แนวทางปฏิบัติของ AWS เพื่อความยืดหยุ่นต่อ DDoS

มิถุนายน 2016

ประกาศ

เอกสารฉบับนี้ให้ไว้เพื่อเป็น ข้อมูลเท่านั้น เนื้อหาของเอกสารนำเสนอข้อมูลผลิตภัณฑ์และบริการ รวมถึงแนวทางปฏิบัติปัจจุบันของ AWS ณ วันที่มีการออกเอกสารฉบับนี้ และสามารถเปลี่ยนแปลงได้โดยไม่ต้องแจ้งให้ทราบ ลูกค้ามีหน้าที่รับผิดชอบต่อการประเมินข้อมูลในเอกสารฉบับนี้ รวมถึงการใช้ผลิตภัณฑ์หรือบริการใดๆ ของ AWS ด้วยตนเองได้อย่างอิสระ ทั้งนี้ผลิตภัณฑ์และบริการแต่ละอย่างให้บริการ “ตามที่เป็น” โดยไม่มีการรับประกันใดๆ ไม่ว่าโดยนัยหรือโดยชัดแจ้ง เอกสารฉบับนี้ไม่มีการรับประกัน การรับรอง การผูกพันตามสัญญา เงื่อนไขหรือการประกันใดๆ จาก AWS บริษัทในเครือ ผู้จัดหา หรือผู้ให้สิทธิ์การใช้งาน หน้าที่และความรับผิดของ AWS ต่อลูกค้าอยู่ภายใต้การควบคุมโดยข้อตกลงของ AWS และเอกสารฉบับนี้ไม่ถือเป็นส่วนหนึ่งของข้อตกลง และไม่ทำให้เกิดการเปลี่ยนแปลงใดๆ กับข้อตกลงระหว่าง AWS กับลูกค้า

สารบัญ

บทคัดย่อ

เอกสารฉบับนี้จัดทำขึ้นสำหรับลูกค้าที่ต้องการเพิ่มความยืดหยุ่นให้กับแอปพลิเคชันที่ใช้งานกับระบบ Amazon Web Services (AWS) ต่อการโจมตี Distributed Denial of Services (DDoS) เอกสารฉบับนี้นำเสนอภาพรวมเกี่ยวกับการโจมตีแบบ DDoS ความสามารถต่างๆ ที่ AWS มี เทคนิคการลดการโจมตี และสถาปัตยกรรมอ้างอิงสำหรับความยืดหยุ่นต่อการโจมตีแบบ DDoS ซึ่งสามารถใช้เป็นแนวทางช่วยปกป้องความพร้อมใช้งานของแอปพลิเคชันได้

ข้อมูลเบื้องต้น

เอกสารนี้จัดทำขึ้นสำหรับผู้มีอำนาจตัดสินใจด้าน IT และบุคลากรด้านความปลอดภัยซึ่งมีความคุ้นเคยกับแนวคิดพื้นฐานเกี่ยวกับระบบเครือข่าย ระบบความปลอดภัย และบริการ AWS แต่ละส่วนมีลิงก์ไปยังเอกสารของ AWS ซึ่งมีข้อมูลเพิ่มเติมเกี่ยวกับแนวทางปฏิบัติหรือความสามารถ คุณยังสามารถดูการประชุม re:Invent ของ AWS SEC307 – การสร้างสถาปัตยกรรมสำหรับความยืดหยุ่นต่อการโจมตีแบบ DDoS ด้วย AWS[1] และ SEC306 – การป้องกันการโจมตีแบบ DDoS[2] เพื่อรับข้อมูลเพิ่มเติม

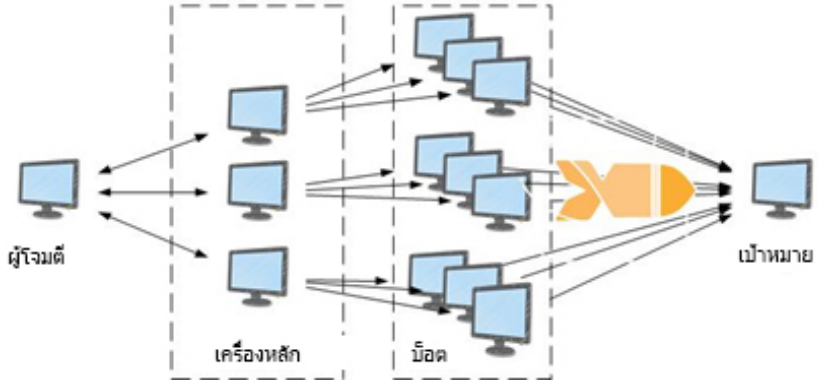
การโจมตีแบบ DDoS

การโจมตีแบบ Denial of Service (DoS) คือการโจมตีที่สามารถทำให้เว็บไซต์หรือแอปพลิเคชันไม่พร้อมใช้งานแก่ผู้ใช้ขั้นปลาย เพื่อบรรลุเป้าหมายดังกล่าว ผู้โจมตีจะใช้เทคนิคที่หลากหลายซึ่งใช้เครือข่ายหรือทรัพยากรอื่นๆ ไปมาก และรบกวนไม่ให้ผู้ใช้ขั้นปลายที่มีสิทธิ์อันชอบธรรมเข้าถึงข้อมูลได้ การโจมตี DoS ในรูปแบบที่เรียบง่ายที่สุดคือผู้โจมตีเพียงคนเดียวจะโจมตีจากแหล่งที่มาแหล่งเดียว ดังที่แสดงไว้ในรูปภาพ 1

รูปภาพ 1: ไดอะแกรมการโจมตีแบบ DoS

ในกรณีของการโจมตีแบบ Distributed Denial of Service (DDoS) ผู้โจมตีจะใช้แหล่งที่มาหลายแหล่ง ซึ่งอาจถูกเจาะระบบหรือควบคุมโดยกลุ่มผู้สมรู้ร่วมคิด เพื่อทำการ

โจมตีเป้าหมาย รูปภาพ 2 แสดงให้เห็นว่าสำหรับการโจมตี DDoS ผู้สมรู้ร่วมคิดแต่ละราย หรือโฮสต์ที่ถูกเจาะระบบ ต่างร่วมกันโจมตี ทำให้เกิดการฟลัดแพ็คเก็ตหรือคำขอไปยังเป้าหมายที่ต้องการจนล้น



รูปภาพ 2: ไดอะแกรมการโจมตีแบบ DDoS

การโจมตีแบบ DDoS พบบ่อยที่สุดในเลเยอร์ 3, 4, 6 และ 7 ของแบบจำลอง Open Systems Interconnection (OSI) ซึ่งอธิบายไว้ในตาราง 1 การโจมตีเลเยอร์ 3 และ 4 นั้นตรงกับเลเยอร์เครือข่ายและการขนส่งของแบบจำลอง OSI เอกสารฉบับนี้เรียกการโจมตีรูปแบบดังกล่าวว่า การโจมตีเลเยอร์โครงสร้างพื้นฐาน การโจมตีเลเยอร์ 6 และ 7 นั้นตรงกับเลเยอร์การนำเสนอและแอปพลิเคชันของแบบจำลอง OSI เอกสารฉบับนี้เรียกการโจมตีรูปแบบดังกล่าวว่า การโจมตีเลเยอร์แอปพลิเคชัน

#	เลเยอร์	หน่วย	คำอธิบาย	ตัวอย่างเส้นทาง
7	แอปพลิเคชัน	ข้อมูล	กระบวนการของเครือข่ายต่อแอปพลิเคชัน	การฟลัด HTTP, การฟลัดการสืบค้น DNS
6	การนำเสนอ	ข้อมูล	การรับรองและเข้ารหัสข้อมูล	การกระทำผิดบน SSL
5	*เซสชัน*	*ข้อมูล*	*การสื่อสารระหว่างโฮสต์*	*ไม่พร้อมใช้งาน*
4	การขนส่ง	เซกเมนต์	การเชื่อมต่อแบบเบ็ดเสร็จและความเชื่อถือได้	การฟลัด SYN
3	เครือข่าย	แพ็คเก็ต	การกำหนดพาธและการกำหนดลอจิคัลแอดเดรส	การโจมตีรีเฟลกชัน UDP
2	*การเชื่อมโยงข้อมูล*	*เฟรม*	*การกำหนดฟิสิคัลแอดเดรส*	*ไม่พร้อมใช้งาน*
1	*ฟิสิคัล*	*บิต*	*สื่อ สัญญาณ และการส่งแบบไบนารี*	*ไม่พร้อมใช้งาน*

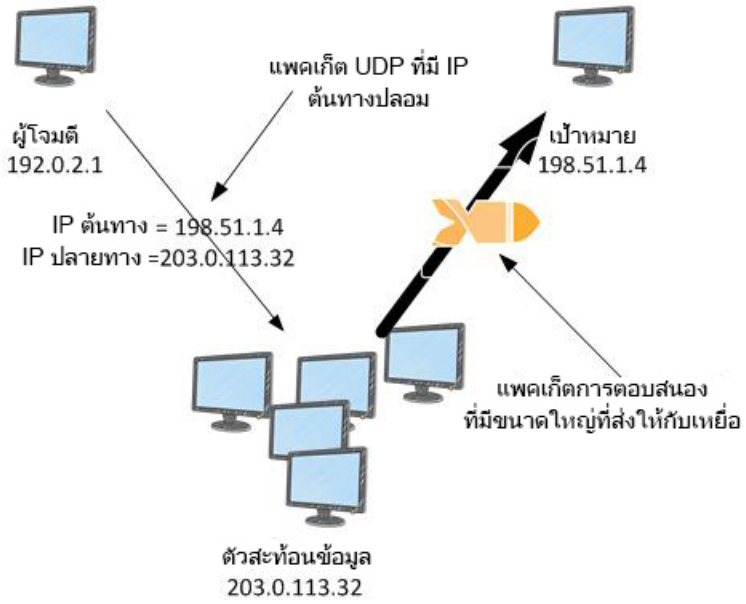
ตาราง 1: แบบจำลอง Open Systems Interconnection (OSI)

ความแตกต่างข้อนี้มีความสำคัญ เนื่องจากการโจมตีประเภทที่เกิดกับเลเยอร์เหล่านี้มีความแตกต่างกัน จึงใช้เทคนิคที่แตกต่างกันในการสร้างความยืดหยุ่น

การโจมตีเลเยอร์โครงสร้างพื้นฐาน

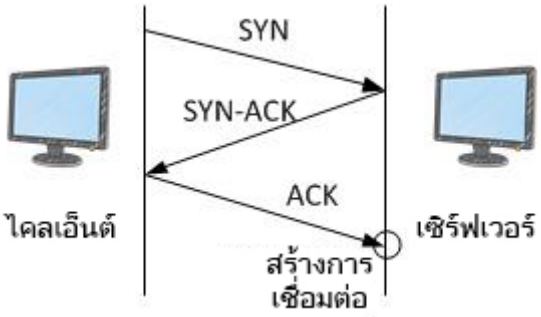
การโจมตีแบบ DDoS ที่พบบ่อยที่สุด อันได้แก่ การโจมตีรีเฟลกชันโปรโตคอลเดทาแกรมผู้ใช้ (UDP) และการฟลัดแบบซิงโครไนซ์ (SYN) เป็นการโจมตีเลเยอร์โครงสร้างพื้นฐาน ผู้โจมตีสามารถใช้วิธีใดวิธีหนึ่งจากวิธีเหล่านี้เพื่อสร้างการรับส่งข้อมูลปริมาณมาก ซึ่งเกินความสามารถของเครือข่ายหรือระบบ อย่างเช่น เซิร์ฟเวอร์ ไฟร์วอลล์ IPS หรือโหลดบาลานเซอร์ได้ การโจมตีเหล่านี้มีลายเซ็นชัดเจนซึ่งทำให้ตรวจพบได้ง่ายขึ้น การลดการโจมตีเหล่านี้ให้มีประสิทธิภาพต้องใช้เครือข่ายหรือทรัพยากรระบบที่มากกว่าปริมาณที่ผู้โจมตีสร้างขึ้น

UDP เป็นโปรโตคอลที่ไม่เก็บสถานะ โปรโตคอลดังกล่าวทำให้ผู้โจมตีสามารถปลอมแปลงแหล่งที่มาของคำขอที่ส่งไปยังเซิร์ฟเวอร์ที่ดึงการตอบกลับในปริมาณมากกว่า ปัจจัยของการทำแอมพลิฟิเคชัน ซึ่งได้แก่ อัตราส่วนของขนาดคำขอต่อขนาดของการตอบกลับนั้นอาจแตกต่างกันไปบนโปรโตคอลที่ใช้ เช่น ระบบชื่อโดเมน (DNS) โปรโตคอลเวลาเครือข่าย (NTP) หรือโปรโตคอลการค้นพบบริการอย่างง่าย (SSDP) ตัวอย่างเช่น ปัจจัยของการทำแอมพลิฟิเคชันสำหรับ DNS อาจอยู่ในช่วง 28 ถึง 54 หมายความว่าผู้โจมตีสามารถส่งคำขอส่วนข้อมูลขนาด 64 ไบต์ไปยังเซิร์ฟเวอร์ DNS และสร้างการรับส่งข้อมูลที่ไม่พึงประสงค์มากกว่า 3400 ไบต์ได้ แนวคิดนี้แสดงไว้ในรูปภาพ 3



รูปภาพ 3: การโจมตีรีเฟลกชัน UDP

การฟลัด SYN อาจดำเนินการหลายสิบ Gbps แต่จุดประสงค์ของการโจมตีประเภทนี้คือเพื่อใช้ทรัพยากรที่มีอยู่ในระบบให้หมดไปโดยปล่อยให้การเชื่อมต่ออยู่ในสถานะกึ่งเปิด ดังที่แสดงไว้ในรูปภาพ 4 เมื่อผู้ใช้ปลายทางเชื่อมต่อกับบริการ TCP เช่น เว็บเซิร์ฟเวอร์ ไคลเอ็นต์จะส่งแพคเก็ต SYN เซิร์ฟเวอร์จะคืน SYN-ACK และไคลเอ็นต์จะคืน ACK ซึ่งเป็นการเสร็จสิ้นกระบวนการแฮนด์เชค 3 ทาง



รูปภาพ 4: การแฮนด์เชค SYN 3 ทาง

ในการฟลัด SYN จะไม่มีทางคืน ACK และระบบจะปล่อยให้เซิร์ฟเวอร์รอการตอบกลับ ผลคือสามารถป้องกันผู้ใช้คนใหม่ไม่ให้เชื่อมต่อเซิร์ฟเวอร์

การโจมตีเลเยอร์แอปพลิเคชัน

ที่เกิดขึ้นบ่อยครั้งน้อยกว่าคือ ผู้โจมตีอาจพุ่งเป้าไปที่แอปพลิเคชันโดยใช้การโจมตีเลเยอร์ 7 หรือการโจมตีเลเยอร์แอปพลิเคชัน การโจมตีเหล่านี้ต่างจากการโจมตีเลเยอร์โครงสร้างพื้นฐาน เนื่องจากผู้โจมตีพยายามให้ฟังก์ชันเฉพาะของแอปพลิเคชันทำงานมากเกินไปเพื่อทำให้แอปพลิเคชันดังกล่าวไม่พร้อมใช้งาน ในบางกรณี อาจทำได้โดยใช้ปริมาณคำขอต่ำมากซึ่งไม่สร้างการรับส่งข้อมูลเครือข่ายในปริมาณมาก ผลคือสามารถทำให้ตรวจพบและลดการโจมตีได้ยากขึ้น ตัวอย่างของการโจมตีเลเยอร์แอปพลิเคชัน เช่น การฟลัด HTTP, การโจมตีแบบแคชระเบิด และการฟลัด XML-RPC บน WordPress

เมื่อดำเนินการฟลัด HTTP, ผู้โจมตีจะส่งคำขอ HTTP ที่ดูเหมือนว่ามาจากผู้ใช้เว็บแอปพลิเคชันที่มีตัวตนอยู่จริง การฟลัด HTTP บางครั้งจะพุ่งเป้าไปที่ทรัพยากรเฉพาะ ในขณะที่การฟลัด HTTP แบบที่ซับซ้อนกว่าจะพยายามเลียนแบบพฤติกรรมมนุษย์ การทำเช่นนี้สามารถทำให้การใช้เทคนิคการลดการโจมตีที่ใช้กันอยู่ทั่วไป เช่น การจำกัดอัตราคำขอ กระทำได้ยากขึ้น การโจมตีแบบแคชระเบิดเป็นการฟลัด HTTP ประเภทหนึ่ง ซึ่งใช้ความแปรผันในสตริงการสืบค้นเพื่อเลี่ยงการแคชเครือข่ายการส่งมอบเนื้อหา (CDN) ส่งผลให้เกิดการดึงข้อมูลต้นทาง ทำให้เว็บเซิร์ฟเวอร์ต้นทางมีความต้องการที่มากเกินไปเพิ่มขึ้น

เมื่อดำเนินการฟลัด XML-RPC บน WordPress หรือเรียกอีกอย่างหนึ่งว่า การฟลัดแบบอาศัยการแสดงความคิดเห็นโดยผ่านลิงก์บน WordPress นั้น ผู้โจมตีสามารถใช้ฟังก์ชัน XML-RPC API ของเว็บไซต์ที่ใช้บริการพื้นที่บนซอฟต์แวร์จัดการเนื้อหาแบรนด์ของ WordPress ในทางที่ผิดได้ เพื่อสร้างคำขอ HTTP จำนวนมากมายมหาศาล คุณสมบัติการอาศัยการแสดงความคิดเห็นโดยผ่านลิงก์ทำให้เว็บไซต์ที่ใช้บริการพื้นที่บน WordPress (ไซต์ A) แจ้งเตือนไซต์อื่นของ WordPress (ไซต์ B) ว่าไซต์ A ได้สร้างลิงก์ไปยังไซต์ B แล้ว ผลลัพธ์คือไซต์ B จะพยายามดึงข้อมูลไซต์ A เพื่อยืนยันว่าลิงก์ดังกล่าวมีอยู่จริง ในกรณีของการฟลัดแบบอาศัยการแสดงความคิดเห็นโดยผ่านลิงก์ ผู้โจมตีจะใช้ความสามารถนี้ในทางที่ผิดเพื่อทำให้ไซต์ B โจมตีไซต์ A การโจมตีประเภทนี้มีลายเซ็นชัดเจน เนื่องจาก “WordPress” ควรจะปรากฏอยู่ใน “User-Agent” ของส่วนหัวของคำขอ HTTP

การโจมตีเลเยอร์แอปพลิเคชันยังสามารถพุ่งเป้าไปที่บริการระบบชื่อโดเมน (DNS) ได้อีกด้วย ในบรรดาการโจมตีเหล่านี้ รูปแบบที่พบบ่อยที่สุดคือการฟลัดการสืบค้น DNS ซึ่งผู้โจมตีจะใช้การสืบค้น DNS จำนวนมากที่มีข้อมูลครบถ้วนเพื่อใช้ทรัพยากรของเซิร์ฟเวอร์ DNS ให้หมดไป การโจมตีเหล่านี้ยังอาจรวมถึงคอมโพเนนต์แคชระเบิดอีกด้วย

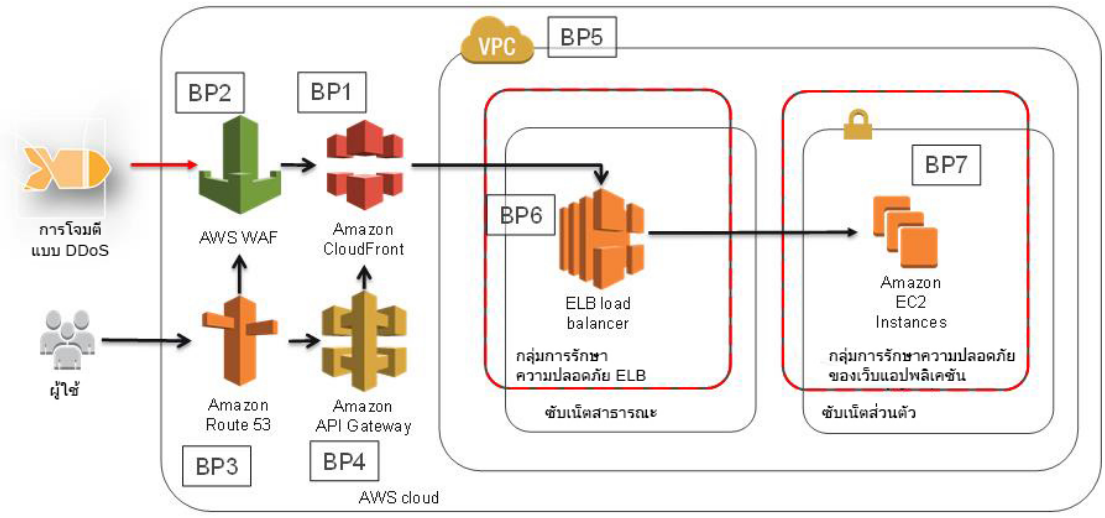
ซึ่งผู้โจมตีจะสุ่มสตริงซับโดเมนเพื่อบายพาสแคช DNS เฉพาะที่ของผู้แก้ปัญหารายใด ก็ตาม ผลลัพธ์คือผู้แก้ปัญหาจะถูกบังคับให้มีส่วนในการโจมตีเซิร์ฟเวอร์ DNS ที่ถูกต้อง

ในกรณีของเว็บแอปพลิเคชันที่นำเสนอผ่าน Secure Sockets Layer (SSL) ผู้โจมตีสามารถเลือกที่จะโจมตีกระบวนการต่อรอง SSL ได้ SSL ต้องใช้การประมวลผลค่อนข้างมาก ซึ่งทำให้ผู้โจมตีสร้างผลกระทบต่อความพร้อมใช้งานของเซิร์ฟเวอร์ได้โดยส่งข้อมูลที่ไม่สามารถอ่านได้ สำหรับการโจมตีประเภทนี้ ผู้โจมตีอาจดำเนินการแฮนด์เชค SSL เสร็จสิ้น ทว่าดำเนินการต่อรองวิธีเข้ารหัสเป็นการถาวรก็ได้ ในทำนองเดียวกัน ผู้โจมตีสามารถเลือกที่จะใช้ทรัพยากรเซิร์ฟเวอร์ให้หมดไปได้โดยเปิดและปิดเซสชัน SSL หลายเซสชัน

เทคนิคการบรรเทาความเสี่ยง

โครงสร้างพื้นฐานของ AWS มีดีไซน์ที่ยืดหยุ่นต่อการโจมตีแบบ DDoS และได้รับการรองรับจากระบบการลดการโจมตีแบบ DDoS ซึ่งสามารถตรวจพบและกรองการรองรับข้อมูลส่วนเกินได้โดยอัตโนมัติ หากต้องป้องกันความพร้อมใช้งานของแอปพลิเคชัน ควรใช้สถาปัตยกรรมที่ให้คุณใช้ประโยชน์จากความสามารถเหล่านี้ได้

หนึ่งในกรณีการใช้ AWS ที่พบเห็นได้บ่อยที่สุดคือ เว็บแอปพลิเคชันที่ให้บริการเนื้อหาแบบสแตติกและไดนามิกแก่ผู้ใช้บนอินเทอร์เน็ต สำหรับสถาปัตยกรรมอ้างอิงที่มีความยืดหยุ่นต่อการโจมตีแบบ DDoS ที่มักใช้กับเว็บแอปพลิเคชันต่างๆ โปรดดูรูปภาพ 5



รูปภาพ 5: สถาปัตยกรรมอ้างอิงที่มีความยืดหยุ่นต่อการโจมตีแบบ DDoS

สถาปัตยกรรมอ้างอิงนี้รวมถึงบริการต่างๆ ของ AWS ที่ช่วยคุณเพิ่มความยืดหยุ่นจากการโจมตีแบบ DDoS ให้กับเว็บแอปพลิเคชันได้ แนวทางปฏิบัติในสถาปัตยกรรมดังกล่าวได้รับการแจกแจงไว้เพื่อให้ง่ายต่อการอ้างอิง โดยแนวทางแต่ละข้อได้รับการอธิบายไว้ตลอดทั้งเอกสาร ตัวอย่างเช่น ส่วนที่อธิบายความสามารถที่ Amazon CloudFront มีจะอ้างอิงโดยใช้ตัวบ่งชี้แนวทางปฏิบัติ (เช่น BP1) สำหรับสรุปข้อมูลบริการเหล่านี้และความสามารถของบริการดังกล่าวแต่ละรายการ โปรดดูตาราง 2

	สถานที่ตั้ง Edge ของ AWS			**ภูมิภาคของ AWS**		
	Amazon CloudFront กับ AWS WAF (BP1, BP2)	Amazon API Gateway (BP4)	Amazon Route 53 (BP3)	Elastic Load Balancing (BP6)	Amazon VPC (BP5)	Amazon EC2 กับ Auto Scaling (BP7)
การลดการโจมตีเลเยอร์ 3 (เช่น รีเฟลกชัน UDP)	✓	✓	✓	✓	✓	
การลดการโจมตีเลเยอร์ 4 (เช่น การฟลัด SYN)	✓	✓	✓	✓		
การลดการโจมตีเลเยอร์ 6 (เช่น SSL)	✓	✓	ไม่พร้อมใช้งาน	✓		
ลดพื้นผิวการโจมตี	✓	✓	✓	✓	✓	
ปรับสัดส่วนเพื่อรองรับการรับส่งเลเยอร์แอปพลิเคชัน	✓	✓	✓	✓		✓
การลดการโจมตีเลเยอร์ 7 (เลเยอร์แอปพลิเคชัน)	✓	✓	✓			
การแยกทางภูมิศาสตร์และการกระจายการรับส่งข้อมูลที่มากเกินกับการโจมตีแบบ DDoS ที่หนักกว่า	✓	✓	✓			

ตาราง 2: สรุปแนวทางปฏิบัติ

บริการที่มีให้ใช้ภายในภูมิภาคต่างๆ ของ AWS เช่น Elastic Load Balancing และ Amazon Elastic Compute Cloud (EC2) ทำให้คุณสามารถสร้างความยืดหยุ่นต่อการโจมตีแบบ DDoS และปรับสัดส่วนเพื่อจัดการกับปริมาณการรับส่งข้อมูลที่ไม่ได้คาดคิดภายในภูมิภาคนั้นๆ ได้ บริการที่มีให้ใช้ในสถานที่ตั้ง Edge ของ AES เช่น Amazon CloudFront, AWS WAF, Amazon Route 53 และ Amazon API Gateway ทำให้คุณสามารถใช้ประโยชน์จากเครือข่ายของสถานที่ตั้ง Edge ที่มีอยู่ทั่วโลกซึ่งช่วยให้แอปพลิเคชันมีความคงทนต่อความเสียหายมากขึ้นและเพิ่มสัดส่วนการจัดการปริมาณการรับส่งข้อมูลที่มากขึ้น ประโยชน์ของการใช้บริการเหล่านี้แต่ละบริการเพื่อสร้างความยืดหยุ่นต่อการโจมตีแบบ DDoS ที่เลเยอร์โครงสร้างพื้นฐานและเลเยอร์แอปพลิเคชันได้รับการอธิบายไว้ในเนื้อหาส่วนที่ตามมา

การป้องกันเลเยอร์โครงสร้างพื้นฐาน (BP1, BP3, BP6, BP7)

ในสภาพแวดล้อมของศูนย์ข้อมูลแบบดั้งเดิม คุณสามารถลดการโจมตีแบบ DDoS ที่เลเยอร์โครงสร้างพื้นฐานได้โดยใช้เทคนิคต่างๆ เช่น การทำให้ความจุล้น การปรับใช้ระบบลดการโจมตีแบบ DDoS หรือการสครับการรับส่งข้อมูลโดยอาศัยบริการการลดการโจมตีแบบ DDoS บน AWS คุณมีตัวเลือกสำหรับออกแบบสถาปัตยกรรมให้แอปพลิเคชันสามารถปรับสัดส่วนและรองรับปริมาณการรับส่งข้อมูลที่มากขึ้นได้โดยไม่ต้องใช้เงินลงทุนมากหรือออกแบบให้ซับซ้อนโดยเกินความจำเป็น ข้อควรพิจารณาหลักในการลดการโจมตีแบบ DDoS ที่วัดปริมาณนั้นรวมไปถึงความพร้อมใช้งานของความสามารถและความหลากหลายในการส่งผ่าน อีกทั้งการป้องกันทรัพยากรของ AWS เช่น Amazon EC2 Instance จากการรับส่งข้อมูลการโจมตี

ขนาดของอินสแตนซ์

ลูกค้า AWS จำนวนมากใช้ Amazon EC2 เพราะมีความจุสำหรับการประมวลผลแบบปรับขนาดได้ ซึ่งช่วยให้คุณเพิ่มหรือลดสัดส่วนลงได้เมื่อความต้องการเปลี่ยนไป คุณสามารถปรับขยายสัดส่วนตามแนวนอนได้โดยเพิ่มอินสแตนซ์ไปยังแอปพลิเคชันตามต้องการ คุณยังสามารถเลือกปรับขยายสัดส่วนตามแนวตั้งได้โดยใช้อินสแตนซ์ที่ใหญ่ขึ้น อินสแตนซ์บางประเภทรองรับคุณสมบัติต่างๆ เช่น อินเทอร์เฟซเครือข่ายแบบ 10 กิกะบิต และการเพิ่มระดับของเครือข่าย ที่ช่วยให้คุณจัดการกับปริมาณการรับส่งข้อมูลที่มากขึ้นได้

เมื่อใช้อินเทอร์เฟซเครือข่ายแบบ 10 กิกะบิต แต่ละอินสแตนซ์จะสามารถรองรับปริมาณการรับส่งข้อมูลที่มากขึ้นได้ ผลคือช่วยป้องกันไม่ให้อินเทอร์เฟซแออัดอยู่ในการรับส่งข้อมูลที่ถึง Amazon EC2 Instance แล้ว อินสแตนซ์ที่รองรับการเพิ่มระดับของเครือข่ายจะมีประสิทธิภาพการทำงานของ I/O สูงกว่า และใช้งาน CPU น้อยกว่าเมื่อเทียบกับการใช้งานแบบดั้งเดิม ผลคือเพิ่มความสามารถให้กับอินสแตนซ์ในการจัดการกับการรับส่งข้อมูลที่มากขึ้นในปริมาณแพคเก็ต บน AWS คุณไม่มีส่วนรับผิดชอบต้นทุนในการโอนย้ายข้อมูลขาเข้า

หากต้องการเรียนรู้เพิ่มเติมเกี่ยวกับ Amazon EC2 Instance ที่รองรับอินเทอร์เฟซเครือข่ายแบบ 10 กิกะบิตและการเพิ่มระดับของเครือข่าย โปรดอ่าน ประเภทของ Amazon EC2 Instance[3] หากต้องการเรียนรู้วิธีเปิดใช้งานการเพิ่มระดับของเครือข่าย โปรดอ่าน การเปิดใช้งานการเพิ่มระดับของเครือข่ายบนอินสแตนซ์ Linux ใน VPC[4]

ตัวเลือกภูมิภาค (BP7)

บริการ AWS หลายอย่าง เช่น Amazon EC2 มีให้เลือกใช้ได้หลายแห่งทั่วโลก พื้นที่ที่แยกตามลักษณะทางภูมิศาสตร์เหล่านี้เรียกว่า ภูมิภาค AWS เมื่อออกแบบโครงสร้างแอปพลิเคชัน คุณสามารถเลือกภูมิภาคได้ตั้งแต่ 1 ภูมิภาคขึ้นไปตามความต้องการของคุณเอง สิ่งที่มักนำมาใช้ประกอบการพิจารณานั้นรวมถึงประสิทธิภาพการทำงาน ต้นทุน และอธิปไตยของข้อมูล ในแต่ละภูมิภาค AWS ยินยอมให้เข้าถึงชุดการเชื่อมต่อ อินเทอร์เน็ตและความสัมพันธ์แบบเพียร์ที่ไม่ซ้ำกันได้ ซึ่งช่วยให้ผู้ใช้ขั้นปลายที่มีตำแหน่งที่ตั้งคล้ายกันมีเวลาแฝงและอัตราความเร็วในระดับที่เหมาะสม

นอกจากนี้ยังควร *พิจารณาตัวเลือกภูมิภาคในแง่ความยืดหยุ่นต่อการโจมตีแบบ DDoS ด้วย ภูมิภาคหลายแห่งอยู่ใกล้ศูนย์แลกเปลี่ยนข้อมูลทางอินเทอร์เน็ตขนาดใหญ่มากกว่า การโจมตีแบบ DDos หลายครั้งมีต้นกำเนิดอยู่ในต่างประเทศ ดังนั้นจึงควรอยู่ใกล้ศูนย์แลกเปลี่ยนข้อมูลที่ผู้ให้บริการขนส่งระหว่างประเทศและเพียร์รายใหญ่มักเป็นที่สังเกตพบได้ง่ายอยู่บ่อยๆ ผลคือช่วยให้ผู้ใช้ขั้นปลายเข้าถึงแอปพลิเคชันเมื่อจัดการกับปริมาณการรับส่งข้อมูลที่มากขึ้นได้*

หากต้องการเรียนรู้เพิ่มเติมเกี่ยวกับการเลือกภูมิภาค โปรดอ่าน ภูมิภาคและพื้นที่ให้บริการ[5] และถามทีมดูแลลูกค้าเกี่ยวกับลักษณะของแต่ละภูมิภาคเพื่อช่วยให้คุณดำเนินการตัดสินใจได้อย่างมีหลักการ

Load Balancing (BP6)

การโจมตีแบบ DDoS ที่หนักขึ้นอาจมีจำนวนครั้งมากเกินขนาดของ Amazon EC2 Instance เพียงอินสแตนซ์เดียว หากต้องการลดความรุนแรงของการโจมตีเหล่านี้ คุณจะต้องพิจารณาตัวเลือกต่างๆ เพื่อดำเนินขั้นตอนโหลดบาลานซ์ให้กับการรับส่งข้อมูลที่มากเกิน เมื่อใช้ Elastic Load Balancing (ELB) คุณสามารถลดความเสี่ยงจากการที่แอปพลิเคชันทำงานหนักเกินไปได้โดยกระจายการรับส่งข้อมูลไปยังอินสแตนซ์แบ็คเอนด์จำนวนมาก ELB สามารถปรับสัดส่วนได้โดยอัตโนมัติ ซึ่งช่วยให้คุณจัดการกับปริมาณการรับส่งข้อมูลที่มากขึ้นโดยไม่ได้คาดการณ์ไว้ได้ เช่น แฟลชคราวด์ หรือการโจมตีแบบ DDoS

ELB ยอมรับเฉพาะการเชื่อมต่อ TCP ที่มีข้อมูลครบถ้วนเท่านั้น นั่นหมายความว่า ELB จะไม่ยอมรับการโจมตีแบบ DDoS หลายครั้งที่พบเห็นได้ทั่วไป เช่น การฟลัด SYN หรือการโจมตีรีเฟลกชัน UDP และการโจมตีเหล่านี้จะไม่ได้รับการส่งต่อไปยังแอปพลิเคชัน เมื่อ

ELB ตรวจพบการโจมตีประเภทเหล่านี้ ELB จะปรับสัดส่วนโดยอัตโนมัติเพื่อรองรับการรับส่งข้อมูลเพิ่มเติม โดยที่คุณไม่ต้องเสียค่าใช้จ่ายใดๆ เพิ่มเติม

หากต้องการเรียนรู้เพิ่มเติมเกี่ยวกับการใช้ ELB เพื่อกระจายโหลดและปกป้อง Amazon EC2 Instance โปรดอ่าน การเริ่มต้นใช้งาน Elastic Load Balancing[6]

ส่งมอบด้วยขนาดเหมาะสมโดยใช้สถานที่ตั้ง Edge ของ AWS (BP1, BP3)

การเข้าถึงการเชื่อมต่ออินเทอร์เน็ตที่มีการปรับสัดส่วนมากและมีความหลากหลายสามารถเพิ่มความสามารถในการปรับเวลาแฝงและอัตราความเร็วให้เหมาะกับผู้ใช้ขั้นปลาย รองรับการโจมตีแบบ DDoS และแยกความเสียหายในระหว่างที่ลดผลกระทบต่อความพร้อมใช้งาน สถานที่ตั้ง Edge ของ AWS มีเลเยอร์โครงสร้างพื้นฐานเครือข่ายเพิ่มเติมที่ก่อให้เกิดประโยชน์เหล่านี้แก่เว็บแอปพลิเคชันที่ใช้ Amazon CloudFront และ Amazon Route 53 บริการเหล่านี้จะแสดงเนื้อหาและแก้ปัญหาการสืบค้น DNS จากสถานที่ตั้งที่มักจะอยู่ใกล้กับผู้ใช้ขั้นปลายมากกว่า

การนำเสนอเว็บแอปพลิเคชันที่ Edge (BP1)

Amazon CloudFront เป็นบริการเครือข่ายการส่งมอบเนื้อหา (CDN) ที่สามารถใช้ส่งมอบเนื้อหาทั้งหมดในเว็บไซต์ได้ซึ่งรวมถึงเนื้อหาแบบสแตติก เนื้อหาแบบไดนามิก เนื้อหาการสตรีม และเนื้อหาแบบโต้ตอบ การเชื่อมต่อ TCP แบบถาวรและค่า time-to-live (TTL) ที่แปรผันได้สามารถใช้เร่งการส่งมอบเนื้อหาให้เร็วขึ้นได้ แม้เนื้อหาดังกล่าวจะไม่สามารถแคชที่สถานที่ตั้ง Edge ได้ ผลคือช่วยให้คุณใช้ Amazon CloudFront เพื่อปกป้องเว็บแอปพลิเคชันได้ แม้จะไม่ได้ให้บริการเนื้อหาแบบสแตติกอยู่ก็ตาม Amazon CloudFront ยอมรับเฉพาะการเชื่อมต่อที่มีข้อมูลครบถ้วนเพื่อป้องกันไม่ให้การโจมตีแบบ DDoS หลายครั้งที่พบเห็นได้ทั่วไป เช่น การฟลัด SYN และการโจมตีรีเฟลกชัน UDP ไปถึงต้นทาง การโจมตีแบบ DDoS จะถูกแยกไว้ตามลักษณะทางภูมิศาสตร์ใกล้กับแหล่งที่มา ซึ่งเป็นการป้องกันไม่ให้การรับส่งข้อมูลส่งผลกระทบต่อสถานที่ตั้งอื่นๆ ความสามารถต่างๆ เหล่านี้ช่วยเพิ่มความสามารถเป็นอย่างมากในการให้บริการการรับส่งข้อมูลแก่ผู้ใช้ขั้นปลายอย่างต่อเนื่องในช่วงที่มีการโจมตีแบบ DDoS ที่หนักกว่า คุณสามารถใช้ Amazon CloudFront เพื่อปกป้องต้นทางบน AWS หรือที่อื่นๆ บนอินเทอร์เน็ตได้

หากต้องการเรียนรู้เพิ่มเติมเกี่ยวกับการปรับประสิทธิภาพการทำงานของเว็บแอปพลิเคชันที่ใช้ Amazon CloudFront โปรดอ่าน การเริ่มต้นใช้งาน CloudFront[7]

การแก้ไขปัญหาเกี่ยวกับชื่อโดเมนที่ Edge (BP3)

Amazon Route 53 เป็นบริการระบบชื่อโดเมน (DNS) ที่พร้อมใช้งานและปรับสัดส่วนได้มากซึ่งสามารถใช้ส่งข้อมูลไปยังเว็บแอปพลิเคชันได้ บริการนี้มีคุณสมบัติขั้นสูงหลากหลายคุณสมบัติอยู่ด้วย เช่น โฟลว์การรับส่งข้อมูล การกำหนดเส้นทางตามเวลาแฝง, Geo DNS, การตรวจสอบสภาพการทำงาน และการเฝ้าสังเกต คุณสมบัติเหล่านี้ช่วยให้คุณควบคุมว่าบริการจะตอบคำขอ DNS อย่างไรเพื่อปรับให้เหมาะกับเวลาแฝง สภาพการทำงาน และข้อควรพิจารณาอื่นๆ คุณสามารถใช้คุณสมบัติเหล่านี้เพิ่มประสิทธิภาพการทำงานของเว็บแอปพลิเคชันและหลีกเลี่ยงการหยุดทำงานของเว็บไซต์

Amazon Route 53 ใช้การสร้าง Shard แบบสลับและการแยกส่วนจัดเก็บข้อมูล Anycast เพื่อให้ผู้ใช้ขั้นปลายเข้าใช้งานแอปพลิเคชันได้ แม้การโจมตีแบบ DDoS จะมุ่งไปที่บริการ DNS ก็ตาม เมื่อสร้าง Shard แบบสลับ เซิร์ฟเวอร์ชื่อแต่ละเซิร์ฟเวอร์ในชุดการรับมอบสิทธิ์จะสอดคล้องกับชุดสถานที่ตั้ง Edge และพาธอินเทอร์เน็ตเฉพาะ ผลคือช่วยให้เกิดการคงทนต่อความเสียหายมากขึ้นและลดการเหลื่อมล้ำกันระหว่างลูกค้า หากเซิร์ฟเวอร์ชื่อ 1 เซิร์ฟเวอร์ในชุดการรับมอบสิทธิ์ไม่พร้อมใช้งาน ผู้ใช้ขั้นปลายสามารถลองใหม่และรับการตอบสนองจากเซิร์ฟเวอร์ชื่ออีกเซิร์ฟเวอร์หนึ่ง ณ สถานที่ตั้ง Edge อื่น การแยกส่วนจัดเก็บข้อมูล Anycast ใช้เพื่อให้สถานที่ตั้งที่เหมาะสมที่สุดให้บริการคำขอ DNS แต่ละรายการ ขั้นตอนดังกล่าวส่งผลให้มีการกระจายโหลดและลดเวลาแฝงของ DNS ซึ่งช่วยให้ผู้ใช้ขั้นปลายได้รับการตอบสนองเร็วขึ้น นอกจากนี้ Amazon Route 53 ยังสามารถตรวจพบความผิดปกติในแหล่งที่มาและปริมาณการสืบค้น DNS อีกทั้งจัดลำดับความสำคัญให้กับคำขอจากผู้ใช้ที่เป็นที่รับรู้ว่าไว้วางใจได้

หากคุณมีพื้นที่ให้บริการของ Amazon Route 53 หลายแห่ง คุณสามารถสร้างชุดการรับมอบสิทธิ์แบบนำกลับมาใช้ใหม่ได้ซึ่งคุณจะได้ชุดเซิร์ฟเวอร์ชื่อที่ถูกต้องชุดเดียวกันสำหรับโดเมนแต่ละโดเมน ผลคือช่วยรักษาพื้นที่ให้บริการของคุณได้ง่ายขึ้น ในช่วงที่มีการโจมตีแบบ DDoS ขั้นตอนนี้ยังช่วยให้ AWS ใช้การลดการโจมตีหนึ่งครั้งที่ครอบคลุมพื้นที่ให้บริการที่ใช้การรับมอบสิทธิ์แบบนำกลับมาใช้ใหม่ได้

หากต้องการเรียนรู้เพิ่มเติมเกี่ยวกับการใช้ Amazon Route 53 เพื่อส่งผู้ใช้ขั้นปลายไปยังแอปพลิเคชัน โปรดอ่าน การเริ่มต้นใช้งาน Amazon Route 53[8] หากต้องการเรียนรู้เพิ่มเติมเกี่ยวกับชุดการรับมอบสิทธิ์แบบนำกลับมาใช้ใหม่ได้ โปรดอ่าน การดำเนินการกับชุดการรับมอบสิทธิ์แบบนำกลับมาใช้ใหม่ได้[9]

การป้องกันเลเยอร์แอปพลิเคชัน (BP1, BP2, BP6)

เทคนิคหลายอย่างที่อธิบายไว้ในเอกสารฉบับนี้จะเกิดประสิทธิภาพเมื่อลดผลกระทบความพร้อมใช้งานของการโจมตีแบบ DDoS ที่เลเยอร์โครงสร้างพื้นฐาน การป้องกันแอปพลิเคชันจากการโจมตีเลเยอร์แอปพลิเคชันต้องใช้สถาปัตยกรรมที่ช่วยให้คุณตรวจพบสัดส่วนเพิ่มเติมในการรองรับและบล็อกคำขอที่ประสงค์ร้าย ที่กล่าวมานี้เป็นข้อควรพิจารณาที่สำคัญ เนื่องจากโดยทั่วไปแล้วระบบการลดการโจมตีแบบ DDoS บนเครือข่ายจะไม่มีประสิทธิภาพเมื่อลดการโจมตีเลเยอร์แอปพลิเคชันที่มีความซับซ้อน

ตรวจจับและกรองคำขอเว็บประสงค์ร้าย (BP1, BP2)

ไฟร์วอลล์สำหรับเว็บแอปพลิเคชัน (WAFs) มักใช้ปกป้องเว็บแอปพลิเคชันจากการโจมตีที่พยายามอาศัยช่องโหว่ในแอปพลิเคชัน ตัวอย่างที่พบได้ทั่วไป เช่น การแทรกข้อมูล SQL หรือการปลอมแปลงคำขอข้ามไซต์ คุณยังสามารถใช้ WAF เพื่อตรวจจับและลดการโจมตีแบบ DDoS ที่เลเยอร์เว็บแอปพลิเคชันได้อีกด้วย

บน AWS คุณสามารถใช้ Amazon CloudFront และ AWS WAF เพื่อป้องกันแอปพลิเคชันจากการโจมตีเหล่านี้ได้ Amazon CloudFront ช่วยให้คุณแคชเนื้อหาแบบสแตติกและให้บริการเนื้อหาดังกล่าวจากสถานที่ตั้ง Edge ของ AWS ที่ช่วยลดโหลดบนต้นทางได้ นอกจากนี้ Amazon CloudFront ยังสามารถปิดการเชื่อมต่อจากผู้โจมตีที่ใช้วิธี slow-reading หรือ slow-writing (เช่น Slowloris) ได้โดยอัตโนมัติ คุณสามารถใช้การจำกัดทางภูมิศาสตร์บน Amazon CloudFront เพื่อป้องกันผู้ใช้ในสถานที่ตั้งทางภูมิศาสตร์เฉพาะจากการเข้าถึงเนื้อหาได้ การทำเช่นนี้อาจก่อให้เกิดประโยชน์ในกรณีที่คุณต้องการบล็อกการโจมตีที่มีต้นกำเนิดมาจากสถานที่ตั้งทางภูมิศาสตร์ที่คุณไม่ได้คาดว่าจะให้บริการผู้ใช้ขั้นปลาย

สำหรับการโจมตีประเภทอื่นๆ เช่น การฟลัด HTTP หรือการฟลัดแบบอาศัยการแสดงความคิดเห็นโดยผ่านลิงก์บน WordPress คุณสามารถใช้ AWS WAF เพื่อสร้างการลดการโจมตีเองได้ หากคุณทราบที่อยู่ IP ของแหล่งที่มาที่ต้องการบล็อก คุณสามารถสร้างกฎที่ดำเนินการบล็อกแล้วโยงกฎนั้นเข้ากับ ACL เว็บได้ จากนั้น คุณสามารถสร้างเงื่อนไขความสอดคล้องกับที่อยู่ IP ใน ACL เว็บเพื่อบล็อกที่อยู่ IP ของแหล่งที่มาที่กำลังมีส่วนในการโจมตีได้ คุณยังสามารถสร้างกฎกำหนดเงื่อนไขบล็อกตาม URI สตริงการสืบค้น วิธี HTTP หรือเฮดเดอร์คีย์ได้อีกด้วย ขั้นตอนหลังจะมีประโยชน์ในกรณีเกิดการโจมตีที่มีลายเซ็นชัดเจน ตัวอย่างเช่น การโจมตีแบบอาศัยการแสดงความคิดเห็นโดยผ่านลิงก์บน WordPress จะมี “WordPress” อยู่ใน User-Agent เสมอ

การระบุลายเซ็นของการโจมตีแบบ DDoS หรือระบุที่อยู่ IP ที่กำลังมีส่วนในการโจมตีอย่างถูกต้องนั้นอาจเป็นเรื่องที่ท้าทาย บางครั้ง เป็นไปได้ที่จะค้นหาข้อมูลนี้โดยตรวจสอบล็อกของเว็บเซิร์ฟเวอร์ คุณยังสามารถใช้คอนโซล AWS WAF เพื่อดูตัวอย่างคำขอที่ Amazon CloudFront ได้ส่งต่อไปยัง AWS WAF ได้อีกด้วย คำขอที่ได้รับการสุ่มตัวอย่างสามารถช่วยให้คุณตัดสินใจว่าอาจต้องใช้กฎใดในการลดการโจมตีเลเยอร์แอปพลิเคชัน หากคุณเห็นคำขอหลายรายการที่มีสตริงการสืบค้นแบบสุ่ม คุณอาจเลือกที่จะปิดการใช้งานการส่งต่อสตริงการสืบค้นใน Amazon CloudFront การทำเช่นนั้นอาจก่อให้เกิดประโยชน์เมื่อลดการโจมตีแบบแคชระเบิดกับต้นทาง

การโจมตีในบางครั้งมีการรับส่งข้อมูลที่ปลอมแปลงให้ดูเหมือนการรับส่งข้อมูลให้ผู้ใช้ขั้นปลายตามปกติ หากต้องการลดการโจมตีประเภทนี้ คุณสามารถใช้ฟังก์ชัน AWS Lambda เพื่อใช้การขึ้นบัญชีดำโดยพิจารณาตามอันดับ เมื่อใช้ขั้นตอนการขึ้นบัญชีดำโดยพิจารณาตามอันดับ คุณสามารถกำหนดเกณฑ์ว่าเว็บแอปพลิเคชันสามารถให้บริการคำขอได้มากเท่าใด หากบ็อตหรือครอว์เลอร์มีมากเกินขีดจำกัดดังกล่าว คุณสามารถใช้ AWS WAF เพื่อบล็อกคำขอเพิ่มเติมโดยอัตโนมัติได้

หากต้องการเรียนรู้เพิ่มเติมเกี่ยวกับการใช้การจำกัดทางภูมิศาสตร์เพื่อจำกัดการเข้าถึงการกระจายของ Amazon CloudFront โปรดอ่าน [การจำกัดการกระจายทางภูมิศาสตร์ให้กับเนื้อหา][10]

หากต้องการเรียนรู้เพิ่มเติมเกี่ยวกับการใช้ AWS WAF โปรดอ่าน [การเริ่มต้นใช้งาน AWS WAF][11] และ [การดูตัวอย่างคำขอเว็บที่ CloudFront ได้ส่งต่อไปยัง AWS WAF][12]

หากต้องการเรียนรู้วิธีกำหนดค่าการขึ้นบัญชีดำโดยพิจารณาอันดับด้วย AWS Lambda และ AWS WAF โปรดอ่าน [วิธีกำหนดค่าการขึ้นบัญชีดำโดยพิจารณาตามอันดับด้วย AWS WAF และ AWS Lambda][13]

ปรับสัดส่วนเพื่อรองรับ (BP6)

อีกวิธีหนึ่งในการจัดการกับการโจมตีเลเยอร์แอปพลิเคชันคือดำเนินการด้วยขนาดเหมาะสม ในกรณีของเว็บแอปพลิเคชัน คุณสามารถใช้ ELB เพื่อกระจายการรับส่งข้อมูลไปยัง Amazon EC2 Instance หลายอินสแตนซ์ที่มีจำนวนมากเกินไปหรือได้รับการกำหนดค่าให้ปรับสัดส่วนโดยอัตโนมัติเพื่อให้บริการการรับส่งข้อมูลที่เพิ่มขึ้น ไม่ว่าจะเป็นผลมาจากแฟลชคลาวด์ หรือการโจมตีแบบ DDoS ที่เลเยอร์แอปพลิเคชันก็ตาม การแจ้งเตือนของ Amazon CloudWatch มีไว้เพื่อใช้งาน Auto Scaling ซึ่งจะปรับขนาดกลุ่ม Amazon

EC2 ให้สอดคล้องกับเหตุการณ์ที่คุณกำหนดไว้โดยอัตโนมัติ ผลคือปกป้องความพร้อมใช้งานของแอปพลิเคชัน แม้ในช่วงที่จัดการกับปริมาณคำขอที่ไม่ได้คาดคิด เมื่อใช้ Amazon CloudFront หรือ ELB การกระจายหรือโหลดบาลานเซอร์จะจัดการเรื่องการต่อรอง SSL ซึ่งสามารถป้องกันอินสแตนซ์ไม่ให้ได้รับผลกระทบจากการโจมตีโดยอาศัย SSL

หากต้องการเรียนรู้เพิ่มเติมเกี่ยวกับการใช้ Amazon CloudWatch เพื่อใช้งาน Auto Scaling โปรดอ่าน การเฝ้าสังเกตอินสแตนซ์และกลุ่ม Auto Scaling โดยใช้ Amazon CloudWatch[14]

การลดพื้นผิวการโจมตี

ข้อควรพิจารณาที่สำคัญอีกประการหนึ่งเมื่อออกแบบสถาปัตยกรรมบน AWS คือให้จำกัดโอกาสของผู้โจมตีในการพุ่งเป้าไปที่แอปพลิเคชัน ตัวอย่างเช่น หากคุณไม่ได้คาดหวังให้ผู้ใช้ขั้นปลายทำงานกับทรัพยากรบางอย่างโดยตรง คุณจะต้องตรวจสอบให้แน่ใจว่าทรัพยากรเหล่านั้นไม่สามารถเข้าถึงได้จากอินเทอร์เน็ต ในทำนองเดียวกัน หากคุณไม่ได้คาดหวังให้ผู้ใช้ขั้นปลายหรือแอปพลิเคชันภายนอกสื่อสารกับแอปพลิเคชันในบางพอร์ตหรือโปรโตคอล คุณจะต้องตรวจสอบให้แน่ใจว่าไม่มีการยอมรับการรับส่งข้อมูล แนวคิดนี้เป็นที่รู้จักกันในชื่อว่า การลดพื้นผิวการโจมตี ในส่วนนี้ คุณจะพบแนวทางปฏิบัติที่ช่วยให้คุณลดพื้นผิวการโจมตีและจำกัดขอบเขตในการแสดงแอปพลิเคชันบนอินเทอร์เน็ต ทรัพยากรที่ไม่แสดงบนอินเทอร์เน็ตนั้นโจมตีได้ยากกว่า ซึ่งเป็นการจำกัดตัวเลือกของผู้โจมตีในการพุ่งเป้าไปที่ความพร้อมใช้งานของแอปพลิเคชัน

การสร้างความซับซ้อนให้กับทรัพยากร AWS (BP1, BP4, BP5)

สำหรับแอปพลิเคชันจำนวนมาก ทรัพยากร AWS ของคุณไม่จำเป็นต้องแสดงทั้งหมดบนอินเทอร์เน็ต ตัวอย่างเช่น Amazon EC2 Instance เบื้องหลัง ELB อาจไม่จำเป็นต้องอนุญาตให้ทุกคนเข้าถึงได้ ในกรณีนี้ คุณอาจเลือกอนุญาตให้ผู้ใช้ขั้นปลายเข้าถึง ELB บนพอร์ต TCP บางพอร์ตได้และอนุญาตให้เฉพาะ ELB สื่อสารกับ Amazon EC2 Instance ได้เท่านั้น คุณสามารถทำเช่นนี้ได้โดยกำหนดค่าให้กับกลุ่มการรักษาความปลอดภัยและรายการควบคุมการเข้าถึงเครือข่าย (NACL) ภายใน Amazon Virtual Private Cloud (VPC) Amazon VPC ช่วยให้คุณเตรียมใช้งานเซกชันแบบแยก

ตามความสมเหตุสมผลใน AWS Cloud ซึ่งคุณสามารถเปิดใช้ทรัพยากร AWS ใน เครือข่ายเสมือนที่คุณกำหนดไว้ได้

กลุ่มการรักษาความปลอดภัยและ ACL เครือข่ายนั้นคล้ายกันตรงที่ช่วยให้คุณควบคุมการเข้าถึงทรัพยากร AWS ภายใน VPC ได้ กลุ่มการรักษาความปลอดภัยช่วยให้คุณควบคุมการรับส่งข้อมูลขาเข้าและขาออกที่ระดับอินสแตนซ์ได้ และ ACL เครือข่ายมีความสามารถคล้ายกัน เฉพาะที่ระดับซับเน็ตของ VPC นอกจากนี้ ยังไม่มีค่าใช้จ่ายสำหรับการโอนย้ายข้อมูลขาเข้าสำหรับกฎของกลุ่มการรักษาความปลอดภัย Amazon EC2 (SG) หรือ ACL เครือข่าย ขั้นตอนนี้ช่วยให้มั่นใจได้ว่าคุณไม่ต้องเสียค่าใช้จ่ายเพิ่มเติมสำหรับการรับส่งข้อมูลที่ถูกกลุ่มการรักษาความปลอดภัยหรือ ACL เครือข่ายของคุณปฏิเสธ

กลุ่มการรักษาความปลอดภัย (BP5)

คุณสามารถระบุกลุ่มรักษาความปลอดภัยเมื่อใช้งานอินสแตนซ์หรือเชื่อมโยงอินสแตนซ์เข้ากับกลุ่มรักษาความปลอดภัยในภายหลัง การรับส่งข้อมูลทั้งหมดไปยังกลุ่มรักษาความปลอดภัยจากอินเทอร์เน็ตจะถูกปฏิเสธโดยนัย เว้นแต่คุณสร้างกฎ *อนุญาต* เพื่ออนุญาตให้มีการรับส่งข้อมูลได้ ตัวอย่างเช่น หากคุณมีเว็บแอปพลิเคชันที่มี ELB และ Amazon EC2 Instance หลายอินสแตนซ์ คุณอาจตัดสินใจสร้างกลุ่มรักษาความปลอดภัยหนึ่งกลุ่มสำหรับ ELB (“กลุ่มรักษาความปลอดภัยของ ELB”) และอีกหนึ่งกลุ่มสำหรับอินสแตนซ์ (“กลุ่มรักษาความปลอดภัยของเซิร์ฟเวอร์เว็บแอปพลิเคชัน”) จากนั้น คุณสามารถสร้างกฎ *อนุญาต* เพื่ออนุญาตให้มีการรับส่งข้อมูลจากอินเทอร์เน็ตไปยังกลุ่มรักษาความปลอดภัยของ ELB และอนุญาตให้มีการรับส่งข้อมูลจากกลุ่มรักษาความปลอดภัยของ ELB ไปยังกลุ่มรักษาความปลอดภัยของเซิร์ฟเวอร์เว็บแอปพลิเคชันได้ ผลลัพธ์คือ การรับส่งข้อมูลจากอินเทอร์เน็ตจะไม่สามารถสื่อสารกับ Amazon EC2 Instance ได้โดยตรง ซึ่งทำให้ผู้โจมตีเรียนรู้เกี่ยวกับแอปพลิเคชันของคุณได้ยากขึ้น

รายการควบคุมการเข้าถึง (ACL) เครือข่าย (BP5)

ใน ACL เครือข่าย คุณสามารถระบุทั้งกฎ *อนุญาต* และกฎ *ปฏิเสธ* ได้ การทำเช่นจะเกิดประโยชน์ในกรณีที่คุณต้องการปฏิเสธการรับส่งข้อมูลบางประเภทไปยังแอปพลิเคชันอย่างชัดเจน ตัวอย่างเช่น คุณสามารถระบุที่อยู่ IP (เป็นช่วง CIDR) โปรโตคอล และพอร์ตปลายทางที่ควรถูกปฏิเสธสำหรับซับเน็ตทั้งหมด หากแอปพลิเคชันใช้เฉพาะสำหรับการรับส่งข้อมูล TCP เท่านั้น คุณสามารถสร้างกฎเพื่อ *ปฏิเสธ* การรับส่งข้อมูล UDP ทั้งหมด หรือในทางตรงกันข้าม เครื่องมือนี้มีประโยชน์เมื่อตอบสนองการโจมตีแบบ DDoS

เนื่องจากช่วยให้คุณสร้างกฎของคุณเองในการลดการโจมตีหากคุณทราบที่อยู่ IP ของแหล่งที่มาหรือลายเซ็นอื่นๆ

การป้องกันต้นทาง (BP1)

หากคุณใช้ Amazon CloudFront ที่มีต้นทางอยู่ใน VPC คุณควรใช้ฟังก์ชัน AWS Lambda เพื่ออัปเดตกฎการ *อนุญาต* ให้มีการรับส่งข้อมูลเฉพาะจาก Amazon CloudFront ของกลุ่มรักษาความปลอดภัยโดยอัตโนมัติ การทำเช่นนี้เพิ่มความปลอดภัยของต้นทางได้โดยช่วยให้แน่ใจว่า Amazon CloudFront และ AWS WAF ไม่สามารถบายพาสได้

หากต้องการเรียนรู้เพิ่มเติมเกี่ยวกับการป้องกันต้นทางโดยอัปเดตกลุ่มการรักษาความปลอดภัยโดยอัตโนมัติ โปรดอ่าน วิธีอัปเดตกลุ่มรักษาความปลอดภัยของคุณสำหรับ Amazon CloudFront และ AWS WAF โดยอัตโนมัติโดยใช้ AWS Lambda[15]

คุณยังอาจต้องการตรวจสอบให้แน่ใจว่ามีเพียงการกระจายข้อมูลของ Amazon CloudFront ของคุณเท่านั้นที่ส่งต่อคำขอไปยังต้นทางอีกด้วย เมื่อใช้ส่วนหัวคำขอ Edge ไปยังต้นทาง คุณสามารถเพิ่มหรือปฏิเสธค่าของส่วนหัวคำขอที่มีอยู่เมื่อ Amazon CloudFront ส่งต่อคำขอไปยังต้นทาง คุณสามารถใช้ส่วนหัว *X-Shared-Secret* เพื่อช่วยยืนยันว่าคำขอที่ส่งไปยังต้นทางเป็นคำขอที่ส่งจาก Amazon CloudFront

หากต้องการเรียนรู้เพิ่มเติมเกี่ยวกับการป้องกันต้นทางด้วยส่วนหัว *X-Shared-Secret* โปรดอ่าน การส่งต่อส่วนหัวแบบกำหนดเองไปยังต้นทาง[16]

การป้องกันตำแหน่งข้อมูล API (BP4)

โดยปกติแล้ว เมื่อมีความจำเป็นต้องแสดง API ให้ทุกคนเห็น ก็จะมีความเสี่ยงที่ว่าการโจมตีแบบ DDoS อาจพุ่งเป้าไปที่ส่วนหน้าของ API ได้ Amazon API Gateway เป็นบริการที่มีการบริหารจัดการอย่างเต็มรูปแบบซึ่งให้คุณสร้าง API ที่ทำตัวเป็น “ประตูหน้า” ให้กับแอปพลิเคชันที่ใช้งานบน Amazon EC2, AWS Lambda หรือเว็บแอปพลิเคชันอื่นได้ เมื่อใช้ Amazon API Gateway คุณไม่จำเป็นต้องใช้งานเซิร์ฟเวอร์ของคุณเองเป็นส่วนหน้าของ API และคุณสามารถสร้างความซับซ้อนให้กับคอมโพเนนต์อื่นๆ ของแอปพลิเคชันของคุณจากทุกคนได้ การทำเช่นนี้ช่วยป้องกันทรัพยากร AWS เหล่านั้นไม่ให้ตกเป็นเป้าของการโจมตีแบบ DDoS ได้ Amazon API Gateway ผนวกเข้ากับ Amazon CloudFront ซึ่งช่วยให้คุณได้ประโยชน์จากความยืดหยุ่นต่อการโจมตีแบบ DDoS ที่เพิ่มขึ้นไปซึ่งมีอยู่ในบริการดังกล่าว คุณยังสามารถปกป้องกันแบ็คเอนด์จากการ

รับส่งข้อมูลมากเกินได้โดยกำหนดค่ามาตรฐานหรือขยายขีดจำกัดอัตราให้กับวิธีแต่ละวิธีใน REST API อีกด้วย

หากต้องการเรียนรู้เพิ่มเติมเกี่ยวกับการสร้าง API ด้วย Amazon API Gateway โปรดอ่าน การเริ่มต้นใช้งาน Amazon API Gateway[17]

เทคนิคการดำเนินการ

เทคนิคการลดการโจมตีในเอกสารฉบับนี้ช่วยให้คุณสามารถออกแบบสถาปัตยกรรมให้กับแอปพลิเคชันที่มีความยืดหยุ่นภายในตัวเองจากการโจมตีแบบ DDoS ในหลายกรณี การทราบว่าการโจมตีแบบ DDoS พุ่งเป้าไปที่แอปพลิเคชันเมื่อใดและสามารถดำเนินการกับข้อมูลนี้ได้ยังนับว่ามีประโยชน์อีกด้วย คุณยังอาจต้องการใช้ทรัพยากรเพิ่มเติมเพื่อประเมินภัยคุกคาม ตรวจสอบสถาปัตยกรรมของแอปพลิเคชัน หรือขอความช่วยเหลืออื่นอีกด้วย เนื้อหาส่วนนี้อธิบายแนวทางปฏิบัติเพื่อให้สามารถมองเห็นพฤติกรรมที่ผิดปกติ แจ้งเตือนและทำงานอัตโนมัติ อีกทั้งใช้ AWS เพื่อขอความช่วยเหลือเพิ่มเติมได้

ความสามารถในการแสดงข้อมูล

การทำความเข้าใจพฤติกรรมปกติของแอปพลิเคชันช่วยให้คุณดำเนินการได้เร็วขึ้นเมื่อตรวจพบความผิดปกติ เมื่อตัววัดผลหลักเบี่ยงเบนไปมากจากค่าที่คาดหวังไว้ เหตุการณ์นี้บ่งบอกว่าผู้โจมตีอาจกำลังพยายามพุ่งเป้าไปที่ความพร้อมใช้งานของแอปพลิเคชันอยู่ เมื่อใช้ Amazon CloudWatch คุณสามารถเฝ้าสังเกตแอปพลิเคชันที่เปิดใช้งานบน AWS ได้ Amazon CloudWatch ช่วยให้คุณเก็บรวบรวมและติดตามตัววัดผลต่างๆ เก็บรวบรวมและเฝ้าสังเกตไฟล์ล็อก และตอบสนองต่อการเปลี่ยนแปลงในทรัพยากร AWS โดยอัตโนมัติได้ สำหรับคำอธิบายตัววัดผลของ Amazon CloudWatch ที่มักใช้ตรวจพบและตอบสนองต่อการโจมตีแบบ DDoS โปรดดูตาราง 3

หัวข้อ	ตัววัด	คำอธิบาย
Auto Scaling	GroupMaxSize	ขนาดสูงสุดของกลุ่ม Auto Scaling
Amazon CloudFront	Requests	จำนวนของคำขอ HTTP/S
Amazon CloudFront	TotalErrorRate	ร้อยละของคำขอทั้งหมดซึ่งมีรหัสสถานะ HTTP เป็น 4xx หรือ 5xx
Amazon EC2	CPUUtilization	ร้อยละของหน่วยประมวลผล EC2 ที่ปันส่วน ซึ่งมีการใช้งานในปัจจุบัน
Amazon EC2	NetworkIn	จำนวนข้อมูล (ไบต์) ที่ได้รับโดยอินสแตนซ์จากอินเทอร์เฟซเครือข่ายทั้งหมด
ELB	SurgeQueueLength	จำนวนคำขอที่โหลดบาลานเซอร์จัดคิว ซึ่งรอให้อินสแตนซ์แบ็คเอนด์ยอมรับการเชื่อมต่อและประมวลผลคำขอ
ELB	UnHealthyHostCount	จำนวนของอินสแตนซ์ที่ไม่สามารถใช้งานได้ในแต่ละ Availability Zone
ELB	RequestCount	จำนวนของคำขอที่เสร็จสมบูรณ์ ซึ่งได้รับและมีการกำหนดเส้นทางไปยังอินสแตนซ์ที่ลงทะเบียน
ELB	Latency	ระยะเวลาที่ใช้ (วินาที) นับจากเวลาที่คำขอถูกส่งออกจากโหลดบาลานเซอร์จนถึงเวลาที่ได้รับการตอบกลับ
ELB	HTTPCode_ELB_4xx HTTPCode_ELB_5xx	จำนวนของรหัสข้อผิดพลาด HTTP 4XX หรือ 5XX ที่สร้างขึ้นโดยโหลดบาลานเซอร์
ELB	BackendConnectionErrors	จำนวนของการเชื่อมต่อที่ไม่ประสบความสำเร็จ
ELB	SpilloverCount	จำนวนของคำขอที่ถูกปฏิเสธเนื่องจากคิวเต็ม
Amazon Route 53	HealthCheckStatus	สถานะของตำแหน่งข้อมูลการตรวจสอบสภาพการทำงาน

ตาราง 3: ตัววัดที่แนะนำสำหรับ Amazon CloudWatch

สำหรับแอปพลิเคชันที่ได้รับการออกแบบสถาปัตยกรรมตามสถาปัตยกรรมอ้างอิงที่มีความยืดหยุ่นต่อการโจมตีแบบ DDoS ในรูปภาพ 5 การโจมตีเลเยอร์โครงสร้างพื้นฐานที่พบเห็นได้บ่อยจะถูกบล็อกก่อนจะไปถึงแอปพลิเคชัน ผลลัพธ์คือ การโจมตีเหล่านี้จะไม่ปรากฏในตัววัดผลของ Amazon CloudWatch ของคุณ

การโจมตีเลเยอร์แอปพลิเคชันอาจเพิ่มระดับให้กับตัววัดผลเหล่านี้หลายตัว ตัวอย่างเช่น การฟลัด HTTP อาจก่อให้เกิดการยกระดับในคำขอและ CPU อีกทั้งการใช้งานเครือข่ายสำหรับตัววัดผลของ Amazon CloudFront, ELB และ Amazon EC2 หากอินสแตนซ์แบ็คเอนด์ไม่สามารถให้บริการคำขอที่มีจำนวนมากเกินได้ คุณยังอาจมองเห็นการเพิ่ม

ระดับใน TotalErrorRate บน Amazon CloudFront และ SurgeQueueLength, UnHealthyHostCount, Latency, BackendConnectionErrors, SpilloverCount หรือ HTTPCode บน ELB อีกด้วย ในกรณีนี้ ปริมาณคำขอ HTTP อาจถูกกดเอาไว้ เนื่องจากแอปพลิเคชันไม่สามารถให้บริการผู้ใช้ขั้นปลายแบบปกติได้ คุณสามารถแก้ไขสภาพดังกล่าวได้โดยปรับสัดส่วนแบ็คเอนด์ของแอปพลิเคชัน หรือโดยบล็อกการรับส่งข้อมูลที่มากเกินด้วย AWS WAF ดังที่ได้อธิบายไว้ก่อนหน้านี้ในเอกสารฉบับนี้

หากต้องการเรียนรู้เพิ่มเติมเกี่ยวกับการใช้ Amazon CloudWatch เพื่อตรวจพบการโจมตีแบบ DDoS ที่เกิดขึ้นกับแอปพลิเคชัน โปรดอ่าน การเริ่มต้นใช้งาน Amazon CloudWatch[18]

เครื่องมืออีกอย่างหนึ่งที่คุณใช้งานได้เพื่อให้มองเห็นการรับส่งข้อมูลที่พุ่งเป้าไปที่แอปพลิเคชัน คือ ล็อกจาก VPC Flow บนเครือข่ายแบบดั้งเดิม คุณอาจใช้ล็อก Flow ของเครือข่ายเพื่อแก้ไขปัญหาการเชื่อมต่อและปัญหาความปลอดภัย และตรวจสอบให้แน่ใจว่ากฎการเข้าถึงเครือข่ายทำงานตามที่คาดไว้ เมื่อใช้ล็อกจาก VPC Flow คุณสามารถรวบรวมข้อมูลเกี่ยวกับการรับส่งข้อมูล IP ไปยังและจากอินเทอร์เฟซของเครือข่ายใน VPC ได้

บันทึกล็อก Flow แต่ละรายการจะมีที่อยู่ IP ของแหล่งที่มาและปลายทาง พอร์ตของแหล่งที่มาและปลายทาง โปรโตคอล และจำนวนแพ็คเก็ตกับข้อมูล (ไบต์) ที่โอนย้ายในช่วงที่ปรากฏหน้าต่างรวบรวมข้อมูล ข้อมูลนี้สามารถนำมาใช้เพื่อช่วยระบุความผิดปกติในการรับส่งข้อมูลเครือข่าย และเพื่อระบุเส้นทางการโจมตีเฉพาะได้ ตัวอย่างเช่น การโจมตีรีเฟลกชัน UDP ส่วนใหญ่จะมีพอร์ตแหล่งที่มาเฉพาะ (เช่น พอร์ตแหล่งที่มา 53 สำหรับรีเฟลกชัน DNS) นี่เป็นลายเซ็นที่ชัดเจนที่คุณสามารถระบุในบันทึกล็อก Flow ได้ ในการตอบสนอง คุณอาจเลือกที่จะบล็อกพอร์ตแหล่งที่มาเฉพาะที่ระดับอินสแตนซ์ หรือสร้างกฎ ACL ของเครือข่ายเพื่อบล็อกโปรโตคอลทั้งหมด หากไม่มีการกำหนดไว้ว่าให้ทำเช่นนั้น

หากต้องการเรียนรู้เพิ่มเติมเกี่ยวกับการใช้ VPC Flow Log เพื่อระบุความผิดปกติของเครือข่ายและเส้นทางการโจมตีแบบ DDoS โปรดอ่าน VPC Flow Log[19] และ VPC Flow Log – บันทึกและดูโฟลว์การรับส่งข้อมูลเครือข่าย[20]

การสนับสนุน

คุณควรสร้างแผนการรับมือกับการโจมตีแบบ DDoS ก่อนเกิดเหตุการณ์ขึ้นจริง แนวทางปฏิบัติที่กล่าวไว้คร่าวๆ ในเอกสารฉบับนี้มีไว้เพื่อเป็นมาตรการล่วงหน้า และควรใช้ก่อนที่จะ

ใช้งานแอปพลิเคชันที่อาจตกเป็นเป้าของการโจมตีแบบ DDoS ทีมดูแลลูกค้าสามารถช่วยตรวจสอบกรณีปัญหาการใช้งานกับแอปพลิเคชัน และช่วยตอบคำถามหรือรับมือกับความท้าทายเฉพาะที่คุณอาจประสบ

บางครั้ง คุณอาจพบว่าการติดต่อ AWS เพื่อขอความช่วยเหลือเพิ่มเติมในช่วงที่มีการโจมตีแบบ DDoS นั้นก่อให้เกิดประโยชน์ AWS จะตอบกรณีปัญหาอย่างรวดเร็วและกำหนดเส้นทางกรณีปัญหาดังกล่าวไปยังผู้เชี่ยวชาญที่สามารถให้ความช่วยเหลือได้ เมื่อลงทะเบียนขอรับบริการช่วยเหลือทางธุรกิจ คุณจะสามารถติดต่อฝ่ายวิศวกรดูแล Cloud ทางอีเมล แชท หรือโทรศัพท์ได้ทุกวันตลอด 24 ชั่วโมง

หากคุณใช้งานเวิร์กโหลดที่สำคัญต่อการดำเนินงานบน AWS คุณควรลองพิจารณาติดต่อฝ่ายบริการช่วยเหลือองค์กร เมื่อติดต่อฝ่ายบริการช่วยเหลือองค์กร กรณีปัญหาเร่งด่วนจะได้รับความสำคัญสูงสุด และได้รับการกำหนดเส้นทางไปยังวิศวกรอาวุโสที่ดูแลระบบคลาวด์ นอกจากนี้ ฝ่ายบริการช่วยเหลือองค์กรยังให้คุณติดต่อผู้จัดการบัญชีฝ่ายเทคนิค (TAM) ได้ ซึ่งคอยทำหน้าที่ให้การสนับสนุนและรับติดต่อเกี่ยวกับปัญหาทางเทคนิค ฝ่ายบริการช่วยเหลือองค์กรยังให้คุณติดต่อฝ่ายบริหารจัดการกิจกรรมโครงสร้างพื้นฐานได้อีกด้วย ซึ่งคุณสามารถขอความช่วยเหลือเกี่ยวกับการดำเนินการแบบเรียลไทม์ในช่วงที่มีกิจกรรม การเปิดตัวผลิตภัณฑ์ และการโอนย้าย

หากต้องการเรียนรู้เพิ่มเติมเกี่ยวกับการเลือกแผนการช่วยเหลือให้ตรงกับความต้องการเฉพาะ โปรดอ่าน เปรียบเทียบแผน AWS Support[21]

บทสรุป

แนวทางปฏิบัติที่อธิบายไว้คร่าวๆ ในเอกสารฉบับนี้ช่วยให้คุณสร้างสถาปัตยกรรมที่มียืดหยุ่นต่อการโจมตีแบบ DDoS ได้ซึ่งสามารถป้องกันความพร้อมใช้งานของแอปพลิเคชันจากการโจมตีแบบ DDoS ที่โครงสร้างพื้นฐานและเลเยอร์แอปพลิเคชันหลายรูปแบบซึ่งพบเห็นได้ทั่วไป ระดับที่คุณสามารถออกแบบสถาปัตยกรรมให้กับแอปพลิเคชันตามแนวทางปฏิบัติเหล่านี้ได้จะมีผลต่อประเภท เส้นทาง และปริมาณของการโจมตีแบบ DDoS ที่คุณสามารถปรับลดได้ AWS แนะนำให้คุณใช้แนวทางปฏิบัติเหล่านี้เพื่อให้ป้องกันความพร้อมใช้งานของแอปพลิเคชันจากการโจมตีแบบ DDoS ที่พบเห็นได้ทั่วไปได้ดียิ่งขึ้น

ผู้ร่วมจัดทำ

บุคคลและหน่วยงานดังต่อไปนี้เป็นผู้ร่วมจัดทำเอกสารฉบับนี้:

- Andrew Kiggins สถาปนิกโซลูชันของ AWS
- Jeffrey Lyons วิศวกร AWS DDoS Ops

หมายเหตุ

[1] https://www.youtube.com/watch?v=OT2y3DzMEmQ

[2] https://www.youtube.com/watch?v=Ys0gG1koqJA

[3] https://aws.amazon.com/ec2/instance-types/

[4] http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/enhanced-networking.html

[5] http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html

[6] http://docs.aws.amazon.com/ElasticLoadBalancing/latest/DeveloperGuide/elb-getting-started.html

[7] http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/GettingStarted.html

[8] http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/getting-started.html

[9] http://docs.aws.amazon.com/Route53/latest/APIReference/actions-on-reusable-delegation-sets.html

[10] http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/georestrictions.html

[11] http://docs.aws.amazon.com/waf/latest/developerguide/getting-started.html

[12] http://docs.aws.amazon.com/waf/latest/developerguide/web-acl-testing.html#web-acl-testing-view-sample

[13] https://blogs.aws.amazon.com/security/post/Tx1ZTM4DT0HRH0K/How-to-Configure-Rate-Based-Blacklisting-with-AWS-WAF-and-AWS-Lambda

[14] http://docs.aws.amazon.com/autoscaling/latest/userguide/as-instance-monitoring.html

[15] https://blogs.aws.amazon.com/security/post/Tx1LPI2H6Q6S5KC/How-to-Automatically-Update-Your-Security-Groups-for-Amazon-CloudFront-and-AWS-W

[16] http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/forward-custom-headers.html

[17] https://aws.amazon.com/api-gateway/getting-started/

[18] http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/GettingStarted.html

[19] http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/flow-logs.html

[20] https://aws.amazon.com/blogs/aws/vpc-flow-logs-log-and-view-network-traffic-flows/

[21] https://aws.amazon.com/premiumsupport/compare-plans/