ยูสเซอร์/พาสเวิร์ด ในการเข้าถึงเว็บ

Transparent Mode การร้องขอเว็บจากเครือข่ายโลคอลจะถูกส่งผ่านพร็อกซี่ โดยอัตโนมัติ

ข้อดี คือไม่ต้องมีการเปลี่ยนการตั้งค่าใดๆบนเวิร์คสเตชั่น

ข้อเสีย คือ HTTPS ไม่สามารถผ่านพร็อกซี่ ไปได้

โดยโหมดนี้จะใช้ได้กับเกตเวย์โหมดเท่านั้น

Performance Level จะระบุขนาดของเครือข่ายที่ระบบของคุณสามารถรองรับได้

การตั้งค่าแคช

Maximum cache size ขนาดบนฮาร์ดดิสก์ที่มากที่สุดที่จะใช้เป็นพร็อกซี่เซิฟเวอร์แคช

Maximum object size ไฟล์ใดๆที่มากกว่า maximum object size จะผ่านพร็อกซี่ แต่จะไม่ถูกเก็บไว้ในแคช ไฟล์ขนาดใหญ่ (เช่นไฟล์หนัง) สามารถใช้พื้นที่ของพร็อกซี่แคชอย่างมาก เช่นถ้าใช้แคชขนาด 2gb และมีคน2คนดาวน์โหลดไฟล์ขนาด 1gb ในเวลาเดียวกัน 2ไฟล์นี้ก็จะแทนที่ทุกอย่างในแคช

Maximum download file size ถ้าต้องการที่จะจำกัดการดาวน์โหลดไฟล์ขนาดใหญ่ ให้กำหนดค่านี้ จะทำให้ไฟล์ที่ขนาดเกินจะถูกปิดกั้น

2.16.5 Content Filter

ทำการปิดกั้นเว็บไซต์ที่ไม่เหมาะสมจากผู้ใช้งานรวมถึงสามารถใช้บังคับให้เป็นไปตามนโยบายขององค์กร

Global Setting จะเป็นการตั้งค่าที่ใช้งานกับทุกผู้ใช้งาน โดยไม่คำนึงถึงกลุ่มของ content filter ที่ถูกใช้งานกับ user browsing website จาก LAN ในความเป็นจริง การตั้งค่านี้มีเพื่อแบนเครื่องมือบน LAN จากการใช้งานพร็อกซี่/คอนเทนท์ฟิลเตอร์โดยเครื่องมือจะถูกระบุด้วยไอพีต้นทาง

Group Policies จะอนุญาตให้ผู้ดูแลระบบปรับการใช้งานนโยบายให้กับผู้ใช้งานที่แตกต่างกัน ด้วยการสร้างและตั้งค่ากลุ่มนโยบายและทำการเพิ่มผู้ใช้งาน เข้ามายังกรุ๊ปตามคำสั่งและนโยบายที่ถูกบังคับตามการใช้งาน

Adding a Group Policies กดเพิ่มกลุ่มนโยบายที่ปุ่ม add และตั้งชื่อของกลุ่มนโยบาย

Editing a Group Policies หลังจากที่เพิ่ม กลุ่มนโยบายให้คลิกที่ configure policy เพื่อปรับการตั้งค่า โดยจะมีหลายหัวข้อให้ปรับค่าดังนี้

General Setting

Sensitivity Level เป็นการอนุญาตให้ปรับ phrase filter sensitivity การเพิ่มระดับ sensitivity ทำให้ยิ่งมีเว็บไซต์ที่มีคำต้องห้ามน้อยๆ อาจจะทำให้ถูกปิดกั้นด้วย

PICS Level มาตรฐานของอินเตอร์เน็ตที่ให้คะแนนเนื้อหาเว็บไซต์การตั้งค่าจะพิสูจน์ความสำคัญของเว็บไซต์รองลงมาเหมือนกับเว็บไซต์ที่ดูแลตัวเอง โดยทั่วไปแล้ว จะแนะนำให้ไม่เปิดใช้งาน

Reporting Level มีหลายตัวเลือกที่ปรับให้ผู้ใช้งาน เห็นเมื่อมีการปิดกั้นหน้าไซต์

- Stealth Mode – เว็บไซต์ไม่ถูกปิดกั้น แต่ไอพีผู้ใช้งาน กับ เว็บไซต์ จะถูกล็อก
- Access denied – user browser จะขึ้นว่า Access denied
- Short report – ข้อความผิดพลาด สั้นๆจะถูกแสดง
- Full report – เหมือน short report แต่ค่าน้ำหนักที่จำกัดจะถูกแสดง
- Custom report – ใช้ HTML เพื่อสร้างเทมเพลทขึ้นมาเอง

Blocked IP Domains ใช้ป้องกันผู้ใช้งานจากการตรวจสอบหา URL-based ของ filter โดยใช้ IP address แทน URL

Blanket Block การตั้งค่าที่มีขอบเขตมากที่สุด ทุกเว็บไซต์จะถูกปิดกั้นด้วยข้อยกเว้นในรายการของพวกนี้ใน exempt list มีประโยชน์สำหรับที่สาธารณะที่ใช้สำหรับเข้าถึงเว็บไซต์ของบริษัท

2.16.6 Web Access Control

จะอนุญาตให้ผู้ดูแลระบบบังคับเวลาในวันสำหรับการเข้าถึงเว็บไซต์ของผู้ใช้งาน ด้วยเว็บพร็อกซี่

Adding Access Control Lists จำนวนของ ACL สามารถถูกสร้างได้อย่างไม่จำกัดเพื่อกำหนดให้ผู้ใช้งานบน LAN ทำให้เข้าสู่เว็บไซต์ผ่านพร็อกซี่เซิร์ฟเวอร์ซึ่งมีการตั้งค่าในส่วนต่างๆดังนี้

Name ชื่อที่ใช้ระบุ access control

ACL Type ให้เป็น allow , deny

Time of Day ACL อ้างอิงจาก time of day rule ที่ได้ทำการสร้างขึ้นมา

Restriction กำหนดว่า ACL rule จะใช้กับช่วงเวลาที่กำหนดขึ้นมา หรือทุกเวลาที่นอกเหนือจากช่วงเวลาที่สร้างขึ้นมา

Method of identification ขึ้นอยู่กับการตั้งค่าของพร็อกซี่ มี 3 วิธีการที่แตกต่างกันที่ใช้ระบุถึงตัวตนของผู้ใช้

username สามารถใช้งานได้ถ้ามีการ authentication

ip address สำหรับจำกัดการใช้งานของคอมพิวเตอร์บางเครื่อง ใช้เป็นไอพีแอดเดรส หรือ ช่วงของ ไอพีแอดเดรส ในการกำหนด

MAC address ใช้สำหรับระบุเจาะจงเฉพาะไปยัง MAC address

ACL Priority

ACL rules ใหม่ๆ จะถูกเพิ่มไปยังล่างสุดของรายการ ซึ่งก็หมายถึงมี priority ต่ำสุดพร็อกซี่จะทำการวิเคราะห์ไปอย่างเป็นลำดับ

2.16.7 Intrusion Detection

IDS ของเคลียร์ จะใช้เป็น snort ซึ่งมีไว้เพื่อให้ผู้ใช้ได้มีการระวังบางทราฟฟิคประจำวันที่ไม่เป็นมิตรที่ผ่านมาทางการเชื่อมต่ออินเทอร์เน็ต โดยจะสามารถตรวจสอบและรายงานทราฟฟิคเครือข่ายที่มีความผิดปกติ ,พยายามจะบุกเข้ามา ,ไวรัส ,โทรจัน บนเครือข่าย และการสแกนพอร์ต

Security and Policy Rules

มีสองชนิดที่แตกต่างกันของ rule ของระบบไอดีเอส

Security Rules จะตรวจสอบประเด็นที่เกี่ยวข้องกับทั้งระบบรักษาความปลอดภัย

Policy Rules จะตรวจสอบประเด็นที่เกี่ยวข้องกับนโยบายการใช้งานอินเทอร์เน็ต ขององค์กร เช่น chat policy rules จะตรวจสอบข้อความโต้ตอบที่ผ่าน ระบบเคลียร์โอเอส

2.16.8 Intrusion Prevention

ระบบ IPS จะแสดงรายการของ IP address ที่ได้รับการปิดกั้นเนื่องจากทราฟฟิคเครือข่ายที่ไม่เหมาะสม

Description

SID หมายถึง IDS ID ที่มีการเรียกการปิดกั้นนี่เป็นการเชื่อมโยงเพื่อที่จะเปิดเผยข้อมูลที่มากขึ้นเกี่ยวกับเงื่อนไขเฉพาะที่ตรงกัน

Blocked IP คือ IP address ที่มีการเรียกการปิดกั้น ถ้าไอพีแอดเดรสนี้ไม่ควรจะถูกปิดกั้น ก็สามารถเพิ่มในรายการที่จะไม่ปิดกั้นด้วย whitelist

Date/Time คือวันและเวลาที่การปิดกั้นเกิดขึ้น

Time Remaining จะระบุเวลาการปิดกั้นที่เหลืออยู่ ซึ่งจะยกเลิกการปิดกั้นเมื่อเป็น 0

Action โฮสต์ที่ถูกปิดกั้นสามารถเพิ่มไปที่ whitelist เพื่อที่จะไม่ทำการปิดกั้นอีกในอนาคต โดยจะสามารถลบการปิดกั้นโฮสต์ด้วยคำสั่ง delete

Whitelist สำหรับใส่ไอพีแอดเดรสที่จะไม่ทำการปิดกั้น

2.16.9 Gateway Antiphishing

เพื่อป้องกัน users จากการถูก phishing และ scam ข้อความที่พยายามจะดึงหรือสอบถาม sensitive information เช่น เลขบัตรเครดิต พาสเวิร์ด ข้อมูลส่วนตัว

การตั้งค่าส่วนใหญ่ของ antiphishing จะเป็นการปรับแต่งบางนโยบายที่เครือข่ายต้องการ โดยส่วนใหญ่จะปรับเป็น enable ทั้งหมด

Signature Engine - antiphishing signature จะถูกใช้และบำรุงรักษาด้วยระบบ ClearOS ควรจะพิจารณาที่จะปรับเป็น disable ก็เมื่อที่ยากที่จะหาเหตุการณ์ false positive

Heuristic Engine - antiphishing engine จะใช้ algorithm เบื้องต้นในการตรวจสอบการพยายาม phishing แม้ว่าบางครั้งจะทำให้เกิด false positive แต่ก็แนะนำให้ตัวเลือกนี้เป็น enable

Block SSL Mismatch - การโจมตี phishing ทั่วๆไปจะใช้เว็บแอดเดรสที่ไม่มีความปลอดภัยใช้ดำเนินการโจมตี แต่ว่าแสดงเว็บแอดเดรสให้กับผู้ใช้งาน ว่าเป็น secure/SSL address ด้วยการเปิดส่วนนี้ตัว antiphishing จะตรวจสอบเจอเทคนิคนี้ และ ปฏิเสธ

Block Cloaked URLs - บาง scammer จะใช้การเข้ารหัสเว็บแอดเดรสและพยายามที่จะหลอกลวงผู้ใช้งาน ดังนั้น URLs ใดๆ ที่มีลักษณะของการเข้ารหัส จะถูกปิดกั้นด้วยตัวเลือกนี้

2.16.10 Gateway Antivirus

ใช้ป้องกันเครือข่ายจากไวรัส โดยเป็นระบบที่ใช้โดยส่วนต่างๆของระบบเคลียร์โอเอสโดยเคลียร์โอเอสจะใช้งาน Clamav เป็นแอนตี้ไวรัส โดยซอร์ฟแวร์จะทำการตรวจสอบอัพเดทหลายครั้งในวันหนึ่งสำหรับแอนตี้ไวรัสซิกเนเจอร์ (Antivirus Signature) ใหม่ๆ

การตั้งค่า

Block Encrypted Files - ไฟล์บางรูปแบบ รวมถึง zip ไฟล์ จะมีการเข้ารหัส และ ใช้รหัสผ่านป้องกัน ระบบแอนตี้ไวรัส จะไม่สามารถสแกนไฟล์ที่ถูกป้องกันโดยรหัสผ่านเหล่านี้ได้ โดยเมื่อมีผู้เขียนไวรัสหลายคนใช้เทคนิคนี้ในการส่งข้ามการตรวจสอบไวรัส จึงต้องมีการตั้งค่าให้ปิดกั้นไฟล์ที่มีการเข้ารหัส

Maximun Files in Zip Files - เมื่อระบบแอนตี้ไวรัสทำการแกะไฟล์ที่ถูกบีบอัด (zip files) จะแนะนำให้มีการจำกัดจำนวนไฟล์เพื่อป้องกันระบบจากการโจมตี denial of service ด้วยเหตุผลนี้จึงไม่แนะนำให้ตั้งค่าเป็น unlimited

Maximum File Size in Zip Files - ไฟล์ไวรัสส่วนใหญ่จะถูกส่งเป็นไฟล์ขนาดเล็กเพื่อที่จะรักษาทรัพยากรของระบบ ไฟล์ใดที่มีขนาดเกินที่จำกัดไว้ จะไม่มีการตรวจสอบหาไวรัส

Maximum Recursion in Zip Files - zip file สามารถบรรจุ zip file ได้ เทคนิคในการบรรจุ zip file หลายๆเลเยอร์ นี้จะสามารถใช้เพื่อสร้าง DoS attack ได้ กำหนดส่วนนี้ให้เป็น default จนกว่าจะมีความต้องการที่ผิดจากปกติ

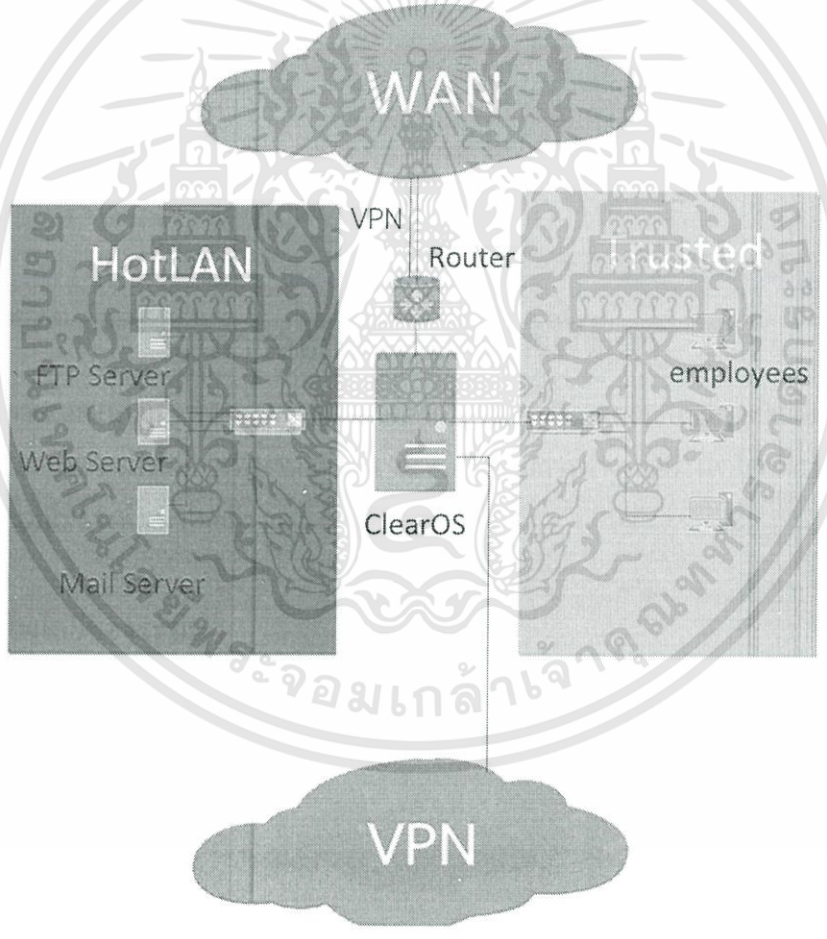
Update Interval - open source antivirus ของเคลียร์โอเอส นี้จะตรวจสอบการอัพเดทไวรัสซิกเนเจอร์ (Virus Signature) ใหม่ๆในช่วงเวลาปกติ ยกเว้นระบบที่มีการทำงานอยู่มีการเชื่อมต่ออินเทอร์เน็ต ที่ช้า โดยควรจะตั้งค่าเป็น minimum

บทที่3

การออกแบบและการพัฒนา

การออกแบบและพัฒนาระบบเป็นขั้นตอนที่วางโครงสร้างของระบบว่าจะมีส่วนประกอบอะไรบ้าง และแต่ละส่วนมีการทำงานอย่างไร และมีขั้นตอนการทำงานอย่างไร โดยมีการใช้เครื่องมือต่างๆ มาช่วยในการพัฒนาโดยมีรายละเอียดดังต่อไปนี้

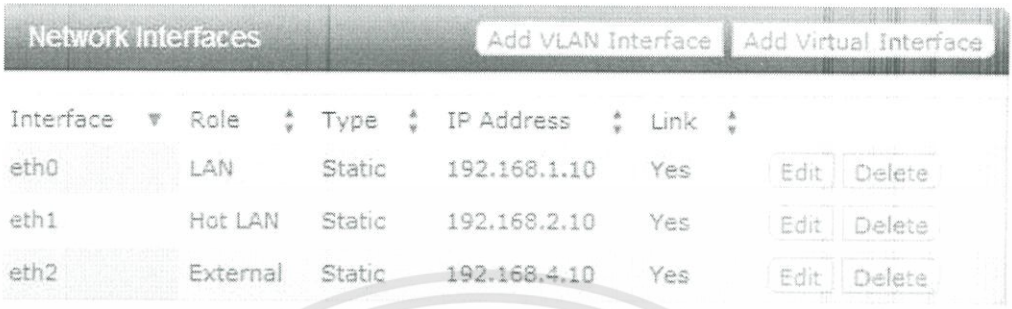
3.1 โทโพโลยีของระบบ



มีการวางการทำงานของส่วนต่างๆของเครือข่ายดังนี้

รูปที่ 3.1 โทโพโลยีของระบบ3.2 การตั้งค่าไอพีแอดเดรส

เคลียร์โอเอส มีการคอนฟิก ไอพีแอดเดรส ของแต่ละ เน็ตเวิร์ค อินเตอร์เฟซ ดังนี้



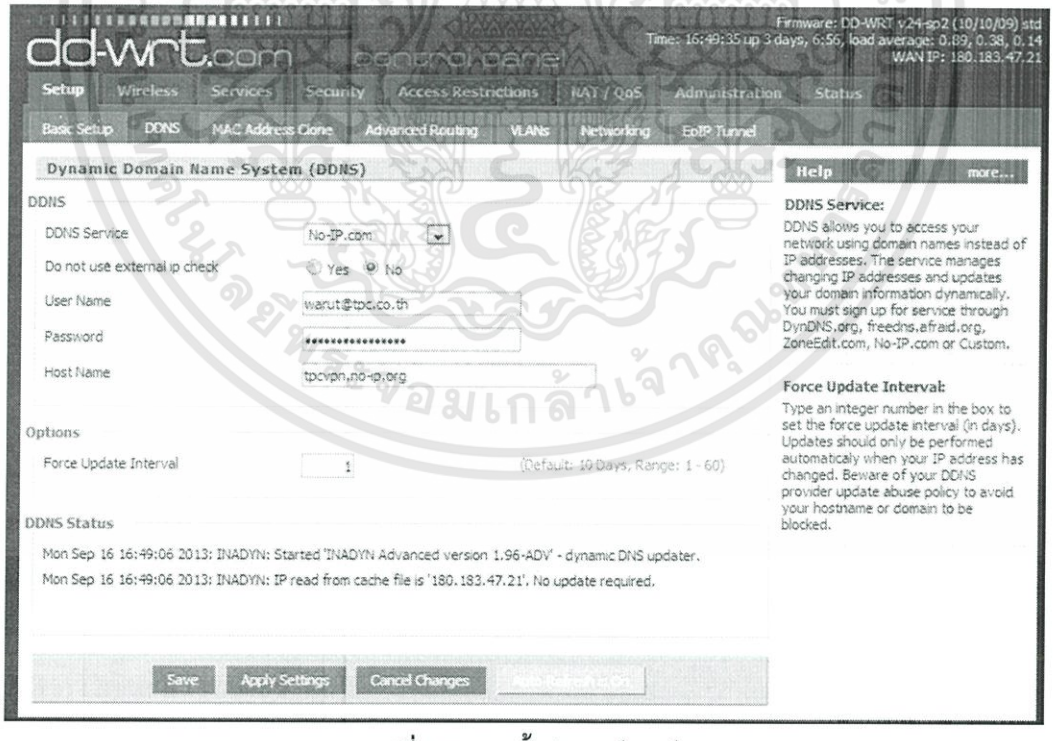
รูปที่ 3.2 การตั้งค่าไอพีแอดเดรส

แลน (trusted zone) – เน็ตเวิร์ค แอดเดรส 192.168.1.0 /24

ฮอตแลน – เน็ตเวิร์ค แอดเดรส 192.168.2.0 /24

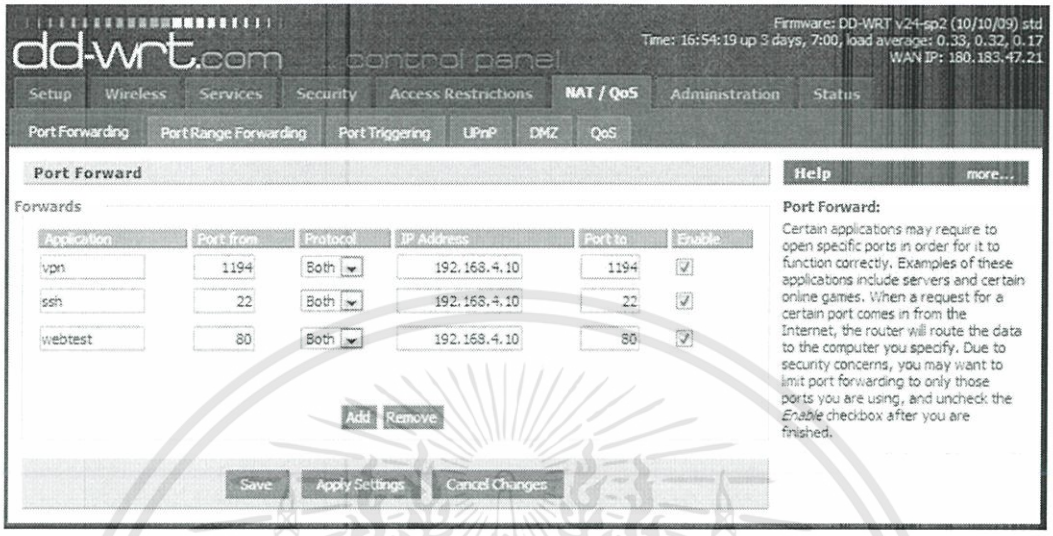
เอ็กซ์เทอร์นอล – เน็ตเวิร์ค แอดเดรส 192.168.4.0 /24

3.3 การตั้งค่าเราท์เตอร์



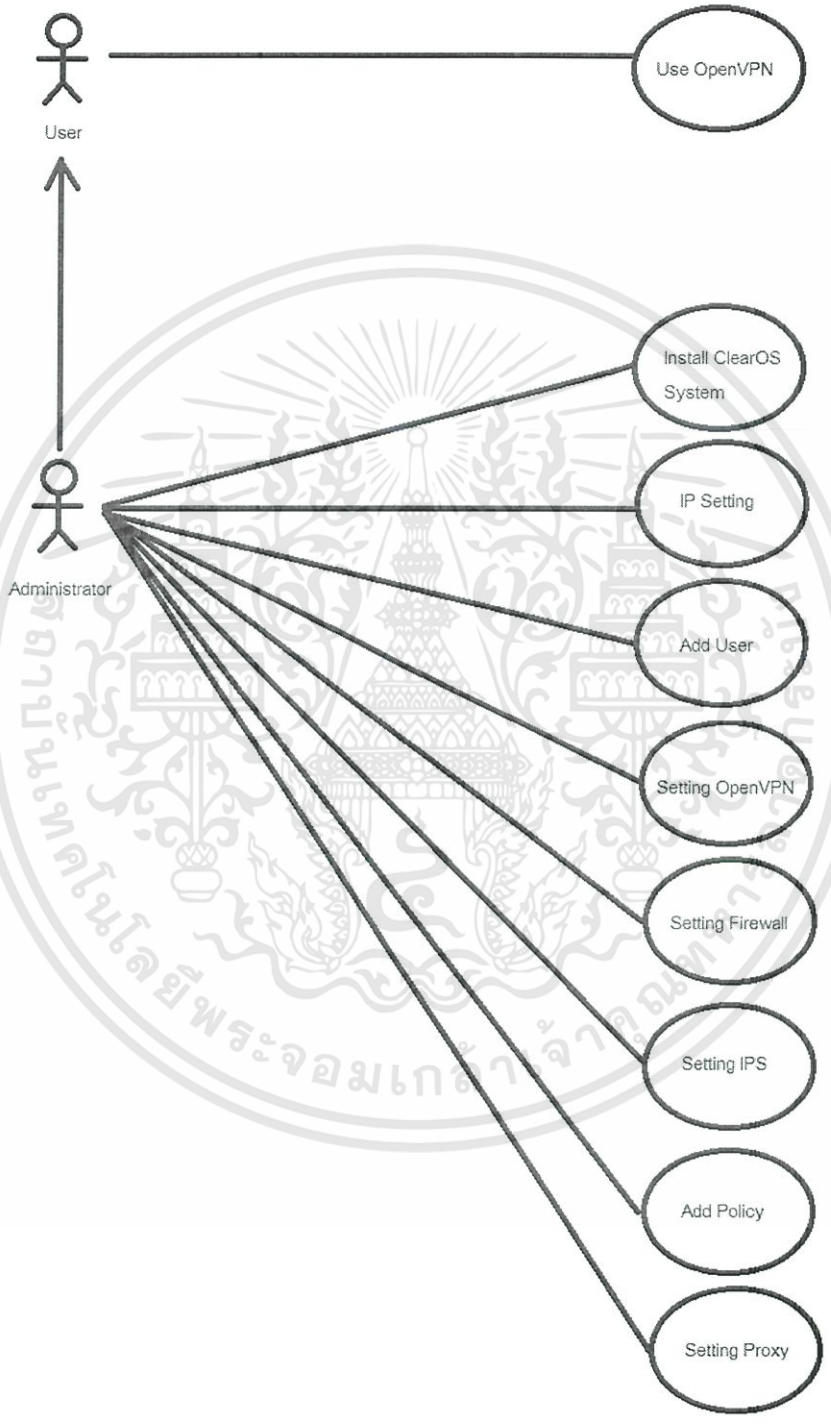
รูปที่ 3.3 การตั้งค่าเราท์เตอร์

เราท์เตอร์ มีการเซ็ท พอร์ต ฟอร์เวิร์ดดิ้ง เพื่อ ฟอร์เวิร์ด พอร์ต ไปที่เครื่อง เคลียร์โอเอส สำหรับผู้ใช้งาน ที่ รีเควสเข้ามาจาก อินเทอร์เน็ต



รูปที่ 3.4 การตั้งค่าฟอร์เวิร์ดพอร์ต

3.4 ยูสเคสไดอะแกรม (Use Case Diagram)



รูปที่ 3.4 use case diagram

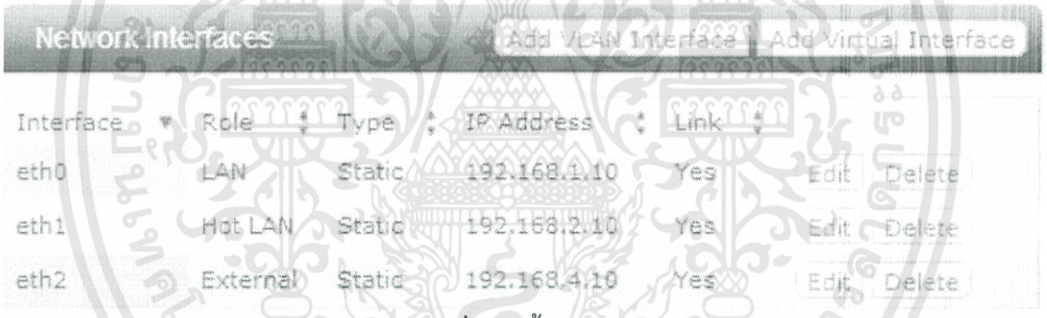
โดยผู้ดูแลระบบ จะสามารถทำการติดตั้งระบบเคลียร์โอเอสและตั้งค่าระบบต่างๆที่อยู่ในเคลียร์โอเอสได้ เริ่มจากตั้งค่า IP Setting ตั้งค่า OpenVPN Firewall IDS/IPS Proxy และทำการกำหนดให้เป็นไปตามนโยบายขององค์กร หลังจากนั้นจึงทำการเพิ่มผู้ใช้งานที่จะทำการอนุญาตให้สามารถใช้งาน OpenVPN ในการเข้ามาใช้งานทรัพยากรเครือข่ายที่อยู่ภายในองค์กรได้

และฝั่งผู้ใช้งานก็สามารถเข้าใช้งาน OpenVPN ได้โดยการดาวน์โหลดเซอร์ทิฟิเคทก่อน

บทที่ 4
การทดลองและผลการทดลอง

ในส่วนของบทนี้จะมีเนื้อหาเกี่ยวกับการตั้งค่าและการทำงานของระบบตั้งแต่ที่ทำให้ทุกโซนในเครือข่ายสามารถติดต่อหากันได้ และ สามารถปิดกั้นการเชื่อมต่อจากเครือข่ายโซนนึงไปยังอีกโซนนึง หรือ สามารถอนุญาตทราฟฟิคโฟลว์ให้ผ่านไปได้ ด้วยรูลล์เซ็ตของไฟร์วอล และรวมถึงการทำวีพีเอ็นเพื่อทำให้ผู้ดูแลระบบ หรือผู้ได้รับอนุญาตจากผู้ดูแลระบบ ให้สามารถเข้ามาใช้งานตั้งค่าระบบจากภายนอกองค์กรได้ โดยมีความปลอดภัย โดยจะสามารถทำการตั้งค่าดังต่อไปนี้ได้ หลังจากทำการติดตั้ง เคลียร์โอเอส ลงบนเครื่องที่ต้องการให้เป็นเซิร์ฟเวอร์ได้แล้ว

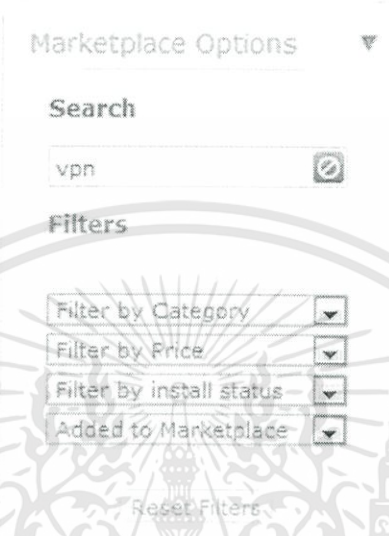
4.1 IP setting



รูปที่ 4.1 ตั้งค่าไอพี

4.2 การติดตั้งโอเพ่นวีพีเอ็นบนเคลียร์โอเอส

ทำการค้นหาด้วยคีย์เวิร์ดวีพีเอ็น



รูปที่ 4.2 ค้นหาโอเพ่นวีพีเอ็น

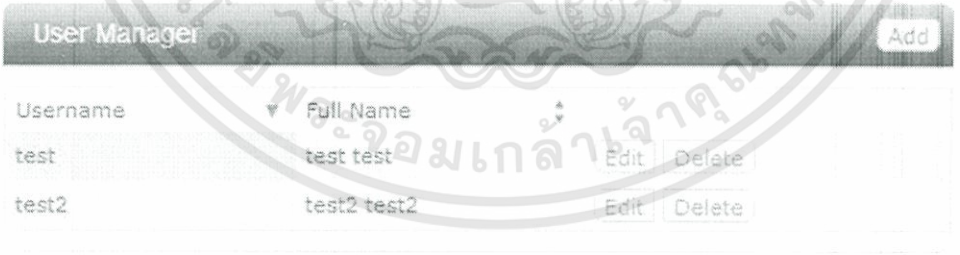
เลือกโอเพนวีพีเอ็นแล้วกดอินสตอลล์

รูปที่ 4.3 อินสตอลล์โอเพ่นวีพีเอ็น

4.3 การเพิ่มผู้ใช้งาน

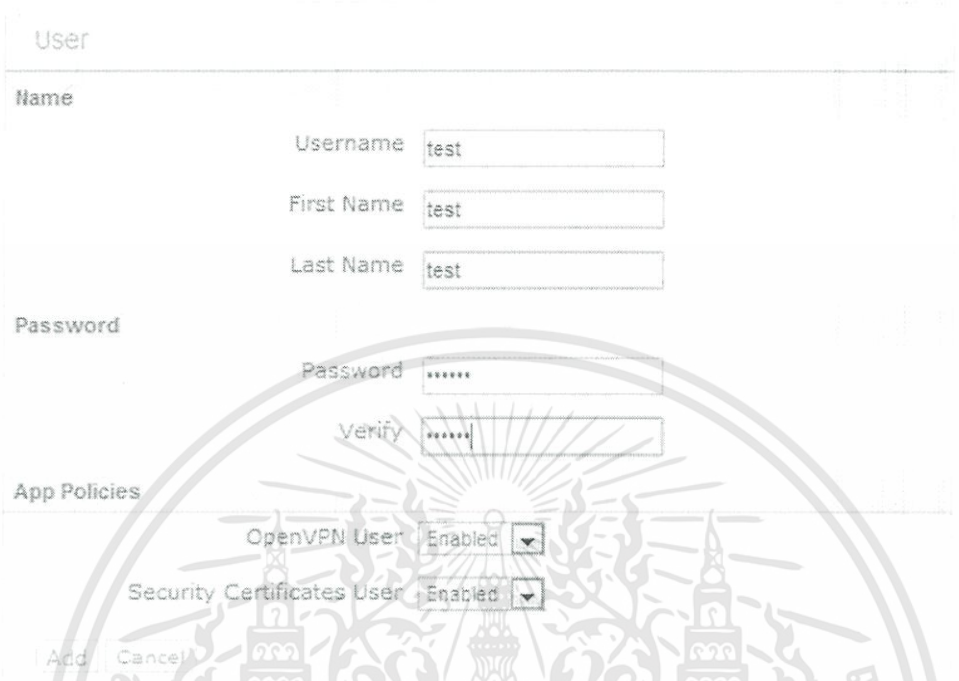
รูปที่ 4.4 เข้าหน้าจอยูสเซอร์

คลิกที่ยูสเซอร์และเลือกแอดยูสเซอร์ที่ยูสเซอร์เมเนเจอร์



รูปที่ 4.5 จัดการยูสเซอร์

ป้อน ยูสเซอร์เนม และ พาสเวิร์ด เลือก openvpn user และ Security Certificares User เป็น Enable แล้วกด add



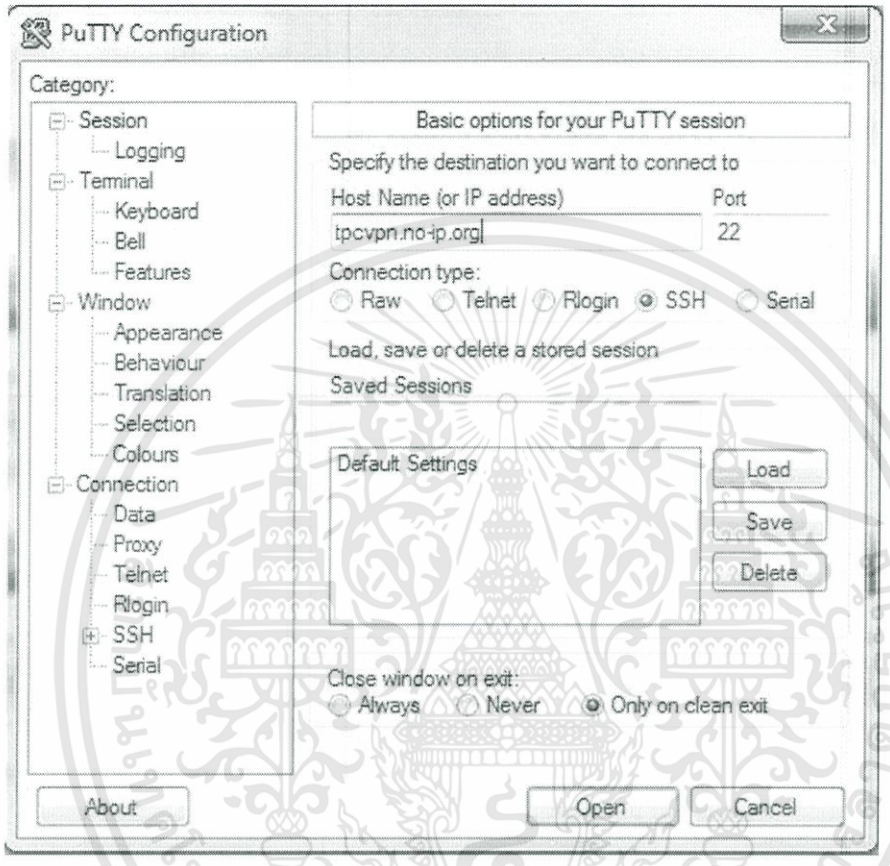
รูปที่ 4.6 เพิ่มยูสเซอร์

จะได้ User ที่เราเพิ่ง Add เข้ามาดังรูปข้างล่างนี้

รูปที่ 4.7 หน้าจอแสดงยูสเซอร์ที่เพิ่มขึ้นมา

4.4 กำหนดเน็ตเวิร์ค ที่ วีพีเอ็นสามารถเราท์ถึงได้

เข้าผ่าน SSH

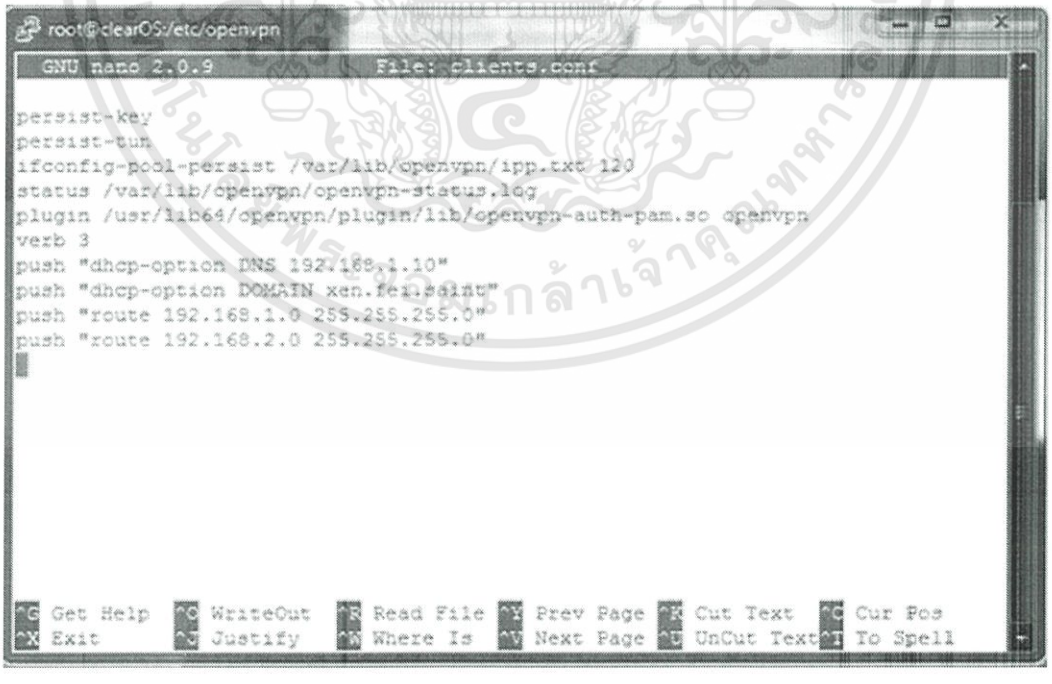


รูปที่ 4.8 เข้าระบบผ่านเอสเอสเอช

ไปที่ /etc/openvpn

รูปที่ 4.9 เข้าสู่ไฟล์เราท์ติ้ง

แก้ไขไฟล์ clients.conf โดยเพิ่ม เน็ตเวิร์ค ที่จะให้ วีพีเอ็น route ถึง ดังรูปข้างล่างนี้



รูปที่ 4.10 แก้ไขเราท์ติ้ง

4.5 Install Firewall

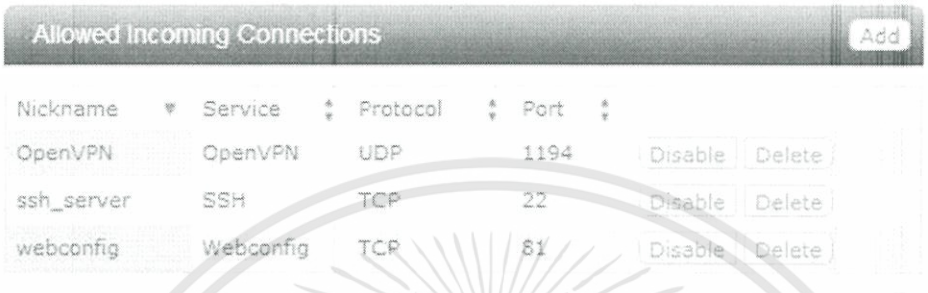
ค้นหาด้วยคีย์เวิร์ดไฟร์วอลล์

รูปที่ 4.11 ค้นหาไฟร์วอลล์

รูปที่ 4.12 อินสตอลล์ไฟร์วอลล์

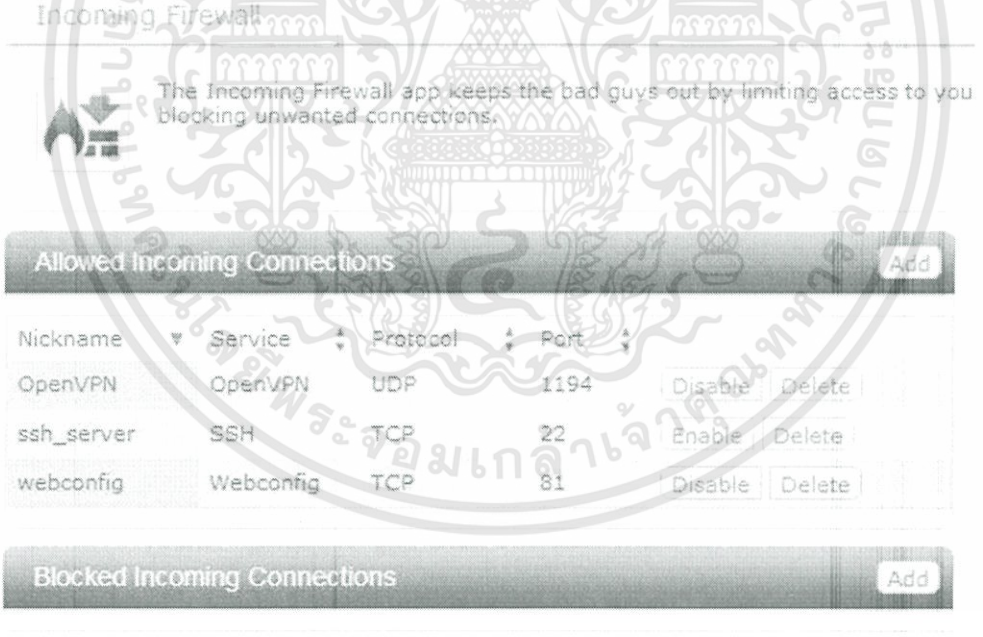
Default ของ Incoming ไฟร์วอลล์ จะ Block ทุก พอร์ต ให้ไม่สามารถ access มาที่ตัว เคลียร์โอเอส ได้

จากรูปด้านล่างเรา allow Incoming Connections ให้ พอร์ต พวกนี้เข้าได้



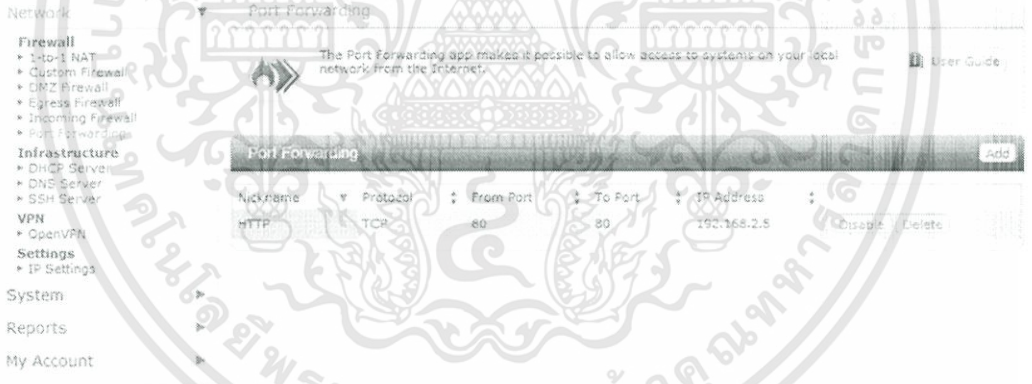
รูปที่ 4.13 ตั้งค่าไฟร์วอลล์

ลอง Disable พอร์ต 22 (SSH)

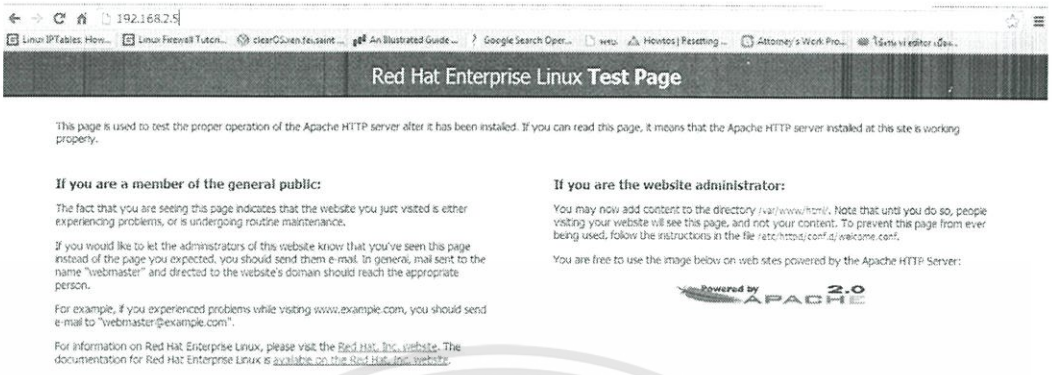


รูปที่ 4.14 แก้ไขการตั้งค่าไฟร์วอลล์

รูปที่ 4.15 ทดสอบเอสเอสเอช



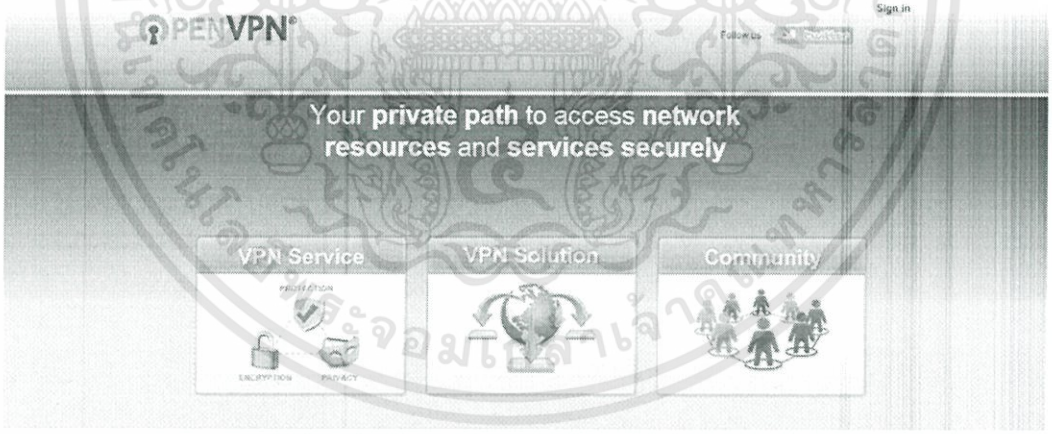
รูปที่ 4.16 ทำพอร์ทฟอเวิดดิ้งเพื่อทำให้สามารถเข้าสู่เว็บเซิฟเวอร์ได้



รูปที่ 4.17 ทดสอบเข้าเว็บเซิฟเวอร์

4.6 Set โอเพ่นวีพีเอ็น บน Desktop สำหรับ วินโดวส์

เข้าเว็บ www.openvpn.net แล้วกดเลือกที่ Community



รูปที่ 4.18 เว็บไซต์ดาวน์โหลดโอเพ่นวีพีเอ็น

เลือกที่ Download แล้วเลือกที่ Access Server Downloads

รูปที่ 4.19 ดาวน์โหลดโอเพ่นวีพีเอ็น1

พอเสร็จแล้วจะได้ดังรูปที่ 4.20 ให้เลือกที่ Access Server Software Packages แล้วเลือกการ Download เป็น วินโดวส์ OS

รูปที่ 4.20 ดาวน์โหลดโอเพ่นวีพีเอ็น2

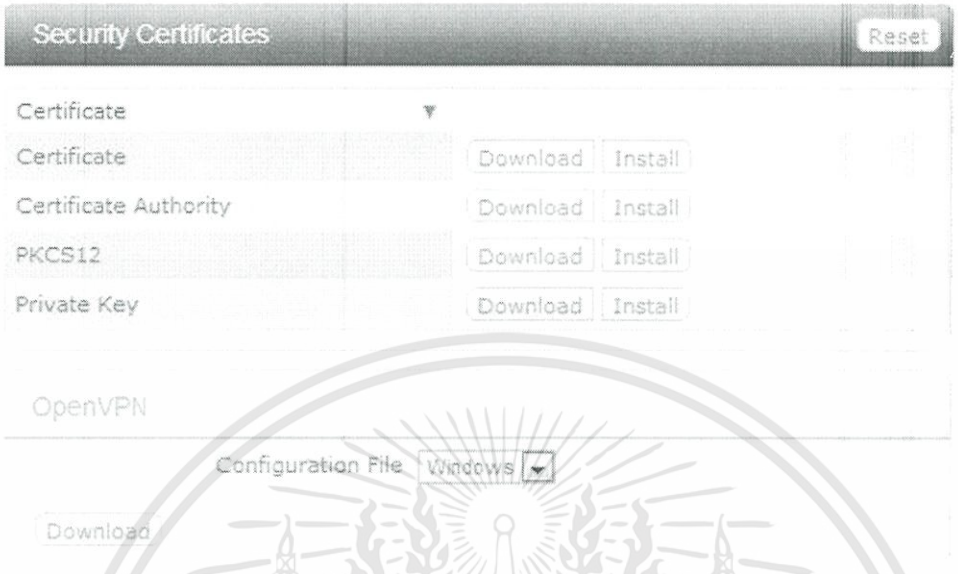
จะได้ดังรูป4.21 ให้เราเลือก OpenVPN Connect Client Download for Windows ซึ่งคือลิ้งค์ที่อยู่บนสุด

รูปที่ 4.21 ดาวน์โหลดโอเพ่นวีพีเอ็น3

พอดาวโหลดเสร็จก็ทำการติดตั้ง

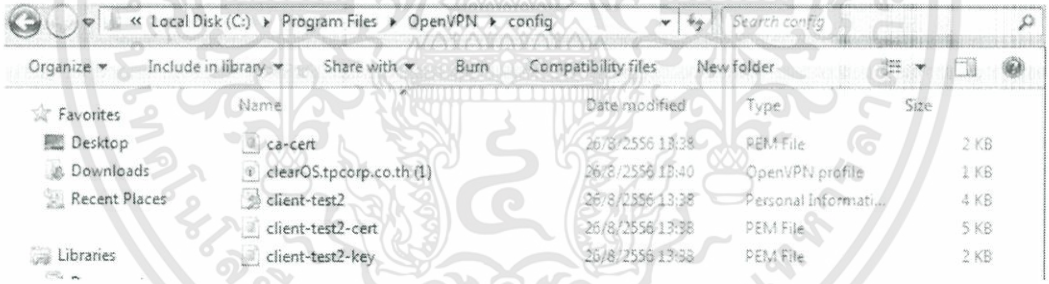
เวลาใช้งาน User ต้องดาวโหลด เซอร์ทิฟิเคท มาเก็บไว้ในเครื่องก่อน

รูปที่ 4.22 ดาวน์โหลดเซอร์ทิฟิเคท1

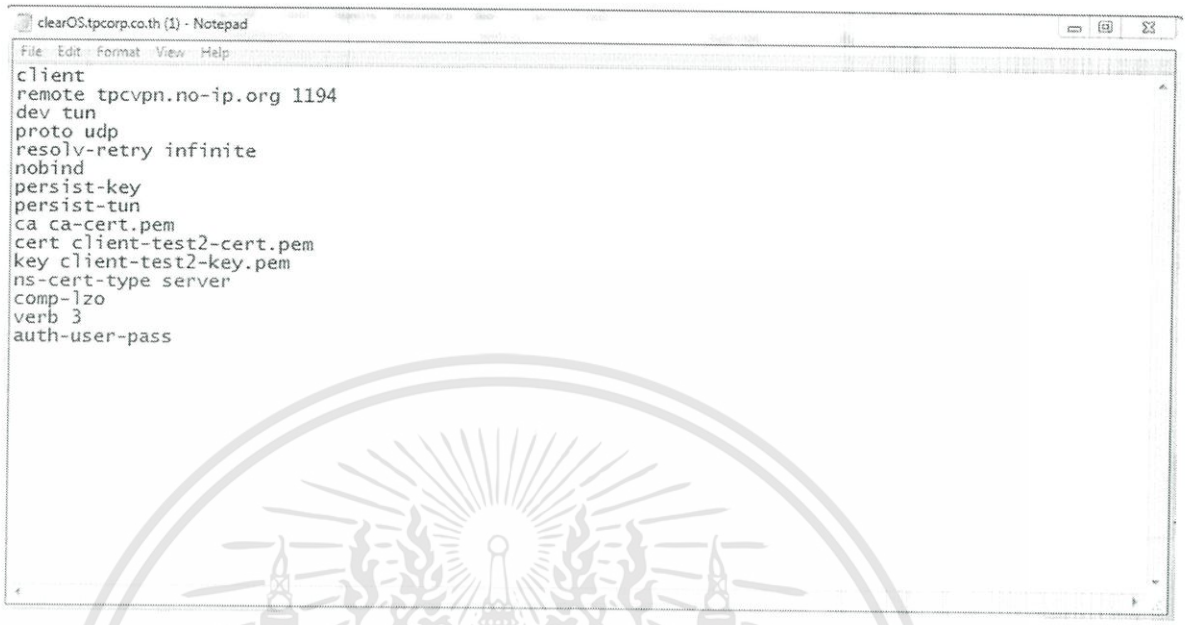


รูปที่ 4.23 ดาวน์โหลดเซอร์ทิฟิเคท2

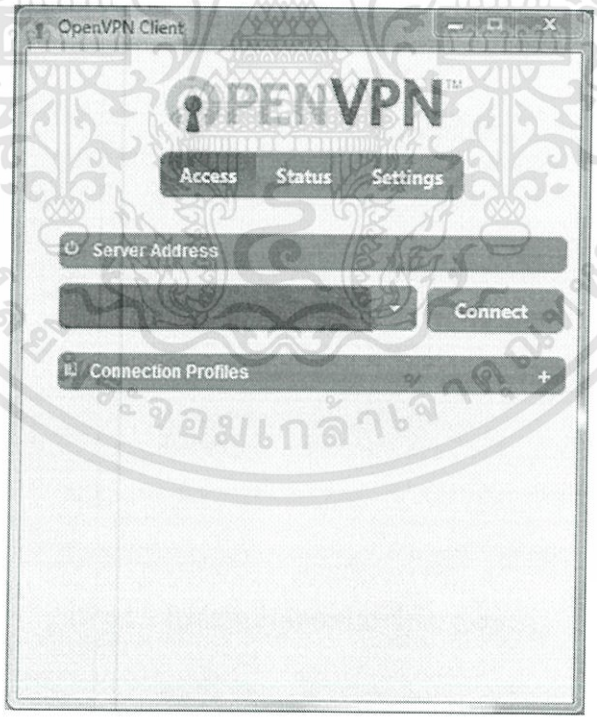
นำไฟล์ certificates ไปใส่ที่ C:\Program Files\openvpn\config จะได้ดังรูปที่ 4.24 นี้



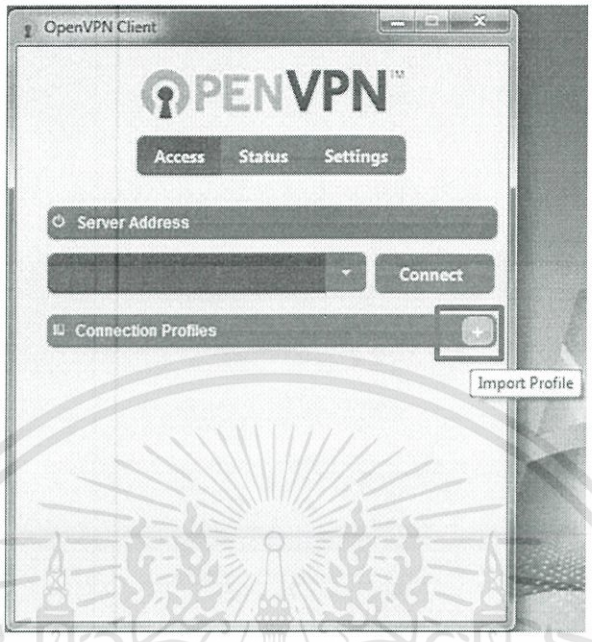
รูปที่ 4.24 ดาวน์โหลดเซอร์ทิฟิเคท3



รูปที่ 4.25 ไฟล์คอนฟิคดอทโอพีวีเอ็น (.opvn)

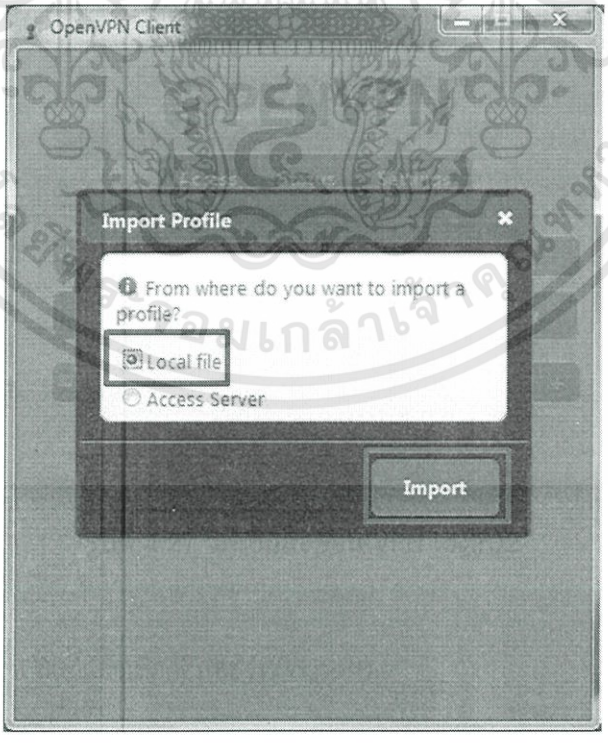


รูปที่ 4.26 วีพีเอ็นล็อคอิน(VPN login)1

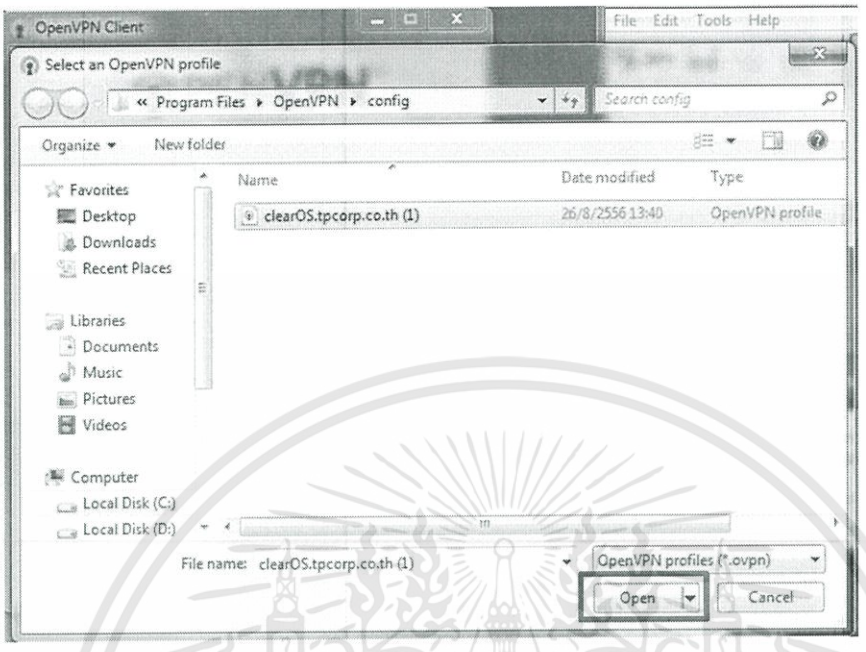


รูปที่ 4.27 วีพีเอ็นล็อคอิน(VPN login)2

เลือกลอคอล์ไฟล์(Local file)แล้วเลือกอิมพอร์ท(import)

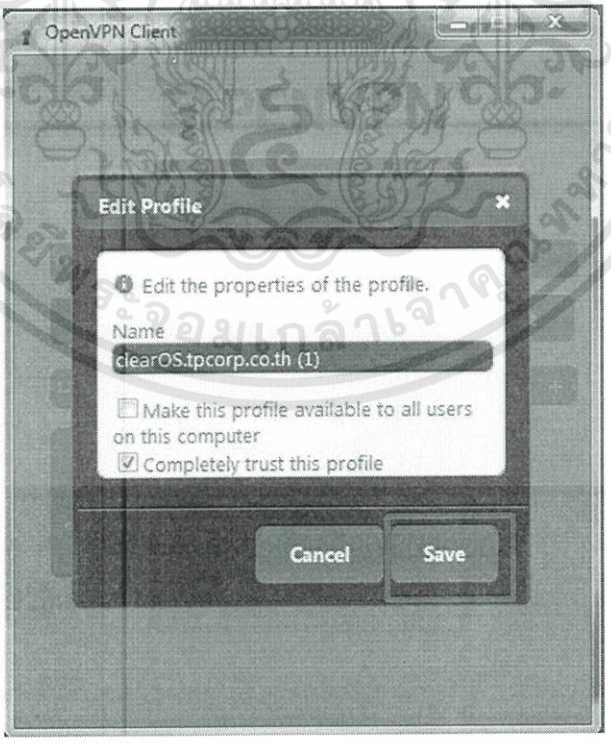


รูปที่ 4.28 วีพีเอ็นล็อคอิน(VPN login)3

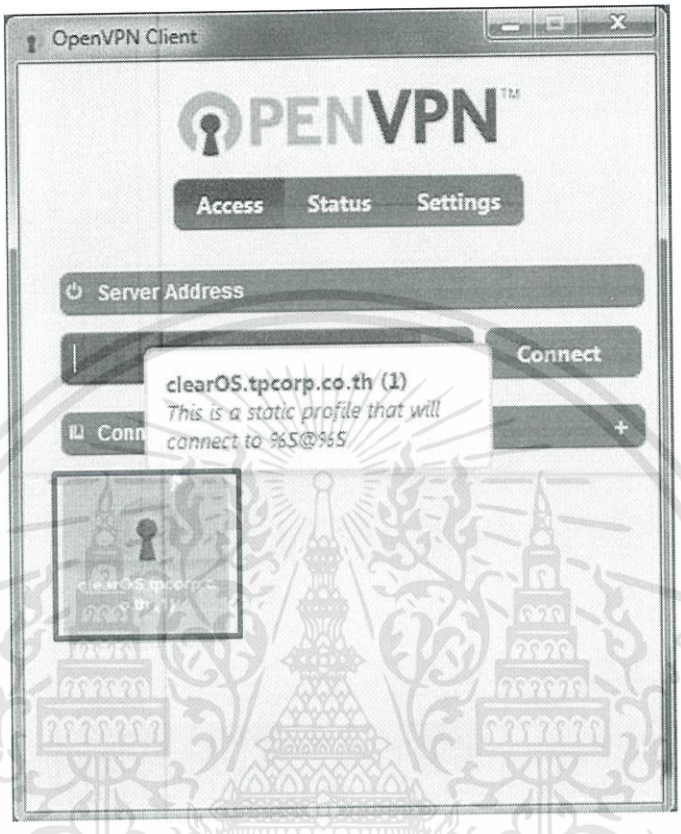


รูปที่ 4.28 วีพีเอ็นล็อคอิน(VPN login)4

ทำการเลือกไฟล์ดอทโอวีพีเอ็นแล้วกดเปิด

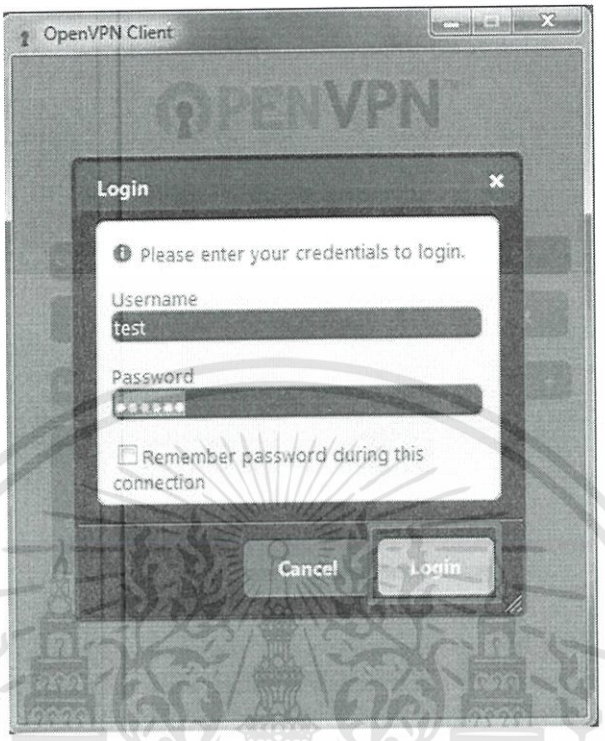


รูปที่ 4.29 วีพีเอ็นล็อคอิน(VPN login)5



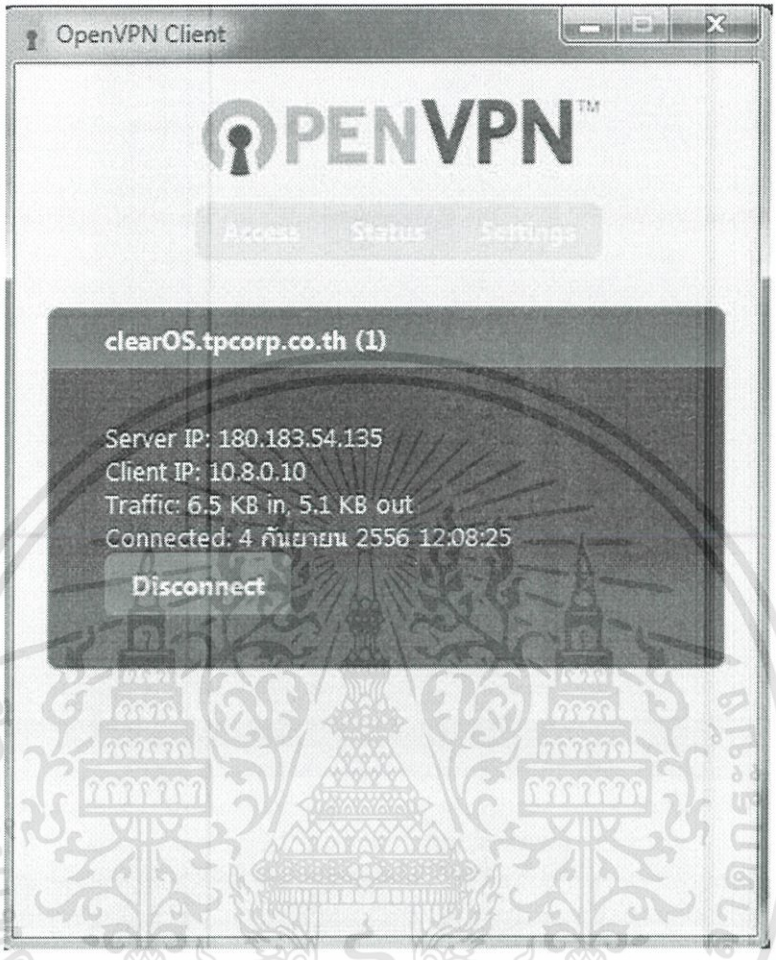
รูปที่ 4.30 วีพีเอ็นล็อคอิน(VPN login)6

เลือกไฟล์ที่เราได้บันทึกไว้



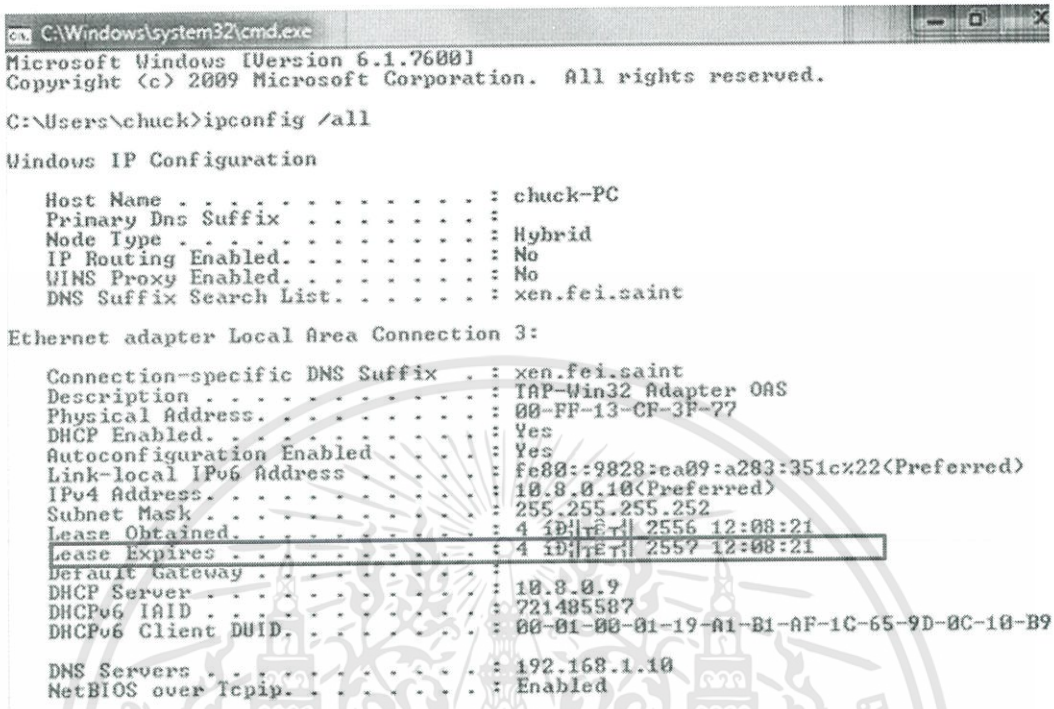
รูปที่ 4.31 วีพีเอ็นล็อคอิน(VPN login)7

ป้อนยูเซอร์เนมและพาสเวิดที่ได้จากผู้ดูแลระบบ



รูปที่ 4.32 วีพีเอ็นล็อคอิน(VPN login)8

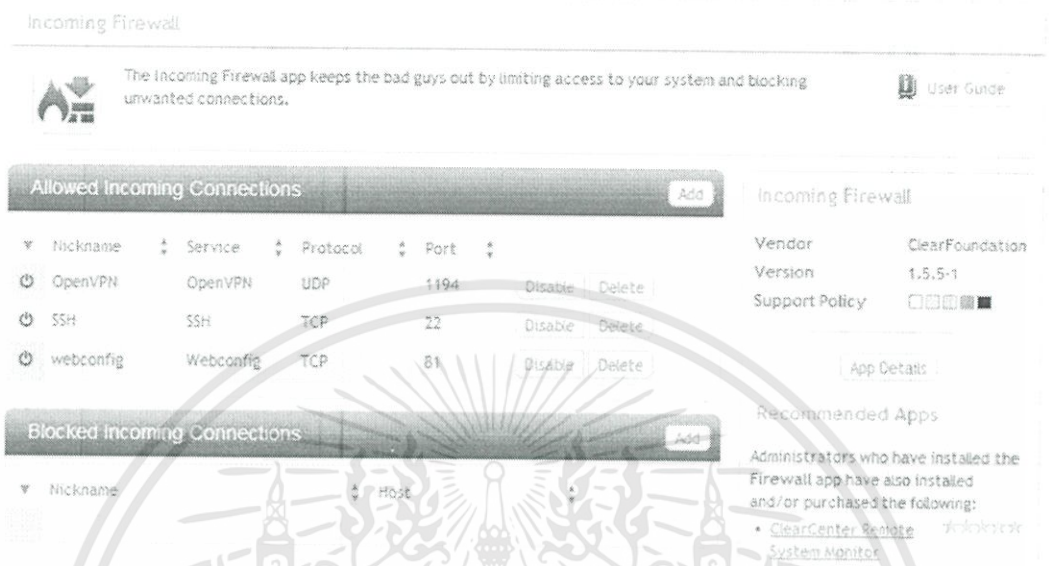
วีพีเอ็นที่สามารถเชื่อมต่อได้



รูปที่ 4.33 วีพีเอ็นล็อคอิน(VPN login)9

ตรวจสอบไอพีแอดเดรสที่ได้ทำวีพีเอ็น

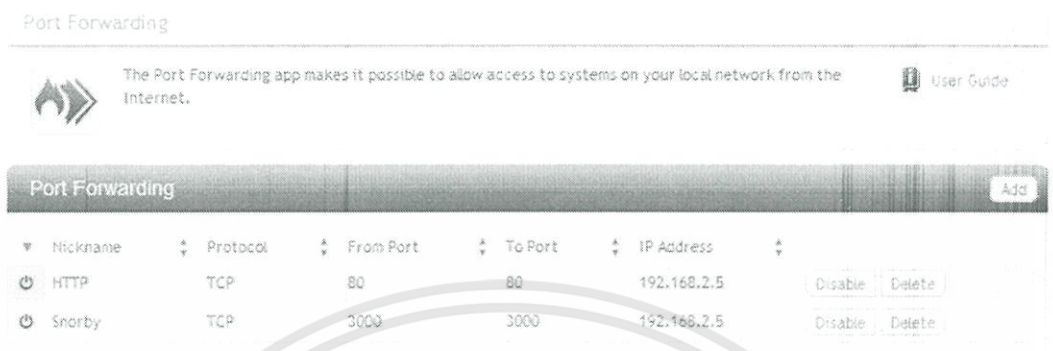
4.7 Incoming Firewall Setting



รูปที่ 4.34 ตั้งค่า Incoming Firewall

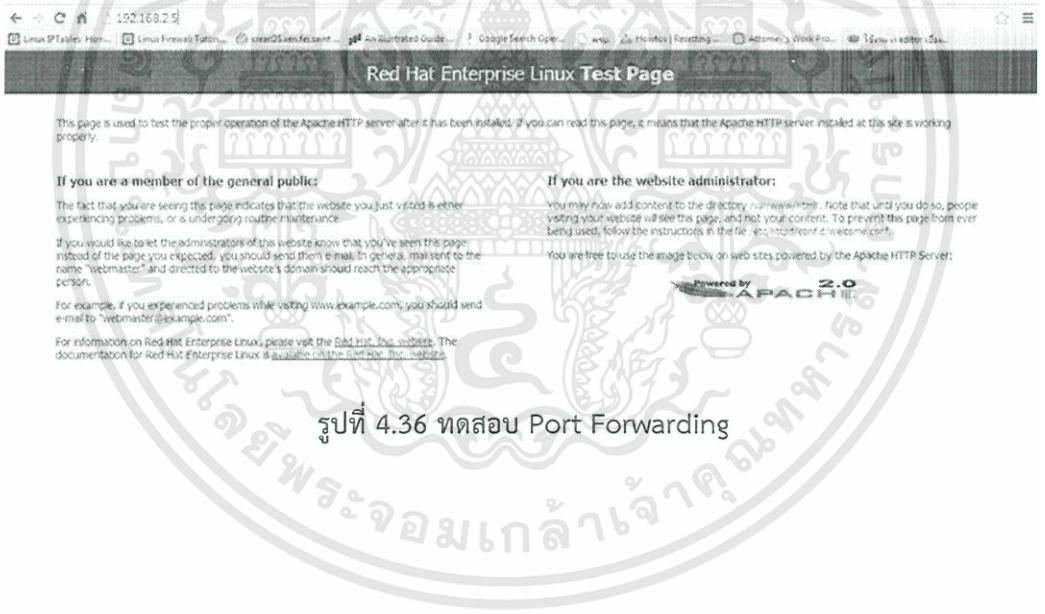
ตั้งค่าให้เปิดพอร์ตสำหรับ OpenVPN SSH และ Webconfig สำหรับใช้ตั้งค่าและใช้งาน OpenVPN

4.8 Port Forwarding Setting



รูปที่ 4.35 ตั้งค่า Port Forwarding

ตั้งค่าให้ฟอร์เวิร์ดไปยังเว็บเซิฟเวอร์ที่ได้มีการตั้งค่าไว้



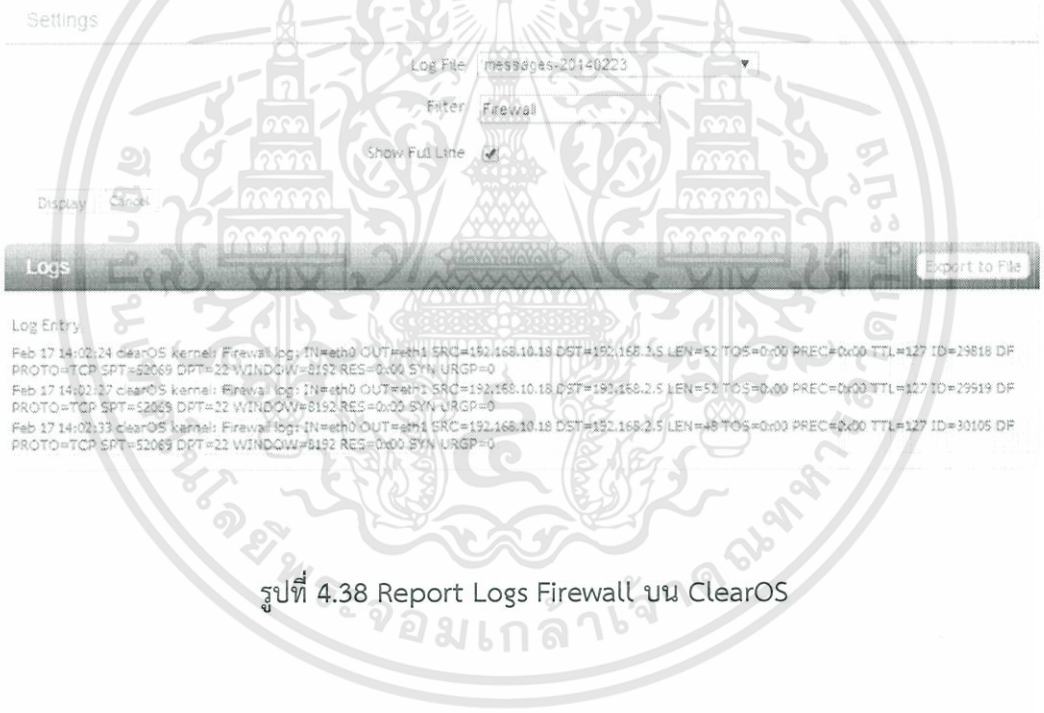
รูปที่ 4.36 ทดสอบ Port Forwarding

4.9 LOGS Firewall Configuration

การตั้งค่าทดสอบ logs ของ firewall โดยการบล็อค SSH จาก Zone LAN ไป Zone HotLAN

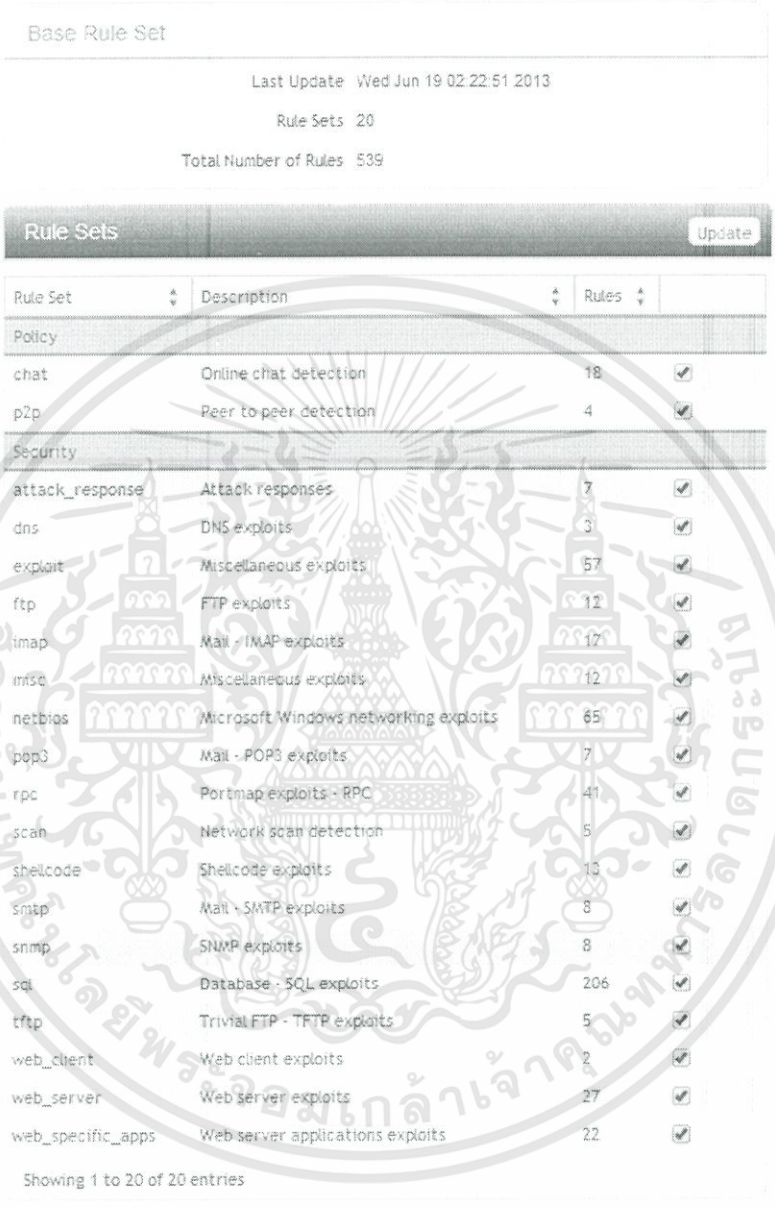
```
iptables -N LOGDROP
iptables -A LOGDROP -j LOG --log-prefix "Firewall log: "
iptables -A LOGDROP -j DROP
iptables -I FORWARD -i eth0 -o eth1 -p tcp --dport 22 -j LOGDROP # block SSH  LAN to snorby
~
~
~
```

รูปที่ 4.37 ทดสอบ Logs Firewall



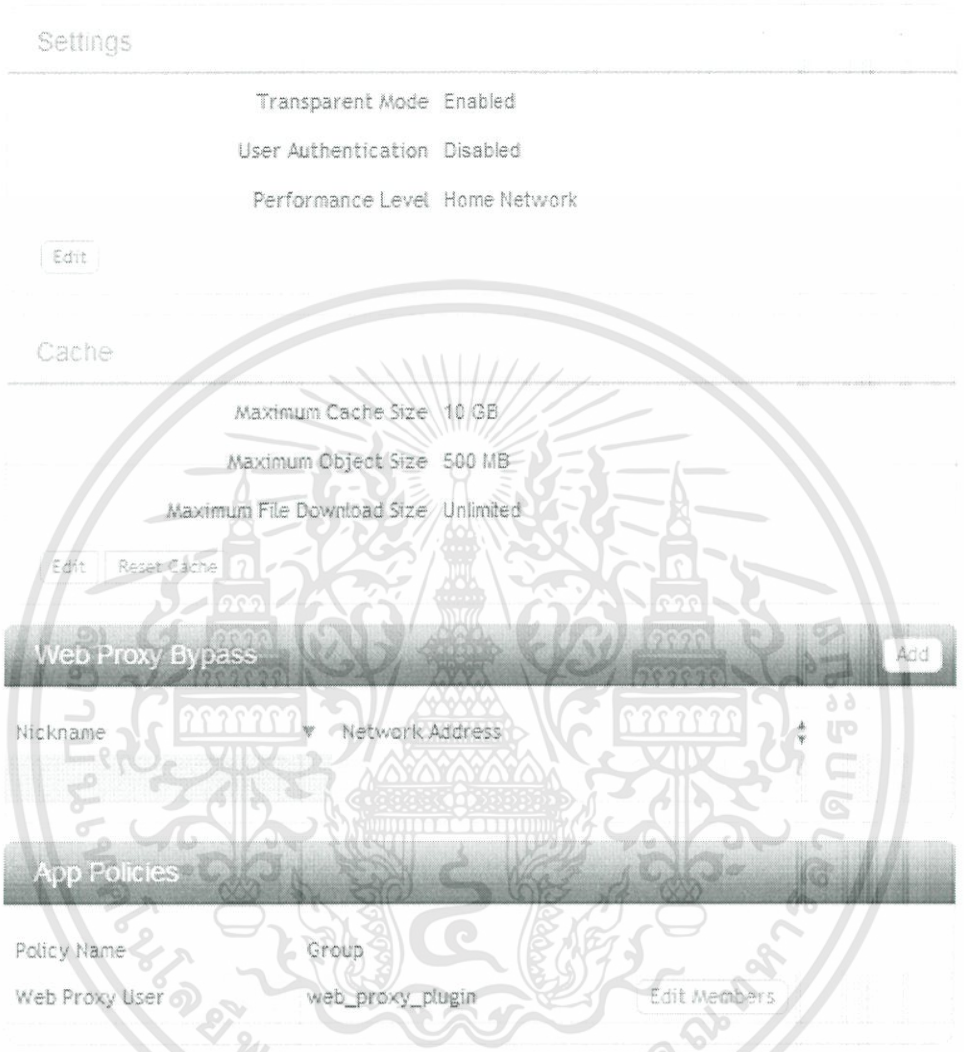
รูปที่ 4.38 Report Logs Firewall บน ClearOS

4.10 Intrusion Detection

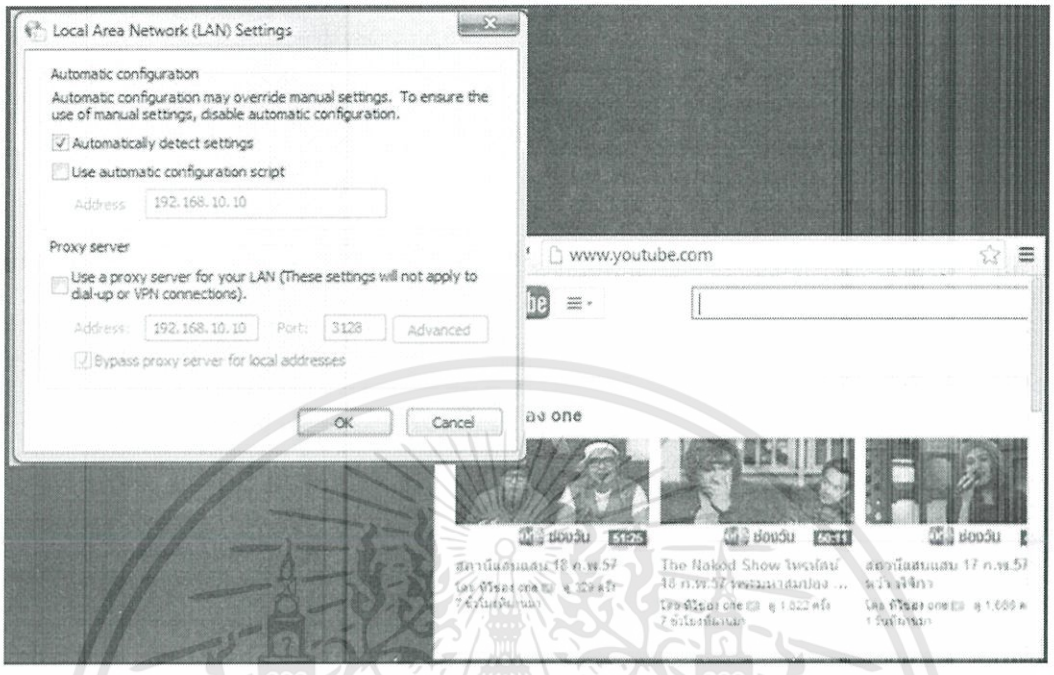


รูปที่ 4.39 Rule Set ของ Intrusion Detection

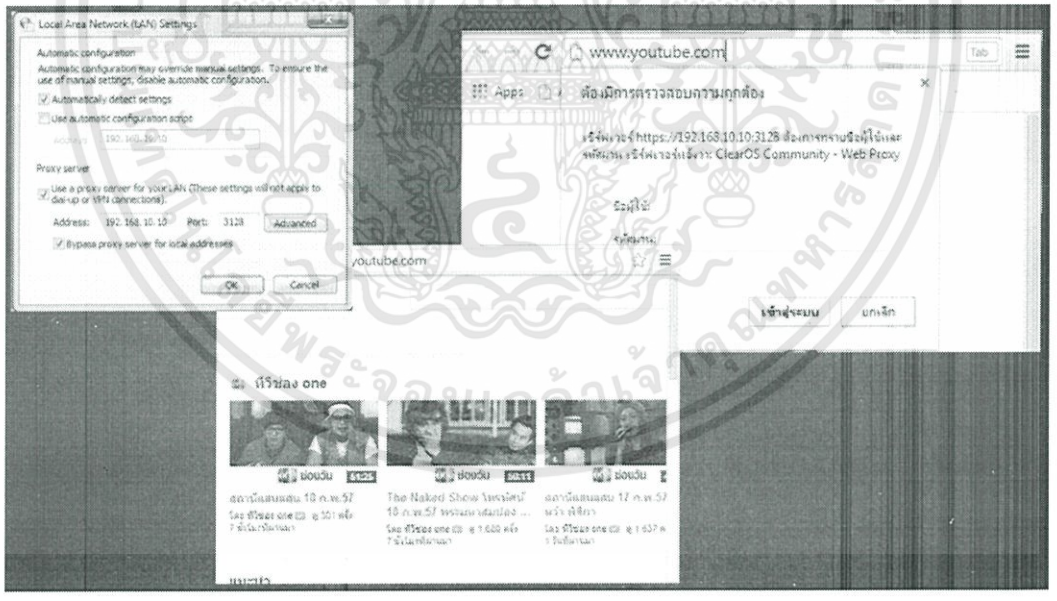
4.11 Web Proxy



รูปที่ 4.40 ตั้งค่า Web Proxy

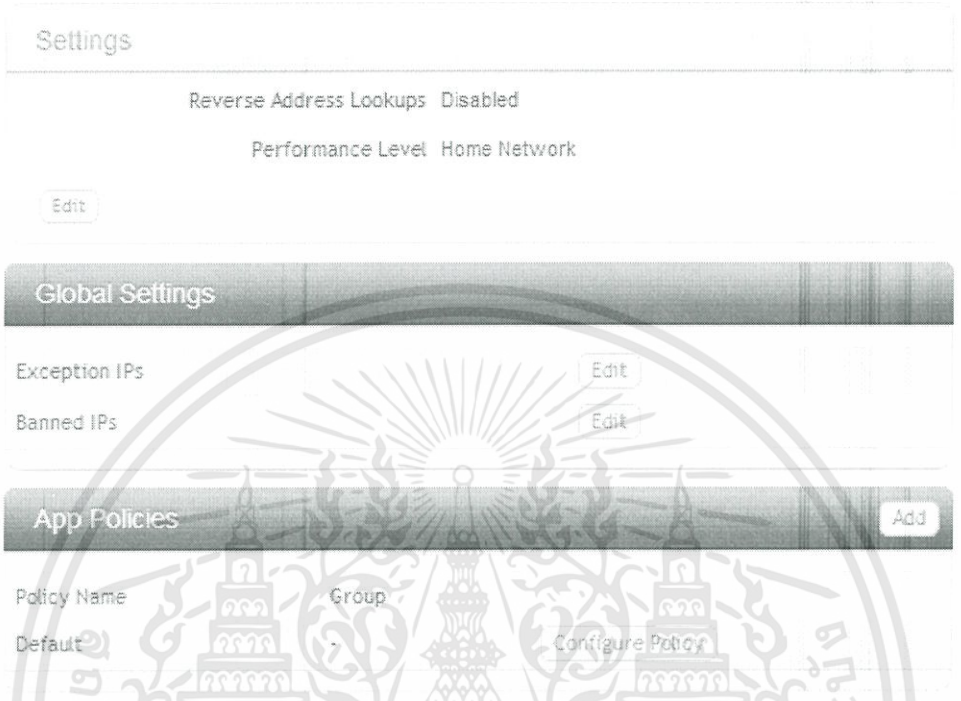


รูปที่ 4.41 ทดสอบ Transparent Mode



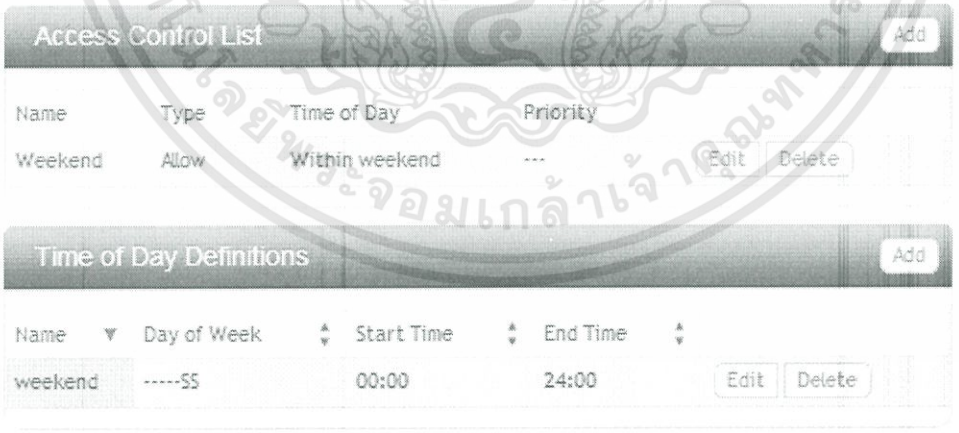
รูปที่ 4.42 ทดสอบ non-Transparent proxy + User Authentication

4.12 Content Filter



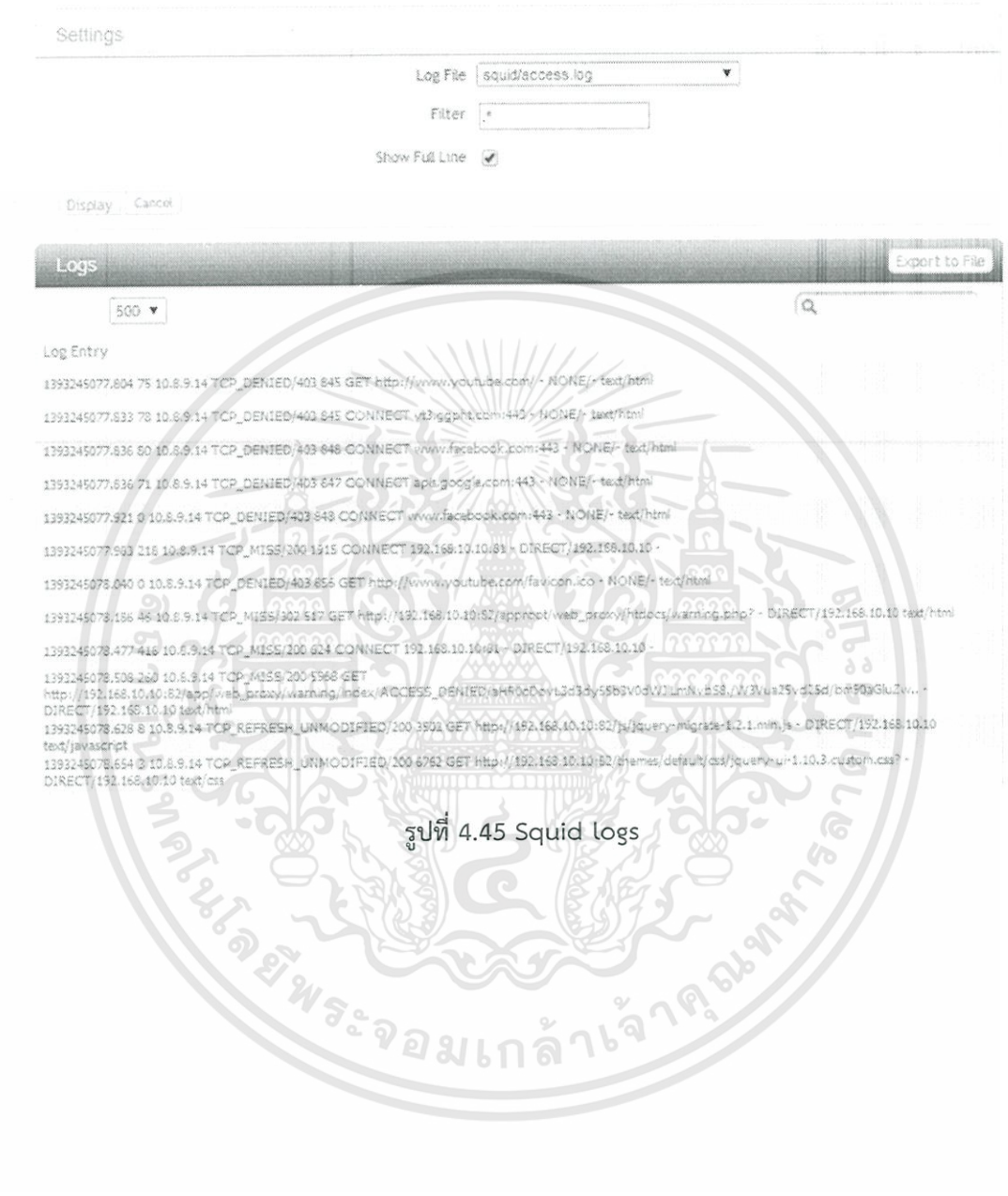
รูปที่ 4.43 ตั้งค่า Content Filter

4.13 Web Access Control



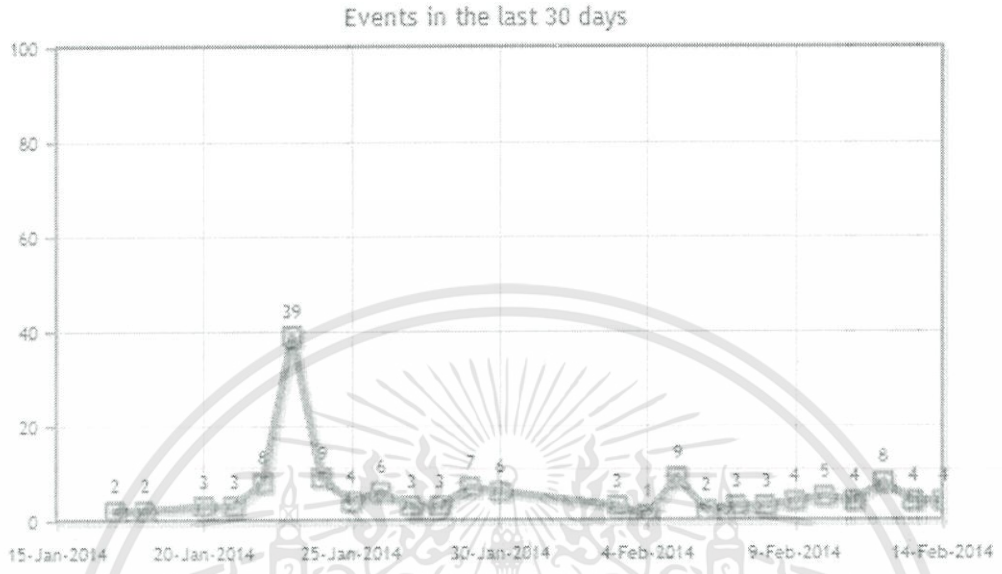
รูปที่ 4.44 ตั้งค่า Web Access Control

4.15 Squid access logs (Proxy)



รูปที่ 4.45 Squid logs

4.16 Developer (IDS LOGS Reports)



รูปที่ 4.46 Snort Graph

Snort Gui

Sev.	Sensor	Event Signature	Timestamp
2	clearOS.xen.fei.saint	GPL SNMP request tcp	2013-12-10 17:16:22
2	clearOS.xen.fei.saint	GPL WEB_SERVER 403 Forbidden	2014-01-10 11:35:44
2	clearOS.xen.fei.saint	GPL WEB_SERVER 403 Forbidden	2014-01-10 11:33:58
2	clearOS.xen.fei.saint	GPL WEB_SERVER 403 Forbidden	2014-01-10 11:33:56
2	clearOS.xen.fei.saint	GPL WEB_SERVER WEB-PHP phpinf	2014-01-10 11:29:13
2	clearOS.xen.fei.saint	GPL WEB_SERVER 403 Forbidden	2014-01-10 11:16:23
2	clearOS.xen.fei.saint	GPL WEB_SERVER 403 Forbidden	2014-01-10 11:16:34
2	clearOS.xen.fei.saint	GPL WEB_SERVER 403 Forbidden	2014-01-10 11:18:59
2	clearOS.xen.fei.saint	GPL WEB_SERVER WEB-PHP phpinf	2014-01-10 11:21:40
2	clearOS.xen.fei.saint	GPL WEB_SERVER 403 Forbidden	2014-01-10 11:36:14
2	clearOS.xen.fei.saint	GPL WEB_SERVER 403 Forbidden	2014-01-10 11:36:19
2	clearOS.xen.fei.saint	GPL WEB_SERVER 403 Forbidden	2014-01-10 11:55:00
2	clearOS.xen.fei.saint	GPL WEB_SERVER 403 Forbidden	2014-01-10 12:52:07
2	clearOS.xen.fei.saint	GPL WEB_SERVER 403 Forbidden	2014-01-10 12:53:28
2	clearOS.xen.fei.saint	GPL WEB_SERVER 403 Forbidden	2014-01-10 12:53:34
2	clearOS.xen.fei.saint	GPL WEB_SERVER 403 Forbidden	2014-01-10 12:56:21
2	clearOS.xen.fei.saint	GPL WEB_SERVER WEB-PHP phpinf	2014-01-10 13:01:45
1	clearOS.xen.fei.saint	GPL WEB_SERVER /usr/bin/id com	2014-01-10 13:04:42
2	clearOS.xen.fei.saint	GPL WEB_SERVER 403 Forbidden	2014-01-10 13:05:13
2	clearOS.xen.fei.saint	GPL WEB_SERVER 403 Forbidden	2014-01-10 13:14:57
2	clearOS.xen.fei.saint	GPL WEB_SERVER 403 Forbidden	2014-01-10 13:32:55
1	clearOS.xen.fei.saint	GPL WEB_SERVER bin/python acce	2014-01-10 13:32:59
2	clearOS.xen.fei.saint	GPL WEB_SERVER 403 Forbidden	2014-01-10 13:39:17
2	clearOS.xen.fei.saint	GPL EXPLOIT php.cgi access	2014-01-10 13:39:20
2	clearOS.xen.fei.saint	GPL WEB_SERVER 403 Forbidden	2014-01-10 15:10:02
2	clearOS.xen.fei.saint	GPL WEB_SERVER 403 Forbidden	2014-01-10 19:45:05
2	clearOS.xen.fei.saint	GPL WEB_SERVER 403 Forbidden	2014-01-11 10:35:40
2	clearOS.xen.fei.saint	GPL WEB_SERVER 403 Forbidden	2014-01-11 11:59:17
2	clearOS.xen.fei.saint	GPL WEB_SERVER 403 Forbidden	2014-01-11 12:12:22
2	clearOS.xen.fei.saint	GPL WEB_SERVER 403 Forbidden	2014-01-11 12:59:52

รูปที่ 4.47 Snort LOGS Report

Sev.	Sensor	Event Signature	Timestamp
2	clearOS.xen.fei.saint	GPL SNMP request tcp	2013-12-10 17:16:22

IP Header Information

Source	Destination	Ver	Source Port	Destination Port
192.168.1.79	192.168.1.10	4	54578	161

Signature Information

Sig ID	Sig Info
1418	Query Signature Database

รูปที่ 4.48 Snort LOGS Report 2

Home

Snort Signature Information

Rule:

--
Sid:
1418

--

Summary:
This event is generated when an SNMP-Trap connection over TCP to an SNMP daemon is made.

--

Impact:
Information gathering

--

Detailed Information:
The SNMP (Simple Network Management Protocol) Trap daemon usually listens on port 161, tcp or udp.

An attacker may attempt to send this request to determine if a device is using SNMP.

--

รูปที่ 4.49 Snort Signature Information

Detailed Information:
The SNMP (Simple Network Management Protocol) Trap daemon usually listens on port 161, tcp or udp.

An attacker may attempt to send this request to determine if a device is using SNMP.

--

Affected Systems:
Devices running SNMP daemons on well known ports.

--

Attack Scenarios:
An attacker sends a packet directed to tcp port 161, if sucessful a reply is generated and the attacker may then launch further attacks against the SNMP daemon.

--

Ease of Attack:
Simple.

--

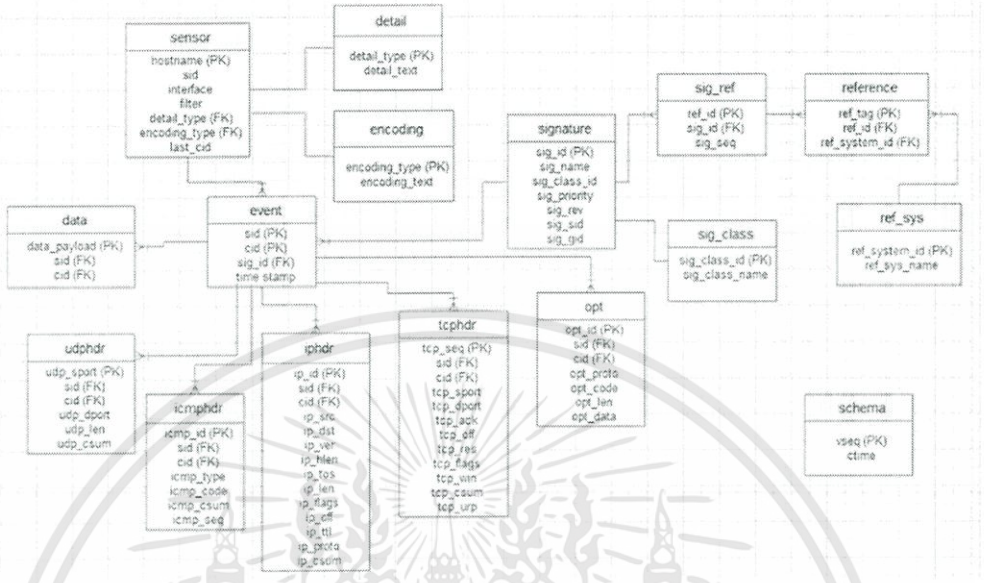
False Positives:
None known.

--

False Negatives:
None known.

--

รูปที่ 4.50 Snort Signature Information 2



รูปที่ 4.51 Snort Database

บทที่ 5
บทสรุปและข้อเสนอแนะ

5.1 สรุปและบทวิจารณ์

ระบบเน็ตเวิร์คในปัจจุบันควรจะต้องมีระบบรักษาความปลอดภัยที่ใช้ในระบบต่างๆที่มีประสิทธิภาพมากพอที่จะป้องกันการถูกบุกรุกเข้ามากระทำการต่างๆจากผู้ประสงค์ร้ายได้ เพราะ ภัยคุกคามทางเน็ตเวิร์คในปัจจุบันมีรูปแบบที่หลากหลาย และ มีการพัฒนารูปแบบไปเรื่อยๆ เราจึงต้องมีระบบรักษาความปลอดภัยที่มั่นใจได้ว่า จะป้องกันภัยคุกคามได้มากที่สุดเท่าที่ทำได้ ซึ่งในปัจจุบันมีทั้งไฟร์วอลล์ที่เป็นโปรดักซ์ขายทั่วไปที่มีประสิทธิภาพ แต่ประสิทธิภาพนั้นก็มากแปรผันตามราคาที่มากขึ้นไปด้วย ซึ่งที่ใช้เคลียร์โอเอสนี้ซึ่งเป็นโอเพ่นซอร์สจะทำให้ประหยัดงบในส่วนนี้ได้เยอะมาก และทั้งยังมีประสิทธิภาพใช้งานได้ในระดับหนึ่ง

5.2 ปัญหาและอุปสรรค

1) ตัวเคลียร์โอเอสที่ใช้ มีผู้ใช้งานจริงน้อย จึงค่อนข้างลำบากในการค้นหาข้อมูลที่เป็นข้อมูลจากผู้ใช้งานจริง
2) เมื่อเราท์เตอร์ล่มจากระบบเครือข่ายเมื่อเชื่อมต่อมาใหม่จะทำให้ไอพีแอดเดรสของเราท์เตอร์เปลี่ยน จึงทำให้เข้าสู่ระบบไม่ได้
3) การตั้งค่าบางครั้งต้องไปทำที่บริษัทเท่านั้นไม่สามารถเข้ามาตั้งค่าจากภายนอกองค์กร
4) คอนเท้นฟิวเตอร์ต้องใช้ทรัพยาการที่มากพอจึงจะเกิดประสิทธิภาพสูงสุด
5) ไอพีเอสต้องมีกฎที่ครอบคลุมจึงจะสามารถป้องกันภัยคุกคามได้อย่างมีประสิทธิภาพ
6) ถ้ามีเร้าเตอร์วางไว้ที่หน้าระบบอาจจะเป็นอุปสรรคต่อการบันทึกเหตุการณ์ของไอพีเอส

5.3 แนวทางแก้ไข

1) ทำการค้นหาข้อมูลจากตัวเว็บไซต์ของผู้ผลิตเคลียร์โอเอสเอง และพยายามทดสอบระบบทำให้สามารถค่อยๆเรียนรู้การตั้งค่าได้
2) ตั้งค่าให้ไดนามิคดีเอนเอสมีการอัพเดทค่าไอพีแอดเดรสบ่อยขึ้น
3) ใช้งานโอเพ่นวีพีเอ็น
4) เพิ่มทรัพยากรของระบบให้เพียงพอต่อการทำงาน
5) ทำการอัพเดทกฎจากหน้าเว็บของโปรแกรมอย่างสม่ำเสมอ

5.4 แนวทางการพัฒนาต่อ

1) ติดตั้งระบบความปลอดภัยในเครือข่ายเพิ่มเติม
2) เขียนโปรแกรมวิเคราะห์บันทึกอื่นๆ
3) เขียนโปรแกรมเพื่อแยกชนิดของการโจมตี

บรรณานุกรม

[1] Guidelines on Firewalls and Firewall Policy - Karen Scarfone Paul Hoffman

[2] Network Security Using Cisco IOS IPS

[3] CRYPTOGRAPHY AND NETWORK SECURITY PRINCIPLES AND PRACTICE FIFTH EDITION – WILLIAM STALLINGS

[4] Handbook of Information and Communication Security" by Stavroulakis, P., Stamp, M. (Eds.) Springer, 2010

[5] Practical Intrusion Analysis: Prevention and Detection for the Twenty-First Century – Ryan Trost

[6] Intrusion Detection and Prevention - Carl F. Endorf, Eugene Schultz, Jim Mellander McGraw Hill