Hillstone A-Series

Next-Generation Firewall

Hillstone next-generation firewall มีคุณสมบัติด้านความปลอดภัยสูง สามารถขยายได้ตามต้องการ มีการตรวจจับและป้องกันภัยคุกคามขั้นสูงที่สมบูรณ์ และการดำเนินการตามนโยบายที่ชาญฉลาดและอัตโนมัติ NGFW เป็นสถาปัตยกรรมฮาร์ดแวร์ใหม่ล่าสุด ซึ่งมอบประสิทธิภาพระดับแอปพลิเคชั่นชั้นนำของอุตสาหกรรมเพื่อตอบสนองความต้องการด้านความปลอดภัยเครือข่ายในโลกแห่งความเป็นจริง

High-density ports ทำให้สามารถเข้าถึงข้อมูลได้อย่างยอดเยี่ยม และตัวเลือกการจัดเก็บข้อมูลขนาดใหญ่ช่วยให้มองเห็นและวิเคราะห์ข้อมูลได้ดีขึ้น ส่วนหนึ่งของโซลูชัน ZTNA NGFW จะควบคุมการเข้าถึงแอปพลิเคชั่นอย่างละเอียดด้วยการลบความน่าเชื่อถือโดยปริยายและการตรวจยืนยันอย่างต่อเนื่อง Hillstone NGFW นำเสนอการป้องกันขั้นสูงที่สมบูรณ์ต่อภัยคุกคามที่ทราบและไม่ทราบ พร้อมทั้งการดำเนินการตามนโยบายที่ชาญฉลาด อัตโนมัติ และมีประสิทธิภาพ ซึ่งทำให้การดำเนินการด้านความปลอดภัยเป็นเรื่องง่าย

จุดเด่นของผลิตภัณฑ์

High-Performance Hardware Architecture
(การตรวจจับและป้องกันภัยคุกคามขั้นสูง)

Hillstone A-Series NGFW มีกลไกครบครันเพื่อให้การตรวจจับและการป้องกันแบบ real-time ตลอดวงจรของการโจมตีเครือข่ายและมัลแวร์ ก่อนที่จะเกิดการละเมิด การป้องกันเชิงรุก เช่น IPS จะบล็อกการใช้ประโยชน์จากช่องโหว่ บริการชื่อเสียง IP จะบล็อกคำขอจากไซต์ที่มีความเสี่ยงซึ่งอาจเกี่ยวข้องกับมัลแวร์และสแปม การกรอง URL จะป้องกันไม่ให้ผู้ใช้เข้าถึงไซต์ที่เกี่ยวข้องกับการฟิชชิ่ง การดาวน์โหลดมัลแวร์ และการโจมตีอื่นๆ โดยไม่ได้ตั้งใจ โปรแกรมป้องกันไวรัสจะตรวจจับและบล็อกมัลแวร์ที่รู้จักในระดับเครือข่ายด้วยฐานข้อมูลsignatureขั้นสูงที่อัปเดตอย่างต่อเนื่อง โปรแกรมป้องกันสแปมจะจัดหมวดหมู่และป้องกันสแปมแบบ real-time สำหรับทั้งการรับส่งข้อมูลขาเข้าและขาออก

ในระหว่างที่เกิดการละเมิด โปรแกรมป้องกันไวรัสก็มีบทบาทสำคัญเช่นกัน โดยจะตรวจจับและบล็อกมัลแวร์ที่รู้จักต่อไป sandbox บนคลาวด์จะตรวจจับและป้องกันไฟล์ที่เป็นอันตรายได้อย่างซับซ้อน ผ่านการวิเคราะห์แบบคงที่และการประมวลผลล่วงหน้า ตามด้วยการวิเคราะห์พฤติกรรมซึ่งรวมถึงการตรวจจับการหลบเลี่ยง จากนั้นระบบ Cloud intelligence จะระบุและบล็อกไฟล์ที่เป็นอันตราย สร้างบันทึกและรายงาน และแบ่งปันระบบ Cloud intelligence ด้านภัยคุกคาม

A-Series ช่วยปกป้องได้ภัยคุกคามทั้งหมดแบบครอบคลุม โดยป้องกันต่อไปแม้ว่าจะเกิดการละเมิดขึ้นแล้วก็ตาม Botnet C&C ขั้นสูงของ Hillstone จะป้องกันการสื่อสารไปยังช่องทางควบคุม และตรวจจับและบล็อกBot ภายในอินทราเน็ตด้วยเช่นกัน นอกจากนี้ A-Series NGFW ยังใช้ประโยชน์จากเทคโนโลยีการเรียนรู้ของเครื่องสำหรับการป้องกันความปลอดภัยอัจฉริยะต่อภัยคุกคามที่ทราบและไม่ทราบ เช่น การตรวจจับ DDoS, DGA และการรับส่งข้อมูลที่เข้ารหัสอย่างชาญฉลาดโดยไม่ต้องถอดรหัส นอกจากนี้ระบบตรวจจับและวิเคราะห์ภัยคุกคามแบบศูนย์รวมของระบบยังประสานงานกับกลไกความปลอดภัยในตัวทั้งหมดเพื่อเพิ่มประสิทธิภาพอย่างมากในขณะที่ลดเวลาแฝงของเครือข่าย

High-Performance Hardware Architecture
(สถาปัตยกรรมฮาร์ดแวร์ประสิทธิภาพสูง)

A-Series ที่พร้อมสำหรับอนาคตมีรูปแบบที่กะทัดรัดและฐานการคำนวณที่มีประสิทธิภาพสูงพร้อมความปลอดภัยที่ไม่มีการประนีประนอม NGFW ของ A-Series มอบประสิทธิภาพที่มั่นคงสำหรับการรับส่งข้อมูลของไฟร์วอลล์ เซสชันที่เกิดขึ้นพร้อมกันและเซสชันใหม่ และประสิทธิภาพที่รวดเร็วอย่างน่าทึ่งสำหรับเลเยอร์แอปพลิเคชัน ซึ่งมีความสำคัญในการตอบสนองความต้องการของสภาพแวดล้อมความปลอดภัยในปัจจุบัน ขับเคลื่อนด้วยความเร็วของฮาร์ดแวร์ที่เป็นกรรมสิทธิ์ของ Hillstone รุ่นhigh-end ของ A-Series NGFW ช่วยให้ส่งต่อแพ็กเก็ตได้อย่างรวดเร็วด้วยปริมาณข้อมูลสูงและความหน่วงเวลาต่ำเป็นพิเศษ จากการออฟโหลดข้อมูลนอกจากนี้ยังมีระบบนิเวศซอฟต์แวร์ที่เป็นมิตรสำหรับการบูรณาการกับบุคคลที่สามเพื่อรองรับคุณสมบัติความปลอดภัยเพิ่มเติมหากต้องการ รุ่นติดตั้งในแร็คทั้งหมดมีช่องระบายอากาศด้านหน้าและด้านหลังเพื่อช่วยในการระบายความร้อน ซึ่งเป็นปัญหาในเครือข่ายเกือบทุกขนาด

Excellent Access Capability and Storage Expansion
(ความสามารถในการเข้าถึงที่ยอดเยี่ยมและการขยายพื้นที่จัดเก็บ)

Hillstone A-Series มี offers high I/O port ช่วยให้ NGFW ทำหน้าที่เป็นสวิตช์หรือเราเตอร์ตามต้องการ ลดต้นทุนการใช้งานและการจัดการ นอกจากนี้ยังมี expansion slots สำหรับ A-Series หลายรุ่นเพื่อเพิ่มประสิทธิภาพการทำงานให้ดียิ่งขึ้น Bypass pairs ใน A-Series ส่วนใหญ่ช่วยให้มั่นใจได้ถึงความต่อเนื่องของธุรกิจ ทุกรุ่น รวมถึงรุ่นเดสก์ท็อป มาพร้อมพื้นที่จัดเก็บออนบอร์ดขนาดใหญ่และมีตัวเลือกขยายสำหรับพื้นที่จัดเก็บ hard disk ขนาดใหญ่สูงสุดถึง 2 TB ด้วยพื้นที่จัดเก็บที่มากขึ้น ระบบจึงสามารถบันทึกบันทึกและข้อมูลได้มากขึ้น เป็นเวลานานขึ้น ทำให้สามารถวิเคราะห์ได้ลึกขึ้น พื้นที่จัดเก็บที่ขยายออกยังช่วยให้ระบบจัดทำรายงานที่สมบูรณ์ยิ่งขึ้น พร้อมข้อมูลมากขึ้น รวมถึงผลลัพธ์ที่มองเห็นได้และคำแนะนำที่ดำเนินการได้ การวิเคราะห์ภัยคุกคามที่ลึกขึ้น WebUI ยังสามารถแสดงข้อมูลการตรวจจับภัยคุกคามที่สมบูรณ์ยิ่งขึ้น ซึ่งทำให้ผู้ดูแลระบบมองเห็นข้อมูลได้ดีขึ้น การมองเห็นที่เพิ่มขึ้นทำให้ผู้ดูแลระบบสามารถมุ่งเน้นไปที่สิ่งผิดปกติและเหตุการณ์หรือปริมาณการใช้งานเครือข่ายที่น่าสงสัยอื่นๆ ได้อย่างรวดเร็ว วิเคราะห์และตอบสนอง

Smart Policy Operation
(การดำเนินการตามนโยบายอัจฉริยะ)

A-Series ประกอบด้วยการจัดการและการดำเนินการอัจฉริยะ ตลอดจน Policy ทั้งหมด ตั้งแต่การปรับใช้ไปจนถึงการจัดการ การเพิ่มประสิทธิภาพและการดำเนินการ ระบบมีคุณลักษณะ การปรับใช้ตามนโยบายผู้ใช้โดยอัตโนมัติโดยใช้การอนุญาตแบบไดนามิก RADIUS การจัดการนโยบายมีประสิทธิภาพมากขึ้นมากผ่านการจัดกลุ่มนโยบายตามความต้องการทางธุรกิจ นอกจากนี้ยังสามารถรวมนโยบายเพื่อให้ชุดนโยบายทำหน้าที่เป็นนโยบายเดียวได้ ผู้ช่วยด้านนโยบายที่สร้างสรรค์ จะวิเคราะห์รูปแบบของปริมาณการใช้งานและแนะนำนโยบายที่ปรับแต่งแล้ว เพื่อการจัดการนโยบายที่รวดเร็ว ง่ายขึ้น และแม่นยำยิ่งขึ้น การดำเนินการตามนโยบายมีประสิทธิภาพและแม่นยำมากขึ้นผ่านการตรวจสอบความซ้ำซ้อนของนโยบาย ซึ่งระบุนโยบายที่ซ้ำซ้อน สำหรับการปิดใช้งานหรือการลบ และการวิเคราะห์จำนวนครั้งที่เข้าถึงนโยบาย ซึ่งช่วยปรับแต่งและปรับเปลี่ยนนโยบายเพิ่มเติม

หมายเหตุ:

1. คุณสมบัติป้องกันสแปมไม่สามารถใช้งานได้กับ SG-6000-A200-IN และ SG-6000-A200W-IN
2. ข้อมูลทรูพุตไฟร์วอลล์จะได้รับภายใต้การรับส่งข้อมูล UDP ที่มีขนาดแพ็กเก็ต 1,518 ไบต์ ทรูพุตไฟร์วอลล์สำหรับ A3700-IN/A3800-IN สามารถเพิ่มเป็น 30/40 Gbps ได้โดยใช้โมดูลขยาย IOC-A-4SFP+-IN เพิ่มเติม สามารถเพิ่มทรูพุตไฟร์วอลล์สำหรับ A5100-IN/A5155-IN/A5200-IN/A5255-IN/A5500-IN/A5555-IN/A5600-IN/A5800-IN/A7600-IN เป็น 50/50/65/65/80/80/85/95/320 Gbps ได้โดยใช้โมดูลขยาย IOC-A-2QSFP+-IN
3. ข้อมูลทรูพุต NGFW จะได้รับภายใต้ทราฟฟิก HTTP 64 Kbytes พร้อมเปิดใช้งานการควบคุมแอปพลิเคชันและ IPS
4. ข้อมูลทรูพุตการป้องกันภัยคุกคามจะได้รับภายใต้ทราฟฟิก HTTP 64 Kbytes พร้อมเปิดใช้งานการควบคุมแอปพลิเคชัน IPS AV และการกรอง URL
5. ได้รับเซสชันพร้อมกันสูงสุดภายใต้ทราฟฟิก HTTP
6. ได้รับเซสชันใหม่ภายใต้ทราฟฟิก HTTP (7) ข้อมูลอัตราการส่งผ่าน IPS จะได้รับภายใต้การตรวจจับการรับส่งข้อมูล HTTP แบบสองทิศทางโดยที่กฎ IPS ทั้งหมดเปิดใช้งานอยู่
8. ข้อมูลอัตราการส่งผ่าน AV จะได้รับภายใต้การรับส่งข้อมูล HTTP พร้อมแนบไฟล์
9. ข้อมูลอัตราการส่งผ่าน IPsec จะได้รับภายใต้การกำหนดค่า Preshare Key AES256+SHA-1 และขนาดแพ็กเก็ต 1,400 ไบต์
10. ข้อมูลอัตราการส่งผ่านพร็อกซี SSL จะได้รับโดยใช้ AES128-GCM-SHA256 โดยที่กฎ IPS ทั้งหมดเปิดใช้งานอยู่
11. พอร์ต SFP+ รองรับ optical module SFP+ 10Gbps,optical module SFP 1000Mbps และ copper module SFP 1000Mbps พอร์ต QSFP+ รองรับโมดูล 40GE 1×40Gbps และโมดูล 4×10GE 4×10Gbps พารามิเตอร์ทั้งหมดของ A6800-IN และ A7600-IN ขึ้นอยู่กับ StoneOS5.5R8 เว้นแต่จะระบุไว้เป็นอย่างอื่น ประสิทธิภาพ ความจุ และฟังก์ชันการทำงานทั้งหมดจะขึ้นอยู่กับ StoneOS5.5R9 ผลลัพธ์อาจแตกต่างกันไปขึ้นอยู่กับเวอร์ชันและการปรับใช้ StoneOS