Hillstone S-Series

Network Intrusion Prevention System (NIPS)

เนื่องจากภัยคุกคามมีการพัฒนาอย่างต่อเนื่อง เทคโนโลยีการป้องกันเครือข่ายจึงเพิ่มขึ้นอย่างรวดเร็ว ในบรรดาเทคโนโลยีต่างๆ เหล่านี้ ระบบป้องกันการบุกรุก (IPS) ยังคงเป็นหนึ่งในโซลูชันที่มีการใช้งานแพร่หลายที่สุด ไม่ว่าจะใช้แพลตฟอร์มหรือรูปแบบใดก็ตาม อุปกรณ์ IPS (NIPS) ที่ใช้เครือข่าย Hillstone ทำงานแบบอินไลน์และด้วยความเร็วสาย โดยทำการตรวจสอบแพ็กเก็ตอย่างละเอียดและรวบรวมการตรวจสอบการรับส่งข้อมูลในเครือข่ายทั้งหมด อุปกรณ์นี้ยังใช้กฎเกณฑ์ตามวิธีการต่างๆ มากมาย รวมถึงการวิเคราะห์ความผิดปกติของโปรโตคอลและการวิเคราะห์ลายเซ็นเพื่อบล็อกภัยคุกคาม อุปกรณ์ NIPS ของ Hillstone สามารถนำไปใช้ในเครือข่ายเพื่อตรวจสอบการรับส่งข้อมูลที่โซลูชันรอบนอกตรวจไม่พบ และเป็นส่วนสำคัญของระบบรักษาความปลอดภัยเครือข่าย เนื่องจากมีประสิทธิภาพสูง ไม่มีการประนีประนอม ความสามารถในการป้องกันที่ดีที่สุด และสถานการณ์การใช้งานที่หลากหลายและยืดหยุ่น

จุดเด่นของผลิตภัณฑ์

Unparalleled Threat Protection without Performance Compromise (การป้องกันภัยคุกคามที่ไม่มีใครเทียบได้โดยไม่กระทบต่อประสิทธิภาพ)

Hillstone NIPS มีกลไกตรวจสอบประสิทธิภาพสูงที่ครอบคลุมที่สุด เมื่อรวมกับ signature ที่ดีที่สุดด้านเทคโนโลยีชั้นนำ ทำให้ลูกค้าได้รับอัตราการตรวจจับภัยคุกคามสูงสุด ด้วยต้นทุนรวมในการเป็นเจ้าของ (TCO) ที่ต่ำที่สุด กลไก Hillstone IPS มีอัตราการบล็อกการโจมตีแบบคงที่ 99.6% และอัตราการบล็อกการโจมตี 98.325%(reported byNSSLabs)Hillstone NIPS ให้ throughput สูง ความหน่วงต่ำ และความพร้อมใช้งานสูงสุดเพื่อรักษาการดำเนินการด้านความปลอดภัยที่มีประสิทธิภาพโดยไม่กระทบต่อประสิทธิภาพของเครือข่าย NIPS การวิเคราะห์โปรโตคอล ของภัยคุกคาม และคุณลักษณะอื่นๆ ที่มอบการป้องกันภัยคุกคามตั้งแต่ Layer 2 ถึง Layer 7 รวมถึงการโจมตี ARP การโจมตี Dos/DDoS โปรโตคอลที่ผิดปกติ URL ที่เป็นอันตราย มัลแวร์ และการโจมตีเว็บ

Granular Reporting with User Targeted Viewpoints
(การรายงานแบบละเอียดพร้อมมุมมองที่กำหนดเป้าหมายโดยผู้ใช้)

Hillstone NIPS ให้การมองเห็นที่ครอบคลุมโดยอิงตาม protocol, application, user และcontent สามารถระบุแอปพลิเคชั่นได้มากกว่า 4,000 รายการ รวมถึงแอปพลิเคชันมือถือและคลาวด์หลายร้อยรายการ ด้วยการนำแหล่งข้อมูลหลายแหล่งมารวมกัน ระบบจึงสามารถระบุ ข้อมูลเชิงบริบทเพื่อตัดสินใจบล็อกได้อย่างเหมาะสม ด้วยฟังก์ชันการรายงานแบบละเอียด จึงให้การมองเห็นในมุมมองต่างๆ

- โดยเฉพาะอิงตามว่าคุณเป็นผู้ดูแลระบบธุรกิจ ผู้ดูแลระบบความปลอดภัย หรือ CIO หรือผู้บริหาร
- เนื้อหาภัยคุกคามที่จัดระเบียบ ไม่ว่าจะเป็นมุมมองด้านความปลอดภัย ความเสี่ยงของระบบ ภัยคุกคามเครือข่าย หรือปริมาณการรับส่งข้อมูล เพื่อช่วยให้คุณเข้าใจความเสี่ยงได้อย่างชัดเจนและตัดสินใจได้ถูกต้อง

Ease of Deployment and Centralized Management
(ความสะดวกในการใช้งานและการจัดการแบบรวมศูนย์)

การใช้งานและการจัดการ Hillstone NIPS นั้นง่ายด้วยค่าใช้จ่ายด้านการจัดการที่น้อยที่สุด สามารถใช้งานในโหมดต่อไปนี้เพื่อตอบสนองความต้องการด้านความปลอดภัยและรับรองการเชื่อมต่อเครือข่ายที่เหมาะสมที่สุด

- Active protection (โหมดป้องกันการบุกรุก) การตรวจสอบแบบ real time และการบล็อก
- Passive detection (โหมดการตรวจจับการบุกรุก) การตรวจสอบแบบ real time และการแจ้งเตือน

Hillstone NIPS สามารถจัดการได้โดย Hillstone Security Management Platform (HSM) ผู้ดูแลระบบสามารถลงทะเบียน ตรวจสอบ และอัปเกรดอุปกรณ์ NIPS ที่ติดตั้งในสาขาหรือสถานที่ต่างๆ ได้จากส่วนกลางด้วยนโยบายการจัดการแบบรวมศูนย์ ทั่วทั้งเครือข่ายเพื่อประสิทธิภาพสูงสุด

หมายเหตุ:

1.ข้อมูลอัตรารับส่งข้อมูล IPS จะได้รับภายใต้การรับส่งข้อมูล HTTP โดยที่ IPSrules ทั้งหมดเปิดใช้งานอยู่

2. จะได้รับการเชื่อมต่อพร้อมกันสูงสุดภายใต้การรับส่งข้อมูล TCP และสามารถอัปเกรดได้ด้วยสิทธิ์ใช้งานเพิ่มเติมที่ปรับปรุงแล้ว (AEL)

3. จะได้รับการเชื่อมต่อใหม่ต่อวินาทีภายใต้การรับส่งข้อมูล TCP โดยที่ IPS rules ทั้งหมดเปิดใช้งานอยู่เว้นแต่จะระบุไว้เป็นอย่างอื่น ประสิทธิภาพ ความจุ และฟังก์ชันการทำงานทั้งหมดจะขึ้นอยู่กับ StoneOS5.5R8 ผลลัพธ์อาจแตกต่างกันไปขึ้นอยู่กับเวอร์ชันและการปรับใช้ StoneOS