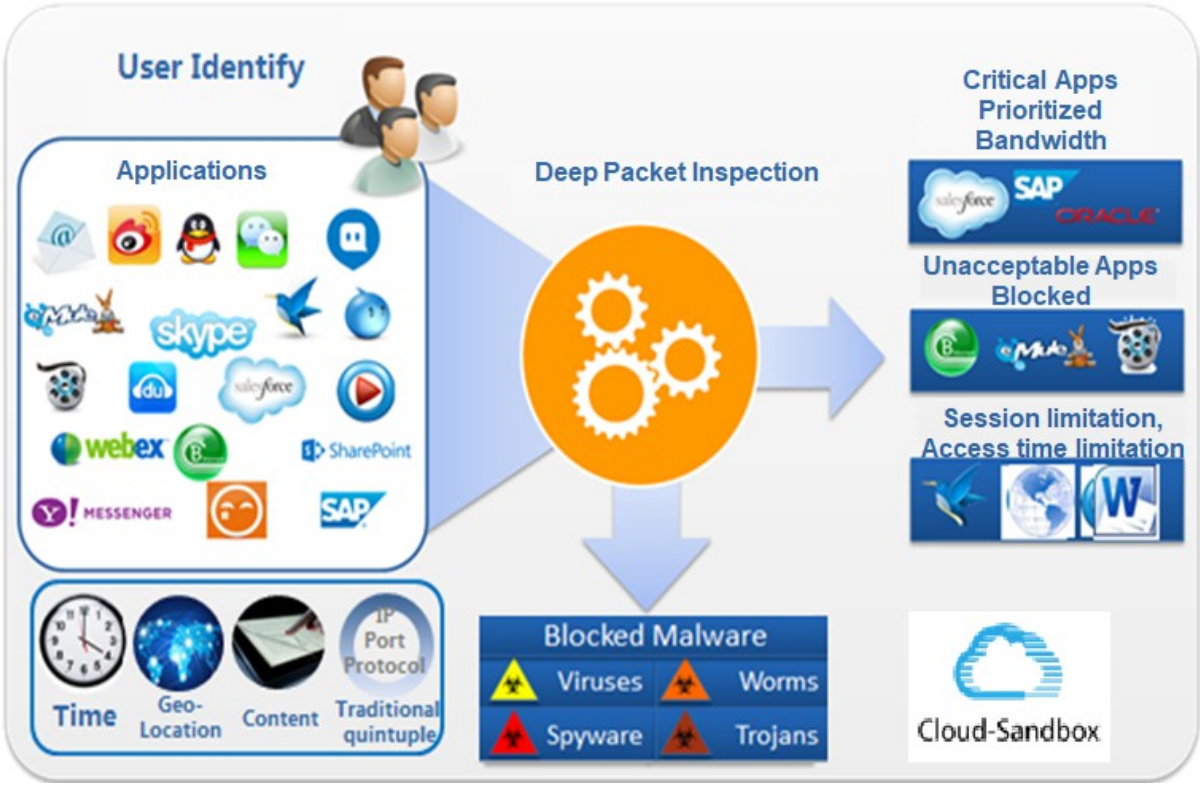
Hillstone ปราการที่แข็งแกร่งด้วยศักยภาพในการจับพฤติกรรมของเหล่าวายร้ายอย่างอัจฉริยะ

Hillstone เป็น Next-generation Firewall (NGFW) นั่นคือ เป็นสถาปัตยกรรมใหม่ที่ถูกออกแบบมาให้สามารถคัดกรองทราฟฟิคและควบคุมการใช้งานได้ถึงระดับแอพพลิเคชัน (Layer 7) แตกต่างจากไฟร์วอลล์รุ่นเก่าที่คัดกรองได้แค่เพียงหมายเลข IP และหมายเลขพอร์ท (L3/L4)

ความจำเป็นที่เราต้องมี Hillstone NGFW เพราะปัจจุบันนี้มีแอพพลิเคชันหลายประเภท แต่ละประเภทไม่ขึ้นกับหมายเลขพอร์ท หรืออาจใช้พอร์ทร่วมกันกับแอพพลิเคชันอื่น เช่น พอร์ท 80 HTTP ที่ยินยอมให้สามารถเข้าถึงเว็บไซต์ รับส่งอีเมลล์ ดูวิดีโอ หรือคุยโทรศัพท์หากันได้ การปิดพอร์ท 80 หมายถึงการปิดบริการเหล่านั้นทั้งหมดโดยไม่สามารถเลือกเป็นรายแอพพลิเคชันได้ NGFW จึงเข้ามามีบทบาทให้การควบคุมแต่ละรายแอพพลิเคชันโดยไม่จำกัดว่าแอพพลิเคชันเหล่านั้นทำงานอยู่บนพอร์ทใด

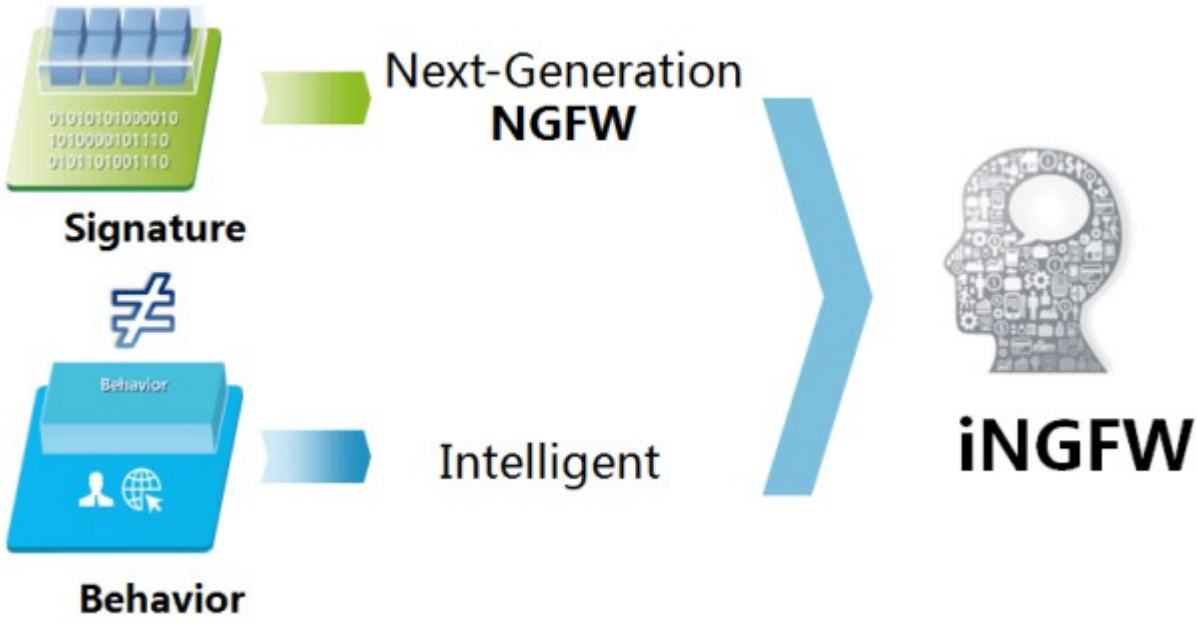
นอกจากการควบคุมการใช้งานระดับแอพพลิเคชันแล้ว NGFW ยังอาศัยขุมพลังฮาร์ดแวร์ในปัจจุบันที่พัฒนาก้าวไปไกลกว่าในอดีตในการให้บริการฟีเจอร์อื่นๆ เพื่อให้ NGFW กลายเป็นปราการด่านแรกและด่านสำคัญในการคัดกรองและควบคุมทราฟฟิคทั้งจากภายนอกวิ่งเข้าสู่ระบบเครือข่าย และจากการใช้งานภายในสู่ระบบอินเตอร์เน็ตภายนอก ฟีเจอร์สำคัญที่พบใน NGFW ในปัจจุบัน ได้แก่ ระบบป้องกันภัยคุกคาม (IPS), ระบบแอนตี้ไวรัส, ระบบพิสูจน์ตัวตนและติดตามผู้ใช้, ระบบคัดกรองการเข้าถึงเว็บไซต์, ระบบ VPN, ระบบ Cloud-Sandbox และอื่นๆ



Hillstone NGFW ที่มาพร้อมกับระบบการเรียนรู้อัจฉริยะ

Hillstone เป็น NGFW ที่ให้บริการทั่วโลก โดยได้รับการันตีจาก Gartner, Inc. ให้อยู่ในตำแหน่ง Niche Player หมายความว่า ฟีเจอร์การใช้งานของ Hillstone NGFW สามารถตอบโจทย์การใช้งานในปัจจุบันได้ค่อนข้างตรงตามความต้องการของผู้ใช้ในปัจจุบัน และมีแผนพัฒนาที่สอดคล้องกับแนวโน้มความต้องการของตลาดในอนาคต

รวมถึง Hillstone NGFW ยังได้นำเสนอระบบไฟร์วอลล์อัจฉริยะ (Intelligent Firewall; iNGFW) ซึ่งช่วยวิเคราะห์และตรวจจับมัลแวร์รูปแบบต่างๆ โดยอาศัยอัลกอริธึมการเรียนรู้พฤติกรรมการใช้งานและการวิเคราะห์ข้อมูลระดับ Big Data ส่งผลให้ Hillstone iNGFW สามารถระบุมัลแวร์ได้อย่างรวดเร็ว รวมทั้งสามารถตรวจจับภัยคุกคามแบบ Zero-day ได้ก่อนที่จะส่งผลกระทบต่อระบบเครือข่าย



Hillstone NGFW มี 4 รุ่น ที่เหมาะกับจำนวนผู้ใช้ และความต้องการของธุรกิจ เริ่มจากบริษัททั่วไป ถึง บริษัทที่มีความต้องการพิเศษในการปกป้องสภาวะแวดล้อมแบบคลาวด์และ Virtualization

- **E-Series**: NGFW สำหรับบริษัททั่วไป จนไปถึงบริษัทขนาดใหญ่
- **T-Series**: iNGFW ที่ผสานศักยภาพการเรียนรู้อัจฉริยะและ NGFW ไว้ด้วยกัน
- **X-Series**: NGFW ที่ถูกออกแบบมาสำหรับห้อง Data Center โดยเฉพาะ
- **CloudHive/CloudEdge**: NGFW สำหรับสภาวะแวดล้อมแบบคลาวด์และ Virtualization

Hillstone E-Series: NGFW ยอดนิยมสำหรับบริษัททั่วไป

E-Series เป็น NGFW ซีรี่ย์ยอดนิยมสำหรับทุกบริษัท รองรับการใช้งานตั้งแต่ออฟฟิสขนาดเล็ก จนไปถึงหน่วยงานหรือองค์กรขนาดใหญ่ที่ต้องการ NGFW ประสิทธิภาพสูง โดยซีรี่ย์นี้รองรับ Firewall Throughput เริ่มต้นตั้งแต่ 1 Gbps (รุ่น SG-6000-E1600) ไปจนถึง 40 Gbps และถ้าเปิดการใช้งานทุกฟีเจอร์ ไม่ว่าจะเป็นระบบป้องกันภัยคุกคาม ระบบแอนตี้ไวรัส และระบบ VPN จะรองรับ Throughput สูงสุดถึง 10 Gbps (รุ่น SG-6000-E5960)

คุณสมบัติเด่นที่สำคัญของ E-Series

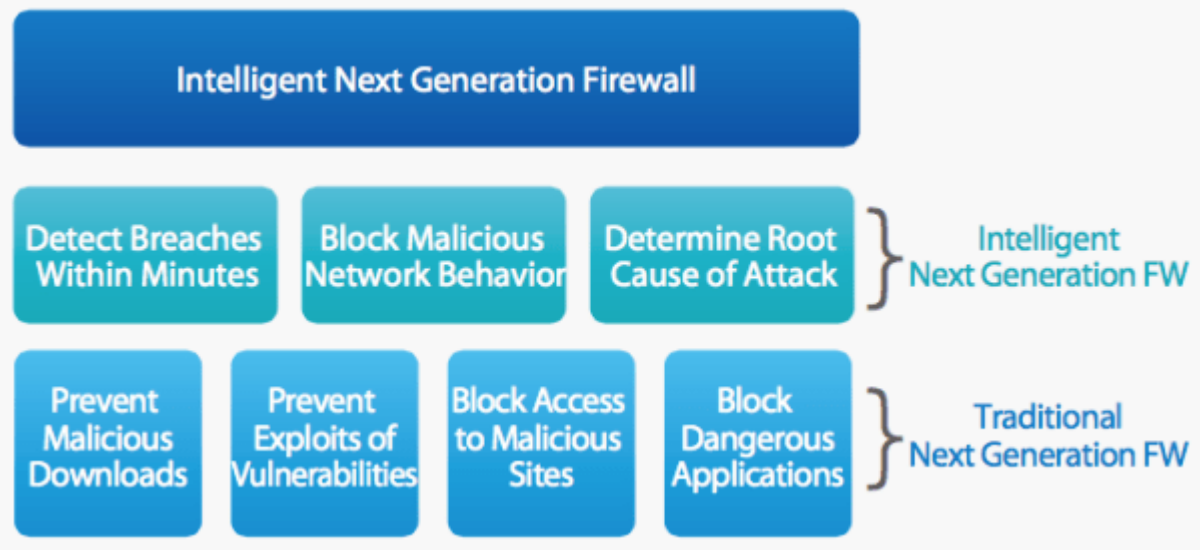
- **มองเห็นและควบคุมการใช้งานได้ถึงระดับแอพพลิเคชัน**: สามารถจำแนกแอพพลิเคชันได้โดยไม่สนใจหมายเลขพอร์ทและโปรโตคอล รวมทั้งสามารถกำหนดกฎไฟร์วอลล์เพื่อควบคุมการใช้งานแอพพลิเคชันได้ตามชื่อผู้ใช้ ซึ่งยืดหยุ่นกว่าการใช้หมายเลข IP เหมือนไฟร์วอลล์สมัยเก่า รวมทั้งสามารถจำกัดและการันตีแบนวิธด์ให้การใช้งานแต่ละแอพพลิเคชันได้อย่างอิสระ โดยปัจจุบันนี้ Hillstone รู้จักแอพพลิเคชันมากกว่า 3,000 แอพพลิเคชัน
- **ระบบป้องกันภัยคุกคามเชิงรุก**: ตรวจจับและป้องกันการบุกรุกโจมตีได้แบบเรียลไทม์ ไม่ว่าจะเป็น ไวรัส, สปายแวร์, เวิร์ม, บ็อทเน็ต, โทรจัน, DoS/DDoS, Buffer Overflow และ SQL Injection เป็นต้น โดยมีฐานข้อมูลรูปแบบการโจมตีมากกว่า 7,000 รูปแบบ และฐานข้อมูลมัลแวร์มากกว่า 1.3 ล้านรูปแบบที่พร้อมอัพเดทตลอดเวลา รวมทั้งสามารถกรองการเข้าถึง URL ของพนักงานในองค์กรตามชื่อหรือประเภทของ URL ได้
- **บริการระบบเครือข่าย**: รองรับการทำ Switching, Routing (Static, OSPF, BGP, RIPv2), การทำ DHCP, NTP, DNS Server และรองรับการใช้งาน IPv6
- **บริการไฟร์วอลล์พื้นฐาน**: รองรับการทำ NAT, QoS Traffic Shaping, Load Balancing และ Virtual Firewall ได้สูงสุดถึง 250 vSYS
- **รองรับการทำ VPN**: ทั้งแบบ Site-to-site และ Client-to-site สำหรับอุปกรณ์ที่ใช้งานระบบปฏิบัติการ iOS, Android และ Windows
- **การพิสูจน์ตัวตนและอุปกรณ์**: สามารถพิสูจน์ตัวตนผู้ใช้งานร่วมกับระบบ LDAP, RADIUS, AD หรือฐานข้อมูลบนตัวอุปกรณ์ได้
- **อื่น ๆ**: รองรับการทำ HA ทั้งแบบ Active/Active และ Active/Passive, บริหารจัดการผ่านหน้าเว็บหรือ CLI และสามารถจัดเก็บ Log เพื่อทำรายงานในรูปแบบกราฟิคสวยงามได้

Hillstone T-Series: iNGFW ล้ำหน้าด้วยระบบการเรียนรู้อัจฉริยะ

T-Series เป็น NGFW ที่พัฒนาต่อยอดจาก E-Series โดยเพิ่มระบบการเรียนรู้อัจฉริยะเพื่อตอบโจทย์หน่วยงานหรือองค์กรที่ต้องการความปลอดภัยขั้นสูง ด้วยการเรียนรู้พฤติกรรมการใช้งานของผู้ใช้ และพฤติกรรมของมัลแวร์ ทำให้ Hillstone T-Series สามารถดักจับมัลแวร์รูปแบบต่างๆ รวมไปถึงมัลแวร์แบบ Zero-day ได้อย่างรวดเร็วและแม่นยำ นอกจากนี้ ยังมีระบบวิเคราะห์หลักฐานเชิงดิจิตอล (Forensic Analysis) ที่ช่วยให้ผู้ดูแลระบบสามารถตรวจสอบต้นตอของปัญหาที่เกิดขึ้นได้ง่ายอีกด้วย

ระบบการเรียนรู้อัจฉริยะประกอบด้วยเทคโนโลยีสำคัญ 3 ประการ ได้แก่

1. **การทำคลัสเตอร์เชิงสถิติ**: อัลกอริธึมเฉพาะของ Hillstone ที่ช่วยให้สามารถตรวจจับมัลแวร์ที่รู้จัก (Known Malware) ได้อย่างรวดเร็วด้วยการวิเคราะห์พฤติกรรมของมัลแวร์ รวมทั้งแจ้งเตือนและแสดงรายละเอียดเกี่ยวกับมัลแวร์เพื่อให้ผู้ดูแลระบบสามารถตรวจสอบและมั่นใจได้ว่าเป็นภัยคุกคามจริง ไม่ใช่ False Positive
2. **การวิเคราะห์เชิงพฤติกรรม**: มีการทำ Machine Learning พฤติกรรมของผู้ใช้ รวมทั้งใช้ Big Data Analytics และโมเดลทางคณิตศาสตร์เพื่อตรวจจับพฤติกรรมที่ผิดปกติที่เกิดขึ้นในระบบเครือข่าย ส่งผลให้สามารถตรวจจับมัลแวร์และภัยคุกคามรูปแบบใหม่ๆและประเภท Zero-day ได้อย่างมีประสิทธิภาพ
3. **การวิเคราะห์หลักฐานเชิงดิจิตอล**: ให้ข้อมูลรายละเอียดเชิงลึกของเหตุการณ์ผิดปกติที่เกิดขึ้น ซึ่งช่วยให้ผู้ดูแลระบบสามารถหาสาเหตุของปัญหาและต้นตอของการโจมตีได้โดยง่าย รวมทั้งให้ข้อมูล Log และจัดทำรายงานแนวโน้มเชิงสถิติสำหรับใช้วิเคราะห์ความเสี่ยงในอนาคตได้



Hillstone T-Series รองรับคุณสมบัติ NGFW เช่นเดียวกับ E-Series และสามารถเลือกอุปกรณ์ฮาร์ดแวร์ได้ถึง 5 รุ่น ตอบโจทย์การใช้งานสำหรับบริษัทขนาดกลางไปจนถึงองค์กรขนาดใหญ่ โดยรุ่นใหญ่สุดอย่าง SG-6000-T5860 รองรับ Firewall Throughput สูงสุดที่ 40 Gbps และเมื่อเปิดการใช้งานทุกฟังก์ชันจะมี Throughput สูงสุดที่ 10 Gbps

Specification	SG-6000-T1860	SG-6000-T2860	SG-6000-T3860	SG-6000-T5060	SG-6000-T5860
					
FW Throughput	8Gbps	10Gbps	20Gbps	25Gbps	40Gbps
IPS Throughput[1]	3Gbps	4Gbps	8Gbps	12Gbps	18Gbps
AV Throughput[2]	1.6Gbps	2Gbps	6Gbps	7Gbps	10Gbps
IPSec Thoughtput[3]	3Gbps	3.8Gbps	12Gbps	15Gbps	28Gbps
New Sessions/ sec(HTTP)	80K	100K	250K	300K	450K
Maximum Concurrent Sessions	1.5 million sessions	3 million sessions	4 million sessions	5 million sessions	6 million sessions
Integrated I/O	6 × GE, 4 × SFP	6 × GE(1 pair bypass port), 4 × SFP, 2 × SFP+	2 × GE, 4 × SFP	2 × GE, 4 × SFP	2 × GE, 4 × SFP
Maximum I/O	26 × GE	26 × GE, 2 × 10GE	22 × GE, 4 × 10GE	38 × GE, 8 × 10GE	38 × GE, 8 × 10GE
Expansion Modules	2 × Generic Slot	2 × Generic Slot	2 × Generic Slot	4 × Generic Slot	4 × Generic Slot
Expansion Module Option	IOC-4GE-B-M, IOC-8GE-M, IOC-8SFP-M	IOC-4GE-B-M, IOC-8GE-M, IOC-8SFP-M	IOC-8GE-M, IOC-8SFP-M, IOC-4GE-B-M, IOC-2XFP-Lite-M	IOC-8GE-M, IOC-8SFP-M, IOC-4GE-B-M, IOC-4XFP, IOC-8SFP+, IOC-4SFP+, IOC-2XFP-Lite-M(only supported at Slot-3/4) ,	IOC-8GE-M, IOC-8SFP-M, IOC-4GE-B-M, IOC-4XFP, IOC-8SFP+, IOC-4SFP+, IOC-2XFP-Lite-M (only supported at Slot-3/4)
Management Ports	1 × Concole Port, 1 × HA, 1 × MGT, 1 × USB 2.0, 1 × AUX Port	1 × Concole Port, 1 × HA, 1 × MGT, 1 × USB 2.0, 1 × AUX Port	1 × Console Port, 1 × AUX Port, 1 × USB 2.0 Port, 2 × HA, 1 × MGT	1 × Console Port, 1 × AUX Port, 1 × USB 2.0 Port, 2 × HA, 1 × MGT	1 × Console Port, 1 × AUX Port, 1 × USB 2.0 Port, 2 × HA, 1 × MGT
Maximum Power Consumption	1 × 150w Redundancy 1 + 1	1 × 150w Redundancy 1 + 1	2 × 450W Redundancy 1 + 1	2 × 450W Redundancy 1 + 1	2 × 450W Redundancy 1 + 1
Storage	500G HDD	500G HDD	80G SSD, 500G HDD or 1T HDD	120G SSD, 500G HDD or 1T HDD	120G SSD, 500G HDD or 1T HDD

Hillstone X-Series: NGFW สมรรถะสูงระดับ Carrier-grade

Hillstone X7180 เป็น Data Center NGFW สมรรถนะสูงที่ถูกออกแบบมาเพื่อใช้กับระบบเครือข่ายระดับ ISP และองค์กรขนาดใหญ่โดยเฉพาะ มีสถาปัตยกรรมแบบ Elastic Security ซึ่งช่วยให้รองรับปริมาณ Througput และจำนวนเซสชันที่สูง รวมทั้งสามารถขยายการใช้งานในรูปของ Virtual Firewall ได้สูงสุดถึง 1,000 vSys นอกจากนี้ X7180 ยังรองรับการตรวจสอบทราฟฟิคแบบ Deep Packet Inpection (DPI) และการทำ QoS แบบ Next-generation อีกด้วย

คุณสมบัติเด่นที่สำคัญของ X7180

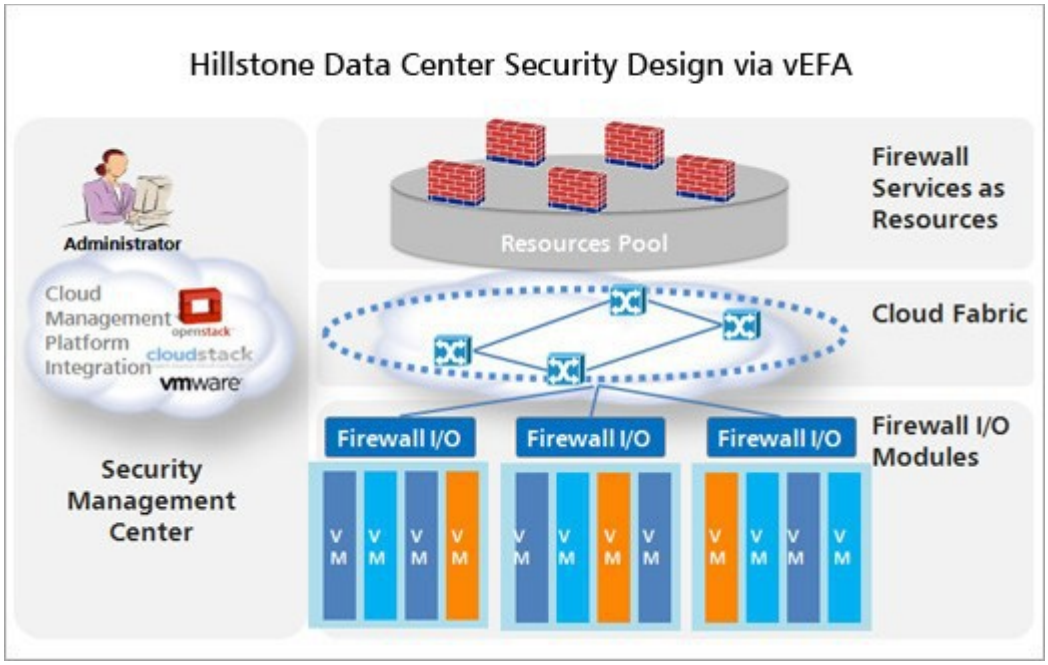
- **สถาปัตยกรรมแบบ** Elastic Security: มีการออกแบบจำนวนและประสิทธิภาพของพอร์ทอินเตอร์เฟสเพื่อรองรับปริมาณการเชื่อมต่อและภาระงานอันมหาศาลในห้อง Data Center โดยรองรับพอร์ทระดับ 10 Gbps สูงสุดถึง 68 พอร์ท หรือพอร์ทระดับ 1 Gbps สูงสุดถึง 144 พอร์ท นอกจากนี้ยังมีการออกแบบฮาร์ดแวร์ให้รองรับปริมาณ Throughput ได้สูงสุดถึง 360 Gbps และจำนวนเซสชันสูงถึง 120 ล้านเซสชัน เพื่อตอบโจทย์จำนวนผู้งานในองค์กรขนาดใหญ่
- **ความเสถียรระดับ** Carrier-grade: อุปกรณ์มีชิ้นส่วนสำรองแบบ Hot-swap ไม่ว่าจะเป็นแหล่งจ่ายไฟ, พัดลม, System Control Module (SCM), Security Service Module (SSM) และ I/O Module (IOM) รวมทั้งรองรับการทำ HA ทั้งแบบ Active/Passive และ Active/Active เพื่อการันตีว่าอุปกรณ์สามารถทำงานได้แบบ 24×7
- **QoS แบบ** Next-generation: สามารถควบคุมการใช้แบนวิธด์ได้ถึงระดับแอพพลิเคชัน หรือตามชื่อผู้ใช้งานได้ ไม่ว่าจะเป็นการจำกัดแบนวิธด์, การันตีแบนวิธด์, จัดลำดับความสำคัญของทราฟฟิค และ FlexQoS ที่ช่วยปรับแต่งแบนวิธด์ให้เหมาะสมกับการใช้งานโดยอัตโนมัติ

Hillstrone X7180 ครอบคลุมฟีเจอร์ NGFW เช่นเดียวกับ E-Series และมีคุณสมบัติด้านฮาร์ดแวร์ ดังนี้

Specification	SG-6000-X7180
FW Throughput (Maximum)	360 Gbps
Maximum Concurrent Sessions	120 million
New Sessions/s	2.4 million per second
IPS Throughput	90 Gbps
Management Ports	1 x Console Port, 1 x AUX Port, 2 x USB 2.0 Port
Fixed I/O Ports	4 x GE Combo slot (1 x MGT + 3 x HA)
Available Slots for Extensible Modules	10 x Generic Slot, 2 x System Control Module Slot, 1 x SD Card Slot
Modules	SCM-100, SSM-100, QSM-100, IOM-16SFP-100, IOM-4XFP-100, IOM-2MM-BE, IOM-2SM-BE, IOM-2Q8SFP+, IOM-8SFP+
Maximum Power Consumption	2+2 redundant power supply, Max.1300W
Power Supply	AC 100-240V 50/60Hz, DC -40 ~ -72V
Dimension (WxDxH)	5U 17.3×23.2×8.9 in (440×590×225 mm)
Weight	<116.6 lb (53 kg)
Temperature	32-104F (0-40℃)
Relative Humidity	10-95%

CloudHive/CloudEdge: NGFW สำหรับระบบคลาวด์และ Virtualization

Hillstone CloudHive/CloudEdge เป็น NGFW ที่ถูกออกแบบมาสำหรับสภาวะแวดล้อมแบบคลาวด์และ Virtualization โดยเฉพาะ โดยให้บริการครบทุกฟังก์ชันเช่นเดียวกับ E-Series ตั้งแต่ Layer 2 – 7 ไม่ว่าจะเป็นการควบคุมการใช้งานถึงระดับแอพพลิเคชัน การป้องกันภัยคุกคามและมัลแวร์ การพิสูจน์ตัวตนและควบคุมสิทธิ์ผู้ใช้งาน รวมไปถึงฟีเจอร์ด้านระบบเครือข่าย และอื่นๆ CloudHive เป็นโซลูชันสำหรับป้องกันแต่ละ Virtual Machine (VM) บนระบบคลาวด์ ในขณะที่ CloudEdge สามารถใช้งานในรูปของ Firewall as a Service บนสภาวะแวดล้อมแบบ Virtualization ผ่าน Cloud Management Platform (CMP) หรือติดตั้งในรูปของ Security Gateway สำหรับ Virtual Private Cloude (VPC) บนระบบคลาวด์สาธารณะได้



CloudEdge รองรับการติดตั้งบนเทคโนโลยี Hypervisor หลากหลายแบบ เช่น KVM, Xen, VMware ESXi และสามารถทำงานร่วมกับระบบ CMP เช่น Amazon AWS, Openstack และ VMware vCenter ได้ แต่สำหรับ CloudHive นั้นรองรับเฉพาะ VMware ESXi และ VMware vCenter ตามลำดับเท่านั้น

สนใจต้องการสาธิตการทำงาน ติดต่อ บริษัท ภัทร โปรเกรส จำกัด 0 2732 2090, marketing@bhatarapro.com