

ลิขสิทธิ์ : กรมทางหลวงชนบท  
ปี : 2559  
ชื่อเรื่อง : พัฒนาระบบเครือข่ายและรักษาความปลอดภัย (ระยะที่2)  
เมือง : กรุงเทพฯ  
ภาษา : ไทย  
สถานที่พิมพ์ : สถาบันวิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์  
นักวิจัย : ผู้ช่วยศาสตราจารย์ ดร. ทวีศักดิ์ กิจกาญจนารัตน์,  
อาจารย์ วชิรา พรหมสาขา ณ สกลนคร, ผู้ช่วยศาสตราจารย์ ดร. ชัยวัฒน์ อุตตมากร,  
อาจารย์ ดร. วศินี หนูนภักดี  
บทคัดย่อ :

เนื่องจากกรมทางหลวงชนบทได้ใช้อุปกรณ์ระบบเครือข่ายและอุปกรณ์รักษาความปลอดภัยหลักที่มีอยู่ในปัจจุบันมาเป็นระยะเวลานานกว่า 5 ปี และอุปกรณ์ดังกล่าวเริ่มเสื่อมสภาพและเกิดขัดข้องบ่อยครั้ง ทำให้ไม่สามารถให้บริการระบบงานต่าง ๆ ได้อย่างมีประสิทธิภาพดีเท่าที่ควร อีกทั้งในปัจจุบันมาตรฐานความเร็วของอุปกรณ์เครือข่ายได้มีการเปลี่ยนแปลงไปเป็นความเร็ว 10 Gbps ดังนั้นเพื่อเป็นการปรับปรุงประสิทธิภาพการทำงานของอุปกรณ์เครือข่ายและอุปกรณ์รักษาความปลอดภัยของกรมทางหลวงชนบทให้เป็นมาตรฐาน และมีประสิทธิภาพสูงสุด สามารถให้บริการระบบงานทางด้านเทคโนโลยีสารสนเทศได้อย่างต่อเนื่องและมีคุณภาพการให้บริการที่ดี ทางกรมมีความจำเป็นต้องเปลี่ยนแปลง ปรับปรุงอุปกรณ์ต่าง ๆ ให้มีความเหมาะสมต่อความต้องการและความจำเป็นในการใช้งานในปัจจุบัน นอกจากนี้ การมีใช้งานเทคโนโลยีสารสนเทศเพิ่มมากขึ้น ทำให้เกิดความเสี่ยงต่อการถูกโจมตีจากบุคคลหรือซอฟต์แวร์ไม่พึงประสงค์เพิ่มมากขึ้นเช่นเดียวกัน นอกจากนี้แล้วการดำเนินงานปกติของผู้ปฏิบัติงานในองค์กรอาจเกิดความเสียหายโดยไม่เจตนาได้ เช่นการเปิดอีเมลที่ติดไวรัสอาจทำให้ระบบเครือข่ายทำงานช้าลง เป็นต้น การป้องกันความเสี่ยงต่อการถูกโจมตีจึงมีความจำเป็นเพื่อปกป้องระบบให้ปลอดภัย ให้สามารถทำงานได้อย่างต่อเนื่อง มีเสถียรภาพ

ภัยคุกคามเทคโนโลยีสารสนเทศมีแนวโน้มเพิ่มสูงขึ้นตลอดเวลา การใช้งานอุปกรณ์ป้องกันภัยคุกคามจำเป็นต้องมีความทันสมัยเป็นปัจจุบัน จึงจำเป็นต้องมีการปรับเปลี่ยนอุปกรณ์ที่ใช้งานมานานและเสื่อมสภาพ เพื่อยกระดับความสามารถในการปกป้องข้อมูล การดำเนินโครงการนี้จะทำให้เกิดผลดังนี้

- 1.) มีระบบการตรวจสอบและป้องกันการเข้าถึงเว็บไซต์และข้อมูลที่ไม่พึงประสงค์
- 2.) มีระบบการปกป้องข้อมูลที่เป็นมาตรฐานสากล
- 3.) เว็บแอปพลิเคชันสามารถให้บริการผู้ใช้ได้อย่างมีประสิทธิภาพ
- 4.) ผู้บริหารระบบงานมีความสะดวกในการดูแลและตรวจสอบความปลอดภัย

อุปกรณ์ป้องกันการบุกรุกเว็บไซต์ Web Application Firewall ช่วยในการปกป้องข้อมูลซึ่งถือทรัพย์สินที่สำคัญ จากการโจมตีของมัลแวร์ การโจมตีแบบ DoS และภัยคุกคามแบบอื่น ๆ ที่เข้าสู่เครือข่ายด้วยโปรโตคอล HTTP/HTTPS ด้วยความสามารถวิเคราะห์การเข้าใช้งานเว็บแอปพลิเคชันที่มีความสำคัญ

และสามารถเรียนรู้การพฤติกรรมการใช้งานแบบปกติหรือแบบเป็นภัยคุกคามได้อัตโนมัติ ตรวจสอบ  
ป้องกันการเข้าถึงระบบงาน

นอกจากการป้องกันการบุกรุกเว็บไซต์แล้ว การป้องกันการบุกรุกฐานข้อมูลก็มีความสำคัญ  
เช่นเดียวกัน แม้ว่าเว็บไซต์ได้รับการปกป้อง แต่การพัฒนาเว็บแอปพลิเคชันอาจมีข้อผิดพลาดทำให้เกิดช่องโหว่  
ต่อการโจมตีได้ รวมถึงความสามารถการเข้าถึงฐานข้อมูลของบุคลากรในองค์กร การปฏิบัติงานที่ผิดพลาด  
อาจนำความเสียหายให้กับฐานข้อมูลได้ อุปกรณ์ป้องกันการบุกรุกฐานข้อมูลมีความสามารถตรวจสอบ  
การเปลี่ยนแปลงของโครงสร้างของฐานข้อมูล วิเคราะห์การเข้าถึงระบบฐานข้อมูล และแจ้งเตือน

**Copyright** : Department of Rural Roads  
**Year** : 2016  
**Title** : Development of Network and Security Systems (Phase 2)  
**City** : Bangkok  
**Language** : Thai  
**Publisher** : Thammasat University Research and Consultancy Institute  
**Researcher** : Assistant Professor Dr. Taweesak Kijkanjanarat,  
Assistant Professor Dr. Chaiwat Oottamakorn, Dr. Wasinee Noonpakdee  
**Abstract** :

The Department of Rural Roads have been using some old network equipment and security devices for more than five years and are beginning to deteriorate and crash often. And now the current standard speed of network devices has been changed to 10 Gbps speeds, so as to improve the performance of network and security equipment, and to provide excellent service and quality. The department needs to change or improve equipment to be appropriate to the needs and the need to use on the current circumstance. The increasing use of information technology, Risk of being attacked by someone or unwanted software increased as well. In addition, the normal operation of a worker in an organization may have unwittingly threatened the network. Such as opening an infected e-mail may cause the network to slow down or prevent the risk of being attacked, it is necessary to protect the system secure. To work continuously stable.

Information technology Threat are increasing all the time. The threat protection devices require the modernization present. It has to be modified and used for aging and to enhance their ability to protect system and data. The implementation of this project will result follows.

- 1.) A system for detecting and blocking suspicious access to websites and web applications.
- 2.) A system for data protection compliant to standards.
- 3.) Web applications functionality to provide users with stability and high availability.
- 4.) A management system which are relatively easy to maintain and monitor safety.

This project will also acquire a Web Application Firewall and Intrusion Prevention Devices to protect information which is considered an important asset from the onslaught of

malware, DoS attacks and other threats from entering the network by HTTP / HTTPS protocol. The device can learn the behavior of normal use or threat automatically and continuously check and prevent unauthorized access to the system.

Furthermore, the database firewall acquired by the project has the same importance. Although the site has been protected but the development of web applications are subject error causes vulnerability to attack. Including the ability to access a database of people in the organization. Operational errors could lead to damage to the database. Database intrusion prevention devices are able to detect changes in the structure of the database. Analysis of access to the database and alerts.