NetkaView Logger
Netka System

อุปกรณ์เก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์

NetkaView Logger | NLG-SW | บริษัท เน็ตก้า ซิสเต็ม จำกัด

ได้รับการรับรองตามมาตรฐาน มศอ. 4003.1-2560

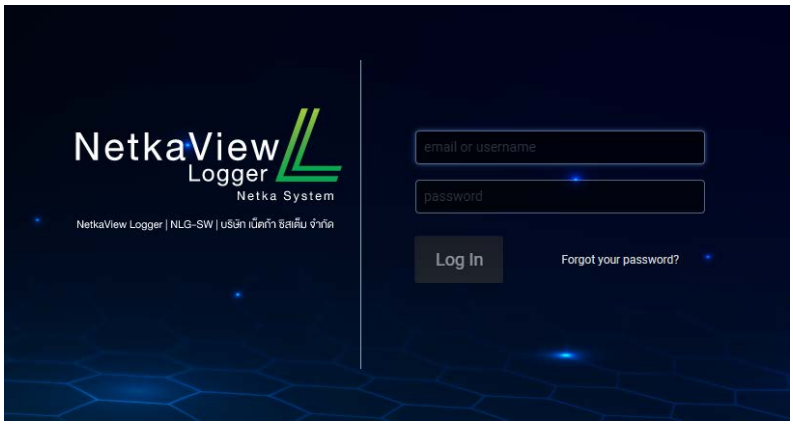
จุดเด่นของผลิตภัณฑ์

- ออกแบบมาเพื่อเก็บบันทึกการทำงานระบบแบบรวมศูนย์
- รองรับการเก็บข้อมูลบันทึกการทำงานด้วยมาตรฐาน Syslog Protocol RFC5424
- สามารถบริหารจัดการอุปกรณ์ผ่านมาตรฐาน HTTPS, Command Line Interface และ SSH
- มีหน้าแสดงจอภาพรวมเพื่อประโยชน์ในการเฝ้าดูบันทึกจากแหล่งต่างๆ
- ซอฟต์แวร์รองรับการติดตั้งบนเครื่องแม่ข่ายจริงและเครื่องแม่ข่ายเสมือนจริง (virtual machine)
- สามารถแจ้งเตือนผ่านอีเมล
- สามารถสำรองข้อมูล (Data Backup) เพื่อไปเก็บที่ External Storage พร้อมตรวจสอบความถูกต้องของไฟล์ด้วย Hashing เช่น MD5, SHA-1, SHA-256
- สามารถกำหนดเวลามาตรฐานด้วย NTP
- สามารถควบคุมระยะเวลาการเก็บข้อมูล (Data retention) และการส่งออกข้อมูล (Export) แบบอัตโนมัติ

NetkaView Logger หรือ NLG

เป็นอุปกรณ์เก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ซึ่งผ่านการทดสอบและได้รับการรับรองตามข้อกำหนดของมาตรฐาน มศอ.4003.1-2560 “ระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์” โดยศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ ซึ่งเป็นข้อกำหนดที่ถูกพัฒนาโดยอ้างอิงพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560

NetkaView Logger สามารถรับ เก็บบันทึก และรักษาบูรณภาพข้อมูลจราจรทางคอมพิวเตอร์ตามหลักการที่ถูกต้องโดยชอบด้วยกฎหมาย เพื่อลดความเสี่ยงต่อการสูญเสียความถูกต้องสมบูรณ์ของข้อมูล (Data Integrity) และเพียงพอสำหรับระบุผู้เกี่ยวข้องได้อย่างน่าเชื่อถือ



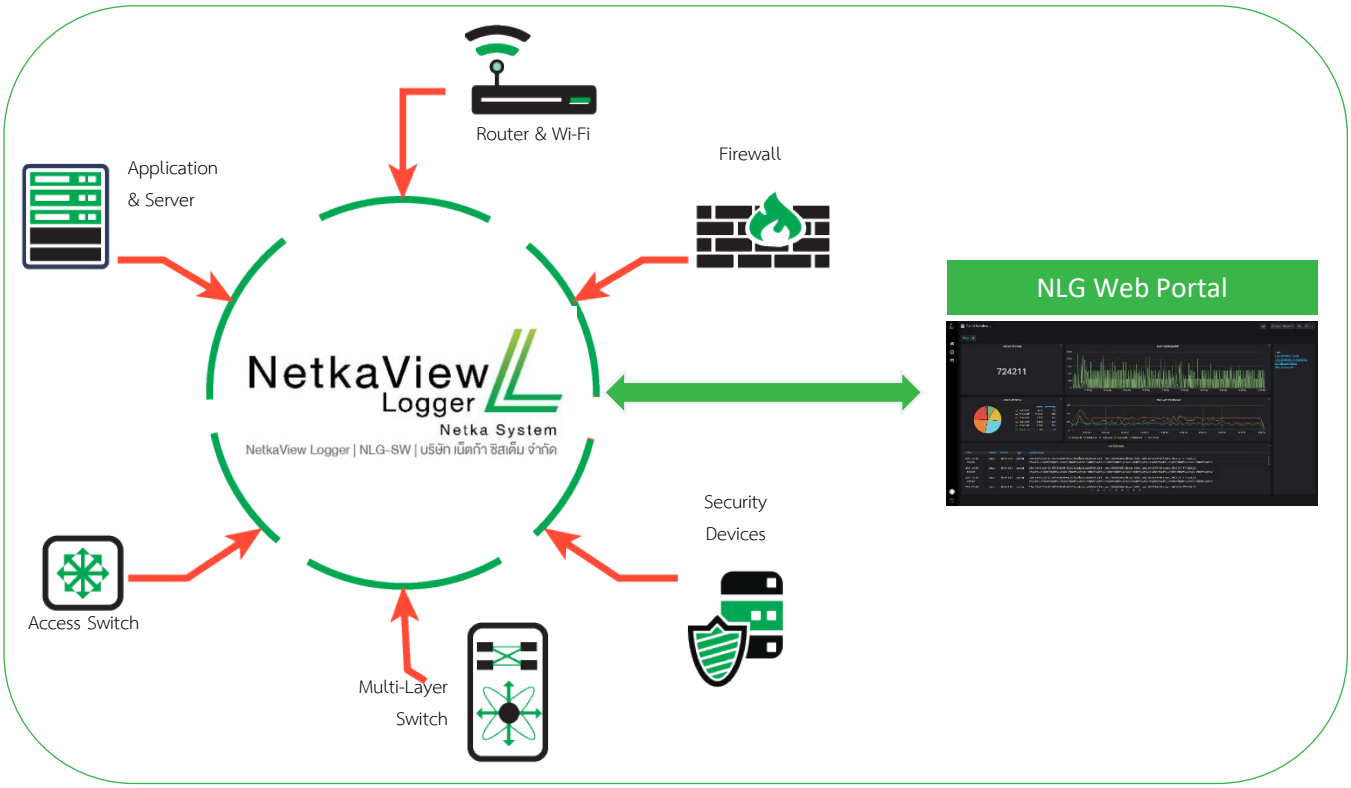
คุณสมบัติของผลิตภัณฑ์ NLG

NetkaView Logger (หรือ NLG) เป็นซอฟต์แวร์หรือ Appliance ที่ได้รับการออกแบบมาให้มีคุณสมบัติความสามารถในการรับข้อมูลเหตุการณ์ที่เกิดขึ้นทางคอมพิวเตอร์ในรูปแบบบันทึกเหตุการณ์หรือ Log จากระบบต่างๆ เช่น Switch, Router, Firewall, VPN, Network devices, Server, OS, Database เป็นต้น เพื่อเก็บรวบรวมข้อมูลดังกล่าวไว้ใช้ในการวิเคราะห์เหตุการณ์ที่ปรากฏ ด้วยมาตรฐาน Syslog ซึ่งมีประโยชน์ในการสืบเสาะหาความเกี่ยวพันของข้อมูลจราจรคอมพิวเตอร์ เช่น ข้อมูลบันทึกการเข้าถึงระบบจากเครื่องลูกข่าย (client) ไปยังเครื่องแม่ข่าย (server) ระบุวันเวลาที่เกิดเหตุการณ์, ระบุแหล่งของเหตุการณ์ เป็นต้น ตามข้อกำหนดของมาตรฐาน มศอ.4003.1-2560 ระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์

NLG รองรับการทำงานทั้งบนเครื่องแม่ข่ายจริง (barebone) และบนเครื่องแม่ข่ายแบบเสมือนจริง (virtual machine) บนระบบจำลองเครื่องแม่ข่าย (Hypervisor) เช่น VMware, Microsoft Hyper-V, Redhat KVM, Oracle Virtual Box เป็นต้น ช่วยให้เกิดความยืดหยุ่นต่อผู้ใช้งาน NLG ได้เป็นอย่างดี

การติดตั้ง NLG เพื่อเก็บข้อมูลบันทึกการทำงานของระบบสารสนเทศ

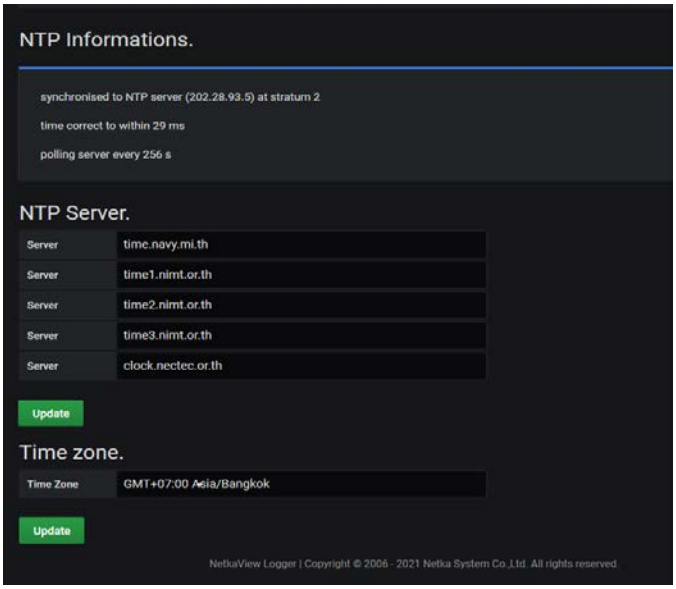
การติดตั้งระบบ NLG ภายในเครือข่ายคอมพิวเตอร์เพื่อเก็บบันทึกการทำงาน (Log) ให้กับระบบสารสนเทศซึ่งประกอบด้วยอุปกรณ์เครือข่าย เครื่องแม่ข่าย ระบบงาน อุปกรณ์รักษาความปลอดภัย และอุปกรณ์ด้านสารสนเทศอื่นๆ

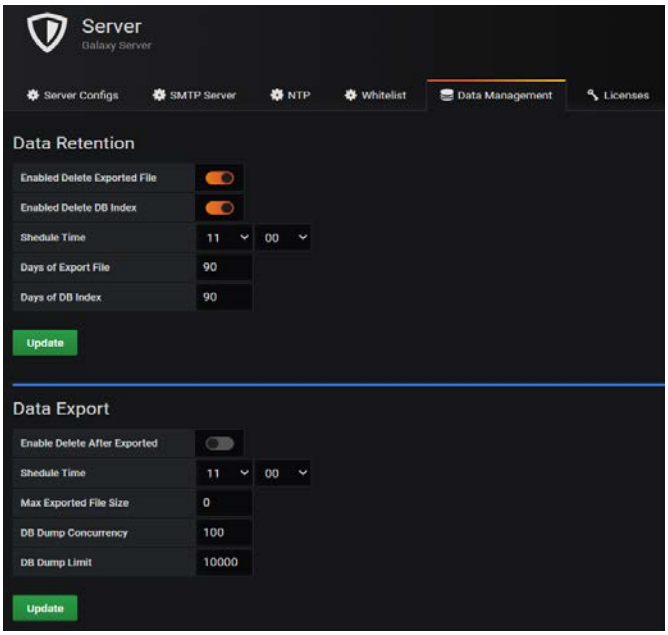


คุณสมบัติของผลิตภัณฑ์ NLG

Network Time Protocol (NTP)

มีคุณสมบัติในการตั้งค่า Network Time Protocol (NTP) และค่าเวลา Time zone ซึ่งใช้สำหรับการกำหนดเวลามาตรฐาน เพื่อตั้งค่าเวลาของระบบจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ให้ตรงกับเวลามาตรฐานสากล



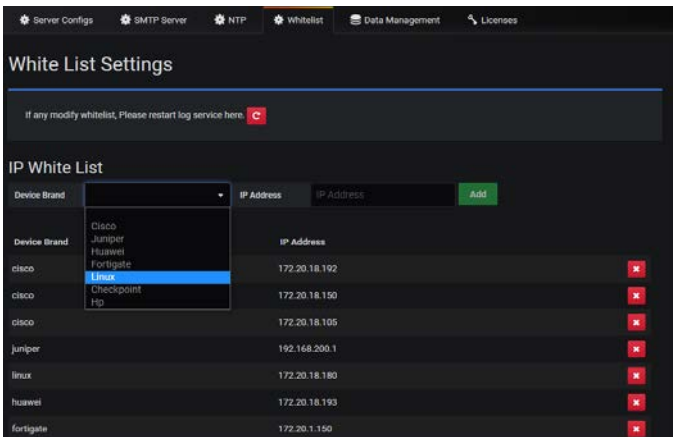


Data Management

สามารถบริหารจัดการข้อมูล (Data Management) ซึ่งใช้สำหรับการควบคุมระยะเวลาเก็บข้อมูล (Data retention) และการส่งออกข้อมูล (Export) แบบอัตโนมัติเพื่อเก็บไว้ในพื้นที่จัดเก็บของระบบ

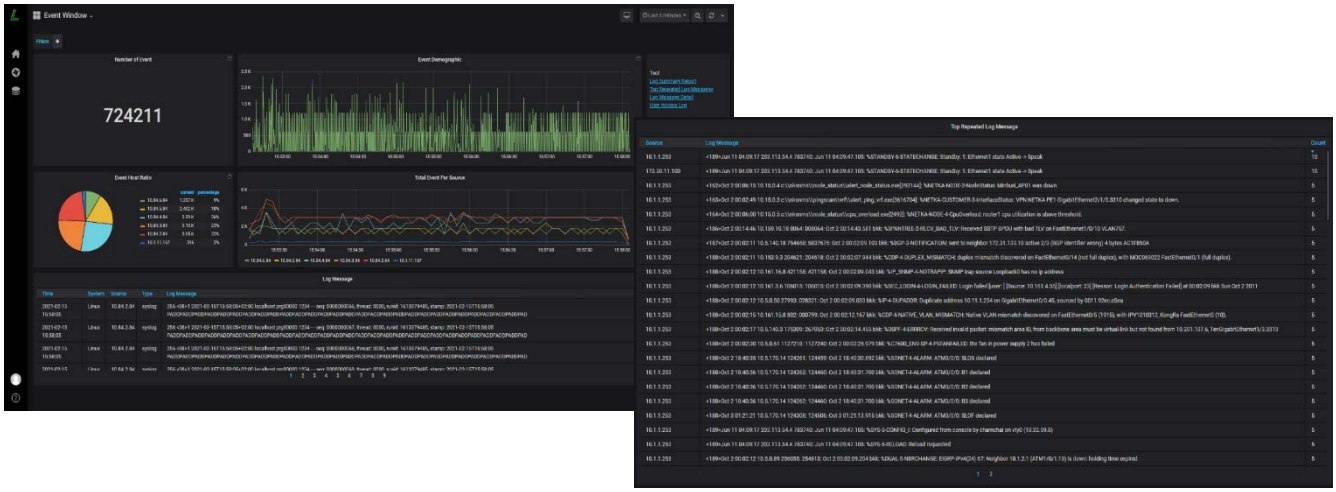
Whitelist / Filtering

หน้าจอเมนู Whitelist ใช้สำหรับการระบุหมายเลข IP address ของอุปกรณ์ หรือเครื่องแม่ข่ายต้นทางที่ NLG จะอนุญาตให้รับข้อมูลจราจรทางคอมพิวเตอร์ (Log or Event) ได้ ช่วยเพิ่ม Security ให้กับระบบ



คุณสมบัติในการวิเคราะห์และแสดงข้อมูล Log จากแหล่งต่างๆ

หน้าจอแสดงผลข้อมูลที่มาจากแหล่งต่างๆ ที่ดูเข้าใจง่ายและสามารถใช้เพื่อค้นหาและวิเคราะห์ข้อมูลได้ง่ายและรวดเร็ว สามารถนำข้อมูลออกจากระบบ (Export) ได้อย่างมีประสิทธิภาพ



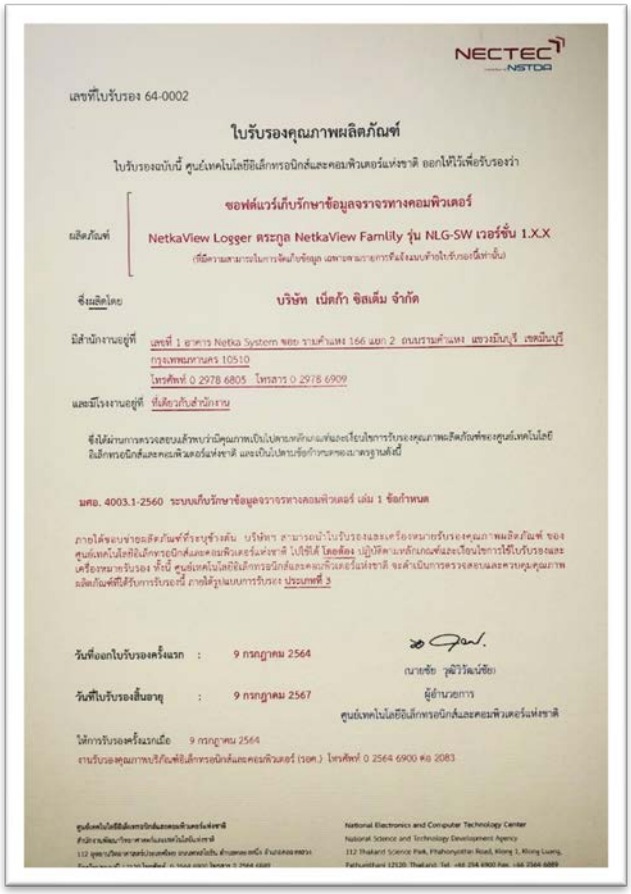
คุณสมบัติหลักของเครื่องแม่ข่ายที่แนะนำสำหรับการติดตั้ง NetkaView Logger

Specification	MDES Spec 1	MDES Spec 2	MDES Spec 3
CPU (vCPU)	4 core (8 vCPU)	8 core (16 vCPU)	16 core (32 vCPU)
Memory (GB)	8	16	32
Storage size (TB)	0.5-2	1-7	2-20
Network Interface (port)	1	2	2
จำนวน EPS สูงสุด	1,000	7,000	20,000
ระยะเวลาเก็บข้อมูล	7-90 วัน	7-90 วัน	7-90 วัน

หมายเหตุ:

- ทดสอบภายใต้มาตรฐาน Syslog protocol แบบ UDP ด้วยขนาด packet 256 bytes
- ระยะเวลาการเก็บข้อมูลให้ได้ 90 วัน ขึ้นอยู่กับจำนวน log ที่จัดเก็บ ซึ่งอาจจะต้องมีการเพิ่มขนาด Disk

ใบรับรองคุณภาพผลิตภัณฑ์ NetkaView Logger ตามมาตรฐาน มศอ.4003.1-2560



NECTEC
NSTDA

เลขที่ใบรับรอง 64-0002

ใบรับรองคุณภาพผลิตภัณฑ์

ใบรับรองฉบับนี้ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ ออกให้ไว้เพื่อรับรองว่า

ผลิตภัณฑ์ ซอฟต์แวร์เก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์
NetkaView Logger ตระกูล NetkaView Family รุ่น NLG-SW เวอร์ชั่น 1.X.X
(ที่มีความสามารถในการจัดเก็บข้อมูล เฉพาะตามรายการที่ส่งมอบด้วยในรับรองนี้เท่านั้น)

ซึ่งผลิตโดย บริษัท เน็ตก้า ซิสเต็ม จำกัด

มีสำนักงานอยู่ที่ เลขที่ 1 อาคาร Netka System ซอย รามคำแหง 166 แยก 2 ถนนรามคำแหง แขวงมีนบุรี เขตมีนบุรี กรุงเทพมหานคร 10510
โทรศัพท์ 0 2978 6805 โทรสาร 0 2978 6909

และมีโรงงานอยู่ที่ ที่เดียวกับสำนักงาน

ซึ่งได้ผ่านการตรวจสอบแล้วพบว่ามีคุณภาพเป็นไปตามหลักเกณฑ์และเงื่อนไขการรับรองคุณภาพผลิตภัณฑ์ของศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ และเป็นไปตามข้อกำหนดของมาตรฐานดังนี้

มศอ. 4003.1-2560 ระบบเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ เล่ม 1 ข้อกำหนด

ภายใต้ขอบข่ายผลิตภัณฑ์ที่ระบุข้างต้น บริษัทฯ สามารถนำใบรับรองและเครื่องหมายรับรองคุณภาพผลิตภัณฑ์ ของศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ ไปใช้ได้ โดยต้อง ปฏิบัติตามหลักเกณฑ์และเงื่อนไขการใช้ใบรับรองและเครื่องหมายรับรอง ทั้งนี้ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ จะดำเนินการตรวจสอบและควบคุมคุณภาพผลิตภัณฑ์ที่ได้รับการรับรองนี้ ภายใต้รายละเอียดการรับรอง ประเภทที่ 3

วันที่ออกใบรับรองครั้งแรก : 9 กรกฎาคม 2564
วันที่ใบรับรองสิ้นอายุ : 9 กรกฎาคม 2567

(นายชัย วุฒิวิวัฒน์ชัย)
ผู้อำนวยการ
ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

ให้การรับรองครั้งแรกเมื่อ 9 กรกฎาคม 2564
งานรับรองคุณภาพผลิตภัณฑ์อิเล็กทรอนิกส์และคอมพิวเตอร์ (รอค.) โทรศัพท์ 0 2564 6900 ต่อ 2083

National Electronics and Computer Technology Center
National Science and Technology Development Agency
112 Thailand Science Park, Phahonyothin Road, Klong 1, Klong Luang, Pathumthani 12120, Thailand. Tel. +66 2564 6900 Fax. +66 2564 6889

ระบบบันทึกข้อมูลจราจรทางคอมพิวเตอร์ (Traffic Data หรือ Log file) สำหรับองค์กร พัฒนาตามหลักเกณฑ์ "พระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์ พ.ศ. 2550 และ พ.ศ. 2560" ซึ่งเป็นผลิตภัณฑ์ที่สามารถเก็บข้อมูลได้ถูกต้องตามหลักกฎหมายและข้อกำหนดต่างๆ ได้อย่างครบถ้วน ที่ผ่านการทดสอบทั้งจากศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (NECTEC) และ สถาบันประเมินและรับรองเทคโนโลยีดิจิทัล (DTEC) ตามมาตรฐาน มศอ.4003.1-2560

แหล่งอ้างอิงข้อมูล: https://www.nectec.or.th/dtec/certification/

Contact Us
Netka System Co., Ltd.
Telephone: +662-978-6805, Fax. +662-978-6909, Email: sales@netkasystem.com
Visit us on the web: https://www.netkasystem.com