รายละเอียดการจัดการกับข้อมูลจราจรทางคอมพิวเตอร์โดย FortiGate และ FortiAnalyzer
ตามประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ พ.ศ. ๒๕๕๐

ข้อมูลจราจรทางคอมพิวเตอร์ ตามภาคผนวก ข ซึ่งผู้ให้บริการตามประกาศข้อ ๕ (๑) ข. ถึง ค. มีหน้าที่ต้องเก็บรักษา

- **ข้อมูลที่เกิดขึ้นบนอุปกรณ์ประเภท Gateway**

ข้อ	ประเภท	รายการ	FortiGate ทำงานร่วมกับ Syslog server	FortiGate ทำงานร่วมกับ FortiAnalyzer	หมายเหตุ
๒	ก. ข้อมูลอินเทอร์เน็ตที่เกิดจากการเข้าถึงระบบเครือข่าย	๑) ข้อมูล Log ที่มีการบันทึกไว้เมื่อมีการเข้าถึงระบบเครือข่าย ซึ่งระบุถึงตัวตนและสิทธิในการเข้าถึงเครือข่าย (Access logs specific to Authentication and Authorization server)	มี	มี	
		๒) วันและเวลาการติดต่อของเครื่องที่เข้ามาใช้บริการและเครื่องให้บริการ (Date and time of connection of client to server)	มี	มี	
		๓) ชื่อที่ระบุตัวตนผู้ใช้ (User ID)	มี	มี	
		๔) หมายเลขชุดอินเทอร์เน็ตที่ถูกกำหนดให้โดยระบบผู้ให้บริการ (Assigned IP address)	มี	มี	
		๕) ข้อมูลที่บอกถึงหมายเลขสายที่เรียกเข้ามา (Calling line identification)	N/A	N/A	เป็นหมายเลขของสายโทรศัพท์ ที่เรียกเข้ามายัง Remote Access Server (RAS) หรือ xDSL ซึ่งเป็นหน้าที่ของ RAS หรือ xDSL ที่จะต้องจัดให้มีข้อมูลนี้

■ **ข้อมูลที่เกิดขึ้นบน e-mail server**

ข้อ	ประเภท	รายการ	FortiGate ทำงานร่วมกับ Syslog server	FortiGate ทำงานร่วมกับ FortiAnalyzer	Local log บน E-mail server
๒	ข. ข้อมูลอินเทอร์เน็ตบนเครื่องผู้ให้บริการจดหมายอิเล็กทรอนิกส์ (e-mail servers)	๑) หมายเลขของข้อความที่ระบุในจดหมายอิเล็กทรอนิกส์ (Message ID)	ไม่มี	ไม่มี	มี
		๒) ชื่อที่อยู่อิเล็กทรอนิกส์ของผู้ส่ง (Sender e-mail address)	มี	มี	มี
		๓) ชื่อที่อยู่อิเล็กทรอนิกส์ของผู้รับ (Receiver e-mail address)	มี	มี	มี
		๔) ข้อมูลที่บอกถึงสถานะในการตรวจสอบ (Status indicator) ซึ่งได้แก่ จดหมายอิเล็กทรอนิกส์ที่ส่งสำเร็จ ส่งคืน ส่งล่าช้า เป็นต้น	ไม่มี	ไม่มี	มี
		๕) ข้อมูลหมายเลขชุดอินเทอร์เน็ตของเครื่องคอมพิวเตอร์ผู้ใช้บริการ (IP address of client connected to server)	มี	มี	มี
		๖) วัน และเวลาการติดต่อ (Date and time of connection of client connected to server)	มี	มี	มี
		๗) ข้อมูลหมายเลขชุดอินเทอร์เน็ตของเครื่องบริการจดหมายอิเล็กทรอนิกส์ (IP address of sending computer)	มี	มี	มี
		๘) ชื่อผู้ใช้งาน (User ID) (ถ้ามี)	มี	มี	มี
		๙) บันทึกการเข้าถึงข้อมูล e-mail โดยผ่านโปรแกรมจากเครื่องของสมาชิก อันได้แก่ POP3 และ IMAP4	มี	มี	มี

■ **ข้อมูลที่เกิดขึ้นบนเครื่องให้บริการโอนแฟ้มข้อมูล**

ข้อ	ประเภท	รายการ	FortiGate ทำงานร่วมกับ Syslog server	FortiGate ทำงานร่วมกับ FortiAnalyzer	Local log โดยเครื่องให้บริการโอนแฟ้มข้อมูล
๒	ค. ข้อมูลอินเทอร์เน็ตจากการโอนแฟ้มข้อมูลบนเครื่องให้บริการโอนแฟ้มข้อมูล	๑) Log ที่บันทึกเมื่อมีการเข้าถึงเครื่องให้บริการ	มี	มี	มี
		๒) วันและเวลาการติดต่อของเครื่องที่เข้ามาใช้บริการและเครื่องให้บริการ (Date and time of connection of client to server)	มี	มี	มี
		๓) หมายเลขชุดอินเทอร์เน็ตของเครื่องคอมพิวเตอร์ผู้เข้าใช้ที่เชื่อมต่ออยู่ขณะนั้น (IP Source address)	มี	มี	มี
		๔) ชื่อผู้ใช้งาน (User ID) (ถ้ามี)	มี	มี	มี
		๕) ตำแหน่ง (Path) และชื่อไฟล์ที่อยู่บนเครื่องให้บริการโอนถ่ายข้อมูลที่มีการส่งขึ้นมาบันทึกหรือให้ดึงข้อมูลออกไป (Path and filename of data object uploaded or downloaded)	ไม่มี	ไม่มี	มี

■ **ข้อมูลที่เกิดขึ้นบนเครื่องผู้ให้บริการเว็บ**

ข้อ	ประเภท	รายการ	FortiGate ทำงานร่วมกับ Syslog server	FortiGate ทำงานร่วมกับ FortiAnalyzer	Local log โดยเครื่องผู้ให้บริการเว็บ
๒	ง. ข้อมูลอินเทอร์เน็ตบนเครื่องผู้ให้บริการเว็บ	๑) Log ที่บันทึกเมื่อมีการเข้าถึงเครื่องผู้ให้บริการเว็บ	มี	มี	มี
		๒) วันและเวลาการติดต่อของเครื่องที่เข้ามาใช้บริการและเครื่องให้บริการ (Date and time of connection of client to server)	มี	มี	มี
		๓) หมายเลขชุดอินเทอร์เน็ตของเครื่องคอมพิวเตอร์ผู้เข้าใช้ที่เชื่อมต่ออยู่ขณะนั้น (IP Source address)	มี	มี	มี
		๔) ข้อมูลคำสั่งการใช้งานระบบ	มี	มี	มี
		๕) ข้อมูลที่บ่งบอกถึงเส้นทางในการเรียกดูข้อมูล (URI: Uniform Resource Identifier) เช่น ตำแหน่งของเว็บเพ็จ	มี	มี	มี

■ **ข้อมูลที่เกิดขึ้นบนเครือข่ายคอมพิวเตอร์ขนาดใหญ่ (Usenet: NNTP)**

ข้อ	ประเภท	รายการ	FortiGate ทำงานร่วมกับ Syslog server	FortiGate ทำงานร่วมกับ FortiAnalyzer	หมายเหตุ
๒	จ. ข้อมูลบนเครือข่ายคอมพิวเตอร์ขนาดใหญ่ (Usenet)	๑) Log ที่บันทึกเมื่อมีการเข้าถึงเครือข่าย NNTP	มี	มี	เป็นระบบเก่าไม่เป็นที่นิยมในปัจจุบัน
		๒) วันและเวลาการติดต่อของเครื่องที่เข้ามาใช้บริการและเครื่องให้บริการ (Date and time of connection of client to server)	มี	มี	
		๓) หมายเลข port ในการใช้งาน (Protocol Process ID)	มี	มี	
		๔) ชื่อเครื่องให้บริการ (Host name)	มี	มี	
		๕) ข้อมูลหมายเลขลำดับข้อความที่ได้ถูกส่งไปแล้ว (Posted message ID)	ไม่มี	ไม่มี	

■ **ข้อมูลที่เกิดจากการตอบโต้กันบนเครือข่ายอินเทอร์เน็ต (Chat หรือ IM)**

ข้อ	ประเภท	รายการ	FortiGate ทำงานร่วมกับ Syslog server	FortiGate ทำงานร่วมกับ FortiAnalyzer	หมายเหตุ
	ฉ.	๑) วันและเวลาการติดต่อของผู้ใช้บริการ	มี	มี	
๒	ช. ข้อมูลที่เกิดจากการตอบโต้กันบนเครือข่ายอินเทอร์เน็ต เช่น IRC หรือ IM	๒) ชื่อเครื่องบนเครือข่าย และหมายเลขเครื่องของผู้ให้บริการที่เครื่องคอมพิวเตอร์เชื่อมต่ออยู่ขณะนั้น (Host name and IP address)	มี	มี	
		๓) ชื่อผู้ใช้บริการที่ตอบโต้กัน (IM user name)	**มี**	**มี**	**ไม่ได้เป็นข้อกำหนดใน พรบ.**
		๔) ชนิดของ Protocol ที่ใช้งาน เช่น MSN Yahoo-MSN ICQ เป็นต้น	**มี**	**มี**	

<u>ข้อมูลจราจรทางคอมพิวเตอร์ ตามภาคผนวก ข ซึ่งผู้ให้บริการตามประกาศข้อ ๕ (๑) ง. มีหน้าที่ต้องเก็บรักษา</u>

■ **ข้อมูลการให้บริการในร้านอินเทอร์เน็ต**

ข้อ	ประเภท	รายการ	FortiGate ทำงานร่วมกับ Syslog server	FortiGate ทำงานร่วมกับ FortiAnalyzer	หมายเหตุ
๓	ก. ผู้ให้บริการร้านอินเทอร์เน็ต	๑) ข้อมูลที่สามารถระบุตัวบุคคล	มี	มี	ผู้ให้บริการจำเป็นต้องบันทึกหมายเลขประจำตัวของผู้ใช้บริการด้วย เช่น หมายเลขบัตรประชาชน เป็นต้น
		๒) เวลาการเข้าใช้ และเลิกใช้ใช้บริการ	มี	มี	
		๓) หมายเลขเครื่องที่ใช้ IP address	มี	มี	