



คำสั่ง โรงเรียนมหิตลวิทยานุสรณ์ นครปฐม
ที่ ๘๗/๒๕๖๒

เรื่อง แต่งตั้ง คณะกรรมการพิจารณาผลการประกวดราคาอิเล็กทรอนิกส์ และคณะกรรมการตรวจรับพัสดุ สำหรับ
การประกวดราคาซื้อระบบป้องกันการบุกรุกโจมตี ด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ (e-bidding)

ด้วย โรงเรียนมหิตลวิทยานุสรณ์ นครปฐม มีความประสงค์จะ ประกวดราคาซื้อระบบป้องกันการบุกรุก
โจมตี ด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ (e-bidding) และเพื่อให้เป็นไปตามระเบียบกระทรวงการคลังว่าด้วยการ
จัดซื้อจัดจ้าง และการบริหารพัสดุภาครัฐ พ.ศ. ๒๕๖๐ จึงขอแต่งตั้งรายชื่อต่อไปนี้เป็น คณะกรรมการพิจารณาผลการ
ประกวดราคาอิเล็กทรอนิกส์ และคณะกรรมการตรวจรับพัสดุ สำหรับการประกวดราคาซื้อระบบป้องกันการบุกรุก
โจมตี ด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ (e-bidding)

คณะกรรมการพิจารณาผลการประกวดราคาอิเล็กทรอนิกส์

- | | |
|----------------------------------|---------------------|
| ๑. นางสาวเลขาขวัญ งามประสิทธิ์ | ประธานกรรมการฯ |
| ครูวิชาการ | |
| ๒. นายนิรุจน์ ทองโสภะ | กรรมการ |
| เจ้าหน้าที่ชำนาญการ | |
| ๓. นางสาวจิรนนท์ เกรียงธีรศักดิ์ | กรรมการและเลขานุการ |
| เจ้าหน้าที่ชำนาญการ | |
| อำนาจและหน้าที่ | |

ลงลายมือชื่อพร้อมตรวจสอบเอกสารหลักฐานการเสนอราคาต่างๆ และพิจารณาผลตามเงื่อนไขที่
ส่วนราชการกำหนดไว้ในประกาศและเอกสารประกวดราคาอิเล็กทรอนิกส์
คณะกรรมการตรวจรับพัสดุ

- | | |
|---------------------------------|----------------------------|
| ๑. นายบุญนที ศักดิ์บุญญารัตน์ | ประธานกรรมการฯ |
| ครูชำนาญการ | |
| ๒. นายสิทธิกร แก้วจินดา | กรรมการ |
| เจ้าหน้าที่ชำนาญการ | |
| ๓. นางสาววลัยลักษณ์ ทุ่งศรีแก้ว | กรรมการและผู้ช่วยเลขานุการ |
| เจ้าหน้าที่ชำนาญการ | |
| อำนาจและหน้าที่ | |
| ตรวจรับพัสดุ | |

สั่ง ณ วันที่ 11 เมษายน พ.ศ. ๒๕๖๒

(นายวิวัฒน์ เรืองเลิศปัญญากุล)

รักษาการในตำแหน่งผู้อำนวยการโรงเรียนมหิตลวิทยานุสรณ์



สัญญาซื้อขาย

สัญญาเลขที่ ๘/๒๕๖๒

สัญญาฉบับนี้ทำขึ้น ณ โรงเรียนมหิตลวิทยานุสรณ์ เลขที่ ๓๖๔ หมู่ ๕ ตำบลศาลายา อำเภอพุทธมณฑล จังหวัดนครปฐม ๗๓๑๗๐ เลขประจำตัวผู้เสียภาษี ๐๙๙๔๐๐๐๕๒๑๔๗๒ เมื่อวันที่ ๖ เดือนมิถุนายน พ.ศ. ๒๕๖๒ ระหว่าง โรงเรียนมหิตลวิทยานุสรณ์ โดย นายวิวัฒน์ เรืองเลิศปัญญากุล ตำแหน่งผู้อำนวยการโรงเรียนมหิตลวิทยานุสรณ์ ซึ่งต่อไปในสัญญานี้เรียกว่า “ผู้ซื้อ” ฝ่ายหนึ่ง กับ บริษัท จีเอเบิล จำกัด ซึ่งจดทะเบียนเป็นนิติบุคคล ณ สำนักงานทะเบียนหุ้นส่วนบริษัทกรุงเทพมหานคร กรมพัฒนาธุรกิจการค้า กระทรวงพาณิชย์ มีสำนักงานใหญ่อยู่เลขที่ ๑๒๗/๒๗,๒๙-๓๑ ถนนนนทบุรี แขวงช่องนนทรี เขตยานนาวา กรุงเทพมหานคร โดย นางสาวสัททยา สิงหเสม ผู้มีอำนาจลงนามผูกพันนิติบุคคลปรากฏตามหนังสือรับรองของสำนักงานทะเบียนหุ้นส่วนบริษัททะเบียนนิติบุคคลเลขที่ ๐๑๐๕๕๓๒๐๐๙๔๖๔ ลงวันที่ ๔ เดือนเมษายน พ.ศ. ๒๕๖๒ (ตามหนังสือมอบอำนาจลงวันที่ ๓๐ เมษายน ๒๕๖๒) แนนท้ายสัญญานี้ ซึ่งต่อไปในสัญญานี้เรียกว่า “ผู้ขาย” อีกฝ่ายหนึ่ง

คู่สัญญาได้ตกลงกันมีข้อความดังต่อไปนี้

ข้อ ๑ ข้อตกลงซื้อขาย

ผู้ซื้อตกลงซื้อและผู้ขายตกลงขาย ระบบป้องกันการบุกรุกโจมตี จำนวน ๑ ระบบ เป็นราคาทั้งสิ้น ๑,๐๗๖,๘๘๘ บาท (หนึ่งล้านเจ็ดหมื่นหกพันแปดร้อยแปดสิบแปดบาทถ้วน) ซึ่งได้รวมภาษีมูลค่าเพิ่มตลอดจนภาษีอากรอื่นๆ และค่าใช้จ่ายทั้งปวงด้วยแล้ว

ข้อ ๒ การรับรองคุณภาพ

ผู้ขายรับรองว่าสิ่งของที่ขายให้ตามสัญญานี้เป็นของแท้ ของใหม่ ไม่เคยใช้งานมาก่อน ไม่เป็นของเก่าเก็บ และมีคุณภาพและคุณสมบัติไม่ต่ำกว่าที่กำหนดไว้ในเอกสารแนบท้ายสัญญาผนวก ๑ และผนวก ๒

ในกรณีที่เป็นการซื้อสิ่งของซึ่งจะต้องมีการตรวจสอบ ผู้ขายรับรองว่า เมื่อตรวจสอบแล้วต้องมีคุณภาพและคุณสมบัติไม่ต่ำกว่าที่กำหนดไว้ตามสัญญานี้ด้วย

ข้อ ๓ เอกสารอันเป็นส่วนหนึ่งของสัญญา

เอกสารแนบท้ายสัญญาดังต่อไปนี้ให้ถือเป็นส่วนหนึ่งของสัญญานี้

๓.๑ ผนวก ๑ แคตตาล็อกและหรือแบบรูปรายการละเอียดคุณลักษณะเฉพาะ

จำนวน ๑๐๒ หน้า

๓.๒ ผนวก ๒ ใบเสนอราคา

จำนวน ๒ หน้า

ความใดในเอกสารแนบท้ายสัญญาที่ขัดหรือแย้งกับข้อความในสัญญานี้ ให้ใช้ข้อความในสัญญานี้บังคับ และในกรณีที่เอกสารแนบท้ายสัญญาขัดแย้งกันเอง ผู้ขายจะต้องปฏิบัติตามคำวินิจฉัยของผู้ซื้อ คำวินิจฉัยของผู้ซื้อให้ถือเป็นที่สุด และผู้ขายไม่มีสิทธิเรียกร้องราคา ค่าเสียหาย หรือค่าใช้จ่ายใดๆ เพิ่มเติมจากผู้ซื้อทั้งสิ้น



ข้อ ๔ การส่งมอบ

ผู้ขายจะส่งมอบสิ่งของที่ซื้อขายตามสัญญาให้แก่ผู้ซื้อ ณ โรงเรียนมหิตลวิทย์ยานุสรณ์ ภายในวันที่ ๔ เดือนกันยายน พ.ศ. ๒๕๖๒ (กำหนดส่งสินค้า ๙๐ วัน) ให้ถูกต้องและครบถ้วนตามที่กำหนดไว้ในข้อ ๑ แห่งสัญญานี้ พร้อมทั้งหีบห่อหรือเครื่องรัดพันผูกโดยเรียบร้อย

การส่งมอบสิ่งของตามสัญญานี้ ไม่ว่าจะเป็นการส่งมอบเพียงครั้งเดียว หรือส่งมอบหลายครั้ง ผู้ขายจะต้องแจ้งกำหนดเวลาส่งมอบแต่ละครั้งโดยทำเป็นหนังสือนำไปยื่นต่อผู้ซื้อ ณ โรงเรียนมหิตลวิทย์ยานุสรณ์ ในวันและเวลาทำการของผู้ซื้อ ก่อนวันส่งมอบไม่น้อยกว่า ๓ วันทำการของผู้ซื้อ

ข้อ ๕ การตรวจรับ

เมื่อผู้ซื้อได้ตรวจรับสิ่งของที่ส่งมอบและเห็นว่าถูกต้องครบถ้วนตามสัญญาแล้ว ผู้ซื้อจะออกหลักฐานการรับมอบเป็นหนังสือไว้ให้ เพื่อผู้ขายนำมาเป็นหลักฐานประกอบการขอรับเงินค่าสิ่งของนั้น

ถ้าผลของการตรวจรับปรากฏว่า สิ่งของที่ผู้ขายส่งมอบไม่ตรงตามข้อ ๑ ผู้ซื้อทรงไว้ซึ่งสิทธิที่จะไม่รับสิ่งของนั้น ในกรณีเช่นว่านี้ ผู้ขายต้องรับนำสิ่งของนั้นกลับคืนโดยเร็วที่สุดเท่าที่จะทำได้ และนำสิ่งของมาส่งมอบให้ใหม่ หรือต้องทำการแก้ไขให้ถูกต้องตามสัญญาด้วยค่าใช้จ่ายของผู้ขายเอง และระยะเวลาที่เสียไปเพราะเหตุดังกล่าวผู้ขายจะนำมาอ้างเป็นเหตุขอขยายเวลาส่งมอบตามสัญญาหรือของดหรือลดค่าปรับไม่ได้

ในกรณีที่ผู้ขายส่งมอบสิ่งของถูกต้องแต่ไม่ครบจำนวน หรือส่งมอบครบจำนวนแต่ไม่ถูกต้องทั้งหมด ผู้ซื้อจะตรวจรับเฉพาะส่วนที่ถูกต้อง โดยออกหลักฐานการตรวจรับเฉพาะส่วนนั้นก็ได้

ข้อ ๖ การชำระเงิน

ผู้ซื้อตกลงชำระเงินค่าสิ่งของตามข้อ ๑ ให้แก่ผู้ขาย เมื่อผู้ซื้อได้รับมอบสิ่งของตามข้อ ๕ ไว้โดยครบถ้วนแล้ว

การจ่ายเงินตามเงื่อนไขแห่งสัญญานี้ ผู้ซื้อจะโอนเงินเข้าบัญชีเงินฝากธนาคารของผู้ขาย ชื่อ ธนาคารทหารไทย จำกัด (มหาชน) ชื่อบัญชี บ.จีเอเบิล เลขที่บัญชี ๒๐๓-๑-๐๐๐๐๓-๓ ทั้งนี้ ผู้ขายตกลงเป็นผู้รับภาระเงินค่าธรรมเนียม หรือค่าบริการอื่นใดเกี่ยวกับการโอน รวมทั้งค่าใช้จ่ายใดๆ (ถ้ามี) ที่ธนาคารเรียกเก็บ และยินยอมให้มีการหักเงินดังกล่าวจากจำนวนเงินโอนในงวดนั้นๆ

ข้อ ๗ การรับประกันความชำรุดบกพร่อง

ผู้ขายตกลงรับประกันความชำรุดบกพร่องหรือขัดข้องของสิ่งของตามสัญญานี้ เป็นเวลา ๓ ปี นับถัดจากวันที่ผู้ซื้อได้รับมอบสิ่งของทั้งหมดไว้โดยถูกต้องครบถ้วนตามสัญญา โดยภายในกำหนดเวลาดังกล่าว หากสิ่งของ ตามสัญญานี้เกิดชำรุดบกพร่องหรือขัดข้องอันเนื่องมาจากการใช้งานตามปกติ ผู้ขายจะต้องจัดการซ่อมแซมหรือแก้ไขให้อยู่ในสภาพที่ใช้การได้ดีดังเดิม ภายใน ๗ วัน นับถัดจากวันที่ได้รับแจ้งจากผู้ซื้อ โดยไม่คิดค่าใช้จ่ายใดๆ ทั้งสิ้น หากผู้ขายไม่จัดการซ่อมแซมหรือแก้ไขภายในกำหนดเวลาดังกล่าว ผู้ซื้อจะมีสิทธิที่จะทำการนั้นเองหรือจ้างผู้อื่นให้ทำการนั้นแทนผู้ขาย โดยผู้ขายต้องเป็นผู้ออกค่าใช้จ่ายเองทั้งสิ้น

ในกรณีเร่งด่วนจำเป็นต้องรีบแก้ไขเหตุชำรุดบกพร่องหรือขัดข้องโดยเร็ว และไม่อาจรอคอยให้ผู้ขายแก้ไขในระยะเวลาที่กำหนดไว้ตามวรรคหนึ่งได้ ผู้ซื้อจะมีสิทธิเข้าจัดการแก้ไขเหตุชำรุดบกพร่องหรือขัดข้องนั้นเอง หรือให้ผู้อื่นแก้ไขความชำรุดบกพร่องหรือขัดข้อง โดยผู้ขายต้องรับผิดชอบชำระค่าใช้จ่ายทั้งหมด



การที่ผู้ซื้อทำการนั้นเอง หรือให้ผู้อื่นทำการนั้นแทนผู้ขาย ไม่ทำให้ผู้ขายหลุดพ้นจากความรับผิดชอบตามสัญญา หากผู้ขายไม่ชดใช้ค่าใช้จ่ายหรือค่าเสียหายตามที่ผู้ซื้อเรียกร้องผู้ซื้อจะมีสิทธิบังคับจากหลักประกันการปฏิบัติตามสัญญาได้

ข้อ ๘ หลักประกันการปฏิบัติตามสัญญา

ในขณะทำสัญญานี้ผู้ขายได้นำหลักประกันเป็นหนังสือค้ำประกัน (หลักประกันสัญญาซื้อ) เลขที่ ๑๐๐๐๒๕๒๘๕๒๗๖ ลงวันที่ ๖ มิถุนายน ๒๕๖๒ ของบริษัท ธนาคารกสิกรไทย จำกัด (มหาชน) สาขาสวนพลู เป็นจำนวนเงิน ๕๓,๘๔๕ บาท (ห้าหมื่นสามพันแปดร้อยสี่สิบบาทถ้วน) ซึ่งเท่ากับร้อยละ ๕ ของราคาทั้งหมดตามสัญญา มามอบให้แก่ผู้ซื้อเพื่อเป็นหลักประกันการปฏิบัติตามสัญญานี้

กรณีผู้ขายใช้หนังสือค้ำประกันมาเป็นหลักประกันการปฏิบัติตามสัญญา หนังสือค้ำประกันดังกล่าวจะต้องออกโดยธนาคารที่ประกอบกิจการในประเทศไทย หรือโดยบริษัทเงินทุนหรือบริษัทเงินทุนหลักทรัพย์ที่ได้รับอนุญาตให้ประกอบกิจการเงินทุนเพื่อการพาณิชย์และประกอบธุรกิจค้ำประกันตามประกาศของธนาคารแห่งประเทศไทย ตามรายชื่อบริษัทเงินทุนที่ธนาคารแห่งประเทศไทยแจ้งเวียนให้ทราบตามแบบที่คณะกรรมการนโยบายการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐกำหนด หรืออาจเป็นหนังสือค้ำประกันอิเล็กทรอนิกส์ตามวิธีการที่กรมบัญชีกลางกำหนดก็ได้ และจะต้องมีอายุการค้ำประกันตลอดไปจนกว่าผู้ขายพ้นข้อผูกพันตามสัญญานี้

หลักประกันที่ผู้ขายนำมามอบให้ตามวรรคหนึ่ง จะต้องมีความครอบคลุมความรับผิดชอบทั้งปวงของผู้ขายตลอดอายุสัญญานี้ ถ้าหลักประกันที่ผู้ขายนำมามอบให้ดังกล่าวลดลงหรือเสื่อมค่าลงหรือมีอายุไม่ครอบคลุมถึงความรับผิดชอบของผู้ขายตลอดอายุสัญญา ไม่ว่าด้วยเหตุใดๆ ก็ตาม รวมถึงกรณีผู้ขายส่งมอบสิ่งของล่าช้าเป็นเหตุให้ระยะเวลาส่งมอบหรือวันครบกำหนดความรับผิดชอบในความชำรุดบกพร่องตามสัญญาเปลี่ยนแปลงไป ไม่ว่าจะเกิดขึ้นคราวใด ผู้ขายต้องหาหลักประกันใหม่หรือหลักประกันเพิ่มเติมให้มีจำนวนครบถ้วนตามวรรคหนึ่งมามอบให้แก่ผู้ซื้อภายใน ๓๐ วัน นับถัดจากวันที่ได้รับแจ้งเป็นหนังสือจากผู้ซื้อ

หลักประกันที่ผู้ขายนำมามอบไว้ตามข้อนี้ ผู้ซื้อจะคืนให้แก่ผู้ขายโดยไม่มีดอกเบี้ยเมื่อผู้ขายพ้นจากข้อผูกพันและความรับผิดชอบทั้งปวงตามสัญญานี้แล้ว

ข้อ ๙ การบอกเลิกสัญญา

ถ้าผู้ขายไม่ปฏิบัติตามสัญญาข้อใดข้อหนึ่ง หรือเมื่อครบกำหนดส่งมอบสิ่งของตามสัญญานี้แล้ว หากผู้ขายไม่ส่งมอบสิ่งของที่ตกลงขายให้แก่ผู้ซื้อหรือส่งมอบไม่ถูกต้อง หรือไม่ครบจำนวน ผู้ซื้อจะมีสิทธิบอกเลิกสัญญาทั้งหมดหรือแต่บางส่วนได้ การใช้สิทธิบอกเลิกสัญญานั้นไม่กระทบสิทธิของผู้ซื้อที่จะเรียกร้องค่าเสียหายจากผู้ขาย

ในกรณีที่ผู้ซื้อใช้สิทธิบอกเลิกสัญญา ผู้ซื้อจะมีสิทธิรับหรือบังคับจากหลักประกันตามข้อ ๖ และข้อ ๘ เป็นจำนวนเงินทั้งหมดหรือแต่บางส่วนก็ได้ แล้วแต่ผู้ซื้อจะเห็นสมควร และถ้าผู้ซื้อจัดซื้อสิ่งของจากบุคคลอื่นเต็มจำนวนหรือเฉพาะจำนวนที่ขาดส่ง แล้วแต่กรณี ภายในกำหนด ๓ เดือน นับถัดจากวันบอกเลิกสัญญา ผู้ขายจะต้องชดใช้ราคาที่เพิ่มขึ้นจากราคาที่กำหนดไว้ในสัญญานี้ด้วย

ข้อ ๑๐ ค่าปรับ

ในกรณีที่ผู้ซื้อมิได้ใช้สิทธิบอกเลิกสัญญาตามข้อ ๙ ผู้ขายจะต้องชำระค่าปรับให้ผู้ซื้อเป็นรายวันในอัตราร้อยละ ๐.๒๐ ของราคาส่งของที่ยังไม่ได้รับมอบ นับถัดจากวันครบกำหนดตามสัญญา จนถึงวันที่ผู้ขายได้นำสิ่งของมาส่งมอบให้แก่ผู้ซื้อจนถูกต้องครบถ้วนตามสัญญา



การคิดค่าปรับในกรณีสิ่งของที่ตกลงซื้อขายประกบกันเป็นชุด แต่ผู้ขายส่งมอบเพียงบางส่วน หรือขาดส่วนประกบส่วนหนึ่งส่วนใดไปทำให้ไม่สามารถใช้ได้โดยสมบูรณ์ ให้ถือว่ายังไม่ได้ส่งมอบสิ่งของนั้นเลย และให้คิดค่าปรับจากราคาส่งของเต็มทั้งชุด

ในระหว่างที่ผู้ซื้อยังมีได้ใช้สิทธิบอกเลิกสัญญานั้น หากผู้ซื้อเห็นว่าผู้ขายไม่อาจปฏิบัติตามสัญญาต่อไปได้ ผู้ซื้อจะใช้สิทธิบอกเลิกสัญญาและรับหรือบังคับจากหลักประกันตาม ข้อ ๖ และข้อ ๘ กับเรียกร้องให้ชดใช้ราคาที่เพิ่มขึ้นตามที่กำหนดไว้ในข้อ ๙ วรรคสองก็ได้ และถ้าผู้ซื้อได้แจ้งข้อเรียกร้องให้ชำระค่าปรับไปยังผู้ขายเมื่อครบกำหนดส่งมอบแล้ว ผู้ซื้อจะมีสิทธิที่จะปรับผู้ขายจนถึงวันบอกเลิกสัญญาได้อีกด้วย

ข้อ ๑๑ การบังคับค่าปรับ ค่าเสียหาย และค่าใช้จ่าย

ในกรณีที่ผู้ขายไม่ปฏิบัติตามสัญญาข้อใดข้อหนึ่งด้วยเหตุใดๆ ก็ตาม จนเป็นเหตุให้เกิดค่าปรับ ค่าเสียหาย หรือค่าใช้จ่ายแก่ผู้ซื้อ ผู้ขายต้องชดใช้ค่าปรับ ค่าเสียหาย หรือค่าใช้จ่ายดังกล่าวให้แก่ผู้ซื้อโดยสิ้นเชิงภายในกำหนด ๑๕ วัน นับถัดจากวันที่ได้รับแจ้งเป็นหนังสือจากผู้ซื้อ หากผู้ขายไม่ชดใช้ให้ถูกต้องครบถ้วนภายในระยะเวลาดังกล่าวให้ผู้ซื้อที่มีสิทธิที่จะหักเอาจากจำนวนเงินค่าสิ่งของที่ซื้อขายที่ต้องชำระ หรือบังคับจากหลักประกันการปฏิบัติตามสัญญาได้ทันที

หากค่าปรับ ค่าเสียหาย หรือค่าใช้จ่ายที่บังคับจากเงินค่าสิ่งของที่ซื้อขายที่ต้องชำระ หรือหลักประกันการปฏิบัติตามสัญญาแล้วยังไม่เพียงพอ ผู้ขายยินยอมชำระส่วนที่เหลือที่ยังขาดอยู่จนครบถ้วนตามจำนวนค่าปรับ ค่าเสียหาย หรือค่าใช้จ่ายนั้น ภายในกำหนด ๑๕ วัน นับถัดจากวันที่ได้รับแจ้งเป็นหนังสือจากผู้ซื้อ

หากมีเงินค่าสิ่งของที่ซื้อขายตามสัญญาที่หักไว้จ่ายเป็นค่าปรับ ค่าเสียหาย หรือค่าใช้จ่ายแล้วยังเหลืออยู่อีกเท่าใด ผู้ซื้อจะคืนให้แก่ผู้ขายทั้งหมด

ข้อ ๑๒ การงดหรือลดค่าปรับ หรือขยายเวลาส่งมอบ

ในกรณีที่มีเหตุเกิดจากความผิดหรือความบกพร่องของฝ่ายผู้ซื้อ หรือเหตุสุดวิสัย หรือเกิดจากพฤติการณ์อันหนึ่งอันใดที่ผู้ขายไม่ต้องรับผิดชอบตามกฎหมาย หรือเหตุอื่นตามที่กำหนดในกฎกระทรวง ซึ่งออกตามความในกฎหมายว่าด้วยการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ ทำให้ผู้ขายไม่สามารถส่งมอบสิ่งของตามเงื่อนไขและกำหนดเวลาแห่งสัญญานี้ได้ ผู้ขายมีสิทธิของงดหรือลดค่าปรับ หรือขยายเวลาส่งมอบตามสัญญาได้ โดยจะต้องแจ้งเหตุหรือพฤติการณ์ดังกล่าวพร้อมหลักฐานเป็นหนังสือให้ผู้ซื้อทราบภายใน ๑๕ (สิบห้า) วัน นับถัดจากวันที่เหตุอันสิ้นสุดลง หรือตามที่กำหนดในกฎกระทรวงดังกล่าว

ถ้าผู้ขายไม่ปฏิบัติให้เป็นไปตามความในวรรคหนึ่ง ให้ถือว่าผู้ขายได้สละสิทธิเรียกร้องในการที่จะงดหรือลดค่าปรับหรือขยายเวลาส่งมอบตามสัญญา โดยไม่มีเงื่อนไขใดๆ ทั้งสิ้น เว้นแต่กรณีที่เกิดจากความผิดหรือความบกพร่องของฝ่ายผู้ซื้อซึ่งมีหลักฐานชัดเจนหรือผู้ซื้อทราบที่อยู่แล้วตั้งแต่นั้น

การงดหรือลดค่าปรับหรือขยายเวลาส่งมอบตามสัญญาตามวรรคหนึ่ง อยู่ในดุลพินิจของผู้ซื้อที่จะพิจารณาตามที่เห็นสมควร

ข้อ ๑๓ การใช้เรือไทย

ถ้าสิ่งของที่จะต้องส่งมอบให้แก่ผู้ซื้อตามสัญญานี้ เป็นสิ่งของที่ผู้ขายจะต้องสั่งหรือนำเข้ามาจากต่างประเทศ และสิ่งของนั้นต้องนำเข้ามาโดยทางเรือในเส้นทางเดินเรือที่มีเรือไทยเดินอยู่ และสามารถให้บริการรับขนได้ตามที่รัฐมนตรีว่าการกระทรวงคมนาคมประกาศกำหนด ผู้ขายต้องจัดการให้สิ่งของดังกล่าวบรรทุกโดยเรือไทยหรือเรือที่มีสิทธิเช่นเดียวกับเรือไทยจากต่างประเทศมายังประเทศไทย



เว้นแต่จะได้รับอนุญาตจากกรมเจ้าท่าก่อนบรรทุกของนั้นลงเรืออื่นที่มีใช้เรือไทยหรือเป็นของที่รัฐมนตรีว่าการกระทรวงคมนาคมประกาศยกเว้นให้บรรทุกโดยเรืออื่นได้ ทั้งนี้ ไม่ว่าการส่งหรือนำเข้าสิ่งของดังกล่าวจากต่างประเทศจะเป็นแบบใด

ในการส่งมอบสิ่งของตามสัญญาให้แก่ผู้ซื้อ ถ้าสิ่งของนั้นเป็นสิ่งของตามวรรคหนึ่ง ผู้ขายจะต้องส่งมอบใบตราส่ง (Bill of Lading) หรือสำเนาใบตราส่งสำหรับของนั้น ซึ่งแสดงว่าได้บรรทุกมาโดยเรือไทยหรือเรือที่มีสิทธิเช่นเดียวกับเรือไทยให้แก่ผู้ซื้อพร้อมกับการส่งมอบสิ่งของด้วย

ในกรณีที่สิ่งของดังกล่าวไม่ได้บรรทุกจากต่างประเทศมายังประเทศไทย โดยเรือไทยหรือเรือที่มีสิทธิเช่นเดียวกับเรือไทย ผู้ขายต้องส่งมอบหลักฐานซึ่งแสดงว่าได้รับอนุญาตจากกรมเจ้าท่าให้บรรทุกของโดยเรืออื่นได้หรือหลักฐานซึ่งแสดงว่าได้ชำระค่าธรรมเนียมพิเศษเนื่องจากการไม่บรรทุกของโดยเรือไทยตามกฎหมายว่าด้วยการส่งเสริมการพาณิชย์แล้วอย่างใดอย่างหนึ่งแก่ผู้ซื้อด้วย

ในกรณีที่ผู้ขายไม่ส่งมอบหลักฐานอย่างใดอย่างหนึ่งดังกล่าวในวรรคสองและวรรคสามให้แก่ผู้ซื้อ แต่จะขอส่งมอบสิ่งของดังกล่าวให้ผู้ซื้อก่อนโดยยังไม่รับชำระเงินค่าสิ่งของ ผู้ซื้อที่มีสิทธิรับสิ่งของดังกล่าวไว้ก่อนและชำระเงินค่าสิ่งของเมื่อผู้ขายได้ปฏิบัติตามต้องครบถ้วนดังกล่าวแล้วได้

สัญญานี้ทำขึ้นเป็นสองฉบับ มีข้อความถูกต้องตรงกัน คู่สัญญาได้อ่านและเข้าใจข้อความโดยละเอียดตลอดแล้ว จึงได้ลงลายมือชื่อพร้อมทั้งประทับตรา (ถ้ามี) ไว้เป็นสำคัญต่อหน้าพยาน และคู่สัญญาต่างยึดถือไว้ฝ่ายละหนึ่งฉบับ



ลงชื่อ

(นายวิวัฒน์ เรืองเลิศปัญญากุล)

ผู้ซื้อ

ลงชื่อ

(นางสาวสัททยา สิงหเสม)

ผู้ขาย

ลงชื่อ

(นางสาวสายสมร ยมวชิราสิน)

พยาน

ลงชื่อ

(นางสาวจิรนนท์ เกรียงธีรศักดิ์)

พยาน

ใบเสนอราคาซื้อด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ (e-bidding)

เรียน ผู้อำนวยการโรงเรียนมหิตลวิทย์วิทยานุสรณ์

๑. ข้าพเจ้า บริษัท จีเอเบิล จำกัด อาคาร ปัญญาธานี ชั้นที่ ๒๔ เลข

ที่ ๑๒๗/๒๗ ถนน นนทรี แขวง ช้องนนทรี เขต ยานนาวา จังหวัด กรุงเทพมหานคร รหัสไปรษณีย์ ๑๐๑๒๐

โทรศัพท์ ๐๖๑๘๓๕๖๙๐๔ โดย นางสาวสัทยา สิงห์สม ผู้ลงนามข้างท้ายนี้ ได้พิจารณาเงื่อนไขต่าง ๆ ในเอกสาร
ซื้อด้วยวิธี e-Bidding และเอกสารเพิ่มเติม (ถ้ามี) เลขที่ ๑๕/๒๕๖๒ โดยตลอดและยอมรับข้อกำหนดและเงื่อนไขนั้น
แล้ว รวมทั้งรับรองว่าข้าพเจ้าเป็นผู้มีคุณสมบัติครบถ้วนตามที่กำหนดและไม่เป็นผู้ทำงานของทางราชการ

๒. ข้าพเจ้าขอเสนอรายการพัสดุ รวมทั้งบริการ ซึ่งกำหนดไว้ในเอกสารซื้อด้วยวิธี e-Bidding ดังต่อไปนี้

ลำดับ ที่	รายการ	ราคาต่อ หน่วย	ภาษีมูลค่า เพิ่ม (ถ้า มี)	จำนวน	รวมเป็นเงิน	กำหนดส่ง มอบ
๑	อุปกรณ์ป้องกันภายในระบบ เครือข่าย (๔๓.๒๒.๒๕.๐๑) ระบบป้องกันการบุกรุก โจมตี	-	-	๑ ระบบ	๑,๐๗๖,๘๘๘.๐๐	๙๐
รวมเป็นเงินทั้งสิ้น					๑,๐๗๖,๘๘๘.๐๐	

(หนึ่งล้านเจ็ดหมื่นหกพันแปดร้อยแปดสิบแปดบาทถ้วน) ซึ่งเป็นราคาที่รวมภาษีมูลค่าเพิ่มรวมทั้ง
ภาษีอากรอื่น และค่าใช้จ่ายทั้งปวงไว้ด้วยแล้ว

๓. คำเสนอนี้จะยื่นอยู่เป็นระยะเวลา ๓๐ วัน นับแต่วันเสนอราคา และ โรงเรียน อาจรับคำเสนอ
นี้ เวลาใดก็ได้ก่อนที่ จะครบกำหนดระยะเวลาดังกล่าว หรือระยะเวลาที่ได้ยืดออกไปตามเหตุผลอันสมควรที่ โรงเรียน

ร้องขอ
๔. ในกรณีที่ข้าพเจ้าได้รับการพิจารณาให้เป็นผู้ชนะการประกวดราคาอิเล็กทรอนิกส์ ข้าพเจ้า
รับรองที่จะ

๔.๑ ทำสัญญาตามแบบสัญญาซื้อขายแนบท้ายเอกสารซื้อด้วยวิธี e-bidding กับ โรงเรียน
ภายใน ๒๐ วัน นับถัดจากวันที่ได้รับหนังสือให้ไปทำสัญญา

๔.๒ มอบหลักประกันการปฏิบัติตามสัญญา ตามที่ระบุไว้ในข้อ ๗ ของเอกสารซื้อด้วยวิธี e-
bidding ให้แก่ โรงเรียน ก่อนหรือขณะที่ได้ลงนามในสัญญาเป็นจำนวนร้อยละ ๕ ของราคาตามสัญญาที่ได้รับไว้ในใบ
เสนอราคานี้ เพื่อเป็นหลักประกันการปฏิบัติตามสัญญาโดยถูกต้องและครบถ้วน

หากข้าพเจ้าไม่ปฏิบัติตามที่ระบุไว้ข้างต้นนี้ ข้าพเจ้ายอมให้ โรงเรียน รับ หลักประกัน
การเสนอราคาหรือเรียกธำนาจจากผู้ออกหนังสือค้ำประกัน รวมทั้งยินดีชดเชยค่าเสียหายใดที่อาจมีแก่ โรงเรียน และ
โรงเรียน มีสิทธิจะให้ผู้เสนอการรายอื่นเป็นผู้ประกวดราคาได้หรือโรงเรียน อาจเรียกประกวดราคาใหม่ก็ได้

๕. ข้าพเจ้ายอมรับว่า โรงเรียน ไม่มีความผูกพันที่จะรับคำเสนอนี้ หรือใบเสนอราคาใดๆ รวมทั้งไม่ต้องรับผิดชอบในค่าใช้จ่ายใด ๆ อันอาจเกิดขึ้นในการที่ข้าพเจ้าได้เข้าเสนอราคา

๖. บรรดาหลักฐานประกอบการพิจารณา เช่น ตัวอย่าง (sample) แคตตาล็อก แบบรูปรายการละเอียด คุณลักษณะเฉพาะ (Specifications) พร้อมใบเสนอราคา ซึ่งข้าพเจ้าได้ลงไว้ในระบบการจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ ข้าพเจ้ายินยอมมอบให้ โรงเรียน ไว้เป็นเอกสารและทรัพย์สินของทางราชการ

สำหรับตัวอย่างที่เหลือหรือไม่ใช้แล้ว ซึ่ง โรงเรียน ส่งคืนให้ ข้าพเจ้าจะไม่เรียกร้องค่าเสียหายใด ๆ ที่เกิดขึ้นกับตัวอย่างนั้น

๗. เพื่อเป็นหลักประกันในการปฏิบัติโดยถูกต้อง ตามที่ได้ทำความเข้าใจและตามความผูกพันแห่งคำเสนอนี้ ข้าพเจ้ามอบ - เพื่อเป็นหลักประกันการเสนอราคาเป็นเงินจำนวน - บาท มาพร้อมนี้

๘. ข้าพเจ้าได้ตรวจทานตัวเลขและตรวจสอบเอกสารต่าง ๆ ที่ได้ยื่นพร้อมใบเสนอราคานี้โดยละเอียดแล้ว และเข้าใจดีว่า โรงเรียน ไม่ต้องรับผิดชอบใด ๆ ในความผิดพลาด หรือ ตกหล่น

๙. ใบเสนอราคานี้ได้ยื่นเสนอโดยบริสุทธิ์ยุติธรรม และปราศจากกลฉ้อฉล หรือการสมรู้ร่วมคิดกัน โดยไม่ชอบด้วยกฎหมายกับบุคคลใดบุคคลหนึ่ง หรือหลายบุคคล หรือกับห้างหุ้นส่วน บริษัทใด ๆ ที่ได้ยื่นเสนอราคาในคราวเดียวกัน

เสนอมา ณ วันที่ ๓๐ เมษายน พ.ศ. ๒๕๖๒

(นางสาวสัททยา สิงหเสม)

ตัวแทนฝ่ายขาย

ใบเสนอราคาเลขที่ 6204160026648

รหัสอ้างอิง OTP SBBs

เลขประจำตัวผู้เสียภาษี ๐๑๐๕๕๓๒๐๐๙๔๖๔





ตารางเปรียบเทียบรายละเอียดคุณลักษณะเฉพาะ
 ประกวดราคาซื้อระบบป้องกันการบุกรุกโจมตี ด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ (e-bidding) เลขที่ ๑๕/๒๕๖๒ ประกาศโรงเรียนมหิตลวิทยานุสรณ์
 วันที่ ๑๑ เมษายน พ.ศ. ๒๕๖๒

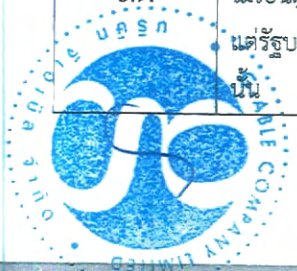
อ้างอิงข้อ	ข้อกำหนด/อุปกรณ์ที่ต้องการ	ข้อกำหนด/อุปกรณ์ที่นำเสนอ	เอกสารอ้างอิง
	ขอบเขตและข้อกำหนด โครงการจัดซื้อระบบป้องกันการบุกรุกโจมตี โรงเรียนมหิตลวิทยานุสรณ์ (องค์การมหาชน)		
1.	ความเป็นมา		
	โรงเรียนมหิตลวิทยานุสรณ์ มีระบบเทคโนโลยีสารสนเทศเพื่อรองรับการ จัดการเรียนการสอน ซึ่งมีการเก็บ ข้อมูลสำคัญไว้มากมาย เช่น ข้อมูลนักเรียน ข้อมูลบุคลากร โดยระบบป้องกันการบุกรุกโจมตีที่มีอยู่เดิมนั้นมี การใช้งานมา นาน (เลขครุภัณฑ์ 53-14-016-02) อาจไม่สามารถป้องกันการบุกรุกโจมตี รูปแบบใหม่ ๆ ซึ่งอาจ ทำให้ถูกโจรกรรมข้อมูลหรือถูกโจมตีจนข้อมูลดังกล่าว เกิดความเสียหาย เพื่อให้ข้อมูลเหล่านั้นมีความปลอดภัยจำเป็นต้องมีการ ปรับปรุงระบบป้องกันการบุกรุกโจมตี	บริษัทฯ รับทราบตามข้อกำหนด	
2.	วัตถุประสงค์และเป้าหมาย		
	เพื่อปรับปรุงระบบป้องกันการบุกรุกโจมตีให้สามารถป้องกันการโจมตีรูปแบบ ใหม่ ๆ ได้อย่างมีประสิทธิภาพมากขึ้น	บริษัทฯ รับทราบตามข้อกำหนด	
3.	คุณสมบัติผู้มีสิทธิ์เสนอราคา		
3.1.	มีความสามารถตามกฎหมาย	บริษัทฯ รับทราบปฏิบัติตามข้อกำหนด	
3.2.	ไม่เป็นบุคคลล้มละลาย	บริษัทฯ รับทราบปฏิบัติตามข้อกำหนด	
3.3.	ไม่อยู่ระหว่างเลิกกิจการ	บริษัทฯ รับทราบปฏิบัติตามข้อกำหนด	





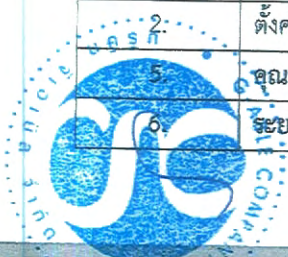
ตารางเปรียบเทียบรายละเอียดคุณลักษณะเฉพาะ
ประกวดราคาซื้อระบบป้องกันการบุกรุกโจมตี ด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ (e-bidding) เลขที่ ๑๕/๒๕๖๒ ประกาศโรงเรียนมหิดลวิทยานุสรณ์
วันที่ ๑๑ เมษายน พ.ศ. ๒๕๖๒

อ้างอิงข้อ	ข้อกำหนด/อุปกรณ์ที่ต้องการ	ข้อกำหนด/อุปกรณ์ที่นำเสนอ	เอกสารอ้างอิง
3.4.	ไม่เป็นบุคคลซึ่งอยู่ระหว่างถูกระงับการยื่นข้อเสนอหรือทำสัญญากับหน่วยงานของรัฐไว้ชั่วคราว เนื่องจากเป็นผู้ที่ไม่ผ่านเกณฑ์การประเมินผลการปฏิบัติงานของผู้ประกอบการตามระเบียบ ที่รัฐมนตรีว่าการกระทรวงการคลังกำหนด ตามที่ประกาศเผยแพร่ในระบบเครือข่ายสารสนเทศ ของกรมบัญชีกลาง	บริษัทฯ รับทราบปฏิบัติตามข้อกำหนด	
3.5.	ไม่เป็นบุคคลซึ่งถูกระงับชื่อไว้ในบัญชีรายชื่อผู้ทำงานและได้แจ้งเวียนชื่อให้เป็นผู้ทำงานของหน่วยงานของรัฐในระบบเครือข่ายสารสนเทศของกรมบัญชีกลาง ซึ่งรวมถึงนิติบุคคลที่ผู้ทำงาน เป็นหุ้นส่วนผู้จัดการ กรรมการผู้จัดการ ผู้บริหาร ผู้มีอำนาจในการดำเนินงานในกิจการของนิติบุคคลนั้นด้วย	บริษัทฯ รับทราบปฏิบัติตามข้อกำหนด	
3.6.	มีคุณสมบัติและไม่มีลักษณะต้องห้ามตามที่คณะกรรมการนโยบายการจัดซื้อจัดจ้าง และการบริหารพัสดุภาครัฐกำหนดในราชกิจจานุเบกษา	บริษัทฯ รับทราบปฏิบัติตามข้อกำหนด	
3.7.	เป็นบุคคลธรรมดาหรือนิติบุคคลผู้มีอาชีพขายพัสดุที่ประกวดราคาอิเล็กทรอนิกส์ดังกล่าว	บริษัทฯ รับทราบปฏิบัติตามข้อกำหนด	
3.8.	ไม่เป็นผู้มีผลประโยชน์ร่วมกันกับผู้ยื่นข้อเสนอรายอื่นที่เข้ายื่นข้อเสนอให้แก่โรงเรียนมหิดลวิทยานุสรณ์ ณ วันประกาศประกวดราคาอิเล็กทรอนิกส์ หรือไม่เป็นผู้กระทำการอันเป็นการขัดขวาง การแข่งขันอย่างเป็นธรรมในการประกวดราคาอิเล็กทรอนิกส์ครั้งนี้	บริษัทฯ รับทราบปฏิบัติตามข้อกำหนด	
3.9.	ไม่เป็นผู้ได้รับเอกสิทธิ์หรือความคุ้มกัน ซึ่งอาจปฏิเสธไม่ยอมขึ้นศาลไทย เว้นแต่รัฐบาล ของผู้ยื่นข้อเสนอได้มีคำสั่งให้สละเอกสิทธิ์และความคุ้มกันเช่นนั้น	บริษัทฯ รับทราบปฏิบัติตามข้อกำหนด	



ตารางเปรียบเทียบรายละเอียดคุณลักษณะเฉพาะ
ประกวดราคาซื้อระบบป้องกันการบุกรุกโจมตี ด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ (e-bidding) เลขที่ ๑๕/๒๕๖๒ ประกาศโรงเรียนมหิดลวิทยานุสรณ์
วันที่ ๑๑ เมษายน พ.ศ. ๒๕๖๒

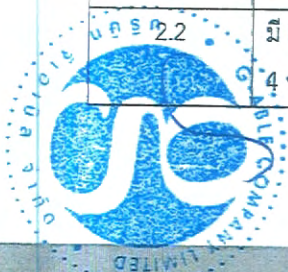
อ้างอิงข้อ	ข้อกำหนด/อุปกรณ์ที่ต้องการ	ข้อกำหนด/อุปกรณ์ที่นำเสนอ	เอกสารอ้างอิง
3.10.	ผู้ยื่นข้อเสนอต้องลงทะเบียนในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (Electronic Government Procurement: e - GP) ของกรมบัญชีกลาง	บริษัทฯ รับทราบปฏิบัติตามข้อกำหนด	
3.11.	ผู้ยื่นข้อเสนอซึ่งได้รับการคัดเลือกเป็นคู่สัญญาต้องลงทะเบียนในระบบจัดซื้อจัดจ้างภาครัฐด้วยอิเล็กทรอนิกส์ (Electronic Government Procurement: e- GP) ของกรมบัญชีกลาง ตามที่คณะกรรมการ ป.ป.ช. กำหนด	บริษัทฯ รับทราบปฏิบัติตามข้อกำหนด	
3.12.	ผู้ยื่นข้อเสนอต้องไม่อยู่ในฐานะเป็นผู้ไม่แสดงบัญชีรายรับรายจ่าย หรือแสดงบัญชี รายรับรายจ่ายไม่ถูกต้องครบถ้วนในสาระสำคัญตามที่คณะกรรมการ ป.ป.ช. กำหนด	บริษัทฯ รับทราบปฏิบัติตามข้อกำหนด	
3.13.	ผู้ยื่นข้อเสนอซึ่งได้รับคัดเลือกเป็นคู่สัญญาต้องรับและจ่ายเงินผ่านบัญชีธนาคาร เว้นแต่การจ่ายเงิน แต่ละครั้งซึ่งมีมูลค่าไม่เกินสามหมื่นบาทคู่สัญญาอาจจ่ายเป็นเงินสดก็ได้ตามที่คณะกรรมการ ป.ป.ช. กำหนด	บริษัทฯ รับทราบปฏิบัติตามข้อกำหนด	
4.	ขอบเขตการดำเนินงาน		
	โรงเรียนมหิดลวิทยานุสรณ์มีความประสงค์จะจัดหาบริษัทหรือตัวแทนที่มีความรู้ความสามารถเกี่ยวกับ ระบบรักษาความปลอดภัยบนระบบเครือข่ายเพื่อดำเนินงานดังต่อไปนี้	บริษัทฯ รับทราบปฏิบัติตามข้อกำหนด	
1.	จัดหาและติดตั้งระบบป้องกันการบุกรุกโจมตีในตำแหน่งตามที่โรงเรียนกำหนด	บริษัทฯ รับทราบปฏิบัติตามข้อกำหนด	
2.	ตั้งค่าระบบป้องกันการบุกรุกโจมตีให้สามารถใช้งานร่วมกับระบบเดิมได้	บริษัทฯ รับทราบปฏิบัติตามข้อกำหนด	
3.	คุณสมบัติเฉพาะของพัสดุ ดังแนบ	บริษัทฯ รับทราบปฏิบัติตามข้อกำหนด	
4.	ระยะเวลาในการส่งมอบ		





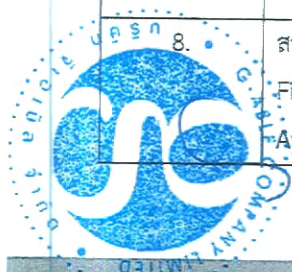
ตารางเปรียบเทียบรายละเอียดคุณลักษณะเฉพาะ
ประกวดราคาซื้อระบบป้องกันการบุกรุกโจมตี ด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ (e-bidding) เลขที่ ๑๕/๒๕๖๒ ประกาศโรงเรียนมหิดลวิทยานุสรณ์
วันที่ ๑๑ เมษายน พ.ศ. ๒๕๖๒

อ้างอิงข้อ	ข้อกำหนด/อุปกรณ์ที่ต้องการ	ข้อกำหนด/อุปกรณ์ที่นำเสนอ	เอกสารอ้างอิง
	กำหนดส่งมอบพัสดุภายใน 90 วัน นับถัดจากวันลงนามในสัญญา	บริษัทฯ รับทราบปฏิบัติตามข้อกำหนด	
7.	วงเงินในการจัดหา		
	จำนวน 1,300,000.00 บาท (หนึ่งล้านสามแสนบาทถ้วน)	บริษัทฯ รับทราบปฏิบัติตามข้อกำหนด	
8.	หลักเกณฑ์การพิจารณาคัดเลือกข้อเสนอ : เกณฑ์ราคา	บริษัทฯ รับทราบปฏิบัติตามข้อกำหนด	
9.	ผู้รับผิดชอบโครงการ : ศูนย์คอมพิวเตอร์ ฝ่ายวิทยบริการ	บริษัทฯ รับทราบปฏิบัติตามข้อกำหนด	
	รายละเอียดคุณลักษณะเฉพาะของพัสดุ		
	โครงการจัดซื้อระบบป้องกันการบุกรุกโจมตี		
	รายละเอียดคุณลักษณะเฉพาะของพัสดุ		
1.	เป็นอุปกรณ์ป้องกันการบุกรุกโจมตีชนิด Stateful Inspection Firewall แบบ Appliance ที่มี	เป็นอุปกรณ์ป้องกันการบุกรุกโจมตีชนิด Stateful Inspection Firewall แบบ Appliance ที่มี	Sophos XG_Technical Page 2, 8
1.1	Firewall Throughput แบบ NGFW ไม่น้อยกว่า 5 Gbps หรือ มี Firewall IMIX ไม่น้อยกว่า 5 Gbps	Firewall Throughput แบบ NGFW ขนาด 6 Gbps และ มี Firewall IMIX ขนาด 14.5 Gbps	Sophos XG_Technical Page 8
1.2	IPSEC VPN Throughput ไม่น้อยกว่า 4 Gbps	มี VPN Throughput จำนวน 4.8 Gbps	Sophos XG_Technical Page 8, หนังสือรับรองผลิตภัณฑ์
2.	การเชื่อมต่อเครือข่าย	การเชื่อมต่อเครือข่าย	
2.1	มี Network Interface แบบ 1 Gigabit Ethernet UTP จำนวนไม่น้อยกว่า 8 ช่อง	มี Network Interface แบบ 1 Gigabit Ethernet UTP จำนวน 8 ช่อง	Sophos XG_Technical Page 8, หนังสือรับรองผลิตภัณฑ์
2.2	มี Network Interface แบบ 1 Gigabit Ethernet SFP จำนวนไม่น้อยกว่า 4 ช่อง	มี Network Interface แบบ 1 Gigabit Ethernet SFP จำนวน 8 ช่อง	Sophos XG_Technical Page 8



ตารางเปรียบเทียบรายละเอียดคุณลักษณะเฉพาะ
ประกวดราคาซื้อระบบป้องกันการบุกรุกโจมตี ด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ (e-bidding) เลขที่ ๑๕/๒๕๖๒ ประกาศโรงเรียนมหิตลิวินาสรณ
วันที่ ๑๑ เมษายน พ.ศ. ๒๕๖๒

อ้างอิงข้อ	ข้อกำหนด/อุปกรณ์ที่ต้องการ	ข้อกำหนด/อุปกรณ์ที่นำเสนอ	เอกสารอ้างอิง
2.3	มี Network Interface แบบ 10 Gigabit Ethernet SFP+ จำนวนไม่น้อยกว่า 4 ช่อง	มี Network Interface แบบ 10 Gigabit Ethernet SFP+ จำนวน 4 ช่อง ✓	Sophos XG_Technical Page 8
2.4	มี Transceiver แบบ SFP 1000Base-LX จำนวนไม่น้อยกว่า 8 หน่วย	มี Transceiver แบบ SFP 1000Base-LX จำนวน 8 หน่วย	อ้างอิงจากใบเสนอราคา
2.5	มี Transceiver แบบ SFP+ 10GBASE-LR จำนวนไม่น้อยกว่า 8 หน่วย	มี Transceiver แบบ SFP+ 10GBASE-LR จำนวน 8 หน่วย	อ้างอิงจากใบเสนอราคา
2.6	มีสายสัญญาณเชื่อมต่อชนิด Single Mode Fiber หัวเชื่อมต่อแบบ LC-LC ความยาวไม่น้อยกว่า 3 เมตร จำนวนไม่น้อยกว่า 6 เส้น	ตรงตามข้อกำหนด ✓	อ้างอิงจากใบเสนอราคา
3.	มีระบบตรวจสอบและป้องกันการบุกรุกรูปแบบ Syn Flood, UDP Flood, ICMP Flood และ DoS หรือ DDOS ได้เป็นอย่างดี	มีระบบตรวจสอบและป้องกันการบุกรุกรูปแบบ Syn Flood, UDP Flood, ICMP Flood และ DoS หรือ DDOS	Sophos XG_Technical Page 9, 10
4.	สามารถทำ Routing แบบ Static และ Dynamic Routing ได้ เช่น RIPV1, RIPV2, OSPF, BGP	สามารถทำ Routing แบบ Static และ Dynamic Routing ได้แก่ RIPV1, RIPV2, OSPF, BGP	Sophos XG_Technical Page 2, 14
5.	สามารถบริหารจัดการอุปกรณ์ผ่านมาตรฐาน HTTPS หรือ SSH ได้เป็นอย่างดี	สามารถบริหารจัดการอุปกรณ์ผ่านมาตรฐาน HTTPS หรือ SSH ได้ ✓	Sophos XG_Technical Page 2, 3
6.	สามารถเก็บรายละเอียดและตรวจสอบการใช้งาน (Logging/Monitoring) โดยเก็บ Syslog ได้หรือดีกว่า	สามารถเก็บรายละเอียดและตรวจสอบการใช้งาน (Logging/Monitoring) โดยเก็บ syslog, Log event และ report ✓	Sophos XG_Technical Page 6
7.	สามารถทำ Static NAT, Source NAT และ Destination NAT ได้	สามารถทำ Static NAT, Source NAT และ Destination NAT ✓	Sophos XG_Technical Page 25, 30, 90, หนังสือรับรองผลิตภัณฑ์
8.	สามารถบริหารจัดการ การส่งข้อมูลแบบ Policy Based Routing หรือ Firewall rule routing โดยสามารถเลือกข้อมูลที่จะส่งโดยดูจาก Application Signature	สามารถบริหารจัดการ การส่งข้อมูลแบบ Firewall rule routing โดยสามารถเลือกข้อมูลที่จะส่งโดยดูจาก Application Signature ✓	Sophos XG_Technical Page 5, 35, 37, หนังสือรับรองผลิตภัณฑ์



ตารางเปรียบเทียบรายละเอียดคุณลักษณะเฉพาะ
ประกวดราคาซื้อระบบป้องกันการบุกรุกโจมตี ด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ (e-bidding) เลขที่ ๑๕/๒๕๖๒ ประกาศโรงเรียนมหิตลิวินาสรณ
วันที่ ๑๑ เมษายน พ.ศ. ๒๕๖๒

อ้างอิงข้อ	ข้อกำหนด/อุปกรณ์ที่ต้องการ	ข้อกำหนด/อุปกรณ์ที่นำเสนอ	เอกสารอ้างอิง
9.	สามารถทำ Anti-Malware ได้	สามารถทำ Anti-Malware	Sophos XG_Technical Page 4
10.	สามารถทำ Application Visibility and Control ได้	สามารถทำ Application Visibility and Control	Sophos XG_Technical Page 5
11.	สามารถกำหนด Policy จาก Application Layer โดยดูจาก Application Signature ได้	สามารถกำหนด Policy จาก Application Layer โดยดูจาก Application Signature	Sophos XG_Technical Page 5
12.	รองรับการทำงานในแบบ High availability ทั้งแบบ Active/Active และ Active/Standby ได้	รองรับการทำงานในแบบ High availability ได้ทั้งแบบ Active/Active และ Active/Standby	Sophos XG_Technical Page 2
13.	สามารถ Upgrade Firmware ของอุปกรณ์ผ่าน USB ได้	สามารถ Upgrade Firmware ของอุปกรณ์ผ่าน USB	Sophos XG_Technical Page 43, 48, 49
14.	มีแหล่งจ่ายไฟ (Power Supply) แบบ internal ที่สามารถทำงานแบบ Hot-Swap และ Redundant จำนวนไม่น้อยกว่า 2 หน่วย	มีแหล่งจ่ายไฟ (Power Supply) แบบ internal สามารถทำงานแบบ Hot-Swap และ Redundant จำนวน 2 หน่วย	Sophos XG_Technical Page 8, หนังสือรับรองผลิตภัณฑ์
15.	รองรับ Concurrent connections ได้ไม่น้อยกว่า 2,000,000 connection และ New connection ได้ไม่น้อยกว่า 50,000 connection	รองรับ Concurrent connections ได้ 20,000,000 connection และ New connection ได้ 200,000 connection	Sophos XG_Technical Page 8
16.	มี Storage ในการเก็บบันทึกข้อมูลแบบ Solid State (SSD) ขนาดไม่น้อยกว่า 100 GB	มี Storage ในการเก็บบันทึกข้อมูลแบบ Solid State (SSD) ขนาด 240 GB	Sophos XG_Technical Page 52
17.	สามารถสร้างรายงานได้ภายในอุปกรณ์หรือเสนออุปกรณ์เพิ่มเติมเพื่อสร้างรายงาน โดยสามารถ custom report ได้	สามารถสร้างรายงานได้ภายในอุปกรณ์ โดยสามารถ custom report ได้	Sophos XG_Technical Page 54





ตารางเปรียบเทียบรายละเอียดคุณลักษณะเฉพาะ
ประกวดราคาซื้อระบบป้องกันการบุกรุกโจมตี ด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ (e-bidding) เลขที่ ๑๕/๒๕๖๒ ประกาศโรงเรียนมหิดลวิทยานุสรณ์
วันที่ ๑๑ เมษายน พ.ศ. ๒๕๖๒

อ้างอิงข้อ	ข้อกำหนด/อุปกรณ์ที่ต้องการ	ข้อกำหนด/อุปกรณ์ที่นำเสนอ	เอกสารอ้างอิง
18.	สามารถทำการเรียกใช้งานค่าคอนฟิกูเรชันการทำงานย้อนหลังได้ภายในตัวเอง (Configuration Rollback) ได้และสามารถทำการเรียกซอฟต์แวร์การทำงานย้อนหลังได้ภายในตัวเอง (Image Rollback) หากอุปกรณ์ที่เสนอไม่สามารถทำได้ สามารถเสนออุปกรณ์ Network Management & Monitoring เพิ่มเติม เพื่อให้สามารถทำตามข้อกำหนดข้างต้นได้	สามารถทำการเรียกใช้งานค่าคอนฟิกูเรชันการทำงานย้อนหลังได้ภายในตัวเอง (Configuration Rollback) ได้และสามารถทำการเรียกซอฟต์แวร์การทำงานย้อนหลังได้ภายในตัวเอง (Image Rollback)	Sophos XG_Techincal Page 57, 62
19.	มีระบบบริหารจัดการการป้องกันการบุกรุกภายในระบบเครือข่าย โดยมีคุณสมบัติดังนี้	มีระบบบริหารจัดการการป้องกันการบุกรุกภายในระบบเครือข่าย โดยมีคุณสมบัติดังนี้	Sophos XG_Techincal Page 4
19.1	มี Function การรับข้อมูลต้องสงสัย (Cloud Security) หรือ Cloud base Service เพื่อ update หรือตรวจสอบ file ที่ต้องสงสัยและป้องกันระบบเครือข่าย	มี Function การรับข้อมูลต้องสงสัย (Cloud Security) เพื่อตรวจสอบ file ที่ต้องสงสัยและป้องกันระบบเครือข่าย	Sophos XG_Techincal Page 3
19.2	สามารถจัดการเข้าถึง (Block) จากเครื่องปลายทางออกจากระบบเครือข่ายโดยอัตโนมัติ เมื่อตรวจพบ Malware หรือ Virus	สามารถจัดการเข้าถึง (Block) จากเครื่องปลายทางออกจากระบบเครือข่ายโดยอัตโนมัติ เมื่อตรวจพบ Malware, Virus	Sophos XG_Techincal Page 4, 65, หนังสือรับรองผลิตภัณฑ์
19.3	สามารถตรวจสอบภัยคุกคามที่ผ่านเข้ามาในระบบเครือข่าย โดยสามารถตรวจสอบทั้งการโจมตี และการติดต่อกับเครื่องที่น่าสงสัยภายนอก เช่น Command and Control Server	มีระบบตรวจสอบภัยคุกคามที่ผ่านเข้ามาในระบบเครือข่าย โดยตรวจสอบทั้งการโจมตี และการติดต่อกับเครื่องที่น่าสงสัยภายนอก เช่น Command and Control Server	Sophos XG_Techincal Page 4
19.4	สามารถแจ้ง IP Address ของเครื่องที่ทำการดาวน์โหลดไฟล์และแสดงระดับความเสี่ยงของเครื่องได้	อุปกรณ์ที่เสนอสามารถแจ้ง IP Address ของเครื่องที่ทำการดาวน์โหลดไฟล์และแสดงระดับความเสี่ยงของเครื่องได้	Sophos XG_Techincal Page 70
19.5	สามารถปลดการ Block หรือ ปลดการ Blacklist IP เครื่องปลายทางจากผู้ควบคุมได้	อุปกรณ์ที่เสนอสามารถปลดการ Block หรือ ปลดการ Blacklist IP เครื่องปลายทางจากผู้ควบคุมได้	Sophos XG_Techincal Page 71



ตารางเปรียบเทียบรายละเอียดคุณลักษณะเฉพาะ
ประกวดราคาซื้อระบบป้องกันการบุกรุกโจมตี ด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ (e-bidding) เลขที่ ๑๕/๒๕๖๒ ประกาศโรงเรียนมหิดลวิทยานุสรณ์
วันที่ ๑๑ เมษายน พ.ศ. ๒๕๖๒

อ้างอิงข้อ	ข้อกำหนด/อุปกรณ์ที่ต้องการ	ข้อกำหนด/อุปกรณ์ที่นำเสนอ	เอกสารอ้างอิง
19.6	รองรับทำงาน URL Filtering โดยมี categories ไม่น้อยกว่า 80 กลุ่ม	อุปกรณ์ที่เสนอรองรับทำงาน URL Filtering โดยมี categories จำนวน 92 กลุ่ม ✓	Sophos XG_Technical Page 4
19.7	สามารถรับข้อมูล Threat Feed จาก Internet โดยข้อมูลที่ได้รับต้องมี Command and Control (C&C), GEO IP ได้เป็นอย่างดี	อุปกรณ์ที่เสนอสามารถรับข้อมูล Threat Feed จาก Internet โดยข้อมูลที่ได้รับต้องมี Command and Control (C&C), GEO IP ได้ ✓	Sophos XG_Technical Page 2, 4
19.8	สามารถแสดงข้อมูลการตรวจจับบนหน้า Dash Board ได้	อุปกรณ์ที่เสนอสามารถแสดงข้อมูลการตรวจจับบนหน้า Dash Board ได้ ✓	Sophos XG_Technical Page 72
19.9	รองรับการเชื่อมต่อกับ 3rd party ผ่าน RestfulAPI หรือ XmlAPI ได้	อุปกรณ์ที่เสนอรองรับการเชื่อมต่อกับ 3rd party ผ่าน XmlAPI ได้ ✓	Sophos XG_Technical Page 2, 80
19.10	สามารถตรวจจับ Advance Malware โดยใช้เทคนิค Sandboxing ได้	อุปกรณ์ที่เสนอสามารถตรวจจับ Advance Malware โดยใช้เทคนิค Sandboxing ได้ ✓	Sophos XG_Technical Page 88
19.11	อุปกรณ์ที่เสนอสามารถทำงานร่วมกับระบบ Centralized Firewall หรือระบบ Centralized Security Policy Management ได้ โดยผู้เสนอราคาต้องจัดเตรียม	อุปกรณ์ที่เสนอสามารถบริหารจัดการได้ด้วยตัวอุปกรณ์เองจึงไม่ได้เสนอ ระบบ Centralized Firewall หรือระบบ Centralized Security Policy Management ✓	Sophos XG_Technical Page 1
19.11.1	Hardware หรือ Software ที่จำเป็นต้องใช้	อุปกรณ์ที่เสนอสามารถบริหารจัดการได้ด้วยตัวอุปกรณ์เองจึงไม่ได้เสนอ Hardware หรือ Software ✓	Sophos XG_Technical Page 1
19.11.2	License หรือ Subscription ต่างๆ ที่จำเป็นเพื่อให้สามารถใช้งานได้ โดยมีจำนวนการใช้งานได้ไม่น้อยกว่า 2,000 device (End user) (ถ้ามี)	อุปกรณ์ที่เสนอ License หรือ Subscription ต่างๆ ที่จำเป็นเพื่อให้สามารถใช้งานได้ โดยมีจำนวนการใช้งานได้ไม่จำกัด user โดยจำกัดที่ Performance ของอุปกรณ์ ✓	Sophos XG_Technical Page 8
20	อุปกรณ์ที่นำเสนอต้องมีขนาดไม่เกิน 1 U เพื่อประหยัดพื้นที่สำหรับการติดตั้ง	อุปกรณ์ที่เสนอมีขนาด 1 U ✓	Sophos XG_Technical Page 8



g able



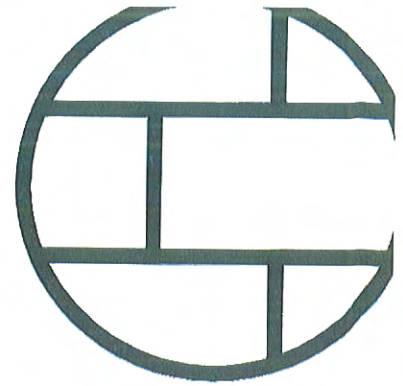
ตารางเปรียบเทียบรายละเอียดคุณลักษณะเฉพาะ
ประกวดราคาซื้อระบบป้องกันการบุกรุกโจมตี ด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ (e-bidding) เลขที่ ๑๕/๒๕๖๒ ประกาศโรงเรียนมหิตลวิทยานุสรณ์
วันที่ ๑๑ เมษายน พ.ศ. ๒๕๖๒

อ้างอิงข้อ	ข้อกำหนด/อุปกรณ์ที่ต้องการ	ข้อกำหนด/อุปกรณ์ที่นำเสนอ	เอกสารอ้างอิง
21	อุปกรณ์ที่นำเสนอ ต้องเป็นสินค้าใหม่ มีการรับประกันสินค้าพร้อม Subscription ไม่น้อยกว่า 3 ปี	อุปกรณ์ที่นำเสนอ เป็นสินค้าใหม่ มีการรับประกันสินค้าพร้อม Subscription 3 ปี	หนังสือแต่งตั้งตัวแทนจำหน่าย



Data Sheet





XG Firewall Features

Sophos XG Firewall

Highlights

- Purpose-built user interface with interactive control center utilizing traffic-light indicators (red, yellow, green) to instantly identify what needs attention at-a-glance
- The Control Center offers instant insights into endpoint health, unidentified Mac and Windows applications, cloud applications and Shadow IT, suspicious payloads, risky users, advanced threats, network attacks, objectionable websites, and much more.
- Optimized two-clicks-to-anywhere navigation
- Policy Control Center Widget monitors policy activity for business, user and network policies and tracks unused, disabled, changed and new policies
- New unified policy model combines all business, user and network firewall rules onto a single screen with grouping, filtering and search options
- Streamlined firewall rule management for large rule sets with custom auto and manual grouping with at-a-glance mouse-over feature and enforcement indicators
- All firewall rules provide an at-a-glance summary of the applied security and control for AV, Sandboxing, SSL, IPS, Web, App, Traffic Shapping (QoS), routing, and Heartbeat
- Pre-defined IPS, Web, App, and Traffic Shaping (QoS) policies enable quick setup and easy customization for common deployment scenarios (e.g. CIPA, typical workplace policies, and more)
- IPS, Web, App, and Traffic Shaping (QoS) policies snap-into firewall rules and can be edited in-place providing a powerful but intuitive model for configuring and managing security and control
- Policy Templates for common business applications including Microsoft Exchange, SharePoint, Lync, and much more defined in XML enabling customization and sharing.
- Sophos Security Heartbeat connecting Sophos endpoints with the Firewall to share health status and telemetry to enable instant identification of unhealthy or compromised endpoints

- Dynamic firewall rule support for endpoint health (Sophos Security Heartbeat) to automatically isolate or limit network access to compromised endpoints
- Synchronized Application Control to automatically, identify, classify and control all unknown Mac/Windows applications on the network
- Cloud Application Visibility enables Shadow IT discovery instantly and offers one-click traffic shaping
- Policy test simulator tool to enable firewall rule and web policy simulation and testing by user, IP and time of day
- User Threat Quotient for identifying risky users based on recent browsing behavior and ATP triggers
- Application Risk Meter provides an overall risk factor based on the risk level of applications on the network
- Configuration API for all features for RMM/PSA integration
- Discover Mode (TAP mode) for seamless integration for trials and PoCs with support for Synchronized Security

- Full-featured centralized management of multiple firewalls with Sophos Firewall Manager available as a hardware, software, or virtual appliance
- Central management of multiple firewalls from Sophos Central providing one management console for all your Sophos IT security products.

19.11
19.11.1

- Easy streamlined setup wizard to enable quick out-of-the box deployment in just a few minutes
- Zero-touch setup and configuration in Sophos Central for new firewalls that remote staff can utilize during the initial startup to configure the device

Base Firewall

General Management

- Purpose-built streamlined user interface and firewall rule management for large rule sets with grouping with at-a-glance rule feature and enforcement indicators
- Two-factor authentication (One-time password) support for administrator access, user portal, IPSec and SSL VPN
- Advanced trouble-shooting tools in



GUI (e.g., Packet Capture)

- 12 ▶ High Availability (HA) support clustering two devices in active-active or active-passive mode.

- 5 ▶ Full command-line-interface (CLI) accessible from GUI

- ▶ Role-based administration
- ▶ Automated firmware update notification with easy automated update process and roll-back features
- ▶ Reusable system object definitions for networks, services, hosts, time periods, users and groups, clients and servers
- ▶ Self-service user portal
- ▶ Configuration change tracking
- ▶ Flexible device access control for services by zones
- ▶ Email or SNMP trap notification options
- ▶ SNMP and Netflow support
- ▶ Central management support from Sophos Firewall Manager or Sophos Cloud Firewall Manager
- ▶ Backup and restore configurations: locally, via FTP or email; on-demand, daily, weekly or monthly

- 19.9 ▶ API for third party integration

- ▶ Remote access option for Sophos Support
- ▶ Cloud-based license management via MySophos

Firewall, Networking, and Routing

- 1 ▶ Stateful deep packet inspection firewall

- ▶ FastPath Packet Optimization
- ▶ User, group, time, or network based policies
- ▶ Access time policies per user/group
- ▶ Enforce policy across zones, networks, or by service type
- ▶ Zone isolation and zone-based policy support.
- ▶ Default zones for LAN, WAN, DMZ, LOCAL, VPN, and WiFi
- ▶ Custom zones on LAN or DMZ
- ▶ Customizable NAT policies with IP masquerading and full object support to redirect or forward multiple services in a single rule
- ▶ Flood protection: DoS, DDoS and portscan blocking

- 19.7 ▶ Country blocking by geo-IP

- 4 ▶ Routing: static, multicast (PIM-SM) and dynamic (RIP, BGP, OSPF)

- ▶ Upstream proxy support
- ▶ Protocol independent multicast routing with IGMP snooping
- ▶ Bridging with STP support and ARP broadcast forwarding
- ▶ VLAN DHCP support and tagging
- ▶ Multiple bridge support
- ▶ WAN link balancing: multiple Internet connections, auto-link health check, automatic failover, automatic and weighted balancing, and granular multipath rules
- ▶ Wireless WAN support (n/a in virtual deployments)
- ▶ 802.3ad interface link aggregation
- ▶ Full configuration of DNS, DHCP and NTP
- ▶ Dynamic DNS
- ▶ IPv6 Ready Logo Program Approval Certification
- ▶ IPv6 tunnelling support including 6in4, 6to4, 4in6, and IPv6 rapid deployment (6rd) through IPSec

Base Traffic Shaping and Quotas

- ▶ Flexible network or user based traffic shaping (QoS) (enhanced Web and App traffic shaping options are included with the Web Protection Subscription)
- ▶ Set user-based traffic quotas on upload/download or total traffic and cyclical or non-cyclical
- ▶ Real-time VoIP optimization
- ▶ DSCP marking

Secure Wireless

- ▶ Simple plug-and-play deployment of Sophos wireless access points (APs) — automatically appear on the firewall control center
- ▶ Central monitor and manage all APs and wireless clients through the built-in wireless controller
- ▶ Bridge APs to LAN, VLAN, or a separate zone with client isolation options
- ▶ Multiple SSID support per radio including hidden SSIDs
- ▶ Support for the latest security and encryption including WPA2 Personal and Enterprise
- ▶ Channel width selection option
- ▶ Support for IEEE 802.1X (RADIUS authentication) with primary and secondary server support
- ▶ Support for 802.11r (fast transition)



XG Firewall Features

- › Hotspot support for (custom) vouchers, password of the day, or T&C acceptance
- › Wireless guest Internet access with walled garden options
- › Time-based wireless network access
- › Wireless repeating and bridging meshed network mode with supported APs
- › Automatic channel selection background optimization
- › Support for HTTPS login

5

Authentication

- › Synchronized User ID utilizes Synchronized Security to share currently logged in Active Directory user ID between Sophos endpoints and the firewall without an agent on the AD server or client
- › Authentication via: Active Directory, eDirectory, RADIUS, LDAP and TACACS+
- › Server authentication agents for Active Directory SSO, STAS, SATC
- › Single sign-on: Active directory, eDirectory, RADIUS Accounting
- › Client authentication agents for Windows, Mac OS X, Linux 32/64
- › Browser SSO authentication: Transparent, proxy authentication (NTLM)
- › Browser Captive Portal
- › Authentication certificates for iOS and Android
- › Authentication services for IPSec, SSL, L2TP, PPTP
- › Google Chromebook authentication support for environments with Active Directory and Google Gsuite
- › API based authentication

User Self-Serve Portal

- › Download the Sophos Authentication Client
- › Download SSL remote access client (Windows) and configuration files (other OS)
- › Hotspot access information
- › Change user name and password
- › View personal internet usage
- › Access quarantined messages and manage user-based block/allow sender lists (requires Email Protection)

Page 3

Base VPN Options

- › Site-to-site VPN: SSL, IPSec, 256-bit AES/3DES, PFS, RSA, X.509 certificates, pre-shared key
- › L2TP and PPTP
- › Remote access: SSL, IPSec, iPhone/iPad/Cisco/Android VPN client support
- › IKEv2 Support
- › SSL client for Windows and configuration download via user portal

Sophos Connect IPSec Client

- › Authentication: Pre-Shared Key (PSK), PKI (X.509), Token and XAUTH
- › Enables Synchronized Security and Security Heartbeat for remote connected users
- › Intelligent split-tunneling for optimum traffic routing
- › NAT-traversal support
- › Client-monitor for graphical overview of connection status
- › Mac and Windows Support

Sandstorm Protection Subscription

19.1

Sandstorm Cloud Sandbox Protection

- › Full integration into your Sophos security solution dashboard
- › Inspects executables and documents containing executable content (including .exe, .com, and .dll, .doc, .docx, .doom and .rtf and PDF) and archives containing any of the file types listed above (including ZIP, BZIP, GZIP, RAR, TAR, LHA/LZH, 7Z, Microsoft Cabinet)
- › Aggressive behavioral, network, and memory analysis
- › Detects sandbox evasion behavior
- › Machine Learning technology with Deep Learning scans all dropped executable files
- › Includes exploit prevention and Cryptoguard Protection technology from Sophos Intercept X
- › In-depth malicious file reports and dashboard file release capability
- › Optional data center selection and flexible user and group policy options on file type, exclusions, and actions on analysis
- › Supports one-time download links



19 Network Protection Subscription

Intrusion Prevention (IPS)

- High-performance, next-gen IPS deep packet inspection engine with selective IPS patterns that can be applied on a firewall rule basis for maximum performance and protection
- Top rated by NSS Labs
- Thousands of signatures
- Granular category selection
- Support for custom IPS signatures

- IPS Policy Smart Filters that enable dynamic policies which automatically update as new patterns are added

19.3 19.2 19.7

ATP and Security Heartbeat™

- Advanced Threat Protection (Detect and block network traffic attempting to contact command and control servers using multi-layered DNS, AFC, and firewall)
- Sophos Security Heartbeat™ instantly identifies compromised endpoints including the host, user, process, incident count, and time of compromise
- Sophos Security Heartbeat™ policies can limit access to network resources or completely isolate compromised systems until they are cleaned up
- Lateral Movement Protection further isolates compromised systems by having healthy Sophos endpoints reject all traffic from unhealthy endpoints preventing the movement of threats even on the same broadcast domain

Remote Ethernet Device (RED) VPN

- Central Management of all RED devices
- No configuration: Automatically connects through a cloud-based provisioning service
- Secure encrypted tunnel using digital X.509 certificates and AES256-encryption
- Virtual Ethernet for reliable transfer of all traffic between locations
- IP address management with centrally defined DHCP and DNS Server configuration
- Remotely de-authorize RED devices after a select period of inactivity
- Compression of tunnel traffic
- VLAN port configuration options (RED 50)

Clientless VPN

- Sophos unique encrypted HTML5 self-service portal with support for RDP, HTTP, HTTPS, SSH, Telnet, and VNC

Web Protection Subscription

9 Web Protection and Control

- Fully transparent proxy for anti-malware and web-filtering

- Enhanced Advanced Threat Protection 19.6

- URL Filter database with millions of sites across 92 categories, backed by SophosLabs

- Surfing quota time policies per user/group
- Access time policies per user/group
- Malware scanning: block all forms of viruses, web malware, trojans, and spyware on HTTP/S, FTP and web-based email
- Advanced web malware protection with JavaScript emulation
- Live Protection real-time, in-the-cloud lookups for the latest threat intelligence
- Second independent malware detection engine (Avira) for dual-scanning
- Real-time or batch mode scanning
- Pharming Protection
- HTTP and HTTPS scanning and enforcement on any network and user policy with fully customizable rules and exceptions
- SSL protocol tunnelling detection and enforcement
- Certificate validation
- High performance web content caching
- Forced caching for Sophos Endpoint updates
- File type filtering by mime-type, extension and active content types (e.g. ActiveX, applets, cookies, etc.)
- YouTube for Schools enforcement per policy (user/group)
- SafeSearch enforcement (DNS-based) for major search engines per policy (user/group)
- Web keyword monitoring and enforcement to log, report or block web content matching keyword lists with the option to upload custom lists
- Block Potentially Unwanted Applications



- › Web policy override option for teachers or staff to temporarily allow access to blocked sites or categories that are fully customizable and manageable by select users
- › User/Group policy enforcement on Google Chromebooks

Cloud Application Visibility

- › Control Center widget displays amount of data uploaded and downloaded to cloud applications categorized as new, sanctioned, unsanctioned or tolerated
- › Discover Shadow IT at a glance
- › Drill down to obtain details on users, traffic and data
- › One-click access to traffic shaping policies
- › Filter cloud application usage by category or volume
- › Detailed customizable cloud application usage report for full historical reporting

Application Protection and Control

- › Synchronized App Control to automatically, identify, classify and control all unknown Windows and Mac applications on the network by sharing information between Sophos Endpoints and the firewall
- › Signature-based application control with patterns for thousands of applications
- › Cloud Application Visibility and Control to discover Shadow IT

10, 11

- › App Control Smart Filters that enable dynamic policies which automatically update as new patterns are added
- › Micro app discovery and control
- › Application control based on category, characteristics (e.g., bandwidth and productivity consuming), technology (e.g., P2P) and risk level

- 8
- › Per-user or network rule application control policy enforcement

Web and App Traffic Shaping

- › Enhanced traffic shaping (QoS) options by web category or application to limit or guarantee upload/download or total traffic priority and bitrate individually or shared

Email Protection Subscription

Email Protection and Control

- › E-mail scanning with SMTP, POP3, and IMAP support
- › Reputation service with spam outbreak

monitoring based on patented Recurrent-Pattern-Detection technology

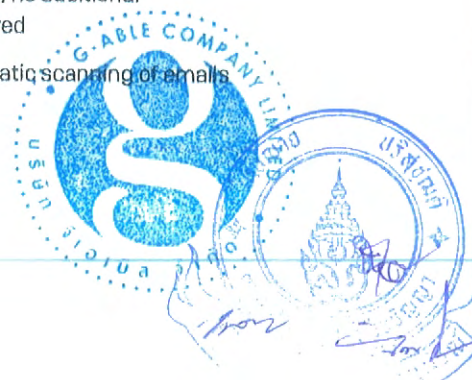
- › Block spam and malware during the SMTP transaction
- › Spam greylisting and Sneder Policy Framework (SPF) protection
- › Recipient verification for mistyped email addresses
- › Second independent malware detection engine (Avira) for dual-scanning
- › Live Protection real-time, in-the-cloud lookups for the latest threat intelligence
- › Automatic signature and pattern updates
- › Smart host support for outbound relays
- › File-Type detection/blocking/scanning of attachments
- › Accept, reject or drop over-sized messages
- › Detects phishing URLs within e-mails
- › Use pre-defined content scanning rules or create your own custom rules based on a variety of criteria with granular policy options and exceptions
- › TLS Encryption support for SMTP, POP, and IMAP
- › Append signature automatically to all outbound messages
- › Email archiver
- › Individual user-based block and allow sender lists maintained through the user portal

Email Quarantine Management

- › Spam quarantine digest and notifications options
- › Malware and spam quarantines with search and filter options by date, sender, recipient, subject, and reason with option to release and delete messages
- › Self-serve user portal for viewing and releasing quarantined messages

Email Encryption and DLP

- › Patent-pending SPX encryption for one-way message encryption
- › Recipient self-registration SPX password management
- › Add attachments to SPX secure replies
- › Completely transparent, no additional software or client required
- › DLP engine with automatic scanning of emails



and attachments for sensitive data

- Pre-packaged sensitive data type content control lists (CCLs) for PII, PCI, HIPAA, and more, maintained by SophosLabs

Web Server Protection Subscription

Web Application Firewall Protection

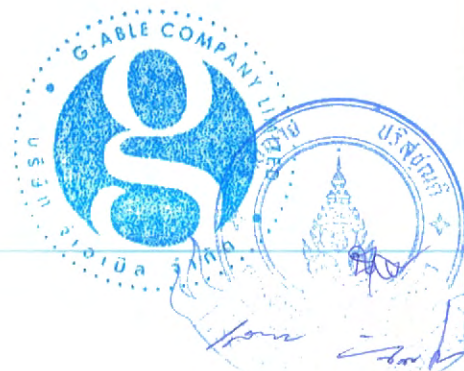
- Reverse proxy
- URL hardening engine with deep-linking and directory traversal prevention
- Form hardening engine
- SQL injection protection
- Cross-site scripting protection
- Dual-antivirus engines (Sophos and Avira)
- HTTPS (SSL) encryption offloading
- Cookie signing with digital signatures
- Path-based routing
- Outlook anywhere protocol support
- Reverse authentication (offloading) for form-based and basic authentication for server access
- Virtual server and physical server abstraction
- Integrated load balancer spreads visitors across multiple servers
- Skip individual checks in a granular fashion as required
- Match requests from source networks or specified target URLs
- Support for logical and/or operators
- Assists compatibility with various configurations and non-standard deployments
- Options to change Web Application Firewall performance parameters
- Scan size limit option
- Allow/Block IP ranges
- Wildcard support for server paths
- Automatically append a prefix/suffix for authentication

6

Logging and Reporting

NOTE: XG Firewall reporting is included at no extra charge but individual log, report, and widget availability may be dependent on their respective protection module license.

- Hundreds of on-box reports with custom report options: Dashboards (Traffic, Security, and User Threat Quotient), Applications (App Risk, Blocked Apps, Synchronized Apps, Search Engines, Web Servers, Web Keyword Match, FTP), Network and Threats (IPS, ATP, Wireless, Security Heartbeat, Sandstorm), VPN, Email, Compliance (HIPAA, GLBA, SOX, FISMA, PCI, NERC CIP v3, CIPA)
- Current Activity Monitoring: system health, live users, IPsec connections, remote users, live connections, wireless clients, quarantine, and DoS attacks
- Report anonymization
- Report scheduling to multiple recipients by report group with flexible frequency options
- Export reports as HTML, PDF, Excel (XLS)
- Report bookmarks
- Log retention customization by category
- Full featured log viewer with column view and detailed view with powerful filter and search options, hyperlinked rule ID, and data view customization



XG Firewall Features by Subscription Summary

Features (as listed above)	FullGuard Plus (included in TotalProtect Plus)					
	FullGuard (included in TotalProtect)					
	EnterpriseGuard Plus (included in EnterpriseProtect Plus)					
	EnterpriseGuard (included in EnterpriseProtect)					
	Base Firewall	Sandstorm Protection	Network Protection	Web Protection	Email Protection	Web Server Protection
General Management (incl. HA)	●					
Firewall, Networking and Routing	●					
Base Traffic Shaping and Quotas	●					
Secure Wireless	●					
Authentication	●					
Self-Serve User Portal	●					
Base VPN Options	●					
Sophos Connect IPSec Client	●					
Sandstorm Protection		●				
Intrusion Prevention (IPS)			●			
ATP and Security Heartbeat™			●			
Remote Ethernet Device (RED) VPN			●			
Clientless VPN			●			
Synchronized Application Control				●		
Web Protection and Control				●		
Application Protection and Control				●		
Cloud Application Visibility				●		
Web and App Traffic Shaping				●		
Email Protection and Control					●	
Email Quarantine Management					●	
Email Encryption and DLP					●	
Web Application Firewall Protection						●
Logging and Reporting	●	●	●	●	●	●

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244188
Email: salesasia@sophos.com

© 2016 Sophos Limited. All rights reserved.
Sophos and the Sophos logo are trademarks of Sophos Limited. All other trademarks are the property of their respective owners. Sophos Limited is not responsible for the content or accuracy of any information published on this website. The information on this website is for informational purposes only and does not constitute an offer of any product or service.

Page 7 of 10



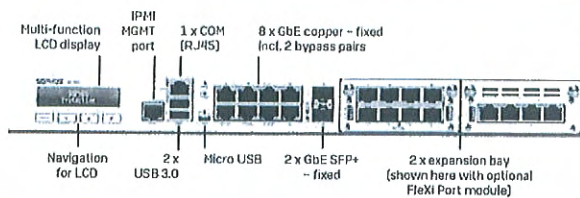
Sophos XG Series Rackmount Appliances: 1

XG 430, XG 450

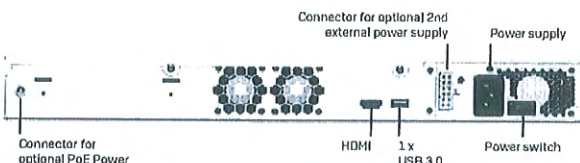
Technical Specifications

The Sophos XG 430 and XG 450 offer enterprise performance for distributed organizations or larger mid-sized companies. The connectivity options are second to none for rack mountable appliances, with each model coming equipped with 8 GbE copper ports, 2 10 GbE SFP+ ports and 2 additional Flexi Port slots which you can configure with your choice of optional modules. For high-availability, the XG 450 also offers unparalleled redundancy features in a 1U appliance with a second SSD (RAID) integrated and an optional second power supply is available for both models.

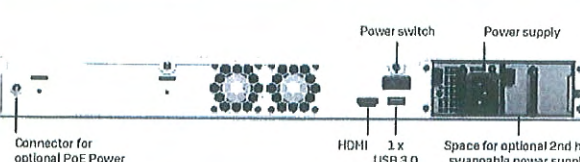
Front View



Back View XG 430



Back View XG 450



Environment

Power consumption	XG 430: 28W, 96 BTU/hr (idle) 79W, 270 BTU/hr (full load) XG 450: 31W, 107 BTU/hr (idle) 83W, 283 BTU/hr (full load)
Operating temperature	0-40°C (operating) -20 to +80°C (storage)
Humidity	10%-90%, non-condensing

Product Certifications

Certifications	CB, UL, CE, FCC Class A, ISED, VCCI, RCM, CCC, KC, BIS
----------------	--

Performance ¹	XG 430 Rev. 2	XG 450 Rev. 2
Firewall throughput	41 Gbps	50 Gbps
1.1 Firewall IMIX	14.5 Gbps	17.5 Gbps
1.2 VPN throughput	4.8 Gbps	5.5 Gbps
IPS throughput	9 Gbps	10 Gbps
1.1 NGFW (IPS + App Ctrl) max.	7 Gbps	9.2 Gbps
Antivirus throughput (proxy)	6.5 Gbps	7 Gbps
15 Concurrent connections	20,000,000	20,000,000
New connections/sec	200,000	200,000
Maximum licensed users	unrestricted	

Physical interfaces

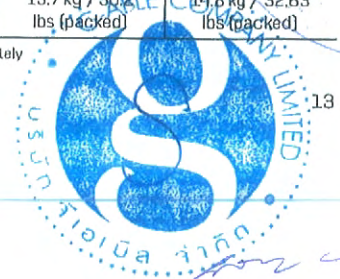
Storage (local quarantine/logs)	Integrated SSD	2 x Integrated SSD
Ethernet interfaces (fixed)	8 GbE copper (incl. 2 bypass pairs)	
2.1	2 10 GbE SFP+ ¹	
2.3		
No. of Flexi Port slots	2	
Flexi Port modules (optional)	8 port GbE copper	
2.2	8 port GbE SFP+ ¹	
2.3	2 port 10 GbE SFP+ ¹	
	4 port 10 GbE SFP+ ¹	
	2 port 40 GbE QSFP+ ¹	
	4 port GbE PoE	
	8 port GbE PoE	
	4 port GbE copper LAN bypass	
Connectivity modules (optional)	SFP DSL module (VDSL2)	
	SFP/SFP+ Transceivers	
I/O ports	2 x USB 3.0 (front)	
	1 x Micro USB (front)	
	1 x USB 3.0 (rear)	
	1 x COM (RJ45) (front)	
	1 x IPMI (front)	
	1 x HDMI (rear)	

Display	Multi-function LCD module	
Power supply	Internal auto-ranging 100-240VAC, 50-60 Hz Redundant PSU optional (external)	Internal auto-ranging 100-240VAC, 50-60 Hz Hot Swap Redundant PSU optional (internal)

Physical specifications

20 Mounting	1U rackmount (sliding rails incl.)	
Dimensions	438 x 507.7 x 44 mm	
Width x Depth x Height	17.24 x 19.99 x 1.75 inches	
Weight	7.6 kg / 16.76 lbs (unpacked)	7.8 kg / 17.2 lbs (unpacked)
	13.7 kg / 30.2 lbs (packed)	14.8 kg / 32.63 lbs (packed)

¹ Transceivers (mini GBICs) sold separately



Sophos XG Firewall: How to prevent DoS and DDoS attacks

123182

13 Jun 2018

5 people found this helpful

[English](#) | [Español](#) | [Italiano](#) | [日本語](#) | [Français](#) | [Deutsch](#)

Overview

This article discuss the best practices for protecting your network from DoS and DDoS attacks.

The following sections are covered:

- [What are DoS & DDoS attacks](#)
 - [Denial of Service \(DoS\)](#)
 - [Distributed Denial of Service \(DDoS\)](#)
- [How to configure DoS & DDoS protection](#)
 - [Protecting your network from a DoS attack](#)
 - [Protecting your network from a DDoS Attack](#)
- [Related information](#)
- [Feedback and contact](#)

Applies to the following Sophos products and versions

Sophos Firewall

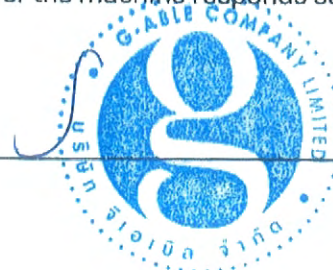
What are DoS & DDoS attacks

3

Denial of Service (DoS)

A Denial of Service (DoS) attack is an attempt to make a machine or network resource unavailable to the intended users. One common method of attack involves saturating the target machine with external communications requests so that it cannot respond to legitimate traffic or the machine responds so slowly that it is essentially useless.

DoS Attacks can be carried out in the following ways:



Handwritten signature in blue ink.

- **ICMP Flood:** In this method, the perpetrators send large numbers of IP packets with the source addresses appearing as the address of the victim. The network's bandwidth is quickly used up and prevents legitimate packets from getting through to their destination.
- **SYN/TCP Flood:** A SYN flood is when a host sends a flood of TCP/SYN packets, often with a forged sender address. Every packet is handled like a connection request; this causes the server to spawn a half-open connection because it sends back a TCP/SYN-ACK packet (Acknowledge) and waits for a packet in response from the sender address [the response to the ACK Packet]. However, as the sender address is forged, the response never comes. These half-open connections occupy the number of available connections the server is able to make and keeping it from responding to legitimate requests until after the attack ends.
- **UDP Flood:** A UDP flood attack can be initiated by sending a large number of UDP packets to random ports on a remote host. For a large number of UDP packets, the victimized system will be forced into sending many ICMP packets, eventually leading it to be unreachable by other clients.

Distributed Denial of Service (DDoS)

A Distributed Denial of Service (DDoS) attack is the attack where multiple (legitimate or compromised) systems perform a DoS Attack on a single target or system. This distributed attack can compromise the targeted machine or force it to shutdown, which shuts down service to the legitimate users.

3

How to configure DoS & DDoS protection

This article describes how you can protect your network against DoS and DDoS attacks using the Sophos XG Firewall (SF). It is divided into two sections:

- Protecting your network from a DoS attack
- Protecting your network from a DDoS attack

Protecting your network from a DoS attack

You can protect your network against DoS attacks for both IPv4 and IPv6 traffic by configuring the appropriate DoS Settings on the Sophos XG Firewall. You can configure DoS Settings by following the steps below:

1. Navigate to **Intrusion Prevention > DoS & Spoof Protection**.
2. Set the Packet and Burst rates under **DoS Settings** section according to your network traffic and check the **Apply Flag** next to the parameter to enable scanning for the respective type of traffic.
 - As an example, we have set **Packet rate per Source (Packet/min)** as 1200 for **ICMP/ICMPv6 Flood** and checked the **Apply Flag** next to it to enable scanning for ICMP and ICMPv6 traffic.



Handwritten signature and initials in blue ink.

DoS Attacks
IPS Policies
Custom IPS Signatures
DoS & Spoof Protection

DoS Settings

Attack Type	Source				Destination				
	Packet rate per Source (Packet/min)	Burst rate per Source (Packet/sec)	Apply Flag	Source Traffic Dropped	Packet rate per Destination (Packet/min)	Burst rate per Destination (Packet/sec)	Apply Flag	Destination Traffic Dropped	
SYN Flood	12000	100	☐	0	12000	100	☐	0	
UDP Flood	12000	100	☐	0	12000	100	☐	0	
TCP Flood	12000	100	☐	0	12000	100	☐	0	
ICMP/ICMPv6 Flood	1200	100	☒	0	300	100	☐	0	
Dropped Source Ported Packets							☒		
Combined ICMP/ICMPv6 Reduced Packet							☒		
ARP Hardening							☐		

Apply
[Click Here for DoS Attack samples](#)

3. Click **Apply** to apply the configured DoS Settings.

Once DoS settings are applied, SF checks the network traffic to ensure that it does not exceed the configured limit.

- For example, once the settings above are applied, SF scans the network traffic for ICMP and ICMPv6 packets. If the number of ICMP/ICMPv6 packets from a particular source exceeds 1200 per minute, it drops the excessive packets and continues dropping until the attack is over.

Protecting your network from a DDoS Attack

You can protect your network against DDoS attacks by using **Intrusion Prevention** policies in SF. To configure an IPS policy, follow the steps below.

- Navigate to **Intrusion Prevention > IPS Policies**.
- Click **Add** to create a new Intrusion Prevention policy named **DDoS_Protection**.



Handwritten signature and date '10/11/20' in blue ink.

Intrusion Prevention

How-To Guides Log Viewer Help admin
Sign Out & Your Area

DoS Attacks

IPS Policies

Custom IPS Signatures

DoS & Spoof Protection

Name *

DDoS_Protection

Description

Clone Rules

Select Policy

Save

Cancel

3. Click **Save**.

4. Click on the  icon for the **DDoS_Protection** policy.

5. Click on **Add** to create a new rule named **DDoS_Signatures**.

6. In the **Smart Filter** field, type "ddos" (without the quotes) and then press enter.

7. Set the **Action** to **Drop Packet**.

Intrusion Prevention

How-To Guides Log Viewer Help admin
Sign Out & Your Area

DoS Attacks

IPS Policies

Custom IPS Signatures

DoS & Spoof Protection

Add IPS Policy Rules

Rule Name *

DDoS_Signatures

Category

Severity

Platform

Target

ddos

Clear Filter

Smart Filter

ddos

Select All

Select Individual Signature

Name	SID	Category	Severity	Platform	Target	Recommended Action
DNS iso.org DDoS	1804117	DNS	2 - Major	Windows	Server	Drop Packet
Incoming LOIC DDoS Tool	1100012	Misc	2 - Major	Windows	Server	Drop Packet
Malware Hidden Cobra Botnet DDoS Handshake Success	3010108	Malware Communication	1 - Critical	Windows	Client	Drop Packet
Outgoing LOIC Tool Participating in DDoS	1100011	Misc	2 - Major	Windows	Server	Drop Packet
Outgoing LOIC Tool Participating in DDoS	1100013	Misc	2 - Major	Windows	Server	Drop Packet

List of Matching Signatures (1 - 5 of 5)

Action

Drop Packet

Save

Cancel

8. Click on **Save** and then click on **Save** again to save the policy.



9. Navigate to Firewall and apply the Intrusion Prevention policy to the User/Network Rule.

Edit User/Network Rule

How-To Guides Log Viewer Help admin
Sophos Anti-Virus Admin

Advanced

User Applications Intrusion Prevention DDoS_Protection	Synchronized Security Minimum Source HB Permitted ☐ GREEN ☐ YELLOW ☒ No Restriction ☐ Block clients with no heartbeat	NAT & Routing ☐ Rewrite source address (Masquerading) Primary Gateway None
Traffic Shaping Policy None	Minimum Destination HB Permitted ☐ GREEN ☐ YELLOW ☒ No Restriction ☐ Block request to destination with no heartbeat	Backup Gateway None
Web Policy None		DSCP Marking Select DSCP Marking
Apply Web Category based Traffic Shaping Policy Application Control None		
Apply Application-based Traffic Shaping Policy		

Related information

- [Sophos Firewall: VOIP calls over XG may encounter call quality issues](#)

Feedback and contact

If you've spotted an error or would like to provide feedback on this article, please use the section below to rate and comment on the article.

This is invaluable to us to ensure that we continually strive to give our customers the best information possible.

Article appears in the following topics

[XG Firewall](#) > [Sophos Firewall](#) > [System](#) > [System Services](#)

Did this article provide the information you were looking for?

Every comment submitted here is read (by a human) but we do not reply to specific technical questions.

For technical support [post a question](#) to the community. Or [click here](#) for new feature/product improvements. Alternatively for [paid/licensed products](#) [open a support ticket](#).



Handwritten signature and date 10/22

Sophos XG Firewall: How to configure Routing Information Protocol (RIP)

132735 20 Sep 2018 0 people found this helpful [English](#) | [Español](#) | [Italiano](#) | [日本語](#) | [Français](#) | [Deutsch](#)

Overview

Routing Information Protocol (RIP) is a widely used routing protocol that uses hop count to determine the best route to a destination.

RIP avoids routing loops from continuing indefinitely by limiting the number of hops permitted between the source and destination. The maximum number of hops supported is 15. Hence, if the hop count becomes 16, it is known as an infinite distance and is considered as unreachable.

With the help of the RIP protocol, the device sends routing update messages at regular intervals to the next router. When the next router receives the changes, it updates them in the routing table and also increases the metric value for the path by 1. The sender of the message is considered as the next hop. The device maintains only the route with the least metric value to a destination.

RIP implements the split horizon, route poisoning and holddown mechanisms to prevent incorrect routing information from being propagated.

In most networking environments, RIP is not the preferred choice for routing as its time to converge and scalability are poor compared to EIGRP, OSPF, or IS-IS. However, it is easy to configure, because RIP does not require any parameters unlike other protocols.

RIP uses the User Datagram Protocol (UDP) as its transport protocol, and is assigned the reserved port number 520.

1.4

XG Firewall implementation of RIP supports following features:

- RIP version 1
- RIP version 2
- Plain text authentication and MD5 authentication for RIP Version 2
- RIPng



Handwritten signature and date '10/10/20' in blue ink.

This article describes how to configure RIP in the Sophos XG Firewall.

The following sections are covered:

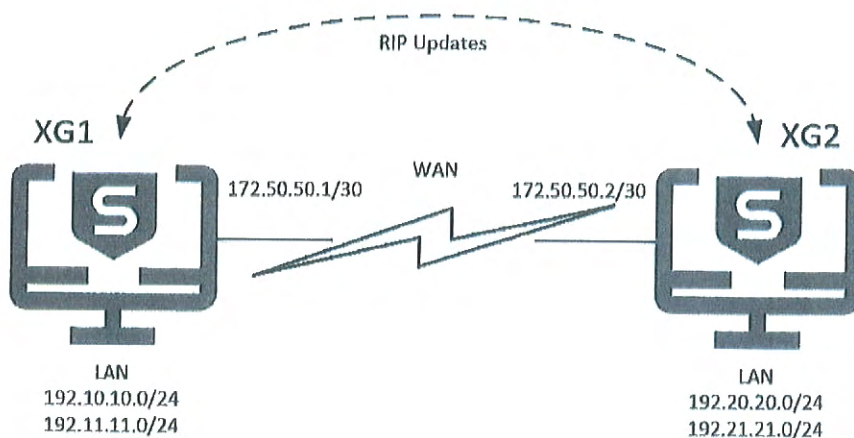
- [Scenario](#)
- [What to do](#)
 - [Web Admin configuration](#)
 - [CLI configuration](#)
- [Related information](#)
- [Feedback and contact](#)

Applies to the following Sophos products and versions

Sophos Firewall

Scenario

Configure RIP routing between two Sophos XG Firewalls. The configuration steps will be similar for both XG Firewalls.



Note: The scenario is for indicative purposes only. RIP configuration in XG Firewall can be implemented in complex network scenarios similarly.

What to do

You must be logged on to the Web Admin Console as an administrator with Read-Write permission for the relevant feature(s).

Web Admin configuration

1. Select RIP version



Handwritten signatures and initials.

Page 16

Go to **Routing > RIP**. Under **Global Configuration** section, select **V2** for the **RIP Version**. Click **Apply**.

Routing

How-To Guides Log Viewer Help admin
Sophos Anti-Virus Asia

Static Routing

Policy Routing

Gateways

BGP

OSPF

Information

RIP

Global Configuration

Default Metric

1 (1-16)

Administrative Distance

120 (1-255)

RIP Version

☐ Send V2 & Receive both ☐ V1 ☒ V2

2. Add networks to be advertised

Under **RIP Networks** section, click **Add**. This is where the networks that will participate in RIP routing will be added.

Specify the **IPv4 address** as **192.10.10.0** and the **Netmask** as **/24 [255.255.255.0]**. Click **Save**. Do this for the other network addresses that will participate in RIP routing.

Routing

How-To Guides Log Viewer Help admin
Sophos Anti-Virus Asia

Static Routing

Policy Routing

Gateways

BGP

OSPF

Information

RIP

RIP Networks

Add

Network

Netmask

Manage

172.50.50.0

255.255.255.252

192.10.10.0

255.255.255.0

192.11.11.0

255.255.255.0

3. Enable authentication (Optional)

To enable authentication for RIP updates:

- Under **Override Interface Configuration** section, click **Select Interface**.
- Specify the interface through which the RIP updates are to be exchanged.
- Click **Enable for Authentication** and specify the **Password**.
- Click **Save**.



Flow

Handwritten signature in blue ink.

Override Interface Configuration

Interface * PortB

RIP Version

Send ☐ V1 ☐ V2

Receive ☐ V1 ☐ V2

Split Horizon ☒ Enable

Poisoned Reverse ☐ Enable

Authentication ☒ Enable

Password * *****

Passive Mode ☐ Enable

Save Cancel

Note: To enable MD5 authentication, refer to the CLI configuration section.

4. Allow Dynamic Routing

Go to **Administration > Device Access**. Under **Local Service ACL** section, enable **Dynamic Routing** for the required zones for your network. For this example, it is enabled for WAN. Click **Apply**.

Administration

How-To Guides Log Viewer Help admin ▼
Sophos Anti-Virus Avia

Licensing Device Access Admin Settings Control Management Time Notification Settings SNMP ...

Local Service ACL

Zone	Admin Services			Authentication Services				Network Services		Other Services						
	HTTPS	Telnet	SSH	NTLM	Captive Portal	Radius SSO	Client Authentication	Ping/Ping6	DNS	Wireless Protection	SSL VPN	Web Proxy	User Portal	Dynamic Routing	SMTP Relay	SNMP
LAN	☒	☐	☒	☐	☒	☒	☒	☒	☒	☒	☒	☒	☒	☐	☒	☒
WAN	☒	☐	☒	☐	☐	☐	☐	☒	☒	☐	☒	☐	☒	☒	☐	☐
DMZ	☒	☐	☒	☐	☐	☐	☐	☒	☒	☐	☒	☐	☒	☐	☐	☒
VPN	☒	☐	☒	☐	☐	☐	☐	☒	☒	☐	☐	☐	☐	☐	☐	☒
WIFI	☒	☐	☒	☐	☒	☒	☒	☒	☒	☒	☒	☒	☒	☐	☒	☒

Apply

Note: Use the same procedures for the other XG firewall.

Verify RIP configuration

To verify the RIP configuration, go to **Routing > Information**. Under **RIP** section, click on **Routes** or **Status**.



Handwritten signatures and initials at the bottom right of the page.

The images below shows the routes and status for XG1. The networks of XG2 appears in the routing table of XG1.

Routing

How-To Guides Log Viewer Help admin
Sophos Anti-Virus Asia

Static Routing

Policy Routing

Gateways

BGP

OSPF

Information

Upstream Proxy

...

RIP

Routes

Codes: R - RIP, C - connected, S - Static, O - OSPF, B - BGP, K - Kernel route
Sub-codes:
(n) - normal, (s) - static, (d) - default, (r) - redistribute,
(i) - interface

Network	Next Hop	Metric From	Tag	Time
C(i) 172.50.50.0/30	0.0.0.0	1 self	0	
C(i) 192.10.10.0/24	0.0.0.0	1 self	0	
C(i) 192.11.11.0/24	0.0.0.0	1 self	0	
R(n) 192.20.20.0/24	172.50.50.2	2 172.50.50.2	0	02:42
R(n) 192.21.21.0/24	172.50.50.2	2 172.50.50.2	0	02:42

Status

Routing

How-To Guides Log Viewer Help admin
Sophos Anti-Virus Asia

Static Routing

Policy Routing

Gateways

BGP

OSPF

Information

Upstream Proxy

...

RIP

Routes

Status

Routing Protocol is "rip"
Sending updates every 30 seconds with +/-50%, next due in 31 seconds
Timeout after 180 seconds, garbage collect after 120 seconds
Outgoing update filter list for all interface is not set
Incoming update filter list for all interface is not set
Default redistribution metric is 1
Redistributing:
Default version control: send version 2, receive version 2
Interface Send Recv Key-chain
PortA 2 2
PortB 2 2
PortC 2 2
Routing for Networks:
172.50.50.0/30
192.10.10.0/24
192.11.11.0/24
Routing Information Sources:
Gateway BadPackets BadRoutes Distance Last Update
172.50.50.2 0 0 120 00:00:16
Distance: (default is 120)



The images below shows the routes and status for XG2. The networks of XG1 appears in the routing table of XG2.



Handwritten signatures and initials in blue ink.

Routing

Page 19

How-To Guides Log Viewer Help admin
Sophos Anti-Virus Asia

Static Routing Policy Routing Gateways BGP OSPF Information Upstream Proxy ...

RIP

Routes

Codes: R - RIP, C - connected, S - Static, O - OSPF, B - BGP, K - Kernel route
Sub-codes:
(n) - normal, (s) - static, (d) - default, (r) - redistribute,
(i) - interface

Network	Next Hop	Metric From	Tag	Time
C(i) 172.50.50.0/30	0.0.0.0	1 self	0	
R(n) 192.10.10.0/24	172.50.50.1	2 172.50.50.1	0	02:47
R(n) 192.11.11.0/24	172.50.50.1	2 172.50.50.1	0	02:47
C(i) 192.20.20.0/24	0.0.0.0	1 self	0	
C(i) 192.21.21.0/24	0.0.0.0	1 self	0	

Status

Routing

How-To Guides Log Viewer Help admin
Sophos Anti-Virus Asia

Static Routing Policy Routing Gateways BGP OSPF Information Upstream Proxy ...

RIP

Routes

Status

Routing Protocol is "rip"
Sending updates every 30 seconds with +/-50%, next due in 21 seconds
Timeout after 180 seconds, garbage collect after 120 seconds
Outgoing update filter list for all interface is not set
Incoming update filter list for all interface is not set
Default redistribution metric is 1
Redistributing:
Default version control: send version 2, receive version 2
Interface Send Recv Key-chain
PortA 2 2
PortB 2 2
PortC 2 2
Routing for Networks:
172.50.50.0/30
192.20.20.0/24
192.21.21.0/24
Routing Information Sources:
Gateway BadPackets BadRoutes Distance Last Update
172.50.50.1 10 0 120 00:00:21
Distance: (default is 120)

CLI configuration

Logon to the CLI using Telnet or SSH and follow the steps mentioned below.

1. Select 3. Route Configuration > 1. Configure Unicast Routing > 1. Configure RIP.



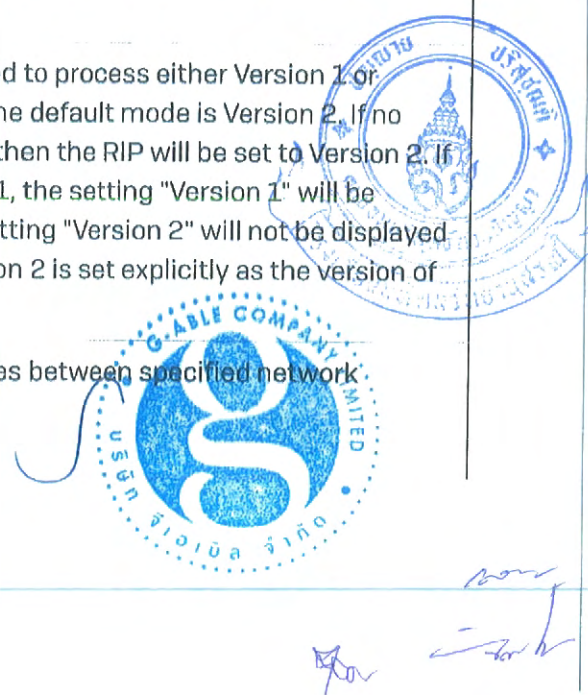
Handwritten signature and date: 16/04/2024

```
Sophos Firmware Version SFOS 17.1.2 MR-2
Unicast Routing Configuration
1. Configure RIP
2. Configure OSPF
3. Configure BGP
0. Exit

Select Menu Number: 1
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
rip>
```

2. To configure RIP, perform the tasks described in the following table as per the requirement. The table enlists all RIP-related commands with description applicable to RIP. Therefore, the configuration shown in the table is not limited to the Scenario shown above.

Command	Purpose
Enable RIP	
rip> en	Enables a RIP routing process and places you into the RIP Enable mode.
Specify a list of networks for the Routing Information Protocol (RIP) routing process	
rip# configure terminal	Enables the RIP configuration mode which places you in the Router Configuration mode and allows you to configure from the terminal.
rip(config)# router rip	Allows to configure RIP routing process. The router rip command is necessary to enable RIP. RIP must be enabled before carrying out any of the RIP commands.
rip(config-router)# no router rip	Disables a RIP routing process and places you into the Disable mode.
rip(config-router)# version 1	RIP can be configured to process either Version 1 or Version 2 packets. The default mode is Version 2. If no version is specified, then the RIP will be set to Version 2. If RIP is set to Version 1, the setting "Version 1" will be displayed, but the setting "Version 2" will not be displayed whether or not Version 2 is set explicitly as the version of RIP being used.
rip(config-router)# version 2	
rip(config-router)# network <i>network</i>	Enables RIP interfaces between specified network address.



Page 21

RIP routing updates will be sent and received only through interfaces on this network.

Also, if the network of an interface is not specified, the interface will not be advertised in any RIP update.

The interfaces which have addresses matching with network are enabled.

For example, if the network for 10.0.0.0/24 is RIP enabled, this would result in all the addresses from 10.0.0.0 to 10.0.0.255 being enabled for RIP.

```
rip(config-router)# no
network network
```

The **no network** command will disable RIP for the specified network.

```
rip(config-router)# neighbor a.b.c.d
```

The neighbor command allows the network administrator to specify a router as a RIP neighbor.

Specify RIP neighbor. When a neighbor does not understand multicast, this command is used to specify neighbors.

In some cases, all routers will not be able to understand multicasting and where packets are sent to a network or a group of addresses. In such a situation where a neighbor cannot process multicast packets, it is necessary to establish a direct link between routers.

```
rip(config-router)# no neighbor
a.b.c.d
```

The **no neighbor a.b.c.d** command will disable the RIP neighbor.

```
rip(config-router)# redistribute kernel
```

Redistribute kernel redistributes routing information from kernel route entries into the RIP tables.

```
rip(config-router)# redistribute kernel
metric <0-16>
```

```
rip(config-router)# redistribute kernel
route-map route-map
```

```
rip(config-router)# no redistribute
kernel
```

no redistribute kernel disables the routes.

```
rip(config-router)# redistribute static
```

Redistribute static redistributes routing information from static route entries into the RIP tables.



Handwritten signatures and initials at the bottom right of the page.

rip(config-router)# redistribute static
metric <0-16>

rip(config-router)# redistribute static
route-map *route-map*

rip(config-router)# no redistribute
static

rip(config-router)# redistribute
connected

rip(config-router)# redistribute
connected metric <0-16>

rip(config-router)# redistribute
connected route-map *route-map*

rip(config-router)# no redistribute
connected

rip(config-router)# redistribute ospf

rip(config-router)# redistribute ospf
metric <0-16>

rip(config-router)# redistribute ospf
route-map *route-map*

rip(config-router)# no redistribute
ospf

rip(config-router)# redistribute bgp

rip(config-router)# redistribute bgp
metric <0-16>

rip(config-router)# redistribute bgp
route-map *route-map*

rip(config-router)# no redistribute bgp

Configure Authentication

To set authentication mode as text

no redistribute static disables the routes.

Redistribute connected routes into the RIP tables. The connected route on RIP enabled interface is announced by default.

no redistribute connected disables the connected routes in the RIP tables. This command redistribute connected of the interface which RIP disabled.

Redistribute ospf redistributes routing information from ospf route entries into the RIP tables.

no redistribute ospf disables the routes.

Redistribute bgp redistributes routing information from bgp route entries into the RIP tables.

no redistribute bgp disables the routes.

Defines authentication mode for each interface. By



Handwritten signature and initials in blue ink.

Page 23

and set the authentication string

```
rip(configure)# interface ifname
```

```
rip(configure-if)# ip rip authentication
mode {text [string]}
```

For example,

```
rip(configure)# interface A
```

```
rip(configure-if)# ip rip authentication
mode text
```

```
rip(configure-if)# ip rip authentication
string teststring
```

To set authentication mode as MD5
and set the authentication string

```
rip(configure)# interface ifname
```

```
rip(configure-if)# ip rip authentication
mode {md5 [key-chain name of key
chain]}
```

For example,

```
rip(configure)# interface A
```

```
rip(configure-if)# ip rip authentication
mode md5
```

```
rip(configure-if)# ip rip authentication
key-chain testkeychain
```

```
rip(config-router)# write
```

default, authentication is on for all the interfaces.

If authentication is not required for any of the interface, it is to be explicitly disabled.

RIP Version 1 does not support authentication.

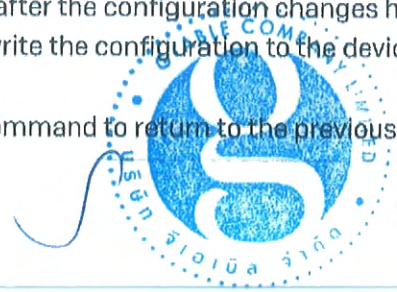
RIP Version 2 supports Clear Text (simple password) or Keyed Message Digest 5 (MD5) authentication.

To enable authentication for RIP Version 2 packets and to specify the set of keys that can be used on an interface, use the ip rip authentication key-chain command in interface configuration mode.

If authentication is not required for any of the interface, use the no form of this command.

Writes the configuration to the device. We need to provide this statement after the configuration changes have been done, so as to write the configuration to the device.

Execute 'exit' command to return to the previous mode.



Handwritten signatures and initials in blue ink.

Show RIP Information	
rip# show running-config	Shows the current configuration saved to the device.
RIP Debug Commands	
rip# show ip rip status	Shows all the RIP information.
rip# debug rip events	Debugging RIP events.
rip# debug rip packet	Debugging RIP packets.
rip# terminal monitor	Monitor the debug logs on telnet window.
rip# no debug rip events	Disable the debugging of RIP events.
rip# no debug rip packets	Disable the debugging of RIP packets.

Related information

- [Sophos XG Firewall: How to configure OSPF](#)

Feedback and contact

If you've spotted an error or would like to provide feedback on this article, please use the section below to rate and comment on the article.

This is invaluable to us to ensure that we continually strive to give our customers the best information possible.

Article appears in the following topics

[XG Firewall](#) > [Sophos Firewall](#) > [System](#) > [Routing](#)

Did this article provide the information you were looking for?

Every comment submitted here is read (by a human) but we do not reply to specific technical questions. For technical support [post a question](#) to the community. Or [click here](#) for new feature/product improvements. Alternatively for paid/licensed products [open a support ticket](#).



Sophos Firewall: How to Create a Source NAT Policy for Web Servers

123295 7 Feb 2018 3 people found this helpful [English](#) | [Español](#) | [Italiano](#) | [日本語](#) | [Français](#) | [Deutsch](#)

Overview

This article explains how to create a Source NAT firewall rule so that outgoing traffic from the internal network will use a different public IP address when connecting to a specific host on the Internet. This can be useful when network restrictions prevent the primary IP for connecting to a website or secure server.

The following sections are covered:

- [How to configure an SNAT rule](#)
 - [Create an Alias](#)
 - [Add an IP Host](#)
 - [Add a NAT Policy](#)
 - [Create a firewall rule](#)
- [Related information](#)
- [Feedback and contact](#)

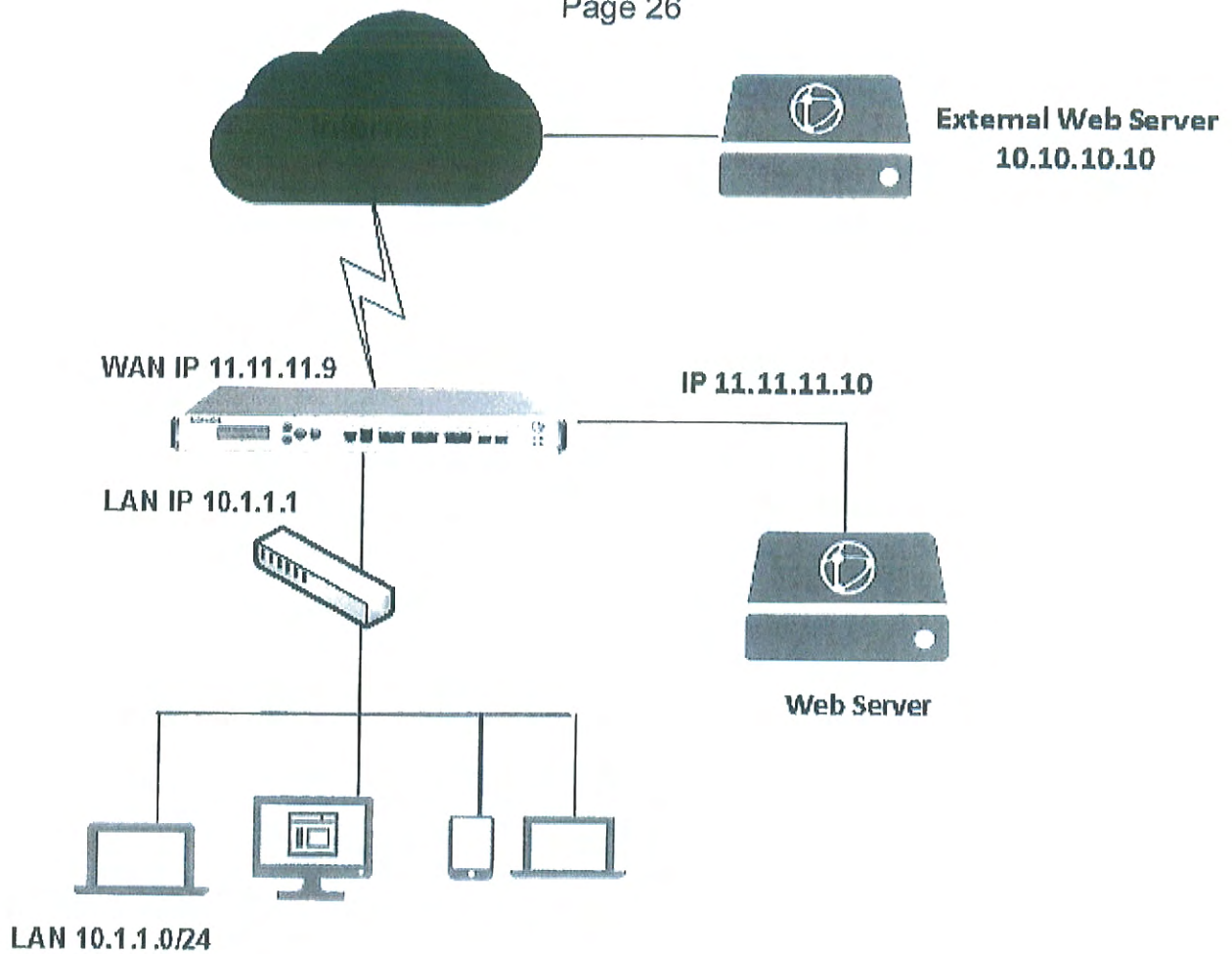
Applies to the following Sophos products and versions
Sophos Firewall

Example scenario

In this example, we have a network with WAN Ports assigned from the IPs 11.11.11.9 – 11.11.11.14. All traffic to the outside network will be sent through 11.11.11.9 by default. The Web Server 10.10.10.10 has blocked the IP 11.11.11.9 due to certain restrictions. To establish a connection between the Web Server 10.10.10.10 and the example network, another IP has to be assigned to the outgoing traffic.



Handwritten signatures and initials in blue ink at the bottom right of the page.



How to configure an SNAT rule

We will create an SNAT Policy to send all the LAN traffic destined to the external webserver to use the IP 11.11.11.10 instead of the default gateway's IP of 11.11.11.9.

Create an Alias

1. Navigate to **Network > Interfaces**.
2. Click on **Add Interface** and then select **Add Alias** from the drop-down menu.
3. Fill out the details as shown below:
 - **Physical Interface:** WAN Interface
 - **IP Version:** IPv4
 - **IPv4/Netmask:** The additional address (alias) for the WAN interface and corresponding netmask.



Handwritten signature and initials.

Add Alias

Page 27

Physical Interface *	Port2
IP Version *	☒ IPv4 ☐ IPv6
IPv4 / Netmask *	11.11.11.10 /28 (255.255.255.248)

4. Click **Save**.

Add an IP Host

1. Navigate to **Hosts and Services > IP Host**
2. Click on **Add** and fill out parameters as shown in the image below:

Name *	SNAT_IP
IP Family *	IPv4
Type *	IP
IP Address *	11.11.11.10
IP Host Group	Add New Item

3. Click on **Save** to add the IP Host.

Add a NAT Policy

1. Go to **Profiles > Network Address Translation**
2. Click **Add** to add a NAT Policy. Enter a name for the NAT policy and select the IP Host created in Step 1.

Name *	SourceNAT
IP Address	SNAT_IP

3. Click **Save** to add the NAT policy.

Create a firewall rule

1. Go to **Firewall** and click **+ Add Firewall Rule** to add a new User/Network Policy.
2. Enter the parameters as shown in the image below.



Handwritten signature and initials in blue ink.

Page 28

Rule Name *	Description	Rule Position
SNAT_Rule	Enter Description	Bottom
Action Accept Drop Reject		

Source

Source Zones *	Source Networks and Devices *	During Scheduled Time
LAN	Any	All the Time
Add New Item	Add New Item	

Destination & Services

Destination Zones *	Destination Networks *	Services *
WAN	Web Server	Any
Add New Item	Add New Item	Add New Item

Identity

☐ Match known users

Malware Scanning

- ☐ Scan HTTP
☐ Decrypt & Scan HTTPS
 | Detect zero-day threats with Sandstorm
☐ Scan FTP

Advanced

User Applications Intrusion Prevention None	Synchronized Security Minimum Source HB Permitted: ☐ GREEN ☐ YELLOW ☒ No Restriction ☐ Block clients with no heartbeat	NAT & Routing ☒ Rewrite source address (Masquerading) ☐ Use Gateway Specific Default NAT Policy
Traffic Shaping Policy None	Minimum Destination HB Permitted: ☐ GREEN ☐ YELLOW ☒ No Restriction Block request to destination with no heartbeat	Use Outbound Address SourceNAT
Web Policy None		Primary Gateway WAN Link Load Balance
☐ Apply Web Category based Traffic Shaping Policy		Backup Gateway None
Application Control None		DSCP Marking Select DSCP Marking
☐ Apply Application-based Traffic Shaping Policy		

Log Traffic

☐ Log Firewall Traffic



3. Click **Save** and the rule is created.

Related information

- [Sophos Firewall: How To Create a Source NAT rule for the Email Server](#)

Feedback and contact

If you've spotted an error or would like to provide feedback on this article, please use the section below to rate and comment on the article.

This is invaluable to us to ensure that we continually strive to give our customers the best information possible.

Article appears in the following topics

[XG Firewall](#) > [Sophos Firewall](#) > [Policies](#)

Did this article provide the information you were looking for?

Every comment submitted here is read (by a human) but we do not reply to specific technical questions. For technical support [post a question](#) to the community. Or [click here](#) for new feature/product improvements. Alternatively for [paid/licensed products](#) [open a support ticket](#).



Handwritten signature in blue ink.

Sophos XG Firewall: How to DNAT to an internal server

122976 16 Mar 2018 31 people found this helpful [English](#) | [Español](#) | [Italiano](#) | [日本語](#) | [Français](#) | [Deutsch](#)

Overview

This article explains how you can publish an internal server in the LAN or DMZ, over the Internet with a Sophos XG Firewall.

The following sections are covered:

- [How to configure DNAT for an internal server](#)
- [Related information](#)
- [Feedback and contact](#)

Applies to the following Sophos products and versions

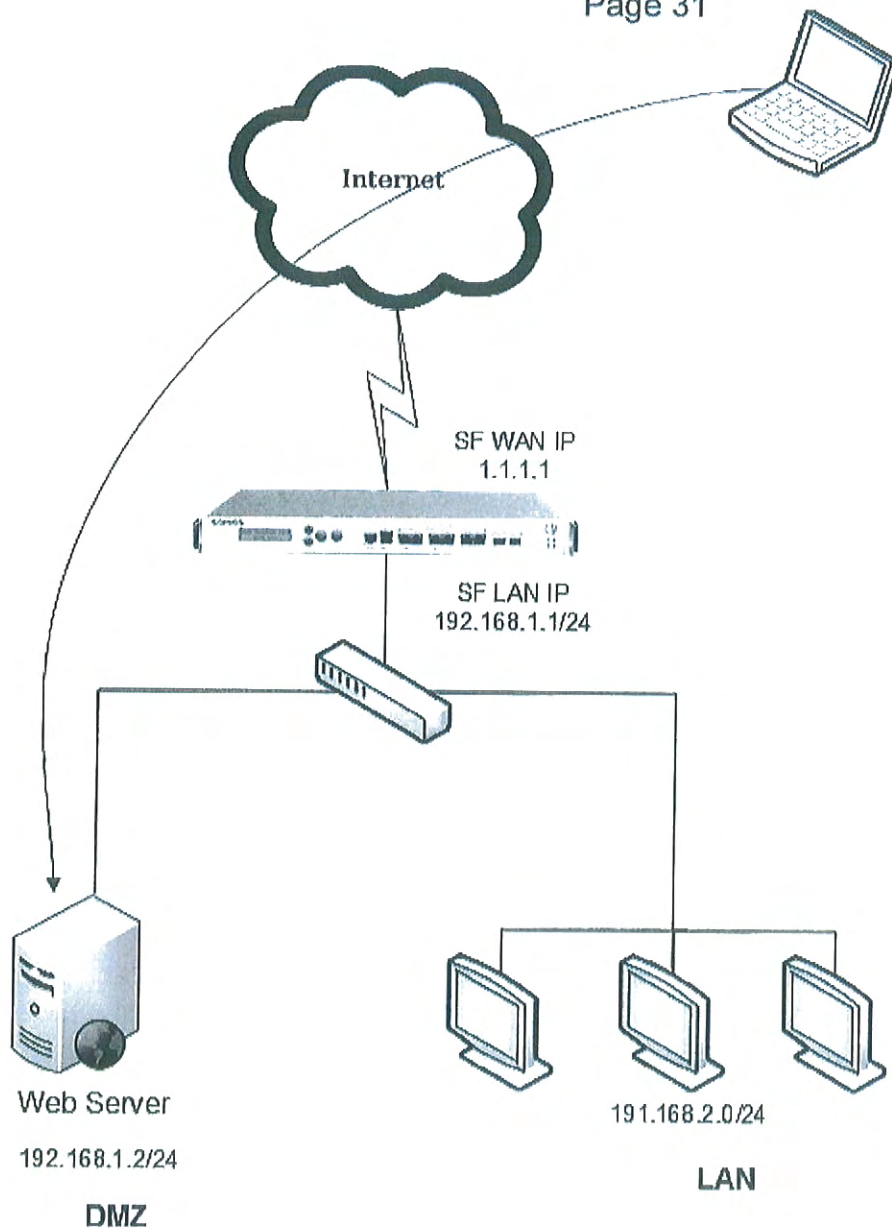
Sophos Firewall

Sophos Firewalls allows you to publish your internal servers (the protected servers), located in the LAN or DMZ, over the Internet. Since the internal servers have private IP Addresses assigned to their network segment, it must be translated to the public IP Addresses (The Hosted Servers), which will be the destination IP Addresses for all incoming requests coming over the Internet. Almost all traffic transit rules can be defined using Policies in Sophos Firewalls.

Example DNAT Scenario



Handwritten signatures and initials in blue ink at the bottom right of the page.

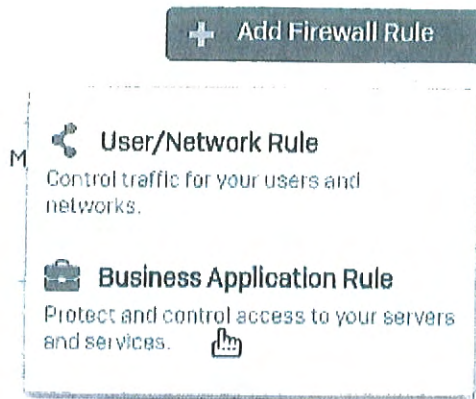


How to configure DNAT for an internal server

1. Navigate to Firewall then click +Add Firewall Rule and select Business Application Policy.



Handwritten signatures and initials in blue ink.



2. Select Application Template and choose DNAT/Full NAT/Load Balancing.

Add Business Application Rule



3. Fill out the settings as shown below:



Handwritten signatures and initials in blue ink at the bottom right of the page.

Add Business Application Rule

How-To Guides Log Viewer Help admin ▼ Sophos

Application Template DNAT/Full NAT/Load Balancing ▼ Rule Name * Rule Name	Description Description	Rule Position Top ▼
--	-----------------------------------	-------------------------------

Source

Source Zones * WAN Add New Item	Allowed Client Networks * Any Add New Item	Blocked Client Networks Add New Item
--	---	--

Destination & Service

Destination Host/Network * #Port2	Services * HTTPS Add New Item
---	--

Forward To

Protected Server(s) * Protected Server(s)	Mapped Port * To
Protected Zone * Protected Zone	☐ Change Destination Port(s)

Advanced

Policies for Business Applications Intrusion Prevention None	Synchronized Security Minimum Source HB Permitted: ☐ GREEN ☐ YELLOW ☒ No Restriction ☐ Block clients with no heartbeat	Routing ☐ Rewrite source address (Masquerading) ☐ Create Reflexive Rule
Traffic Shaping None	Minimum Destination HB Permitted: ☐ GREEN ☐ YELLOW ☒ No Restriction ☐ Block request to destination with no heartbeat	

- **Source Zones:** WAN
- **Allowed Client Networks:** Any
- **Destination Host/Network:** WAN Interface
- **Forward Type:** Select the port, port range or port list that need to be forward from the WAN to the internal server.
- **Protected Servers:** Select or create an existing host entry for the server.
- **Protected Zone:** Select the Zone in which the host resides (LAN or DMZ).
- **Change Destination Port(s):** Only check this if you wish to change ports like redirecting port 80 to port 9000.
- **Rewrite source address (Masquerading):** unchecked



Handwritten signatures and initials at the bottom right of the page.

- Optional
- **Create Reflexive Rule:** Check if the server will be initiating outgoing connections.

Note: Under the **Destination and Service** section, in the **Services** field, you can add a customized service by clicking **Add New Item > Create New > Services**. Enter a **Name** for the custom service and select **TCP/UDP**. Enter **1:65535** for the **Source Port** and enter your custom port for the **Destination Port**. Click **Save** to save the configuration. See sample below.

Add Service

Name *

Type *

ROP

☒ TCP/UDP ☐ IP ☐ ICMP ☐ ICMPv6

Protocol	Source Port	Destination Port
TCP	1:65535	3389

+

-

Save

Cancel

4. Click **Save** to save the configuration.

Related information

- [Sophos Firewall: WAF configuration and troubleshooting](#)

Feedback and contact

If you've spotted an error or would like to provide feedback on this article, please use the section below to rate and comment on the article.

This is invaluable to us to ensure that we continually strive to give our customers the best information possible.

Article appears in the following topics

[XG Firewall](#) > [Sophos Firewall](#) > [Policies](#)

Did this article provide the information you were looking for?

Every comment submitted here is read (by a human) but we do not reply to specific technical questions. For technical support [post a question](#) to the community. Or [click here](#) for new feature/product improvements. Alternatively for **paid/licensed** products [open a support ticket](#).



Handwritten signatures and initials in blue ink at the bottom right of the page.

Sophos Firewall: How create policy-based routes with firewall rules

123579 8 Mar 2017 9 people found this helpful [English](#) | [Español](#) | [Italiano](#) | [日本語](#) | [Français](#) | [Deutsch](#)

Overview

8

Policy-based routing extends the scope of static routes by providing more flexible traffic handling capabilities. It allows for routing based upon source addresses, services/applications, users and gateway weights for load balancing. It offers granular control for forwarding packets, based upon a number of user defined variables such as: Destination, Source, Application, User, Service, Server or any combination of these variables.

This article discusses the use of firewall rules to route traffic by user groups, servers or the service used. The article only discusses policy based routing in relation to firewall rules and does not touch on the rules under Routing > Policy Routing.

The following sections are covered:

- [User-based or Group-based routing](#)
- [Service-based routing](#)
- [Server-based routing](#)
- [Feedback and contact](#)

Applies to the following Sophos products and versions

Sophos Firewall

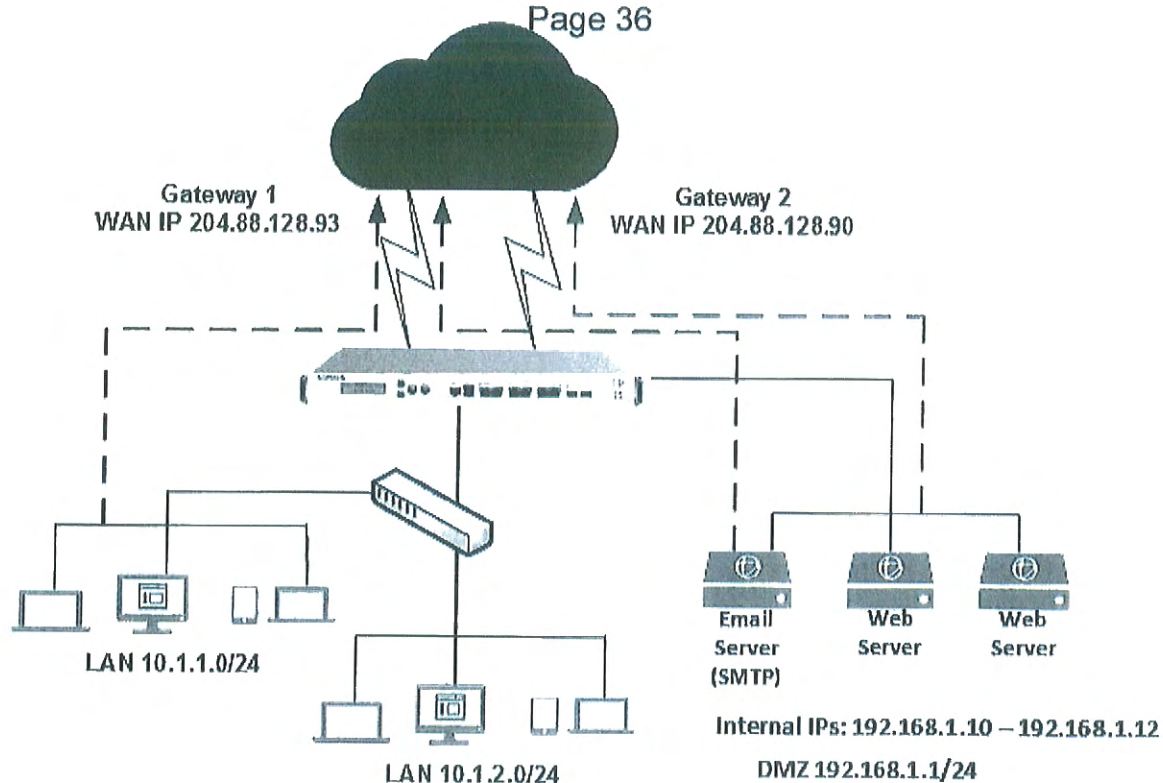
This article contains three example configurations for policy-based routes:

- User-based or Group-based Routing (RED)
- Service-based Routing (BLUE)
- Server-based Routing (GREEN)

These scenarios are explained in detail based on the following network diagram.



Handwritten signature and date: 10/11/2017



User-based or Group-based routing

In this example we will configure all traffic from the Marketing group to route through Gateway 1. This scenario is depicted in the network diagram as the red arrow.

1. Go to Firewall and click +Add Firewall Rule to create a new User/ Network Policy using the following parameters.



Handwritten signatures and initials in blue ink.

Rule Name *

Marketing_Through_Gateway

Description

Enter Description

Action

Accept

Drop

Reject

Source

Source Zones *

LAN

Add New Item

Source Networks and Devices *

Any

Add New Item

Using Scheduled Time

All the Time

Destination & Services

Destination Zones *

WAN

Add New Item

Destination Networks *

Any

Add New Item

Services *

Any

Add New Item

Identity

☒ Match known users
 ☐ Show captive portal to unknown users

User or Groups *

Marketing

Add New Item

Malware Scanning

☐ Scan HTTP
 ☐ Decrypt & Scan HTTPS
 ☐ Detect zero-day threats with Sandstorm
 ☐ Scan FTP

Advanced

Use Applications

Intrusion Prevention

Traffic Shaping Policy

Web Policy

Apply Web Category based Traffic Shaping Policy

Application Control

Apply Application-based traffic Shaping Policy

Synchronized Security

Minimum Source HB Permitted

☐ GREEN
 ☐ YELLOW
 ☒ No Restriction

☐ Block clients with no heartbeat

Minimum Destination HB Permitted

☐ GREEN
 ☐ YELLOW
 ☒ No Restriction

☐ Block request to destination with no heartbeat

NAT & Routing

☒ Rewrite source address (Masquerading)
 ☐ Use Gateway Specific Data if NAT Policy

Use Unbound Address

NAT

192.168.1.100 (10.100.201.200)

Primary Gateway

Gateway1

Backup Gateway

None

DSCP Marking

Reset DSCP Marking

Summary

Marketing_Through_Gateway

Rule

Apply this rule to traffic from source LAN to destination WAN. The rule is applied to all traffic from source LAN to destination WAN.

Source & Schedule

Source

LAN

Schedule

All the Time

Destination & Services

Destination

WAN

Services

All the Time

Identity

Marketing

Advanced

Use Applications

Intrusion Prevention

Traffic Shaping Policy

Web Policy

Apply Web Category based Traffic Shaping Policy

Application Control

Apply Application-based traffic Shaping Policy

- Name: Enter a rule name
- Action: Accept
- Source Zone: LAN
- Source Networks and Devices: Any
- Destination Zones: WAN
- Destination Networks: Any
- Services: Any



Handwritten signature and date 1/10/2021.

- Match known users: Check
 - User or Groups: Marketing
 - Rewrite source address (Masquerading): Check
 - Primary Gateway: Select the gateway you wish this traffic to go out
2. Click **Save** to save the rule.

Service-based routing

In this example we will configure all SMTP traffic to be routed through Gateway 1. This scenario is depicted in the network diagram as the blue arrow.

1. Go to Firewall and click **+Add Firewall Rule** to create a new User/ Network Policy using the following parameters.



11/01/2017
for
Lok

Add User/Network Rule

Log Viewer Help admin Sophos

Rule Name *

SMTP_Through_Gateway

Description

Enter Description

Rule Position

Bottom

Action

Accept

Deny

Reject

Source

Source Zones *

LAN

Add New Item

Source Networks and Devices *

Any

Add New Item

During Scheduled Time

All the Time

Destination & Services

Destination Zones *

WAN

Add New Item

Destination Networks *

Any

Add New Item

Services *

SMTP

Add New Item

Identity

☐ Match known users

Malware Scanning

☐ Scan HTTP
 ☐ Decrypt & Scan HTTPS
 ☐ Detect zero-day threats with Sandstorm
 ☐ Scan FTP

Advanced

User Applications

Intrusion Prevention

Traffic Shaping Policy

Web Policy

Application Control

Synchronized Security

Minimum Source HB Permitted

Minimum Destination HB Permitted

NAT & Routing

Use Outbound Address

Primary Gateway

Backup Gateway

OSCP Marking

Log Traffic

☐ Log Firewall Traffic

Summary

SMTP_Through_Gateway

Allow

Rule

Accepts SMTP traffic going to WAN from LAN zone at any time of day.

Source & Schedule

LAN

Source Networks and Devices: Any

During Scheduled Time: All the Time

Destination & Services

WAN

Destination Networks: Any

Services: SMTP

Advanced

System and Security

Scan HTTP: ☒ Scan HTTPS: ☐ Detect zero-day threats with Sandstorm: ☐ Scan FTP: ☐

System and Security

Match known users: ☐

System and Security

Match known users: ☐

System and Security

Match known users: ☐

- Name: Enter a rule name
- Action: Accept
- Source Zone: Lan
- Source Networks and Devices: Any
- Destination Zones: WAN
- Destination Networks: Any
- Services: SMTP
- Match known users: Unchecked



Handwritten signature and date 10/2

- Rewrite source address (Masquerading): Checked
 - Primary Gateway: Select the gateway you wish this traffic to go out
2. Click **Save** to save the rule.

Server-based routing

In this example we will configure all traffic from the Web Server to route through Gateway 2. This scenario is depicted in the network diagram as the green arrow.

1. Go to **Firewall** and click **+Add Firewall Rule** to create a new User/ Network Policy using the following parameters.



Handwritten signature and date (10/12/22) in blue ink.

Advanced
by *James H. Doolittle*
A highly innovative and authoritative text, this book is
highly illustrated.
Comprehensive coverage of the field of human psychology
is presented in a clear and concise manner.

- Rewrite source address (Masquerading): Checked
 - Primary Gateway: Select the gateway you wish this traffic to go out
2. Click **Save** to save the rule.

Feedback and contact

If you've spotted an error or would like to provide feedback on this article, please use the section below to rate and comment on the article.

This is invaluable to us to ensure that we continually strive to give our customers the best information possible.

Article appears in the following topics

[XG Firewall](#) > [Sophos Firewall](#) > [Policies](#)

Did this article provide the information you were looking for?

Every comment submitted here is read (by a human) but we do not reply to specific technical questions. For technical support [post a question](#) to the community. Or [click here](#) for new feature/product improvements. Alternatively for paid/licensed products [open a support ticket](#).



Handwritten signature and date: 10/11/2021

Sophos XG Firewall: How to re-image the appliance

126906 2 Oct 2018 16 people found this helpful [English](#) | [Español](#) | [Italiano](#) | [日本語](#) | [Français](#) | [Deutsch](#)

Overview

This article describes the steps to re-image a Sophos XG Firewall appliance.

Important note: Re-imaging **will destroy all the data** on the Sophos XG Firewall, so ensure that you have created and saved a recent configuration backup.

In the following steps, we will be using a bootable USB flash drive to re-image the Sophos XG Firewall.

The following sections are covered:

- [What to do](#)
 - [Download and burn an ISO image to a bootable USB flash drive](#)
 - [Steps to re-image your appliance](#)
- [Feedback and contact](#)

Applies to the following Sophos products and versions

Sophos Firewall

What to do

Download and burn an ISO image to a bootable USB flash drive

Download the required version of your Sophos XG Firewall from [MySophos portal](#). Go to **Network Protection > Download Installers** and select the download for your type of XG Firewall whether it is a Hardware, Virtual or Software Installers.



Handwritten signatures and marks at the bottom right of the page.

18/3/2562

My Account

Endpoint / Server
Protection

Network Protection

Contact Information

View Devices

Register Device

Firmware Updates

Download Installers

Share Devices

Change Registrant

Transfer License

Logout

Sophos XG Firewall: How to re-image the appliance - Sophos Community

Page 44

Download Installers

This is for new installations only. If you already have an active Sophos Firewall, SFM, or iView Instance and want to get the latest firmware update, you can either do that within the device management console or by visiting the View Devices page to download it here.

You can find Release Notes in our Up2Date Blog

WARNING: Installing any of these on an existing device instance will wipe all data and settings to factory defaults.

TRIALS: If you are looking to trial a product, you will need to visit the trial page to register for a trial serial number.

To download an installer, select the desired product, platform, and then click download. You will need a Serial Number to activate and register your install. Serial numbers for virtual and software appliances are provided via your license schedule as part of your order. Serial numbers for hardware appliances are embedded in the hardware.

Sophos Firewall OS

Sophos Firewall OS (SF-OS) is the operating system for the Sophos XG Firewall. It's available for multiple platforms including hardware appliances, virtual environments and as a software ISO to install on Intel x86 hardware of your choice.

Hardware Installers

Firewall OS for XG Series

Download ▼

Virtual Installers

Firewall OS for VMware

Download ▼

Download [Etcher](#), a free tool to make a bootable USB flash drive.

Run Etcher and accept the license agreement.

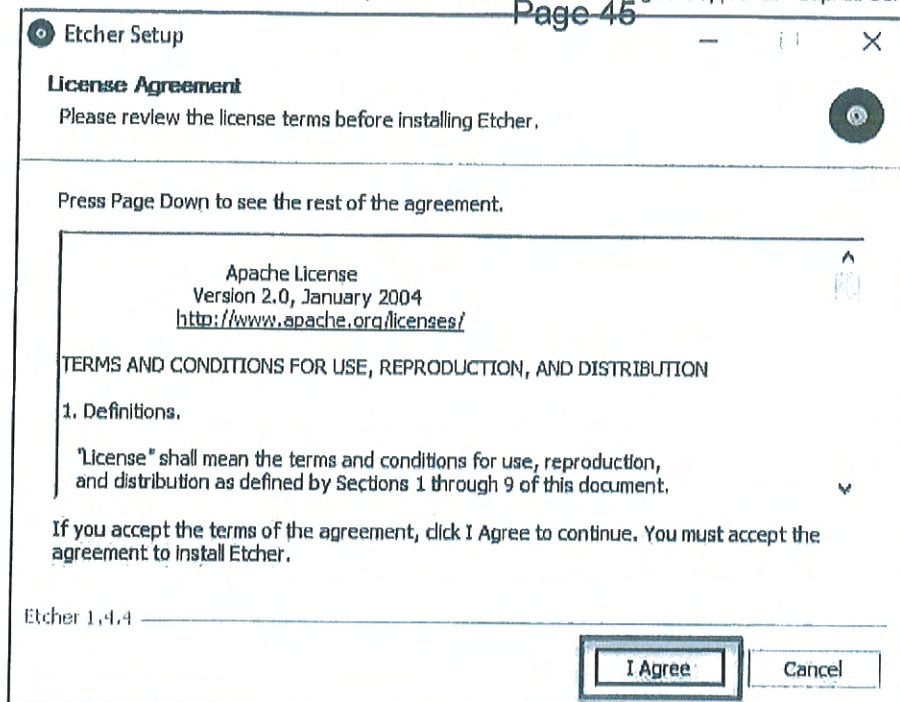


for

18/3/2562

Sophos XG Firewall: How to re-image the appliance - Sophos Community

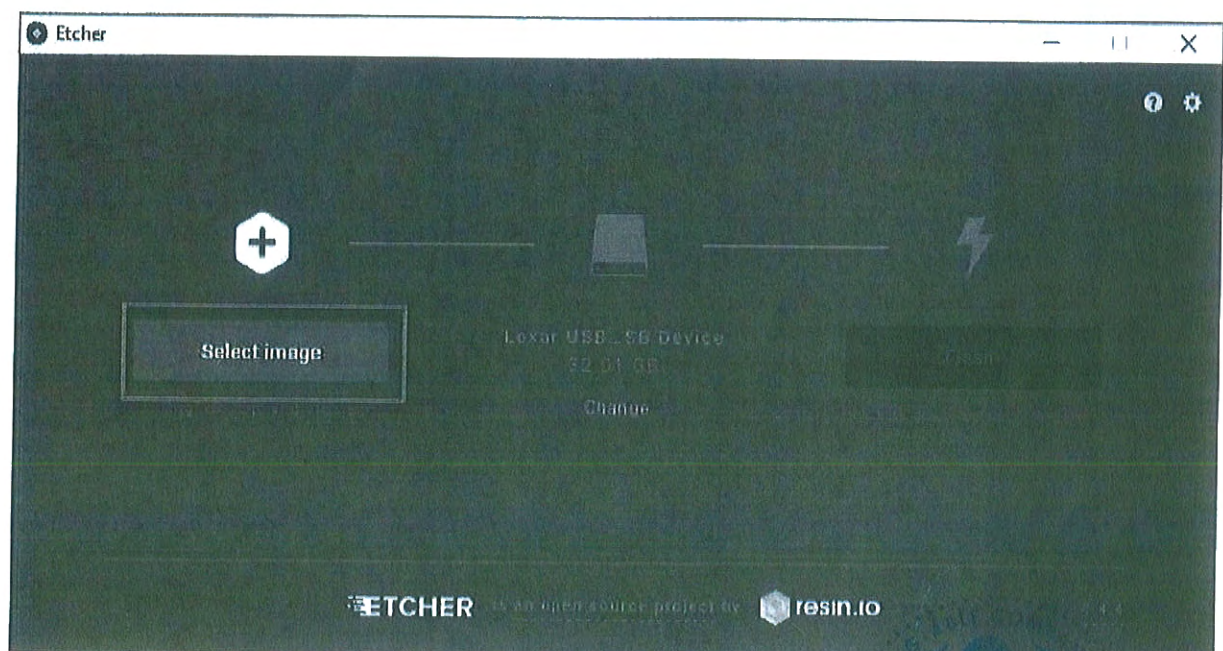
Page 46



Insert a USB flash drive into your computer.

Note: The USB flash disk will be formatted and all its existing content will be lost.

Select the image downloaded earlier.



Click on Flash!

<https://community.sophos.com/kb/en-us/126906>



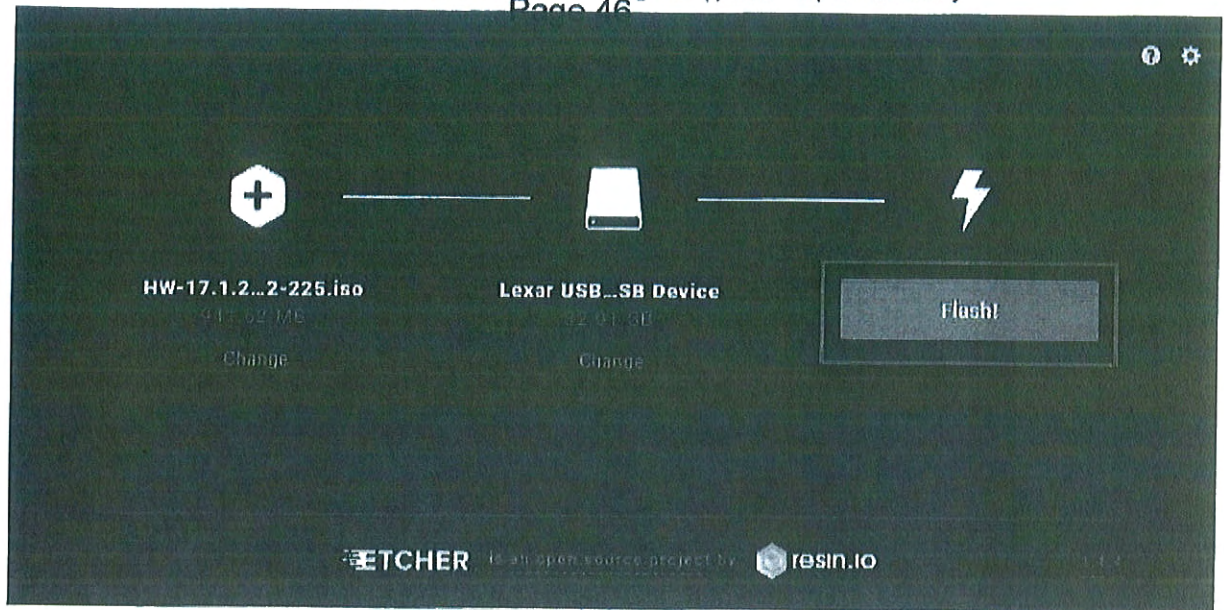
3/9

Handwritten signatures and initials in blue ink.

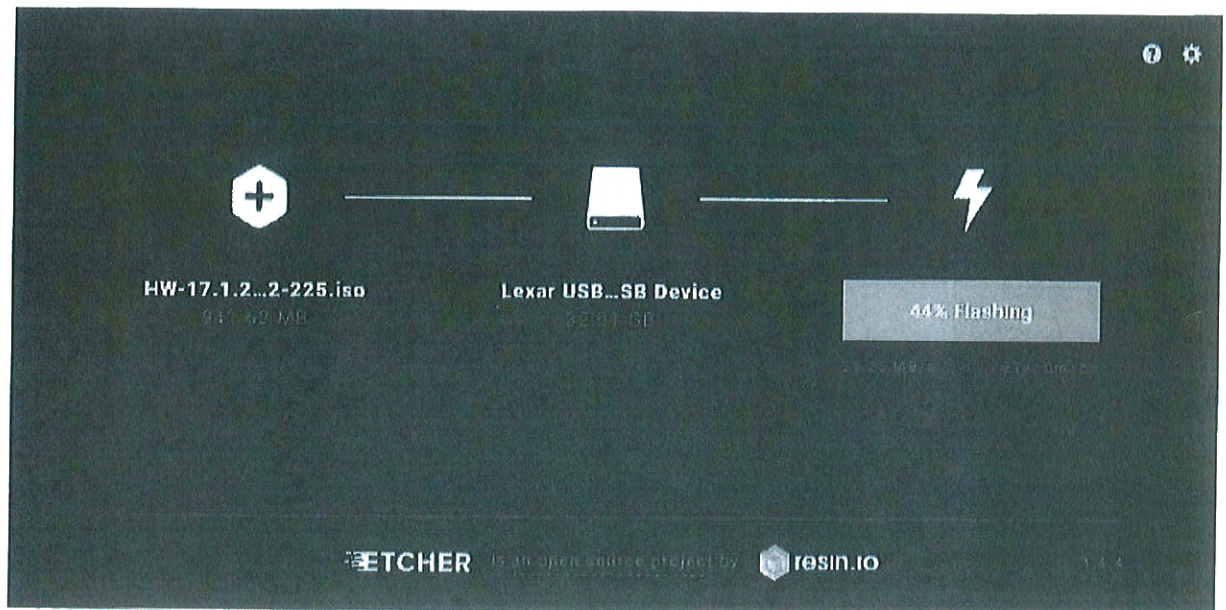
18/3/2562

Sophos XG Firewall: How to re-image the appliance - Sophos Community

Page 46



Wait until the flashing and validating process is completed.

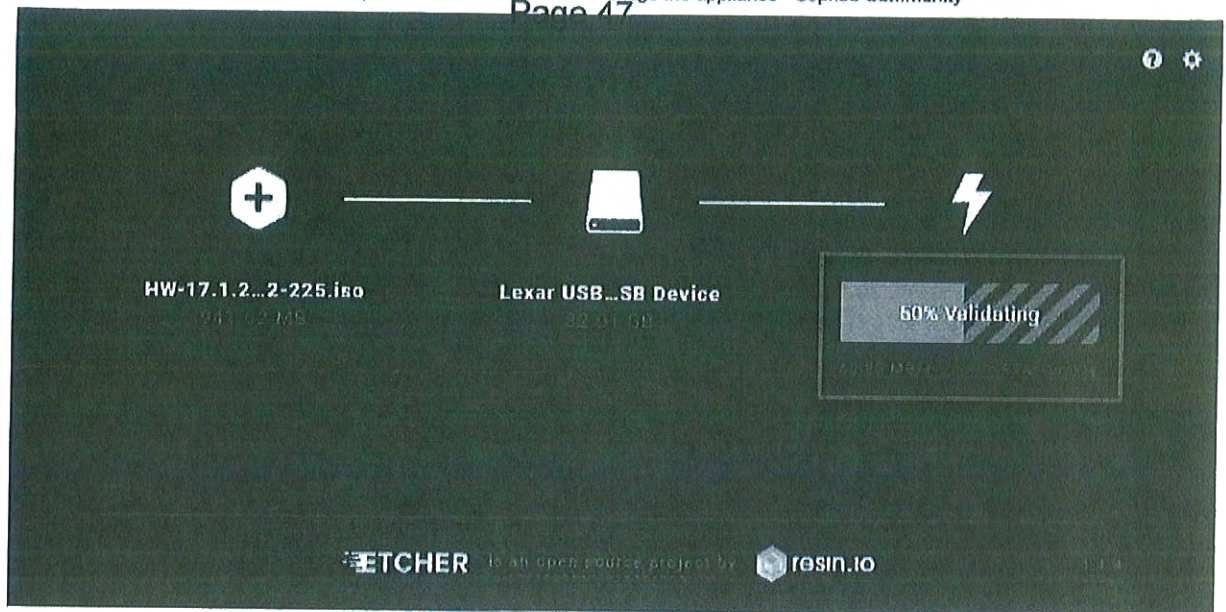


Handwritten signatures and initials in blue ink.

18/3/2562

Sophos XG Firewall: How to re-image the appliance - Sophos Community

Page 47

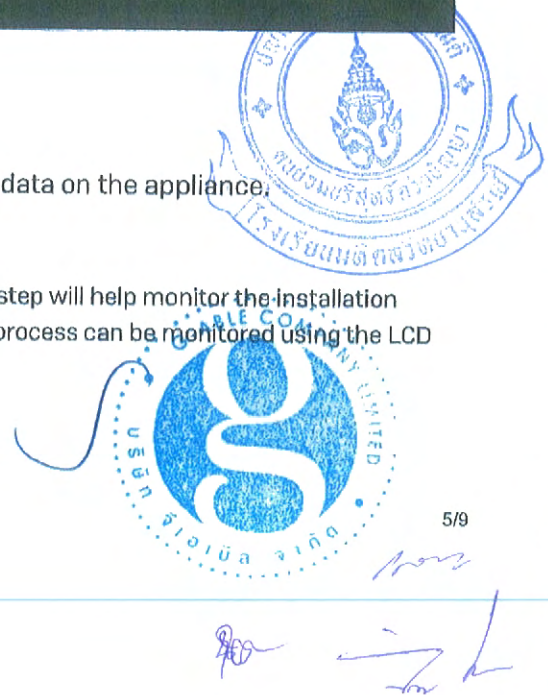


Steps to re-image your appliance

Note: The following procedure will permanently delete your existing data on the appliance.

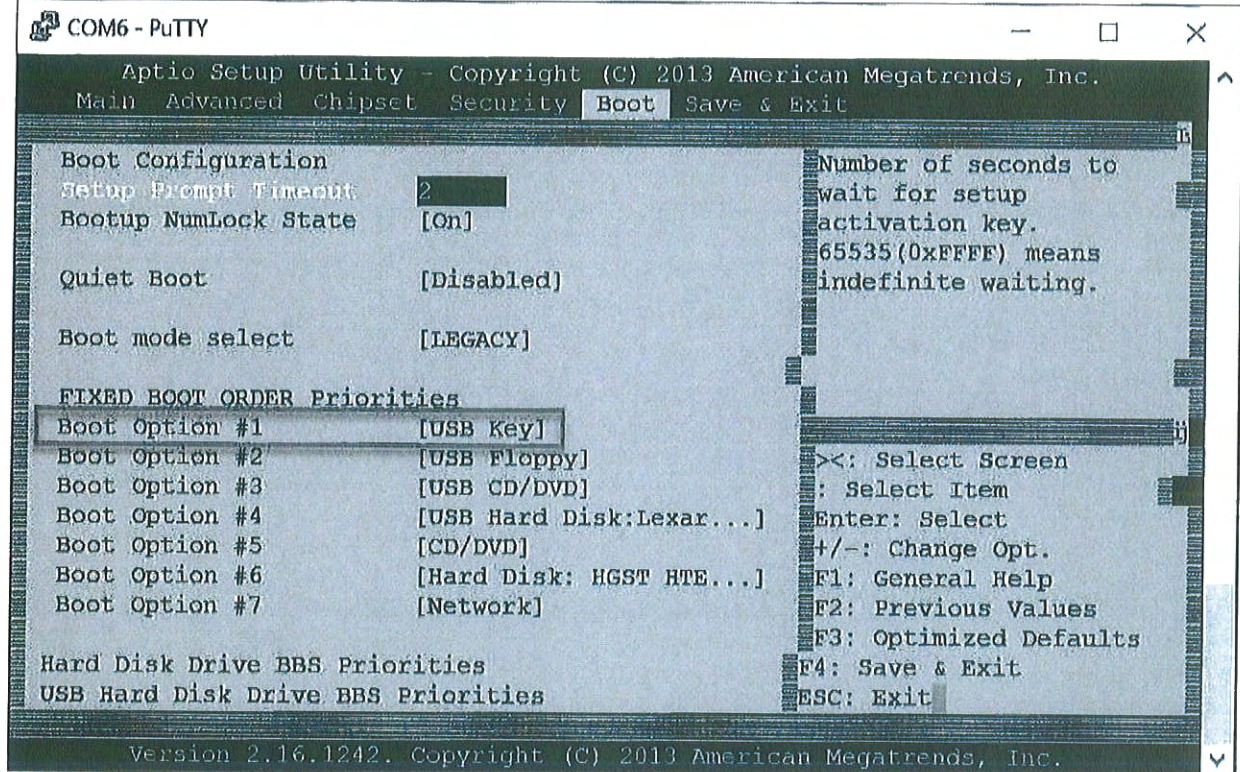
1. Power-off Sophos Firewall appliance.
2. Optionally plug a SVGA monitor to the SVGA port of your appliance. This step will help monitor the installation process. If the Sophos Firewall doesn't have a VGA port, the installation process can be monitored using the LCD panel.
3. Plug in the bootable USB flash drive created earlier.
4. Power-on the Sophos Firewall appliance.

<https://community.sophos.com/kb/en-us/126906>

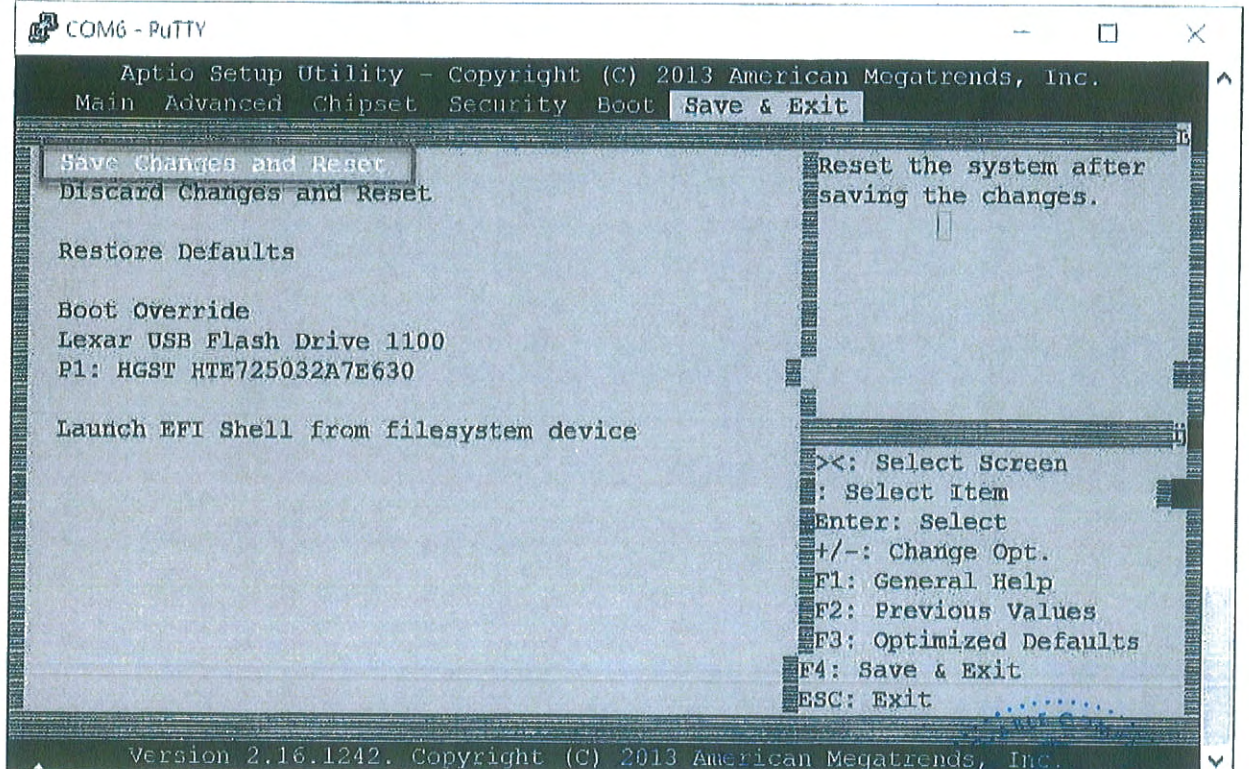


5. Make sure that **USB key** is the first boot option in the BIOS. To enter the BIOS, press Delete key when the appliance is booting.

13



6. Save and exit from the BIOS, the appliance will reboot.



Signature

Signature

7. The installer starts to re-image the appliance.

```
COM6 - PuTTY
Starting Firmware Installation

#####

Sophos FIRMWARE INSTALLER

Created on: #Thu May 11 01:52:07 UTC 2017
Firmware version: #16.05.4.215
Contains Firmware for: SG105_XN01 SG105_XN02 SG105w_XN01 SG105w_XN02 SG115_XN01
SG115_XN02 SG115w_XN01 SG115w_XN02 SG125_XN01 SG125_XN02 SG125w_XN01 SG125w_XN02
SG135_XN01 SG135_XN02 SG135w_XN01 SG135w_XN02 SG210_WP01 SG210_WP02 SG230_WP01
SG310_WP01 SG330_WP01 SG430_WP01 SG450_WP01 SG550_XN01 SG650_XN01 XG105_XN02 XG1
05w_XN02 XG115_XN02 XG115w_XN02 XG125_XN02 XG125w_XN02 XG135_XN02 XG135w_XN02 XG
210_WP02 XG210_WP03 XG230_WP01 XG230_WP02 XG310_WP01 XG310_WP02 XG330_WP01 XG330
_WP02 XG430_WP01 XG430_WP02 XG450_WP01 XG450_WP02 XG550_RL02 XG550_XN01 XG650_RL
02 XG650_XN01 XG750_RL01 XG750_RL02 XG85_XN01 XG85w_XN01
```

8. Monitor the installation progress.

```
COM6 - PuTTY
#####
Completed: [===== 80%]
#####
Formatting Configuration Partition [OK]
Formatting Signature Partition [OK]
Creating Swap Space [OK]
Formatting Report Partition [OK]
Installing Loader for appliance SG115w_XN01 [OK]
Installing firmware for appliance SG115w_XN01 .....
```



Handwritten signatures and initials in blue ink at the bottom right of the page.

9. Once the firmware is installed, remove the USB flash disk and type **y** to reboot.

```
COM6 - PuTTY
#####
Completed: [ ===== 100%]
#####
Formatting Configuration Partition [OK]
Formatting Signature Partition [OK]
Creating Swap Space [OK]
Formatting Report Partition [OK]
Installing Loader for appliance SG115w_XN01 [OK]
Installing firmware for appliance SG115w_XN01 [OK]
Firmware Installed
Remove Installer disk
press y to reboot
y
```

10. Once the installation is complete, default factory values are set on the device.

```
Doing Appliance Specific Setting
Loading firstboot configuration
Installing default config
Firstboot completed successfully

### System Detail ###

Number of cores: 2
Total RAM: 3872 MB
Total Number of interfaces: 4
Total Disk Size: 298 GB

#####

Password: 
```

11. You can now login to the newly installed firmware and restore your configuration as required.

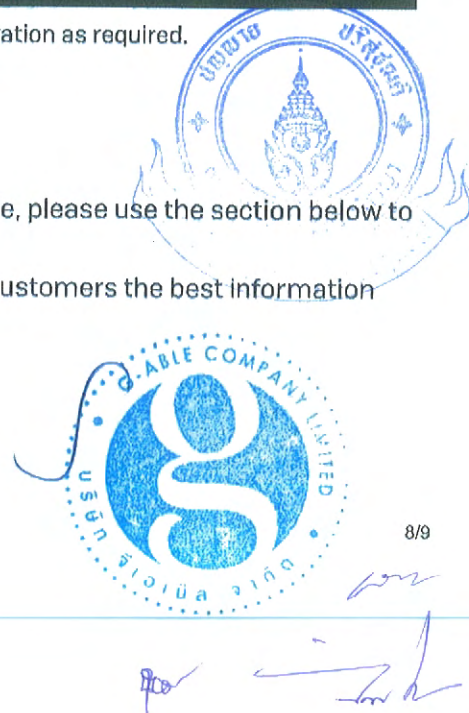
Feedback and contact

If you've spotted an error or would like to provide feedback on this article, please use the section below to rate and comment on the article.

This is invaluable to us to ensure that we continually strive to give our customers the best information possible.

Article appears in the following topics

<https://community.sophos.com/kb/en-us/126906>



18/3/2562

Sophos XG Firewall: How to re-image the appliance - Sophos Community

Page 51

[XG Firewall](#) > [Sophos Firewall](#) > [System](#)

Did this article provide the information you were looking for?

Every comment submitted here is read (by a human) but we do not reply to specific technical questions. For technical support [post a question](#) to the community. Or [click here](#) for new feature/product improvements. Alternatively for **paid/licensed** products [open a support ticket](#).



[Handwritten signatures and marks]

SOPHOS

Security made simple.

Sophos SG/XG Series Appliances

Technical Specifications

2017 1U MODELS		Available as SG and XG	Available as SG and XG	Available as SG and XG	Available as SG and XG	Available as SG and XG	Available as SG and XG
MODEL		210 Rev.3	250 Rev.2	310 Rev.2	380 Rev.2	480 Rev.2	450 Rev.2
Form factor		1U rackmount	1U rackmount	1U rackmount	1U rackmount	1U rackmount	1U rackmount
TECHNICAL SPECS							
Processor		Intel Celeron Dual Core G3900 @ 2.8GHz	Intel Pentium Dual Core G4400 @ 3.3GHz	Intel Core i3 Dual Core 6100 @ 3.7GHz	Intel Core i5 Quad Core 6500 @ 3.2 GHz	Intel Xeon Quad Core E3-1225v5 @ 3.3 GHz	Intel Xeon Quad Core E3-1275v5 @ 3.6 GHz
Memory		8 GB DDR4	8 GB DDR4	12 GB DDR4	12 GB DDR4	16 GB DDR4	16 GB DDR4
Hard Drive ¹		120 GB SSD	120 GB SSD	180 GB SSD	180 GB SSD	240 GB SSD	2*240 GB SSD (RAID-1)
Ethernet Ports						16	
GigEth Copper		6	6	8	8	8	8
GigEth SFP		2	2	2	2	-	-
GigEth SFP+		-	-	2	2	2	2
LAN module slots		1	1	1	1	2	2
IPMI		-	-	-	-	1	1
I/O Ports							
USB		3 (2 front, 1 rear)	3 (2 front, 1 rear)	3 (2 front, 1 rear)	3 (2 front, 1 rear)	3 (2 front, 1 rear)	3 (2 front, 1 rear)
COM		2 (front)	2 (front)	2 (front)	2 (front)	2 (front)	2 (front)
HDMI		RJ45/Micro USB	RJ45/Micro USB	RJ45/Micro USB	RJ45/Micro USB	RJ45/Micro USB	RJ45/Micro USB
PHYSICAL SPECS							
Dimensions w*h*d (mm)		438x44x344.4	438x44x344.4	438x44x405.5	438x44x405.5	438x44x507.7	438x44x507.7
Weight (kg) unpacked/packed		SG: 5.2 / 7.2 XG: 5.2 / 7.7	SG: 5.2 / 7.2 XG: 5.2 / 7.7	SG: 5.8 / 8.1 XG: 5.8 / 8.8	SG: 5.8 / 8.1 XG: 5.8 / 8.8	SG: 7.6 / 12.7 XG: 7.6 / 13.7	SG: 7.8 / 13.8 XG: 7.8 / 14.8
POWER							
Power Supply		Internal auto-ranging 100-240VAC, 50-60 Hz	Internal auto-ranging 100-240VAC, 50-60 Hz	Internal auto-ranging 100-240VAC, 50-60 Hz	Internal auto-ranging 100-240VAC, 50-60 Hz	Internal auto-ranging 100-240VAC, 50-60 Hz	Internal auto-ranging 100-240VAC, 50-60 Hz
2nd Power Supply Option		External redundant PSU option	External redundant PSU option	External redundant PSU option	External redundant PSU option	External redundant PSU option	Internal hot swap redundant PSU option
Power Consumption (Idle)		19W, 66 BTU/h	21W, 72 BTU/h	32W, 109 BTU/h	36W, 122 BTU/h	28W, 96 BTU/h	31W, 107 BTU/h
Power Consumption (full load)		35W, 118 BTU/h	41W, 141 BTU/h	49W, 167 BTU/h	54W, 184 BTU/h	78W, 270 BTU/h	83W, 283 BTU/h
ENVIRONMENT							
Noise level (avg.) (with/without smart fan)		36.9 / 57.6 dBA	36.9 / 57.6 dBA	25.4 / 58 dBA	25.4 / 58 dBA	37.5 / 55 dBA	37.5 / 55 dBA
Operating Temperature		0°C - 40°C	0°C - 40°C	0°C - 40°C	0°C - 40°C	0°C - 40°C	0°C - 40°C
Storage Temperature		-20°C - 80°	-20°C - 80°	-20°C - 80°	-20°C - 80°	-20°C - 80°	-20°C - 80°
Humidity		10% - 90% non-condensing	10% - 90% non-condensing	10% - 90% non-condensing	10% - 90% non-condensing	10% - 90% non-condensing	10% - 90% non-condensing
CERTIFICATIONS							
Certifications (Safety, EMD)		CB, UL, CE, FCC Class A, ISED, VCCI, RCM, CCC, BIS (planned), MSIP/KCC (planned)	CB, UL, CE, FCC Class A, ISED, VCCI, RCM, CCC, BIS (planned), MSIP/KCC (planned)	CB, UL, CE, FCC Class A, ISED, VCCI, RCM, CCC, BIS (planned), MSIP/KCC (planned)	CB, UL, CE, FCC Class A, ISED, VCCI, RCM, CCC, BIS (planned), MSIP/KCC (planned)	CB, UL, CE, FCC Class A, ISED, VCCI, RCM, CCC, BIS (planned), MSIP/KCC (planned)	CB, UL, CE, FCC Class A, ISED, VCCI, RCM, CCC, BIS (planned), MSIP/KCC (planned)
MTBF (hours) (Ballistic TR-882 Issue B)		112650 hrs	112650 hrs	109451 hrs	109451 hrs	94332 hrs	88700 hrs

¹ Capacity may vary if in short supply.

© 2017 Sophos Limited. All rights reserved. Sophos, the Sophos logo, and the Sophos logo are trademarks of Sophos Limited. All other trademarks are the property of their respective owners.

Page 52 of 52



Sophos XG Firewall: How to configure a custom view report with report notification

123201 12 Mar 2018 0 people found this helpful [English](#) | [Español](#) | [Italiano](#) | [日本語](#) | [Français](#) | [Deutsch](#)

Overview

The Sophos XG Firewall (SF) allows grouping of multiple reports under a Custom View Profile. This is aimed at providing an administrator a single page view of all the grouped reports. Custom Views can be created as needed by selecting up to eight (8) individual reports.

SF also allows you to configure email notifications about custom views, which are periodically sent to the administrators at the scheduled times.

The following sections are covered:

- [Scenario](#)
- [Configuration](#)
 - [Create a custom view profile](#)
 - [Configure the report notification](#)
- [Related information](#)
- [Feedback and contact](#)

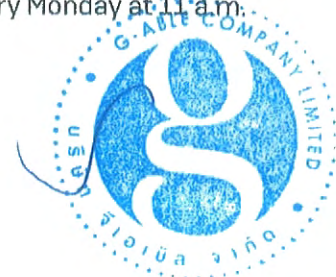
Applies to the following Sophos products and versions

Sophos Firewall

Scenario

Create the custom view profile Users and configure a Report Notification that notifies the administrator John Smith about the users responsible for maximum data transfer, every Monday at 11 a.m.

Configuration



Handwritten signatures and initials in blue ink at the bottom right of the page.

You must be logged in to the Admin Console as an administrator with Read-Write permissions for the relevant feature(s).

1.17

Create a custom view profile

As an example, we are creating a custom view profile for users responsible for maximum data transfer.

1. Go to **Reports > Show Reports Settings > Custom View** and click **Add** to create a new custom view profile.
2. Under the **Report Groups** section, expand **User Data Transfer Report** and select **Users**.
3. Click **Save** to create a custom view profile for users, as shown in the image below.

Add New Custom View Profile

How-To Guides Log Viewer Help admin Sophie, Admin User, Admin

Settings Close Reports Settings

Custom View Report Scheduling Data Management Manual Page Bookmarks Management Custom Logs

Custom View Users

Custom View Description List of users responsible for maximum data transfer

Report Groups [You can select up to 10 reports.]

- ▶ User App Risks & Usage
- ▶ Blocked User Apps
- ▶ Synchronized Applications
- ▶ Web Risks & Usage
- ▶ Blocked Web Attempts
- ▶ Search Engine
- ▶ Web Content
- ▶ Web Server Usage
- ▶ Web Server Protection
- ▶ User Data Transfer Report (1)
 - ☐ User Groups
 - ☒ Users
 - ☐ Date-wise Usage Report
 - ☐ Client Type
- ▶ FTP Usage

Save Cancel

Configure the report notification

1. Go to **Reports > Show Reports Settings > Report Scheduling** and click **Add** to create a new notification using the parameters in the table below.

Parameter	Value	Description
Name	Users	Name to identify the notification.



Handwritten signature and initials.

To Email Address john.smith@sophos.com Enter the email address of the recipient.

Report Type Report Group Select the notification type: Report Group or Bookmark.

Report Group Users This lists all the configured Custom View Profiles in addition to the default Report Groups. As an example, we have selected the Custom View Profile created in step 1.

Weekly

Email Frequency Send the email at 11 a.m. every Specify the frequency of the email notifications. The frequency can be set to be daily or weekly.

Monday

Add Report Schedule

How-To Guides Log Viewer Help admin
Sophos Anti-Virus Admin

Settings Close Reports Settings

Custom View **Report Scheduling** Data Management Manual Range Bookmark Management Custom Logo

Report

Security Audit Report

Name*

Users

(Spaces of Characters: 1-255. No special characters)

Description

Report Notification with list of users responsible for maximum data transfer

(Spaces of Characters: 1-255. No special characters)

To Email Address*

john.smith@sophos.com

(Spaces of Characters: 1-255. No special characters)

Report Type

Report Group

Bookmark

Report Group*

Users

Email Frequency*

Daily

Weekly

Send email at

11

Hour[s]

on every

Sunday

Monday

Tuesday

Wednesday

Thursday

Friday

Saturday

Note: Mail distribution contains report and log data

Save

Cancel

2. Click **Save** to create the report notification.

The configuration above will email a notification to john.smith@sophos.com every Monday at 11 a.m. that contains the reports configured in the **Users** Custom View Profile.



Handwritten signature and date 2/2/2558.

Related information

Page 56

- [Sophos XG Firewall: How to bookmark a report](#)
- [Sophos XG Firewall: How to manually purge report data](#)

Feedback and contact

If you've spotted an error or would like to provide feedback on this article, please use the section below to rate and comment on the article.

This is invaluable to us to ensure that we continually strive to give our customers the best information possible.

Article appears in the following topics

[XG Firewall](#) > [Sophos Firewall](#) > [Reports](#)

Did this article provide the information you were looking for?

Every comment submitted here is read (by a human) but we do not reply to specific technical questions. For technical support [post a question](#) to the community. Or [click here](#) for new feature/product improvements. Alternatively for [paid/licensed products](#) [open a support ticket](#).



[Handwritten signature]

18

Sophos XG Firewall: How to backup and restore a configuration

123145

6 Mar 2019

9 people found this helpful

[English](#) | [Español](#) | [Italiano](#) | [日本語](#) | [Français](#) | [Deutsch](#)

Overview

This article describes how to create and restore backups on a Sophos XG Firewall. We advise you create backups on a regular basis so if the system fails, you can quickly get the system back to a previously saved state. Taking backups of the configuration before making any major changes to the system is a best practice.

- Higher firmware versions cannot be restored on lower firmware versions, you must update first then restore.
- The Sophos XG Firewall importing the backup file must have the same or higher number of ports than the device the backup was created on.
- The admin password is not stored in the backup and will not be overwritten by a backup restoration.
- All certificates are included in the backup.
- The HA configuration is included in the backup.
- If a backup with HA configuration is restored on the primary device, it will restore the configuration and then reboot the primary device. It will then restore the configuration to the auxiliary device and then reboot the auxiliary device. HA will be restored automatically and no additional configuration is required.
Note: No failover will take place during the backup restoration. This will cause downtime.
- If a backup with HA configuration is restored to a new device or a factory-reset device, HA will be disabled for that device. You need to run through the whole HA configuration process again.

The following sections are covered:

- [How to create a backup](#)
 - [Local backup](#)
 - [FTP backup](#)
 - [Email backup](#)
 - [Scheduled backup](#)
- [How to restore a backup](#)
- [Feedback and contact](#)

Applies to the following Sophos products and versions
Sophos Firewall



Handwritten signatures and initials in blue ink at the bottom right of the page.

How to create a backup

A backup of the SFOS configuration data can be made in three ways, **Local**, **FTP**, and **Email**. A scheduled backup can also be configured.

Local backup

1. Navigate to **Backup & firmware > Backup & restore** tab.
2. Click **Backup now**.

Backup & Firmware

Backup has been taken successfully

Backup & Restore API Import Export Firmware Pattern Updates

Backup

Backup Mode ☒ Local ☐ FTP ☐ Email

Backup Prefix

Frequency ☐ Never ☐ Daily ☐ Weekly ☒ Monthly

Schedule Date HH MM

Apply Backup Now

Last backup taken on Mon 06 Mar 2017 10:16:41L Download

Backup Restore

Restore Configuration No file chosen

Upload and Restore

3. The backup is now stored locally on the device.
4. Download the backup file to your system by clicking  Download

FTP backup

1. Navigate to **Backup & firmware > Backup & restore** tab.
2. For the **Backup mode** field, select **FTP**.
3. Specify a **Backup prefix** for the backup file name. If a prefix is not provided, the default format is used for the backup file. Backup prefix will be useful in case you need to make backup from multiple devices.
4. Provide the FTP server information such as the **FTP server IP**, **Username**, and **Password** as you are using for FTP access through a web browser.
5. Provide the **FTP path**. It can be up to the folder name where you will save the backup on the FTP Server.
E.g. Test\Auto_Backup (ignore d:\test\Auto_Backup)
6. Click **Apply**.



Handwritten signatures and initials in blue ink.

Backup & Firmware



Backup schedule settings have been updated

Backup & Restore	API	Import/Export
Backup		
Backup Mode	☐ Local ☒ FTP ☐ Email	
Backup Prefix	test	
FTP Server IP	10.10.10.1	
Username *	admin	
Password *	***** Change Password	
FTP Path	Test\Auto_Backup	
Frequency	☐ Never ☐ Daily ☒ Weekly ☐ Monthly	
Schedule	Tuesday ▼ Day 10 ▼ HH 00 ▼ MM	
Apply Backup Now		

Email backup

1. Navigate to **Backup & firmware > Backup & restore** tab.
2. For the **Backup mode** field, select **Email**.
3. Specify a **Backup prefix** for the backup file name. If a prefix is not provided, the default format is used for the backup file. Backup prefix will be useful in case you need to make backup from multiple devices.
4. Provide an **Email address**.
5. Click **Apply**.

Backup & firmware	API	Import/Export	Firmware	Pattern updates
☒ Backup schedule settings have been updated successfully				
How-to guides Log viewer Help admin ▼				
Sophos Anti-Virus Asia				
Backup & restore				
Backup				
Backup mode	☐ Local ☐ FTP ☒ Email			
Backup prefix				
Email address *	test@sophos.com			
Frequency	☒ Never ☐ Daily ☐ Weekly ☐ Monthly			
Apply Backup now				

Scheduled backup



1. Navigate to **Backup & firmware > Backup & restore** tab.

2. Fill out the settings as below:

- **Backup mode:** Local, FTP or Email.
- **Backup prefix:** Adds prefix to the filename.
- **Email address:** Automatically emails this address in email backup mode.
- **Frequency:** Daily, Weekly or Monthly.
- **Schedule:** Select day of week, hour and minutes.

Backup & Firmware

How-To Guides Log Viewer Help Admin Local Anix Virus Area

Backup & Restore API Import/Export Firmware Pattern Updates

Backup

Backup Mode: ☐ Local ☐ FTP ☒ Email

Backup Prefix: DallasOffice

Email Address: testmaria@esphos.com * Guarantee Email will be sent to the first email address only

Frequency: ☐ Never ☐ Daily ☒ Weekly ☐ Monthly

Schedule: Sunday Day 00 141 00 MM

Apply Backup Now

3. Click **Apply** and the backups will automatically be emailed, sent via FTP or stored locally on the device at the scheduled time.

Backup file format

The backup file name format is as follows:

- **With a Prefix:** <Prefix>_Backup_<Device Key>_<timestamp>
- **Example:** Dallas_Backup_ABCDEY190_26Nov2014_12.09.24
- **Without a Prefix (Default):** Backup_<Device Key>_<timestamp>
- **Example:** Backup_ABCDEY190_26Nov2014_12.09.24

How to restore a backup

1. You can restore a backup instance to SF from **Backup & firmware**.
2. Click **Browse** under the Backup Restore section and select the backup file to be uploaded.



Handwritten signatures and initials in blue ink.

Backup & Firmware

How-to Guides Log Viewer Help Admin ▾
Search Articles

Backup & Restore

API

Import/Export

Firmware

Pattern Updates

Backup

Backup Mode

☒ Local
 ☐ FTP
 ☐ Email

Backup Prefix

Frequency

☐ Never
 ☐ Daily
 ☒ Weekly
 ☐ Monthly

Schedule

Sunday
 Day
 00
 HH
 00
 MM

Apply

Backup Now

Last backup taken on Thu 15 Mar 2018 00:25:33

Download

Backup Restore

Restore Configuration

Choose File

No file chosen

Upload and Restore

3. Click **Upload and restore** to restore the selected backup.

- When you restore to a backup configuration, the current configuration is overwritten.
- The firewall will reboot.
- VPN tunnels reconnect automatically.

Related information

- [Sophos XG Firewall: How to configure High Availability](#)

Feedback and contact

If you've spotted an error or would like to provide feedback on this article, please use the section below to rate and comment on the article.

This is invaluable to us to ensure that we continually strive to give our customers the best information possible.

Article appears in the following topics

[XG Firewall](#) > [Sophos Firewall](#) > [System](#) > [Administration](#)

Did this article provide the information you were looking for?



Handwritten signatures and initials in blue ink.

Sophos Firewall: How to upgrade the firmware

123285 7 Jun 2018 9 people found this helpful [English](#) | [Español](#) | [Italiano](#) | [日本語](#) | [Français](#) | [Deutsch](#)

Overview

This article shows how to upgrade the firmware of the Sophos Firewall device to the latest version.

The following sections are covered:

- [How to upgrade the firmware manually](#)
- [How to upgrade the firmware automatically](#)
- [Related information](#)
- [Feedback and contact](#)

Applies to the following Sophos products and versions

Sophos Firewall

Prerequisites

- Verify the Sophos Firewall has a valid support subscription.
- Schedule a maintenance window, device will reboot during the upgrade.
- Create a backup of the device.

18

How to upgrade the firmware manually

With this method you manually upload an already downloaded copy of the firmware from your local computers hard drive to the Sophos Firewall.

1. Browse to [Sophos.com](#) and login with your Sophos ID. Download the latest firmware from your account. For more information on this process see [Sophos XG Firewall: How to download firmware updates](#).
2. On the Sophos Firewall's GUI, Navigate to **Backup & Firmware > Firmware** and click the upload icon (📁) next to the inactive firmware to upload the downloaded firmware.



Handwritten signatures and initials in blue ink.

Backup & Firmware

Page 63

Log Viewer Help admin ▼
Sophos

Backup & Restore	API	Import/Export	Firmware	Pattern Updates
Firmware				
Version	Active	Manage		
SFOS 16.05.3 MR-3		🔍 📄 🔄		
SFOS 16.05.2 MR-2		🔍 📄 🔄		

2. The Firmware Upgrade/Downgrade screen will appear. **Browse** and select the firmware, and then click **Upload & Boot**.

Firmware Upgrade/Downgrade



Upload File

Choose file

No file chosen

Upload Firmware

Upload & Boot

Cancel

Upload & Boot process

Once **Upload & Boot** is clicked, the firewall performs the following actions:

- The Firmware is uploaded to the device.
- All active sessions on the device are closed.
- The firewall performs a restart and then boots up with the latest firmware.

You may click **Upload Firmware** instead of **Upload & Boot** if you want to upload now and reboot later.

To boot the device and use the uploaded firmware, go to **Backup & Firmware > Firmware** and click 🔍.



Handwritten signatures and initials in blue ink.

Firmware

Version	Active	Manage
SFOS 16.05.3 MR-3		🔍 ⚙️
SFOS 16.05.2 MR-2		🔍 📥 ⚙️

How to upgrade the firmware automatically

You do not need to download the firmware on your system before upgrading. You can check for new firmware versions and install them directly from the GUI.

1. Go to **Backup & Firmware > Firmware**.
2. Click on **Check for new Firmware**.
3. The new firmware will display along with the Download button, click on this to download to the firewall.
4. Click the **Install** button to install the latest firmware on your Sophos Firewall.

Latest Available Firmware

Firmware Version
VI-SFOS_16.05.3_MR-3_AZU-183

Check for new Firmware	
Type	Actions
MR	Install

High Availability

- For devices in High Availability (HA) mode, when you upgrade the Primary Device, the Auxiliary Device is updated automatically.
- If the **Upload firmware** option is used, the firewalls will not boot up with the new firmware on a normal reboot. To boot with the new firmware, the administrator has to go to **System > Maintenance > Firmware** and click **🔍** next to the newly uploaded firmware.

Related information

- [Sophos Firewall: How to backup and restore a configuration](#)
- [Sophos XG Firewall: How to download firmware updates](#)

Feedback and contact



Handwritten signature and date in blue ink.

19.2

Sophos Firewall: How to configure Sophos Sandstorm

125835 23 Aug 2017 0 people found this helpful [English](#) | [Español](#) | [Italiano](#) | [日本語](#) | [Français](#) | [Deutsch](#)

Overview

Sophos Sandstorm on Sophos Firewall scans unknown files to be analyzed in a sandbox environment before being released. This article explains how to enable and configure Sophos Sandstorm on the Sophos Firewall for Email and Web Protection.

The following sections are covered:

- [How to activate Sandstorm](#)
- [How to configure Sandstorm for Web Protection](#)
- [How to configure Sandstorm for Email Protection](#)
- [Related information](#)
- [Feedback and contact](#)

Applies to the following Sophos products and versions

Sophos Firewall 16.05

How to activate Sandstorm

Sandstorm is a separate module and must be purchased in order to work. You can evaluate Sandstorm for free for thirty days. To activate the trial follow the instructions in [Sophos Firewall: How to activate Sophos Sandstorm](#).

How to configure Sandstorm for Web Protection

1. Navigate to **Firewall** and edit the rule used to scan web traffic.
2. Go to the **Malware Scanning** section and enable **Detect zero-day threats with Sandstorm**. In 16.05 MR 5, it has moved to a firewall rule. Therefore you need to enable **Scan HTTP** first and then enable **Detect zero-day threats with Sandstorm**.



Handwritten signatures and initials in blue ink at the bottom right of the page.

Edit User/Network Rule

Identity

☐ Match known users

Malware Scanning

☐ Scan HTTP

☐ Decrypt & Scan HTTPS

☐ Detect zero-day threats with Sandstorm

☐ Scan FTP

Edit User/Network Rule

Identity

☐ Match known users

Malware Scanning

☒ Scan HTTP

☐ Decrypt & Scan HTTPS

☒ Detect zero-day threats with Sandstorm

☐ Scan FTP

3. Verify Sophos Anti-virus (AV) is running from **System Services > Services** and check if **Anti-virus** is started.



Handwritten signatures in blue ink at the bottom right of the page.

Page 67

Services	Status	Manage
Anti-Spam	Running	Stop
Anti-Spam Center Connectivity	Connected	Stop
Anti-virus	Running	Restart
Authentication	Running	Stop
DNS Server	Running	Stop
IPS	Running	Restart
Web Proxy	Running	Restart

4. Sophos Sandstorm explicitly works with Sophos AV, so make sure that **Single scan engine** set to **Sophos** in **Web > Protection**.

Malware Scanning

The firewall provides a number of methods for protecting against malware and inappropriate web usage. Use this page to configure how the firewall scans content for malware and viruses, and to enable and disable other protection mechanisms.

Scan Engine Selection
 Single Engine (Optimal Performance)
 Single scan engine is set to **Sophos**

Malware Scan Mode
 Batch (Maximum Protection)

Content that could not be scanned
 Block (Best Protection)
 Files that cannot be fully scanned because they are encrypted or corrupted may contain undetected threats

Do not scan files larger than 1 MB

Advanced Settings >

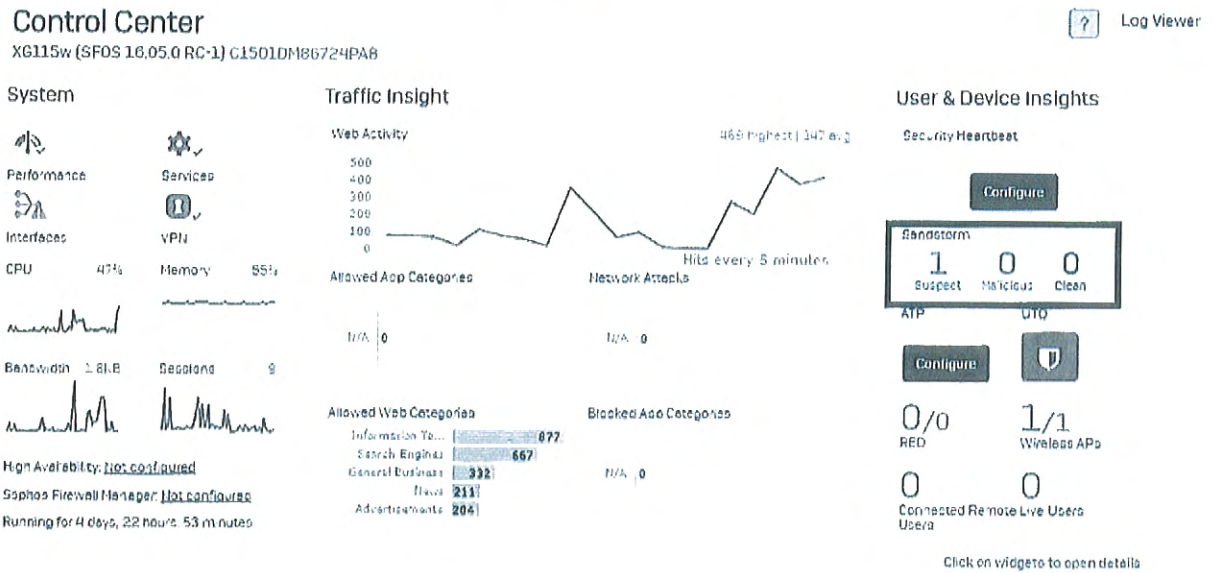
How to configure Sandstorm for Email Protection

Sandstorm scanning is only enabled for MTA mode; Legacy Mode is not compatible with Sandstorm.

1. Navigate to **Email > Policies** and make sure that **Detect zero-day threats with Sandstorm** is enabled.
2. Make sure that Sophos AV or Dual-Antivirus is selected for the SMTP policy.



Handwritten signatures and initials in blue ink at the bottom right of the page.



Related information

- [Sophos Firewall: How to activate Sophos Sandstorm](#)
- [Sophos Firewall: How to troubleshoot Sandstorm](#)

Feedback and contact

If you've spotted an error or would like to provide feedback on this article, please use the section below to rate and comment on the article.

This is invaluable to us to ensure that we continually strive to give our customers the best information possible.

Article appears in the following topics

[XG Firewall](#) > [Sophos Firewall](#) > [Protection](#)

Did this article provide the information you were looking for?

Every comment submitted here is read (by a human) but we do not reply to specific technical questions. For technical support [post a question](#) to the community. Or [click here](#) for new feature/product improvements. Alternatively for paid/licensed products [open a support ticket](#).



Handwritten signatures and initials in blue ink.

What's New in this Release

Introduction

Using Admin Console

Monitor and Analyze

Protect

Firewall

Intrusion Prevention

Web

Applications

Wireless

Email

Web Server

Advanced Threat

Advanced Threat Protection

Security Heartbeat

Sandstorm Activity

Sandstorm Settings

Configure

System

Appendix A - Logs

Appendix B - IPS - Custom Pattern
SyntaxAppendix C - Default File Type
Categories

Appendix D - Supported Micro-Apps

Appendix E - USB Compatibility List

Appendix F - Compatibility with SFMOS
15.01.0

Protect : Advanced Threat : Sandstorm Activity

Sandstorm Activity

Activity records provide basic information such as the date and time on which files were sent to Sandstorm. They also indicate analysis and release status. Use the links provided to view report details and release files.

To filter the list, click the Filter button () and specify criteria. For example, you can filter on a date range or file type.

19.4

To view details of a Sandstorm analysis, click Show report. Reports contain the following:

- Download details, for example, the source and download time
- File details, for example, the file name and type
- Result of the Sandstorm analysis
- Description of the potential threats contained by the file
- A list of all users who have downloaded the file

To release a file, click Release Now. When you release a file, users can download it immediately. Only files that are currently being analyzed or that have been returned with error status are eligible for release.

Sandstorm continues to analyze the file even if you release it.

Releasing an item before the analysis is complete may result in the downloading of malicious content.

Date

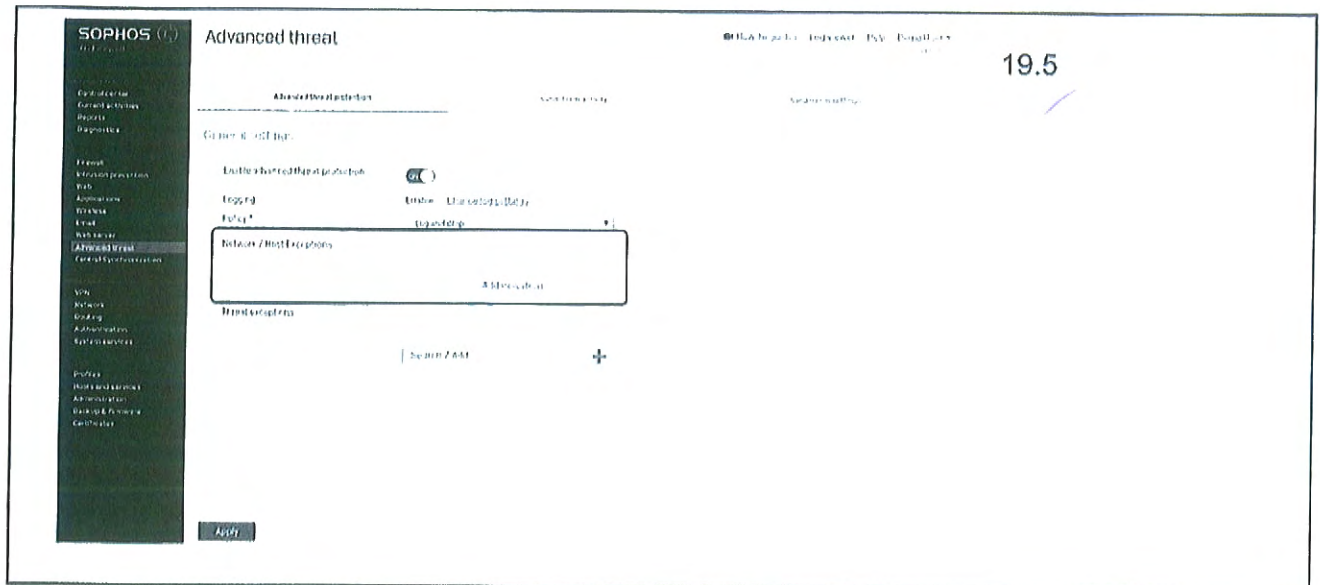
Date and time on which the file was sent to Sandstorm.

Recipient

IP address and user name associated with the download.

Source

Domain or IP address from which the user downloaded the file and the



Handwritten signature and initials in blue ink.

What's New in this Release

Introduction

Using Admin Console

Monitor and Analyze

Control center

Current Activities

Reports

Diagnostics

Protect

Configure

System

Appendix A - Logs

Appendix B - IPS - Custom Pattern Syntax

Appendix C - Default File Type Categories

Appendix D - USB Dongle Compatibility List

Appendix E - Compatibility with SFMOS
15.01.0

Appendix F - Additional Documents

Copyright Notice

Monitor and Analyze

19.8

Monitor and Analyze

Control center

The control center appears as soon as you log on to the admin console.

Control center provides a single screen snapshot of the state and health of the security system, which is easy to explore and drill.

System panel

System panel displays the real-time state of device services, VPN connections, WAN links and performance as well as number of days since the device is up and running. Status is displayed as an icon and colored icons are used to differentiate statuses. On clicking the icon, detailed information of the services is displayed.

The icons and their various status are:

Performance widget

Icon	Status
	Normal
	Warning
	Alert
	Unknown

Normal

Load average of the device is less than 2 units.

Warning

Load average is between 2 to 5 units.

Alert

Load average more than 5 units.

Unknown

On clicking the icon, the load average graph of the device is displayed.

Load average is a measure of the average number of processes waiting for execution



Sophos XG Firewall: How to use API

132560

2 Oct 2018

1 people found this helpful

[English](#) | [Español](#) | [Italiano](#) | [日本語](#) | [Français](#) | [Deutsch](#)

Overview

This article describes the steps how to use Sophos XG Firewall's API.

The following sections are covered:

- [What to do](#)
 - [Enable the API](#)
 - [Download the API Help](#)
 - [List of tags used in API](#)
 - [How to use API](#)
 - [Status code and description](#)
- [Related information](#)
- [Feedback and contact](#)

Applies to the following Sophos products and versions

Sophos XG Firewall

What to do

Enable the API

Go to **Authentication > Users** to create a new user for the API call. The user type will need to be **Administrator** and its profile will require read/write permissions. This API user is optional, its purpose is to lock the user down to certain rights in the XG, you can always use the Admin account.

ต้นฉบับ

Servers Services Groups **Users** One-Time Password Captive Portal Guest Users Clientless Users STAS ***

Total Active User 5 Out of 5

Show additional properties

☐ User ID	Name	Username	Type	Profile	Group	Status	Manage
☐ 10	apiuser	apiuser	Administrator	apiuser_profile	Open Group	Enabled	

Buttons: Add, Delete, Import, Export, Change Status, Purge AD Users

As an example, we configured this apiuser to have read/write permissions to the **Web & Content Filter** configuration.



Servers Services Groups Users One-Time Password Captive Portal Guest Users Clientless Users STAS

Edit Profile

Profile Name *

80 user profile

Configuration	☒ None	☐ Read-Only	☐ Read-Write
Control Center	☐	☐	☐
Initial Setup	☐	☐	☐
System	☐	☐	☐
Objects	☐	☐	☐
Network	☐	☐	☐
Wireless Protection	☐	☐	☐
Identity	☐	☐	☐
Security Policy	☐	☐	☐
VPN	☐	☐	☐
IPS	☐	☐	☐
Web & Content Filter	☐	☐	☒
Cloud Application Dashboard	☐	☐	☐
Application Filter	☐	☐	☐
Sandstorm activity	☐	☐	☐

Go to Backup & Firmware > API to enable the API Configuration and input the IP addresses you will make the call from in the Allowed IP Address field.



Backup & Firmware

How-To Guides Log Viewer Help admin
Sophos

Backup & Restore	API	Import Export	Firmware	Pattern Updates
API Configuration				
API Configuration	☒ Enabled			
Allowed IP Address	192.168.2.14			
	192.168.2.1			
	192.168.2.113			
	192.168.2.52			
	Search / Add			

This IP address needs to be in a zone that has access to the **HTTPS Admin Services**, if not, it needs a **Local Service ACL Exception Rule**.

Go to **Administration > Device Access** to verify its associated **Zone** or to create a **Local Service ACL Exception Rule**.



Administration

✓ Local Service ACL Rule has been added successfully

admin
Sophos

Licensing Device Access Admin Settings Central Management Time Notification Settings SNMP Netflow Messages

Local Service ACL

Zone	Admin Services							Authentication Services			Network Services		Other Services						
	HTTPS	Telnet	SSH	NTLM	Captive Portal	Radius SSO	Client Authentication	Ping/Ping6	DNS	Wireless Protection	SSL VPN	Web Proxy	User Portal	Dynamic Routing	SMTP Relay	SNMP			
LAN	☒	☐	☒	☐	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒			
WAN	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☒	☐	☐	☐	☐	☒			
DMZ	☐	☐	☒	☐	☐	☐	☐	☒	☐	☒	☐	☐	☐	☐	☐	☒			
VPN	☐	☐	☐	☐	☐	☐	☐	☒	☐	☒	☐	☐	☐	☐	☐	☒			
WIFI	☐	☐	☒	☐	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒			

Apply

Local Service ACL Exception Rule

Rule Name	IP Version	Add
<u>ApiException</u>	IPv4	Manage
		 

Download the API Help

Refer to the API documentation on how to format the XML request which is available in [XG Firewall documentation](#), different versions have different API documentation. For example, below is how to find the API for XG v17.1:

1. Open the [XG Firewall documentation](#)
2. Select the Sophos Firewall OS version 17.1

Sophos Ltd. [GB] | <https://www.sophos.com/en-us/support/documentation/sophos-xg-firewall.aspx?platform=Sophos-Firewall-OS-Version-17.1#Sophos-Firewall-OS-Version-17.1>

Apps Sophos XG Firewall Sophos JIRA Salesforce Sophos Hub Outlook Web App Sophos World Cup Terminologies Self Serve Operations Azure/AWS Subscrip XGUTM

SOPHOS PRODUCTS SOLUTIONS PARTNERS SUPPORT COMPANY

Overview Support Packages Downloads Documentation Training

Sophos XG Firewall

Find your product

Sophos XG Firewall

Sophos Firewall OS Version 17.1

3. Scroll down

SOPHOS PRODUCTS SOLUTIONS PARTNERS SUPPORT COMPANY SIGN IN

DOCUMENT

- Sophos Firewall OS Help
- Sophos XG Firewall Command Line Reference Guide
- Sophos XG Firewall Reports Guide
- Sophos XG Firewall Web Interface Reference and Admin Guide
- Release Notes
- API Help**

4. Click on **API Help** to download it, then click on **index.html** to open it.



ต้นฉบับ

20087

APIDocument (1).zip\APIDocument - ZIP archive, unpacked size 4,245,156 bytes

Name	Size	Packed	Type	Modified	CRC32
Local Disk					
CONFIGURE			File folder	9/25/2017 9:15 ...	
MONITOR & ANALYZE			File folder	9/25/2017 9:14 ...	
PROTECT			File folder	9/25/2017 9:15 ...	
SYSTEM			File folder	9/25/2017 9:15 ...	
UIResources			File folder	9/25/2017 7:16 ...	
closeFolder.png	2,916	2,916	PNG File	9/25/2017 7:16 ...	4A3995CE
common.js	537,169	155,574	JavaScript File	9/25/2017 7:14 ...	6D6BD377
common.js.old	466,904	107,643	OLD File	9/25/2017 7:16 ...	2D0A7E28
favicon.ico	6,518	614	Icon	9/25/2017 7:16 ...	1A3AE677
functions.js	7,324	2,244	JavaScript File	9/25/2017 7:16 ...	E3A69237
group-small-on-dark.png	2,873	2,873	PNG File	9/25/2017 7:16 ...	34CBB736
helpDoc.css	3,782	1,006	Cascading Style Sh...	9/25/2017 7:16 ...	101C99CD
index.html	1,110	501	Chrome HTML Doc...	9/25/2017 7:16 ...	664DF3D1
list.html	235,123	19,934	Chrome HTML Doc...	9/25/2017 9:15 ...	85227C25
logo.jpg	4,657	4,491	JPG File	9/25/2017 7:16 ...	B0AB8D16
openFolder.png	2,856	2,856	PNG File	9/25/2017 7:16 ...	F9368E88
search.jpg	11,921	5,924	JPG File	9/25/2017 7:16 ...	82458F44
sophos.html	1,097	601	Chrome HTML Doc...	9/25/2017 7:16 ...	E24485D8
sophosContentPage.html	18,541	3,260	Chrome HTML Doc...	9/25/2017 7:16 ...	62FBC551
SophosLogo.png	2,873	2,873	PNG File	9/25/2017 7:16 ...	34CBB736
updateRegexDesc.html	3,141	1,170	Chrome HTML Doc...	9/25/2017 7:16 ...	5B81B39B

5. Once opened, it looks like this. it includes XML tags, status codes used in the API and how to format the XML requests for all XG components organized the same way as in the XG's GUI.



file:///C:/Users/TAHERS-1/AppData/Local/Temp/RarSExa0.100/API/Document/index.html

SOPHOS SOPHOSAPI Help

How to use API ?

Please use the below link to use API:
<https://<Sophos IP>:<port>/webconsole/API/Controller?request=<Add the XML request here>>
 Note: Port you mention in above URL should be same as the port you have configured as Admin Console HTTPS Port from System > Administration > Settings.
 Example:

1. Set Request
<https://<Sophos IP>:<port>/webconsole/API/Controller?request=<Request>=<Login><Username>admin/<Username><Password>passwordform=<encrypt>8b1e4eb7b182b1826290f6e99733fc/<Password>=<Login><Set><IPHost>transactionId=<Name><Ip2></Name><IPFamily>IP4</IPFamily><HostType>IP</HostType><IPAddress>2.2.2.9</IPHost></Set></Request>>
2. Get Request
<https://<Sophos IP>:<port>/webconsole/API/Controller?request=<Request>=<Login><Username>admin/<Username><Password>passwordform=<encrypt>8b1e4eb7b182b1826290f6e99733fc/<Password>=<Login><Get><IPHost></IPHost></Get></Request>>

Status Code and Description

Status	Message
200	Configuration applied successfully.
201	Operation partially successful.
203	Operation successful but few configurations could not be applied. Please contact Support.
204 - 210	Operation partially failed.
211 - 215	Warning messages will be displayed. For more information, refer to the section "Status Message Information" on each page.
216	Operation Successful. For more information, refer to the section "Status Message Information" on each page.
500	Operation could not be performed on Entity.
501	Configuration parameters validation failed.
502	Operation failed. Entity having same name already exists.
503	Operation failed. Entity having same parameter details already exists.
504 - 510	Operation failed. Deleting entity relayed by another entity.
511 - 520	Operation failed. Please contact Support.
521	XML Request not compatible with current API version.
522 - 525	Maximum limit reached for entity.
526	Record does not exist.
528	Trying to update default entities which are not editable.
529	Invalid XML request for entity/entities.
530	API Version not supported for specific entity.
541 - 590	Operation failed. For more information, refer to the section "Status Message Information" on each page.
596	Not having permission to add/delete configuration

Now you can make the API request to the XG using a browser or any remote application that support API like [curl](#). [Sophos XG Firewall: How to use API to import web exceptions](#) is an example.

Note: Make sure you pass the certificate error if using a self signed certificate.

19.9

List of tags used in API

XML tags are used for applying the configurations on the appliance.

Tag Name

<Request>

Description

It is used for sending XML Request. To apply any configuration this tag is necessary. API Version also needs to be specified for configurations to be applied successfully.

จำนวน

8889

Usage Attribute – APIVersion

Attribute Value – Version of API used. For example: "1500.2"

Example

<Request APIVersion="1500.2">

<Login>

<Username>admin</Username>

<Password passwordform="encrypt">8b1e6eb1b182b1806390ffefc99753fc</Password>

</Login>

</Request>

Tag Name <Login>

Description It is used for Authentication.

Usage Attribute – N/A
Attribute Value – N/A

Example Please refer to the example above.

Tag Name <Username>

Description Specify the username in this tag.

Usage Attribute – N/A
Attribute Value – N/A

Example Please refer to the example above.

Tag Name <Password passwordform="encrypt">

Description Specify the encrypted password in this tag.



Usage Attribute – N/A
Attribute Value – N/A

Example Please refer to the example above.

Tag Name <Set>

Description It is used to inform that the request is to be served as Add/Update depending on the Attribute value.
Note: If, no "operation" attribute/value is defined in the tag, then Add operation will be performed followed by Update.

Usage Attribute – operation
Attribute Value – Add/Update

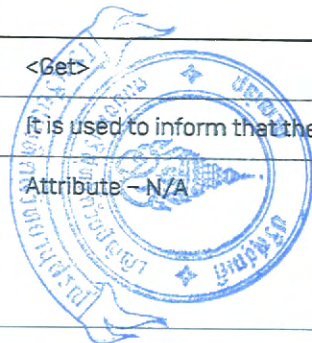
Example

```
<Request>
  <Login>
    <Username>admin</Username>
    <Password passwordform="encrypt">8b1e6eb1b182b1806390ffefc99753fc</Password>
  </Login>
  <Set operation="add">
    <IPHost>
      <Name>CustomIPHostTypeIPv4</Name>
      <IPFamily>IPv4</IPFamily>
      <HostType>IP</HostType>
      <IPAddress>1.1.1.1</IPAddress>
    </IPHost>
  </Set>
</Request>
```

Tag Name <Get>

Description It is used to inform that the request needs to be served for retrieving data of the entity specified.

Usage Attribute – N/A



ព្រះរាជាណាចក្រកម្ពុជា

7600

Example

```

<Request>
  <Login>
    <Username>admin</Username>
    <Password passwordform="encrypt">8b1e6eb1b182b1806390ffefc99753fc</Password>
  </Login>
  <Get>
    <IPHost></IPHost>
  </Get>
</Request>

```

Tag Name <Filter>

Description It is used for retrieving entity data based on the criteria specified in the <Key> tag. It is only applicable for entity 'Name'.

Usage Attribute - N/A
Attribute Value - N/A

Example

```

<Request>
  <Login>
    <Username>admin</Username>
    <Password passwordform="encrypt">8b1e6eb1b182b1806390ffefc99753fc</Password>
  </Login>
  <Get>
    <IPHost>
      <Filter>
        <key name="Name" criteria="like">CustomIPHostTypeIPv4</key>
      </Filter>
    </IPHost>
  </Get>
</Request>

```



Example

```

<Request>
  <Login>
    <Username>admin</Username>
    <Password passwordform="encrypt">8b1e6eb1b182b1806390ffefc99753fc</Password>
  </Login>
  <Get>
    <IPHost></IPHost>
  </Get>
</Request>

```

Tag Name <Filter>

Description It is used for retrieving entity data based on the criteria specified in the <Key> tag. It is only applicable for entity 'Name'.

Usage Attribute - N/A
Attribute Value - N/A

Example

```

<Request>
  <Login>
    <Username>admin</Username>
    <Password passwordform="encrypt">8b1e6eb1b182b1806390ffefc99753fc</Password>
  </Login>
  <Get>
    <IPHost>
      <Filter>
        <key name="Name" criteria="like">Custom.IPHostTypeIPV4</key>
      </Filter>
    </IPHost>
  </Get>
</Request>

```

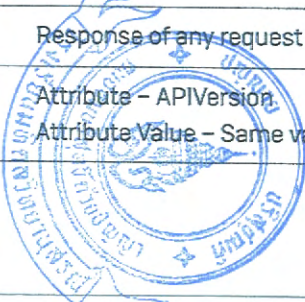


Tag Name	<Key>
Description	It is used within the <Filter> tag to specify the filter key and Filter criteria.
Usage	Attribute - name, criteria Attribute Value - name = "Name", criteria = ["=", "!=", "like"]
Example	Please refer to the example above.

Tag Name	<Remove>
Description	It is used to delete data.
Usage	Attribute - N/A Attribute Value - N/A

Example	<Request>
	<Login>
	<Username>admin</Username>
	<Password passwordform="encrypt">8b1e6eb1b182b1806390ffefc99753fc</Password>
	</Login>
	<Remove>
	<IPHost>
	<Name>CustomIPHostTypeIPv4</Name>
	</IPHost>
	</Remove>
	</Request>

Tag Name	<Response>
Description	Response of any request will be displayed in this tag.
Usage	Attribute - APIVersion Attribute Value - Same value as specified in the XML Request or if it is not specified then active firmware API Version will be considered.



ต้นฉบับ

Example

```
<Response APIVersion="1500.2">
  <Login>
    <status>Authetication Successful</status>
  </Login>
  <IPHost transactionid="">
    <Status code="502">Message.IPHostRecordExists</Status>
  </IPHost>
</Response>
```

Tag Name <Status>

Description It is a part of the <Response> tag and it indicates the configuration status based on the code.

Usage
Attribute – code
Attribute Value – code value.

Example

```
<Response APIVersion="1500.2">
  <Login>
    <status>Authetication Successful</status>
  </Login>
  <IPHost transactionid="">
    <Status code="502">Operation failed. Entity having same name already exists</Status>
  </IPHost>
</Response>
```

How to use API

Please use the link below to use API:

<https://<Sophos IP>:<port>/webconsole/APIController?reqxml=<Add the XML request here>>

Note: The port mentioned in the URL above should be the same as the port that is configured in the **Admin Console HTTPS Port** from **System > Administration > Admin Settings**.

Example:

• Set Request

```
https://<Sophos IP>:<port>/webconsole/APIController?reqxml=<Request><Login><Username>admin</Username><Password
passwordform="encrypt">8b1e6eb1b182b1806390ffefc99753fc</Password></Login><Set> <IPHost transactionid=""><Name>ip2</Name>
<IPFamily>IPv4</IPFamily><HostType>IP</HostType><IPAddress>2.2.2.9</IPAddress></IPHost> </Set></Request>
```

Get Request

```
https://<Sophos IP>:<port>/webconsole/APIController?reqxml=<Request><Login><Username>admin</Username><Password
passwordform="encrypt">8b1e6eb1b182b1806390ffefc99753fc</Password></Login><Get> <IPHost></IPHost> </Get></Request>
```

Status code and description

When XML response is received, it contains a status code with the description about the success/failure of the operation.

Status	Message
200	Configuration applied successfully.
201	Operation partially successful.
203	Operation successful but few configurations could not be applied. Please contact Support.
204 - 210	Operation partially failed.
211 - 215	Warning messages will be displayed. For more information, refer to the section "Status Message Information" on each page.
216	Operation Successful. For more information, refer to the section "Status Message Information" on each page.
500	Operation could not be performed on Entity.
501	Configuration parameters validation failed.
502	Operation failed. Entity having same name already exists.
503	Operation failed. Entity having same parameter details already exists.
504 - 510	Operation failed. Deleting entity referred by another entity.
511 - 520	Operation failed. Please contact Support.

521	XML Request not compatible with current API version.
522 - 525	Maximum limit reached for entity.
526	Record does not exist.
528	Trying to update default entities which are not editable.
529	Invalid XML request for entity/entities.
530	API Version not supported for specific entity.
541 - 590	Operation failed. For more information, refer to the section "Status Message Information" on each page.
599	Not having privilege to add/modify configuration.

Related information

- [Sophos XG Firewall: How to use API to import web exceptions](#)

Feedback and contact

If you've spotted an error or would like to provide feedback on this article, please use the section below to rate and comment on the article. This is invaluable to us to ensure that we continually strive to give our customers the best information possible.

Article appears in the following topics

[XG Firewall](#)

Did this article provide the information you were looking for?

Every comment submitted here is read (by a human) but we do not reply to specific technical questions. For technical support [post a question](#) to the community. Or [click here](#) for new feature/product improvements. Alternatively for paid/licensed products [open a support ticket](#).

หน้า 87

000000

SOPHOS

Cybersecurity made simple.

Sophos Sandstorm

Next-generation advanced threat defense made simple

Sophos Sandstorm uses next-gen, cloud sandbox technology to give your organization an extra layer of security against ransomware and targeted attacks.

The only network sandbox to use deep learning analysis for more effective detection, it integrates with Sophos XG Firewall, Sophos UTM, Sophos Web Appliance, Sophos Email Appliance, and Sophos Email on Sophos Central — no additional hardware required.

And it's great value for money. You get all the benefits of enterprise-grade protection without the enterprise price tag.



Highlights

- Seamless integration with your Sophos security solution
- Up and running in minutes
- Protects against ransomware APTs, unknown malware, PUA and targeted attacks
- Threat intelligence you can act on
- Deep learning analysis
- Granular, incident-centric reports

19.10

Advanced protection from targeted attacks

Keep ransomware and unknown data-stealing malware off your network. Powerful, cloud-based, next-generation sandbox technology and deep learning analysis means you quickly and accurately detect, block, and respond to APTs and zero-day threats.

We keep it simple

Sophos Sandstorm is fully integrated into your Sophos security solution. Simply update your subscription, apply the Sandstorm policy and you're protected instantly against targeted attacks. You'll be up and running in minutes.

19.10

Block evasive threats that others don't see

Detect ransomware and unknown threats specifically designed to evade first-generation sandbox appliances. Our full-system emulation approach provides the deepest level of visibility into the behavior of unknown malware and the detection of malicious attacks that others simply miss.

Deep forensic reporting

Accelerate response to advanced threats with simple incident-centric breach analysis. We provide you with prioritized APT intelligence by correlating the evidence. This approach both reduces noise and saves you time.

Lightning performance

Your Sophos security solution accurately pre-filters traffic, so only suspicious files are submitted to Sandstorm, ensuring minimal latency and end user impact.

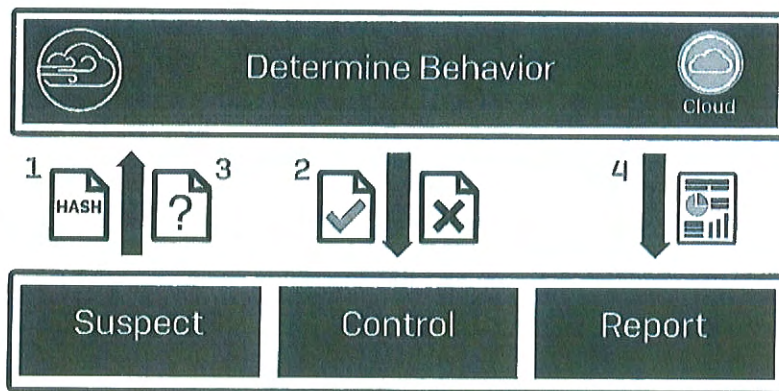


Handwritten signatures and initials in blue ink.

Sophos Sandstorm Features

- Full integration into your Sophos security solution dashboard
- Inspects executables and documents containing executable content
 - Windows executables (including .exe, .com, and .dll)
 - Word documents (including .doc, .docx, .docm and .rtf)
 - PDF documents
 - Archives containing any of the file types listed above (ZIP, BZIP, GZIP, RAR, TAR, LHA/LZH, 7Z, Microsoft Cabinet)
 - Supports more than 20 file types
- Dynamic malware behavior analysis and deep learning runs files in real environments
- In-depth malicious file reports and dashboard file release capability
 - Average analysis time less than 120 seconds
 - Flexible user and group policy options on file type, exclusions, and actions on analysis
 - Supports one-time download links

How it Works



1. The Sophos security solution scans files against all conventional security checks (e.g., anti-malware signatures, bad URLs, etc.). If the file is executable or has executable content and is not downloaded from a safe website, the file is treated as suspicious. The Sophos security solution sends the suspicious file hash to Sophos Sandstorm to determine if it has been previously analyzed.
2. If the file hash has been previously analyzed, Sophos Sandstorm passes the threat intelligence to the Sophos security solution. Here, the file is delivered to the user's device or blocked, depending on the information provided by Sophos Sandstorm.
3. If the hash has not been seen before, a copy of the suspicious file is sent to Sophos Sandstorm. Here, the file is detonated and its behavior is monitored. Once fully analyzed, Sophos Sandstorm passes the threat intelligence to the Sophos security solution. Again, the file is delivered to the user's device or blocked, depending on the information provided by Sophos Sandstorm.
4. The Sophos security solution uses the detailed intelligence supplied by Sophos Sandstorm to create deep forensic reports on each threat incident.

Try it now for free

Register for a free 30-day evaluation
at sophos.com/sandstorm

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

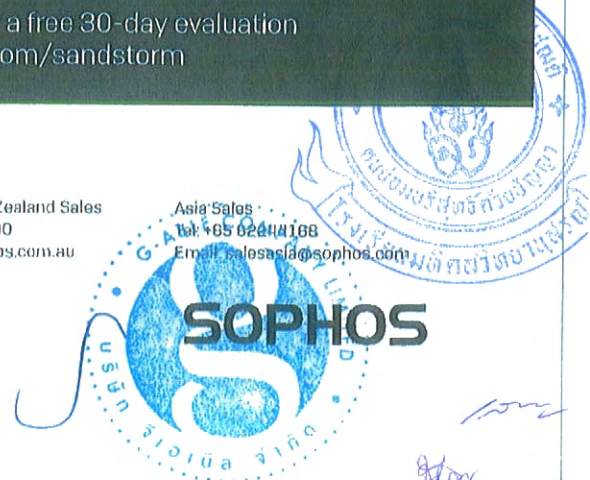
North American Sales
Toll Free: 1-866-866-2802
Email: na-sales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 6244 1168
Email: salesasia@sophos.com

© Copyright 2017 Sophos Limited. All rights reserved.
Sophos, the Sophos logo, and the Sophos Sandstorm logo are trademarks of Sophos Limited. All other trademarks are the property of their respective owners.
Sophos and the Sophos logo are registered trademarks of Sophos Limited. All other trademarks are the property of their respective owners.

25/06/2017 10:00:00



Edit User/Network Rule 7

How-To Guides Log Viewer Help admin
united analyst and engineering consultant co.,ltd

Rule Name *

#Default_Network_Policy

Description

Enter Description

Action

Accept

Drop

Reject

Source

Source Zones *

LAN

Add New Item

Source Networks and Devices *

Any

Add New Item

During Scheduled Time

All the Time

Destination & Services

Destination Zones *

WAN

Add New Item

Destination Networks *

Any

Add New Item

Services *

Any

Add New Item

Identity

☐ Match known users

Web Malware and Content Scanning

Save

Cancel

ต้นฉบับ

66666

SOPHOS
 XG Firewall

MONITOR & ANALYZE
 Control Center
 Current Activities
 Reports
 Diagnostics

PROTECT

Firewall

Intrusion Prevention
 Web
 Applications
 Wireless
 Email
 Web Server
 Advanced Threat
 Synchronized Security

CONFIGURE

VPN
 Network
 Routing
 Authentication
 System Services

SYSTEM

Profiles
 Hosts and Services
 Administration
 Backup & Firmware
 Certificates

Edit User/Network Rule

☐ Scan FTP for Malware

Advanced

User Applications

Intrusion Prevention

None

Traffic Shaping Policy

None

Web Policy

GUEST-Policy

☐ Apply Web Category based Traffic Shaping Policy

Application Control

Allow All

☐ Apply Application-based Traffic Shaping Policy

Synchronized Security

Minimum Source HB Permitted:

☐ GREEN ☐ YELLOW ☒ No Restriction
☐ Block clients with no heartbeat

Minimum Destination HB Permitted:

☐ GREEN ☐ YELLOW ☒ No Restriction
☐ Block request to destination with no heartbeat

NAT & Routing

☒ Rewrite source address (Masquerading)
☐ Use Gateway Specific Default NAT Policy

Use Outbound Address

MASQ

MASQ (Interface Default IP)

Primary Gateway

JASTEL

Backup Gateway

WAN1

DSCP Marking

Select DSCP Marking

Log Traffic

☒ Log Firewall Traffic

Save

Cancel

00100

หนังสือแต่งตั้งตัวแทนจำหน่าย และรับรองผลิตภัณฑ์



SOPHOS

Sophos Limited

92/4, Room 209, 2FL Sathorn Thani Tower 2, Khwaeng Silom, Khet Bang Rak, Krung Thep MahaNakhon 10500 THAILAND

www.sophos.com

วันที่ 18 เม.ย. 2562

เรียน ประธานและคณะกรรมการพิจารณาโครงการ
เรื่อง แต่งตั้งตัวแทนจำหน่ายผลิตภัณฑ์ และ รับรองผลิตภัณฑ์
อ้างถึง เอกสารประกวดราคาซื้อด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ (e-bidding) เลขที่ ๑๕/๒๕๖๒
การซื้อระบบป้องกันการบุกรุกโจมตี ตามประกาศโรงเรียนมหิดลวิทยานุสรณ์ ลงวันที่ ๑๑ เมษายน ๒๕๖๒

หนังสือฉบับนี้ทำขึ้นเพื่อแสดงว่า บริษัท โซฟอส จำกัด สำนักงานตั้งอยู่เลขที่ 92/4 ชั้น 2 อาคาร สาทรรธานี 2 ห้องเลขที่ 209 แขวงสีลม เขตบางรัก กรุงเทพมหานคร 10500 ซึ่งได้รับอนุญาตอย่างถูกต้องตามกฎหมายให้เป็นสำนักงานสาขาประจำประเทศไทย ซึ่งมีสำนักงานใหญ่อยู่ที่ประเทศอังกฤษ โดยเป็นเจ้าของผลิตภัณฑ์ภายใต้เครื่องหมายการค้า โซฟอส (SOPHOS) มีความยินดีแต่งตั้งให้

บริษัท จีเอเบิล จำกัด
สำนักงานใหญ่ตั้งอยู่เลขที่ 127/27, 29-31 ถนนนนทรี
แขวงช่องนนทรี เขตยานนาวา กรุงเทพฯ 10120

เป็นตัวแทนจำหน่ายผลิตภัณฑ์ของบริษัท ยี่ห้อโซฟอส (SOPHOS) ต่อ โรงเรียนมหิดลวิทยานุสรณ์ บริษัทฯ ขอรับรองว่าผลิตภัณฑ์ที่เสนอในโครงการนี้ว่ายังอยู่ในสายการผลิต โดยไม่เป็นของเก่าที่ยกเลิกการผลิต และเป็นสินค้าใหม่ มีการรับประกันสินค้าพร้อม Subscription ไม่น้อยกว่า 3 ปี

จึงเรียนมาเพื่อทราบ

ขอแสดงความนับถือ

5

K. Kattapha

นาย ณัฐพันธ์ เรืองรังษีรัตน์
(Territory Manager)



Sophos Ltd.

92/4, Room 209, 2FL Sathorn Thani Tower 2, Khwaeng Silom, Khet Bang Rak, Krung Thep Maha Nakhon 10500
Tel: (662) 673 9512

Handwritten signature and initials in blue ink.

SOPHOS

Sophos Limited

92/4, Room 209, 2FL Sathorn Thani Tower 2, Khwaeng Silom, Khet Bang Rak, Krung Thep MahaNakhon 10500 THAILAND

www.sophos.com

วันที่ 22 เม.ย. 2562

เรียน ประธานและคณะกรรมการพิจารณาโครงการ
เรื่อง หนังสือรับรองผลิตภัณฑ์
อ้างถึง เอกสารประกวดราคาซื้อด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ (e-bidding) เลขที่ ๑๕/๒๕๖๒
การซื้อระบบป้องกันการบุกรุกโจมตี ตามประกาศโรงเรียนมหิดลวิทยานุสรณ์
ลงวันที่ ๑๑ เมษายน ๒๕๖๒

หนังสือฉบับนี้ทำขึ้นเพื่อแสดงว่า บริษัท โซฟอส จำกัด สำนักงานตั้งอยู่เลขที่ 92/5 ชั้น 2 อาคาร สาทรธานี 2 ห้องเลขที่ 209 แขวงสีลม เขตบางรัก กรุงเทพมหานคร 10500 ซึ่งได้รับอนุญาตอย่างถูกต้องตามกฎหมายให้เป็นสำนักงาน สาขาประจำประเทศไทย ซึ่งมีสำนักงานใหญ่อยู่ที่ประเทศอังกฤษ โดยเป็นเจ้าของผลิตภัณฑ์ภายใต้เครื่องหมายการค้าโซฟอส (SOPHOS) ขอรับรองคุณสมบัติผลิตภัณฑ์ดังนี้

1. เป็นอุปกรณ์ป้องกันการบุกรุกโจมตีชนิด Stateful Inspection Firewall แบบ Appliance ที่มี
- 1.2 IPSEC VPN Throughput ไม่น้อยกว่า 4 Gbps
- 2.1 มี Network Interface แบบ 1 Gigabit Ethernet UTP จำนวนไม่น้อยกว่า 8 ช่อง
7. สามารถทำ Static NAT, Source NAT และ Destination NAT ได้
8. สามารถบริหารจัดการ การส่งข้อมูลแบบ Policy Based Routing หรือ Firewall rule routing โดยสามารถเลือกข้อมูลที่จะส่งโดยดู Application Signature
14. มีแหล่งจ่ายไฟ (Power Supply) แบบ internal ที่สามารถทำงานแบบ Hot-Swap และ Redundant จำนวนไม่น้อยกว่า 2 หน่วย
- 19.2 สามารถตัดการเข้าถึง (Block) จากเครื่องปลายทางออกจากระบบเครือข่ายโดยอัตโนมัติ เมื่อตรวจพบ Malware หรือ Virus

จึงเรียนมาเพื่อทราบ

ขอแสดงความนับถือ

K. Kattapha

นาย ณัฐพันธ์ เรืองรังษีรัตน์
(Territory Manager)

Sophos Ltd.

92/4, Room 209, 2FL Sathorn Thani Tower 2, Khwaeng Silom, Khet Bang Rak, Krung Thep Maha Nakhon 10500
Tel: (662) 673 9512

