أفضل ممارسات AWS لمعدل مرونة DDoS

يونيو ٢٠١٦

إشعارات

هذا المستند مقدم لأغراض معلوماتية فقط. يحتوي على عروض منتجات AWS وممارساتها الحالية في تاريخ إصدار هذا المستند، والتي تخضع للتغيير دون إشعار مسبق. إن العملاء مسؤولون عن تقييمهم المستقل للمعلومات الموجودة في هذا المستند وعن أي استخدام لمنتجات AWS أو خدماتها، والتي تتاح كل منها "كما هي" بدون ضمان من أي نوع، سواء صريح أو ضمني. ولا يمثل هذا المستند أي ضمانات أو تمثيلاً أو التزامات تعاقدية أو شروطًا أو تأكيدات من AWS أو أي من الشركات التابعة لها أو مورديها أو الحاصلين على تراخيصها. وتتحكم اتفاقية AWS في مسؤوليات AWS والتزاماتها نحو عملائها، وهذا المستند ليس جزءًا من أي اتفاقية مبرمة بين AWS وعملائها كما لا يمثل تعديلاً لها.

المحتويات

الملخص

يهدف هذا المستند إلى مخاطبة العملاء الذين يرغبون في تحسين معدل مرونة التطبيقات التي تعمل على خدمات Amazon عبر الويب (AWS) مقابل هجمات رفض الخدمة الموزع (DDoS). ويوفر المستند نظرة عامة حول هجمات DDoS والقدرات الي توفرها AWS وأساليب التخفيف بالإضافة إلى تصميم مرجعي لمرونة مواجهة DDoS يمكن استخدامه كدليل للمساعدة في حماية توافر التطبيقات.

المقدمة

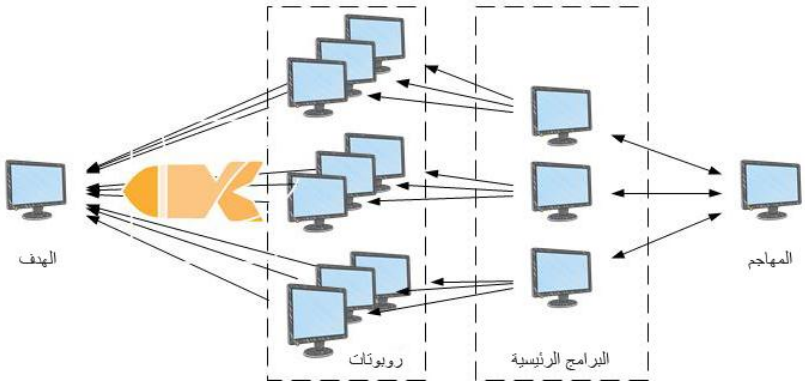
ويستهدف هذا المستند مخاطبة صناع قرارات تقنية المعلومات والمسؤولين عن الأمان الذين لديهم دراية بالمفاهيم الأساسية في مجال الشبكات والأمان وAWS. يتضمن كل قسم ارتباطات إلى وثائق AWS توفر المزيد من التفاصيل حول أفضل الممارسات أو القدرات. يمكنك أيضًا عرض جلستي عمل مؤتمر AWS re:Invent SEC307 – بناء تصميم مرجعي لمرونة مواجهة DDoS مع AWS[1] وSEC306 – الحماية من هجمات DDoS[2] للحصول على مزيد من المعلومات.

هجمات DDoS

إن هجمة رفض الخدمة (DoS) عبارة عن هجمة من شأنها أن تجعل موقع الويب أو التطبيق غير متوفر للمستخدمين النهائيين. ولتحقيق هذا الأمر، يستعين المهاجمون بمجموعة من الأساليب التي تستهلك الشبكة أو الموارد الأخرى، مما يؤدي إلى عرقلة وصول المستخدمين النهائيين المخولين. ويتم تنفيذ هجمة DoS، في أبسط شكل لها، ضد هدف من قِبل مهاجم واحد من مصدر فردي، كما هو موضح في الشكل ١.

الشكل ١: رسم بياني لهجمة DOS

عندما يتعلق الأمر بهجمة رفض الخدمة الموزع (DDoS)، يستخدم المهاجم مصادر متعددة – يمكن اختراقها أو التحكم فيها من خلال مجموعة من المتعاونين – لتنظيم هجمة ضد أحد الأهداف. وكما يوضح الشكل ٢، في هجمة DDoS، يشارك كل متعاون أو جهاز مضيف مخترق في الهجمة، مما يؤدي إلى إنشاء تدفق من حزم البيانات أو الطلبات للتسبب في إنهاك الهدف المستهدف.



الشكل ٢: رسم بياني لهجمة DDOS

تحدث هجمات DDoS الأكثر شيوعًا عند الطبقات ٣ و٤ و٦ و٧ من نموذج اتصال الأنظمة المفتوحة (OSI)، الذي تم وصفه في الجدول ١. وتتطابق الهجمات على الطبقتين ٣ و٤ مع طبقات Network and Transport (الشبكة والنقل) في نموذج OSI: ويشير هذا المستند إليها بالهجمات على طبقة البنية التحتية. أما الهجمات على الطبقتين ٦ و٧ فتتطابق مع طبقات Presentation and Application (التقديم والتطبيق) في نموذج OSI: ويشير هذا المستند إليها بالهجمات على طبقة التطبيق.

#	الطبقة	الوحدة	الوصف	أمثلة الموجهات
٧	التطبيق	بيانات	عملية الشبكة للتطبيق	تدفقات HTTP، تدفقات استعلام DNS
٦	التقديم	بيانات	تمثيل البيانات وتشفيرها	سوء استعمال SSL
٥	*جلسة العمل*	*بيانات*	*الاتصالات بين الأجهزة المضيفة*	*غير متوفر*
٤	النقل	أقسام	اتصالات بنظام نهاية إلى نهاية والموثوقية	تدفقات SYN
٣	الشبكة	حزم	تحديد المسار والعنونة المنطقية	هجمات انعكاس UDP
٢	*ارتباط البيانات*	*إطارات*	*العنونة الفعلية*	*غير متوفر*
١	*فعلية*	*البت*	*الإرسال عبر الوسائط والإشارات والإرسال الثنائي*	*غير متوفر*

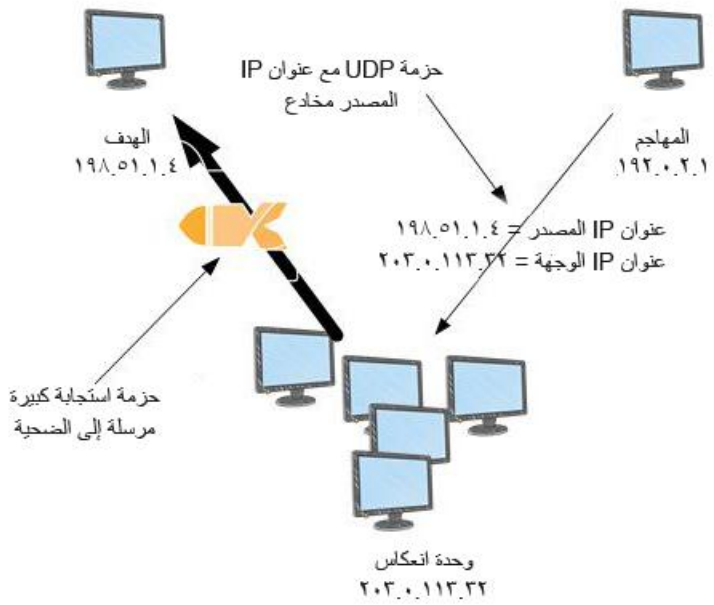
الجدول ١: نموذج اتصال الأنظمة المفتوحة (OSI)

يُعد هذا التمييز مهمًا نظرًا لاختلاف أنواع الهجمات الموجهة إلى هذه الطبقات، وبالتالي يتم استخدام أساليب مختلفة لبناء المرونة.

الهجمات على طبقة البنية التحتية

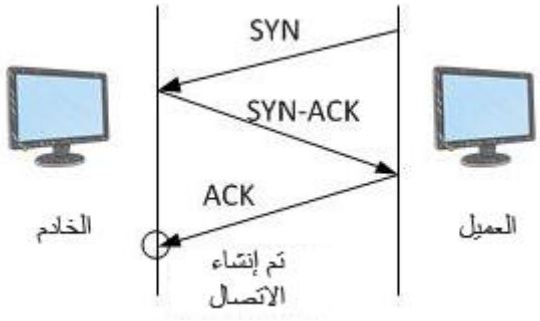
تُعد هجمات DDoS الأكثر شيوعًا، وهي هجمات انعكاس بروتوكول مخطط بيانات المستخدم (UDP) وتدفقات التزامن (SYN)، هجمات على طبقة البنية التحتية. باستطاعة المهاجم استخدام أي أسلوب من هذين الأسلوبين لتوليد أحجام كبيرة من عمليات النقل التي تؤدي إلى استنزاف سعة الشبكة أو النظام مثل الخادم أو جدار الحماية أو IPS أو موازن الحمل. وتتميز هذه الهجمات بتوقيعات واضحة مما يجعل الكشف عنها أكثر سهولة. يحتاج التخفيف الفعال لهذه الهجمات إلى موارد الشبكة أو النظام بما يتجاوز الحجم الذي يتم توليده بواسطة المهاجم.

إن بروتوكول UDP عبارة عن بروتوكول عديم الحالة. من شأن ذلك أن يسمح للمهاجم بانتحال مصدر الطلب المرسل إلى الخادم الذي يستدعي استجابة كبيرة. ويختلف عامل التضخيم، وهو نسبة حجم الطلب إلى حجم الاستجابة، استنادًا إلى البروتوكول المستخدم، مثل نظام أسماء المجالات (DNS) أو بروتوكول وقت الشبكة (NTP) أو بروتوكول اكتشاف الخدمات البسيطة (SSDP). على سبيل المثال، بإمكان نطاق عامل التضخيم لـ DNS أن يكون من ٢٨ إلى ٥٤ – مما يعني أن المهاجم يمكنه إرسال حمولة طلب بحجم ٦٤ بايت إلى خادم DNS وإنشاء عمليات نقل غير مطلوبة يزيد حجمها عن ٣٤٠٠ بايت. تم توضيح هذا المفهوم في الشكل ٣.



الشكل ٣: هجمة انعكاس UDP

بإمكان تدفقات SYN أن تكون تقريبًا بالعشرات من الغيغابت في الثانية، ولكن الهدف من الهجمة هو استنزاف موارد النظام المتوفرة من خلال ترك الاتصالات في حالة نصف مفتوحة. وكما تم توضيحه في الشكل ٤، عندما يتصل المستخدم النهائي بخدمة TCP، كخادم الويب مثلاً، سوف يرسل العميل حزمة SYN. سوف يرجع الخادم SYN-ACK وسوف يرجع العميل ACK، مما يؤدي إلى إكمال تأكيد الاتصال الثلاثي الاتجاه.



الشكل ٤: تأكيد الاتصال الثلاثي الاتجاه SYN

في تدفق SYN، لا يتم إرجاع ACK إطلاقًا، ويبقى الخادم منتظرًا الاستجابة. من شأن هذا الأمر أن يمنع المستخدمين الجدد من الاتصال بالخادم.

الهجمات على طبقة التطبيق

بطريقة أقل تكرارًا، قد يستهدف المهاجم التطبيق بحد ذاته مع الهجمة على الطبقة ٧ أو الهجمة على طبقة التطبيق. تختلف هذه الهجمات عن الهجمات على طبقة البنية التحتية لأن المهاجم يحاول تشغيل وظائف معينة خاصة بالتطبيق بشكل زائد بهدف جعله غير متوفر. وفي بعض الحالات، يمكن تحقيق ذلك من خلال أحجام طلبات منخفضة للغاية لا تؤدي إلى توليد حجم كبير من عمليات النقل على الشبكة. من شأن ذلك أن يجعل عملية الكشف عن الهجمة وتخفيفها أكثر صعوبة. تشتمل الأمثلة عن الهجمات على طبقة التطبيق تدفقات HTTP وهجمات cache-busting (لمنع المستعرض أو الوكيل من استخدام عنصر تم تحميله وتخزينه مؤقتًا) وتدفقات WordPress XML-RPC.

عندما يتعلق الأمر بتدفق HTTP، يرسل المهاجم طلبات HTTP تبدو وكأنها صادرة عن مستخدم حقيقي لتطبيق الويب. ستستهدف بعض تدفقات HTTP موردًا معينًا، في حين أن بعض تدفقات HTTP الأكثر تعقيدًا ستحاول محاكاة السلوك البشري. من شأن ذلك أن يزيد من صعوبة استخدام أساليب التخفيف الشائعة مثل تحديد معدل الطلبات. تُعد هجمات Cache-busting نوعًا من تدفقات HTTP يستخدم أشكالاً مختلفة في سلسلة الاستعلام لتجنب التخزين المؤقت لشبكة تسليم المحتوى (CDN) مما يؤدي إلى عمليات إحضار من الخادم الأصل، ويتسبب بالتالي في وضع ضغوط إضافية على خادم الويب الأصل.

عندما يتعلق الأمر بتدفق WordPress XML-RPC، والذي يُعرف أيضًا بتدفق pingback (الإعلام التلقائي بإنشاء ارتباط جديد) لـ WordPress، باستطاعة المهاجم إساءة استعمال وظيفة XML-RPC API لموقع ويب مستضاف على برنامج إدارة محتوى العلامة التجارية WordPress لتوليد تدفق من طلبات HTTP. تسمح ميزة pingback لموقع مستضاف على WordPress (الموقع أ) بإعلام موقع WordPress آخر (الموقع ب) بأن الموقع أ أنشأ ارتباطًا إلى الموقع ب. ونتيجة لذلك، سيحاول الموقع ب إحضار الموقع أ للتحقق من وجود الارتباط. فيما يتعلق بتدفق pingback، يسيء المهاجم استعمال هذه القدرة لكي يتسبب في قيام الموقع B بمهاجمة الموقع A. يتضمن هذا النوع من الهجمات توقيعًا واضحًا إذ يجب أن تكون الكلمة "WordPress" موجودة في "User-Agent" في رأس طلب HTTP.

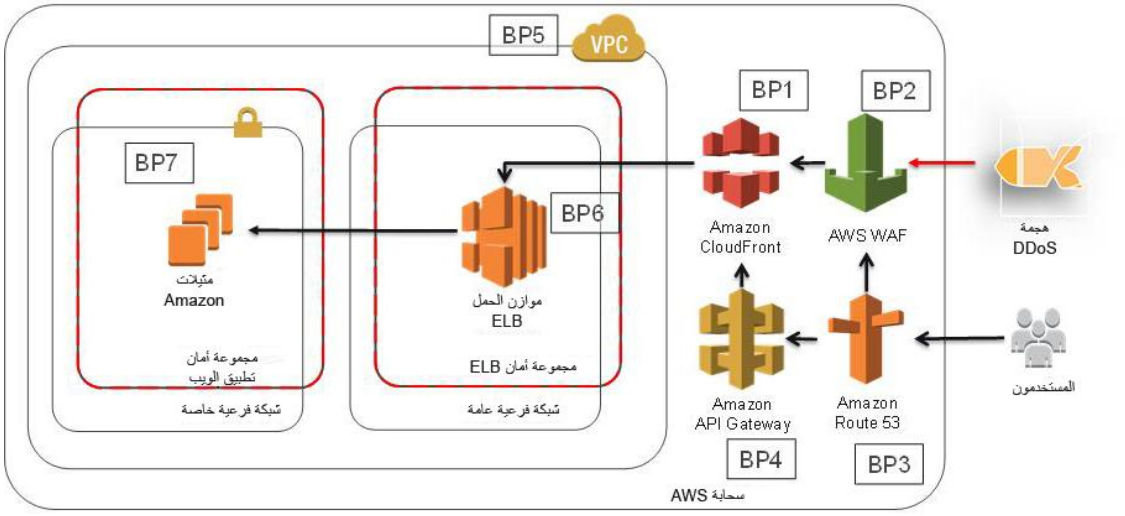
يمكن للهجمات على طبقة التطبيق أن تستهدف أيضًا خدمات نظام أسماء المجالات (DNS). ويُعتبر النوع الأكثر شيوعًا لهذه الهجمات تدفق استعلام DNS حيث يستخدم المهاجم عددًا كبيرًا من استعلامات DNS مشكّلة بطريقة جيدة لاستنزاف موارد خادم DNS. يمكن لهذه الهجمات أن تتضمن أيضًا مكون cache-busting حيث يختار المهاجم بشكل عشوائي سلسلة المجال الفرعي لتجاوز مخزن DNS المؤقت المحلي لأي محلل معين. ونتيجة لذلك، يتم تطويع المحلل للقيام بهجمة ضد خادم DNS الموثوق.

فيما يتعلق بتطبيقات الويب التي يتم تسليمها عبر طبقة مآخذ التوصيل الآمنة (SSL)، يستطيع المهاجم اختيار عملية مفاوضات SSL. تُعتبر SSL باهظة التكاليف من الناحية الحسابية، الأمر الذي يسمح للمهاجم بالتأثير على توافر الخادم عن طريق إرسال بيانات غامضة. تشتمل الأشكال الأخرى لهذه الهجمة على مهاجم يكمل عملية تأكيد اتصال SSL ولكنه يعيد التفاوض بشكل مستمر بشأن أسلوب التشفير. بطريقة مماثلة، يستطيع المهاجم استنزاف موارد الخادم عن طريق فتح عدد كبير من جلسات عمل SSL وإغلاقها.

أساليب التخفيف

تتميز بنية AWS التحتية بالمرونة في مواجهة DDoS بفضل تصميمها، وتدعمها أنظمة تخفيف هجمات DDoS التي يمكنها الكشف عن عمليات النقل الزائدة وتصفيتها بشكل تلقائي. ولكي تتمكن من حماية توافر تطبيقك، من الضروري تطبيق تصميم يسمح لك بالاستفادة من هذه القدرات.

إحدى حالات استخدام AWS الأكثر شيوعًا هي تطبيق ويب الذي يقدم محتوى ثابتًا وديناميكيًا للمستخدمين عبر الإنترنت. للاطلاع على تصميم مرجعي لمرونة مواجهة DDoS يُستخدم عادةً مع تطبيقات الويب، يمكنك مراجعة الشكل ٥.



الشكل ٥: التصميم المرجعي لمرونة مواجهة DDoS

يتضمن هذا التصميم المرجعي الكثير من خدمات AWS التي يمكنها مساعدتك في تحسين مرونة تطبيق الويب في التعامل مع هجمات DDoS. ويتم تعداد أفضل الممارسات في هذا التصميم لتسهيل الرجوع إليها إذ ستتم مناقشتها في المستند بكامله. على سبيل المثال، سيُشار إلى القسم الذي يناقش القدرات التي توفرها ميزة Amazon CloudFront بواسطة مؤشر أفضل الممارسات (على سبيل المثال، BP1). للاطلاع على ملخص لهذه الخدمات والقدرات التي تستطيع توفيرها، راجع الجدول ٢.

	مواقع حافة AWS			مناطق AWS		
	Amazon CloudFront مع AWS WAF (BP1 وBP2)	Amazon API Gateway (BP4)	Amazon Route 53 (BP3)	الموازنة المرنة للأحمال (BP6)	Amazon VPC (BP5)	Amazon EC2 مع التكيف التلقائي (BP7)
التخفيف من الهجمة على الطبقة ٣ (على سبيل المثال، انعكاس UDP)	✓	✓	✓	✓	✓	
التخفيف من الهجمة على الطبقة ٤ (على سبيل المثال، تدفق SYN)	✓	✓	✓	✓		
التخفيف من الهجمة على الطبقة ٦ (على سبيل المثال، SSL)	✓	✓	غير متوفر	✓		
تقليل مساحة سطح الهجمة	✓	✓	✓	✓	✓	
التكيف لامتصاص عمليات النقل على طبقة التطبيق	✓	✓	✓	✓		✓
التخفيف من الهجمة على الطبقة ٧ (طبقة التطبيق)	✓	✓	✓			
العزل الجغرافي وتشتت عمليات النقل الزائدة وهجمات DDoS أكبر حجمًا	✓	✓	✓			

الجدول ٢: ملخص أفضل الممارسات

تسمح لك الخدمات المتوفرة ضمن مناطق AWS، مثل الموازنة المرنة للأحمال وسحابة Amazon للحوسبة المرنة (EC2)، ببناء مرونة DDoS والتكيف للتعامل مع أحجام عمليات النقل غير المتوقعة ضمن منطقة معينة. أما الخدمات المتوفرة في مواقع حافة AWS، مثل Amazon CloudFront وAWS WAF و Amazon Route 53 وAmazon API Gateway، فتسمح لك بالاستفادة من شبكة عالمية من مواقع الحافة التي يمكنها أن تزوّد تطبيقك بمستوى أكبر من التسامح مع الخطأ ومستوى متزايد من التكيف لإدارة أحجام أكبر من عمليات النقل. سنناقش في الأقسام التالية فوائد استخدام كل خدمة من هذه الخدمات لبناء المرونة لمواجهة هجمات DDoS على طبقة البنية التحتية وطبقة التطبيق.

الدفاع عن طبقة البنية التحتية (BP1 وBP3 وBP6 وBP7)

في بيئة خاصة بمركز بيانات تقليدي، يمكنك تخفيف هجمات DDoS على طبقة البنية التحتية باستخدام بعض الأساليب مثل التزويد الزائد للسعة أو نشر أنظمة تخفيف هجمات DDoS أو تنظيف عمليات النقل من خلال المساعدة التي توفرها خدمات تخفيف هجمات DDoS. على AWS، لديك خيارات تسمح لك بتصميم تطبيقك لكي يكون قادرًا على التكيف مع أحجام أكبر من عمليات النقل وامتصاصها من دون استثمارات كبيرة في رأس المال أو تعقيدات غير ضرورية. تتضمن الاعتبارات الرئيسية المتعلقة بتخفيف هجمات DDoS الحجمية توفر سعة النقل وتنوعه وحماية موارد AWS مثل مثيلات Amazon EC2 من الهجمات التي تتعرض لها عمليات النقل.

حجم المثيل (BP7)

يستخدم الكثير من عملاء AWS خدمة Amazon EC2 لسعة الحوسبة القابلة لتغيير الحجم، مما يسمح لك بزيادة السعة أو خفضها بسرعة عندما تتغير متطلباتك. يمكنك التوسع أفقيًا عبر إضافة مثيلات إلى تطبيقك، كما تقتضي الحاجة. ويمكنك أيضًا أن تختار التوسع عموديًا باستخدام مثيلات كبيرة. يدعم بعض أنواع المثيلات ميزات، مثل واجهات شبكة ١٠ غيغابت والشبكة المحسنة التي يمكنها تحسين قدرتك على التعامل مع أحجام أكبر من عمليات النقل.

باستخدام واجهات شبكة ١٠ غيغابت، يستطيع كل مثيل دعم حجم أكبر من عمليات النقل. من شأن ذلك أن يساعد في منع ازدحام الشبكة نتيجة أي عملية نقل وصلت إلى مثيل Amazon EC2. توفر المثيلات التي تدعم ميزة الشبكة المحسنة مستوى أعلى من أداء الإدخال/الإخراج (I/O) واستهلاك أقل لوحدة المعالجة المركزية (CPU) مقارنةً بعمليات التنفيذ التقليدية. ويؤدي ذلك إلى تحسين قدرة المثيل على التعامل مع عملية نقل أكبر من حيث حجم الحزمة. على AWS، لن تتحمل مسؤولية تكلفة نقل البيانات الواردة.

لمعرفة المزيد حول مثيلات Amazon EC2 التي تدعم واجهات شبكة ١٠ غيغابت والشبكة المحسنة، راجع أنواع مثيلات Amazon EC2[٣]. لمعرفة كيفية تمكين الشبكة المحسنة، راجع تمكين الشبكة المحسنة على مثيلات Linux في VPC[٤].

اختيار المنطقة (BP7)

يتوفر الكثير من خدمات AWS، مثل Amazon EC2، في مواقع متعددة حول العالم. وتسمى هذه المناطق المنفصلة جغرافيًا مناطق AWS. عندما تعمل على تصميم تطبيقك، تتوفر لديك القدرة على اختيار منطقة واحدة أو أكثر استنادًا إلى متطلباتك. تشتمل الاعتبارات الشائعة على الأداء والتكلفة وسيادة البيانات. في كل منطقة، توفر AWS إمكانية الوصول إلى مجموعة فريدة من اتصالات الإنترنت وعلاقات النظراء التي تسمح بالحصول على زمن انتقال ومعدل نقل مثاليين للمستخدمين المتواجدين بمنطقة مماثلة.

علاوةً على ذلك، يُعتبر اختيار المنطقة مهمًا على صعيد مرونة DDoS. هناك مناطق كثيرة تكون أقرب إلى نقاط تبادل إنترنت كبيرة. وهناك الكثير من هجمات DDoS عالمية المصدر، وبالتالي من المفيد التواجد على مقربة من نقاط التبادل حيث تحتفظ شركات الاتصالات العالمية والشركات النظيرة الكبرى بحضور قوي. من شأن ذلك أن يساعد المستخدمين النهائيين على الوصول إلى تطبيقك عند التعامل مع أحجام أكبر من عمليات النقل.

لمعرفة المزيد حول اختيار منطقة، راجع المناطق ومناطق التوافر[٥] واسأل فريق حسابك عن خصائص كل منطقة لمساعدتك في اتخاذ القرار الصائب.

موازنة الأحمال (BP6)

باستطاعة هجمات DDoS الكبيرة أن تتجاوز حجم مثيل Amazon EC2 واحد. وللتخفيف من هذه الهجمات، يمكنك الاستعانة بخيارات تتعلق بموازنة أحمال عمليات النقل الزائدة. من خلال الموازنة المرنة للأحمال (ELB)، يمكنك التخفيف من مخاطر التحميل الزائد للتطبيق عن طريق توزيع عمليات النقل عبر عدد كبير من المثيلات الخلفية. باستطاعة ELB التكيف تلقائيًا، مما يسمح لك بإدارة أحجام أكبر من عمليات نقل غير متوقعة، مثل التدفق المفاجئ والضخم لعمليات النقل أو هجمات DDoS.

يقبل ELB اتصالات TCP المشكّلة بطريقة جيدة فقط. وهذا يعني أن ELB لن يقبل الكثير من هجمات DDoS الشائعة، مثل تدفقات SYN أو تدفقات انعكاس UDP، ولن يتم تمرير هذه الهجمات إلى تطبيقك. عندما يكشف ELB عن أنواع هذه الهجمات، سوف يتكيف تلقائيًا لامتصاص عمليات النقل الإضافية ولكنك لن تتكبد أي مصروفات إضافية.

لمعرفة المزيد حول استخدام ELB لتوزيع الأحمال ولحماية مثيلات Amazon EC2، راجع بدء استخدام الموازنة المرنة للأحمال[٦].

التسليم على نطاق واسع باستخدام مواقع حافة AWS (BP1 وBP3)

قد يؤدي الوصول إلى اتصالات إنترنت متدرجة ومتنوعة إلى زيادة قدرتك على تحسين زمن الانتقال ومعدل النقل للمستخدمين النهائيين بشكل ملحوظ وامتصاص هجمات DDoS وعزل الأخطاء مع تقليل التأثير على التوفر. توفر مواقع حافة AWS طبقة إضافية من البنية التحتية للشبكة التي توفر هذه الفوائد لتطبيقات الويب التي تستخدم Amazon CloudFront وAmazon Route 53. ومن خلال هذه الخدمات، يتم تقديم المحتوى التابع لك ويتم حل استعلامات DNS من مواقع تكون في أغلب الأحيان قريبة من المستخدمين النهائيين.

تسليم تطبيق الويب عند الحافة (BP1)

إن Amazon CloudFront عبارة عن خدمة لشبكة تسليم المحتوى (CDN) يمكن استخدامها لتسليم موقعك على الويب بأكمله، بما في ذلك المحتوى الديناميكي والثابت والمتدفق والتفاعلي. ويمكن استخدام اتصالات TCP الدائمة ومدة البقاء (TTL) المتغيرة لتسريع عملية تسليم المحتوى، حتى لو تعذر تخزينه مؤقتًا في موقع الحافة. ويسمح لك ذلك باستخدام Amazon CloudFront لحماية تطبيق الويب، حتى لو كنت لا تقدم محتوىً ثابتًا. تقبل خدمة Amazon CloudFront الاتصالات المشكّلة بطريقة جيدة فقط بهدف منع الكثير من هجمات DDoS الشائعة، مثل تدفقات SYN وهجمات انعكاس UDP، من الوصول إلى الخادم الأصل. يتم عزل هجمات DDoS جغرافيًا بالقرب من المصدر، مما يحول دون تأثير عمليات النقل على المواقع الأخرى. باستطاعة هذه القدرات أن تحسّن كثيرًا من قدرتك على متابعة التعامل مع عمليات النقل إلى المستخدمين النهائيين أثناء وقوع هجمات DDoS كبيرة. ويمكنك استخدام Amazon CloudFront لحماية الخادم الأصل على AWS أو في أي مكان آخر على الإنترنت.

لمعرفة المزيد حول تحسين أداء تطبيقات الويب باستخدام Amazon CloudFront، راجع بدء استخدام CloudFront[٧].

حل اسم المجال على الحافة (BP3)

إن Amazon Route 53 عبارة عن خدمة لنظام أسماء المجالات (DNS) قابلة للتكيف ومتوفرة على مستوى عالٍ يمكن استخدامها لتوجيه عمليات النقل إلى تطبيق الويب. وتتضمن هذه الخدمة الكثير من الميزات المتقدمة مثل تدفق عمليات النقل والتوجيه القائم على وقت الانتقال وDNS الجغرافي وعمليات فحص السلامة والمراقبة. تسمح لك هذه الميزات بالتحكم في طريقة استجابة الخدمة لطلبات DNS من أجل تحسين وقت الانتقال والسلامة واعتبارات أخرى. ويمكنك استخدام هذه الميزات لتحسين أداء تطبيق الويب ولتفادي حالات انقطاع العمل بالموقع.

تستخدم ميزة Amazon Route 53 إمكانيتي خلط التفكيك وتوجيه قدرة الاتصال الفردية لتمكين المستخدمين النهائيين من الوصول إلى التطبيق، حتى في حال استهدفت هجمة DDoS خدمة DNS. باستخدام خلط التفكيك، يتطابق كل خادم اسم في مجموعات تفويضاتك مع مجموعة فريدة من مواقع الحافة ومسارات الإنترنت. يؤدي ذلك إلى توفير مستوى أكبر من التسامح مع الخطأ وإلى تقليل التداخل بين العملاء. إذا لم يتوفر خادم اسم في مجموعة التفويضات، فباستطاعة المستخدمين النهائيين إعادة المحاولة والحصول على استجابة من خادم اسم آخر في موقع حافة مختلف. يتم استخدام إمكانية توجيه قدرة الاتصال الفردية لكي يتم التعامل مع كل طلب DNS من قِبل الموقع الذي يتسم بأكبر مستوى من المثالية. يتميز ذلك بتأثير توزيع الحمل وتقليل زمن انتقال DNS، مما يسمح للمستخدمين النهائيين بتلقي الاستجابة بشكل أسرع. علاوةً على ذلك، باستطاعة Amazon Route 53 الكشف عن حالات الشذوذ في المصدر وحجم طلبات DNS وتحديد أولويات الطلبات الصادرة عن مستخدمين معروفين بموثوقيتهم.

إذا كان لديك الكثير من المناطق المستضافة على Amazon Route 53، فيمكنك إنشاء مجموعة تفويضات قابلة لإعادة الاستخدام ستعمل على تزويدك بالمجموعة نفسها من خوادم الأسماء الموثوقة لكل مجال. من شأن هذه المجموعة أن تساعدك في المحافظة على مناطقك المستضافة. وهي تسمح أيضًا لـ AWS بتطبيق عملية تخفيف واحدة تغطي أي منطقة مستضافة يتم فيها استخدام مجموعة التفويضات، وذلك عند وقوع هجمة DDoS.

لمعرفة المزيد حول استخدام Amazon Route 53 لتوجيه المستخدمين النهائيين إلى تطبيقك، راجع بدء استخدام Amazon Route 53[٨]. لمعرفة المزيد حول مجموعات التفويضات القابلة لإعادة الاستخدام، راجع إجراءات على مجموعات التفويضات القابلة لإعادة الاستخدام[٩].

الدفاع عن طبقة التطبيق (BP1 وBP2 وBP6)

يناقش هذا المستند عددًا كبيرًا من الأساليب التي تُعتبر فعالة في تخفيف التأثير الناتج عن هجمات DDoS على طبقة البنية التحتية. يتطلب منك الدفاع عن التطبيق من الهجمات على طبقة التطبيق تنفيذ تصميم يسمح لك بالكشف عن الطلبات الضارة والتكيف لامتصاصها وحظرها. ويمكن اعتبار ذلك فكرة مهمة لأن أنظمة تخفيف هجمات DDoS القائمة على الشبكة تعتبر عادةً غير فعالة على صعيد تخفيف الهجمات المعقدة على طبقة التطبيق.

الكشف عن طلبات الويب الضارة وتصفيتها (BP1 وBP2)

تُستخدم جدران حماية تطبيقات الويب (WAF) في الكثير من الأحيان لحماية تطبيقات الويب من الهجمات التي تحاول استغلال الثغرات الأمنية الموجودة في التطبيق. وتشتمل الأمثلة الشائعة حقن SQL أو تزييف الطلبات بين التطبيقات. يمكنك أيضًا استخدام WAF للكشف عن هجمات DDoS على طبقة تطبيق الويب وتخفيفها.

على AWS، يمكنك استخدام Amazon CloudFront وAWS WAF للدفاع عن التطبيق في مقابل هذه الهجمات. تسمح لك ميزة Amazon CloudFront بتخزين المحتوى الثابت بشكل مؤقت وتقديمه من مواقع حافة AWS التي يمكنها أن تساعد في تخفيف الحمل على الخادم الأصل. علاوةً على ذلك، باستطاعة ميزة Amazon CloudFront إغلاق الاتصالات بشكل تلقائي من مهاجمين لديهم سرعة قراءة أو سرعة كتابة بطيئة (على سبيل المثال، Slowloris). ويمكنك استخدام التقييد الجغرافي في Amazon CloudFront لمنع المستخدمين في مناطق جغرافية معينة من الوصول إلى المحتوى. بإمكان هذا الأمر أن يكون مفيدًا إذا أردت حظر الهجمات الصادرة من مواقع جغرافية لا تتوقع فيها التعامل مع مستخدمين نهائيين.

بالنسبة إلى أنواع الهجمات الأخرى، مثل تدفقات HTTP أو تدفقات pingback لـ WordPress، يمكنك استخدام AWS WAF لإنشاء عمليات تخفيف خاصة بك. إذا كنت تعرف عناوين IP المصدر التي تريد حظرها، فيمكنك إنشاء قاعدة تتضمن إجراء الحظر وربطها بقائمة التحكم بالوصول (ACL) إلى الويب. ويمكنك عندئذٍ إنشاء شرط مطابقة عناوين IP في قائمة التحكم بالوصول (ACL) إلى الويب لحظر عناوين IP المصدر التي تشارك في الهجمة. ويمكنك أيضًا إنشاء قواعد مع شروط لإجراء الحظر حسب URI أو سلسلة الاستعلام أو أسلوب HTTP أو مفتاح الرأس. ويعتبر هذا الأخير مفيدًا عند وقوع هجمات تحمل توقيعات واضحة. على سبيل المثال، ستتضمن دائمًا هجمة pingback لـ WordPress الكلمة "WordPress" في User-Agent.

قد يكون من الصعب التعرّف على توقيع هجمة DDoS أو التعرّف بدقة على عناوين IP المشاركة في الهجمة. وفي بعض الأحيان، يمكن العثور على هذه المعلومات عبر مراجعة سجلات خادم الويب. يمكنك أيضًا استخدام وحدة تحكم AWS WAF لعرض عينة من الطلبات التي أعادت ميزة Amazon CloudFront توجيهها إلى AWS WAF. باستطاعة عينات الطلبات أن تساعدك في تحديد القواعد التي قد تكون ضرورية لتخفيف الهجمات على طبقة التطبيق. إذا رأيت الكثير من الطلبات مع سلسلة استعلام عشوائية، فقد تقرر تعطيل إعادة توجيه سلسلة الاستعلام في Amazon CloudFront. وبإمكان هذا الأمر أن يكون مفيدًا في التخفيف من هجمة cache-busting على الخادم الأصل.

تتكوّن بعض الهجمات من عمليات نقل على الويب تتخفى لكي تبدو مماثلة لعمليات النقل العادية الخاصة بالمستخدم النهائي. للتخفيف من هذا النوع من الهجمات، يمكنك استخدام وظيفة AWS Lambda لتطبيق قائمة الحظر التي تستند إلى معدل. من خلال قائمة الحظر التي تستند إلى معدل، يمكنك تعيين الحد الأقصى لعدد الطلبات التي يمكن لتطبيق الويب التعامل معها. وإذا قام روبوت أو متتبع الارتباطات بتجاوز هذا الحد، فيمكنك استخدام AWS WAF لحظر أي طلبات إضافية بشكل تلقائي.

لمعرفة المزيد حول استخدام التقييد الجغرافي للحد من الوصول إلى توزيع Amazon CloudFront، راجع تقييد التوزيع الجغرافي للمحتوى[١٠].

لمعرفة المزيد حول استخدام AWS WAF، راجع بدء استخدام AWS WAF[١١] وعرض عيّنة من طلبات الويب التي أعادت ميزة CloudFront توجيهها إلى AWS WAF[١٢].

لمعرفة كيفية تكوين قائمة الحظر التي تستند إلى معدل باستخدام وظيفة AWS Lambda وAWS WAF، راجع كيفية تكوين قائمة الحظر التي تستند إلى معدل باستخدام AWS WAF وAWS Lambda[١٣].

التكيف لامتصاص الهجمة (BP6)

هناك طريقة أخرى للتعامل مع الهجمات على طبقة التطبيق وهي التشغيل من خلال التكيف. عندما يتعلق الأمر بتطبيقات الويب، يمكنك استخدام الموازنة المرنة للأحمال (ELB) لتوزيع عمليات النقل على عدد كبير من مثيلات Amazon EC2 ذات التزويد الزائد أو التي تم تكوينها للتكيف التلقائي بغرض التعامل مع حالات تدفق عمليات النقل، سواء كان ذلك نتيجة التدفق المفاجئ والضخم لعمليات النقل أو هجمة DDoS على طبقة التطبيق. يتم استخدام تنبيهات Amazon CloudWatch لبدء التكيف التلقائي، الذي يكيف تلقائيًا حجم مجموعة Amazon EC2 كبيرة في إطار الاستجابة للأحداث التي تحددها أنت. ويؤدي ذلك إلى حماية توافر التطبيق عند التعامل مع حجم طلبات غير متوقع. من خلال استخدام Amazon CloudFront أو ELB، يتم التعامل مع مفاوضات SSL من قِبل موازن التوزيع أو الحمل، الذي يمكنه منع تأثر المثيلات بالهجمات التي تستند إلى SSL.

لمعرفة المزيد حول استخدام Amazon CloudWatch لاستدعاء التكيف التلقائي، راجع مراقبة مثيلات ومجموعات التكيف التلقائي باستخدام Amazon CloudWatch[١٤].

تقليل مساحة سطح الهجمة

هناك فكرة مهمة أخرى يجب أخذها في الاعتبار عند التصميم على AWS وهي الحد من الفرص التي قد تسمح للمهاجم باستهداف تطبيقك. على سبيل المثال، إذا لم تتوقع أن يتفاعل المستخدم النهائي مع بعض الموارد بشكل مباشر، فعليك أن تتأكد من أنه يتعذر الوصول إلى هذه الموارد من الإنترنت. بطريقة مماثلة، إذا لم تتوقع حدوث تواصل بين المستخدمين النهائيين أو التطبيقات الخارجية من جهة مع تطبيقك من جهة أخرى على بعض المنافذ أو البروتوكولات، فعليك أن تتأكد من عدم الموافقة على عملية النقل. يُعرف هذا المفهوم بتقليل مساحة سطح الهجمة. سوف تعثر في هذا القسم على أفضل الممارسات التي تسمح لك بتقليل مساحة سطح الهجمة وتحديد المدى الذي يمكن من خلاله تعريض تطبيقك للإنترنت. تجدر الإشارة إلى أن مهاجمة الموارد التي لا يتم تعريضها للإنترنت تكون أصعب، مما يؤدي بدوره إلى الحد من الخيارات التي قد تتوفر للمهاجم لاستهداف توافر تطبيقك.

إخفاء موارد AWS (BP1 وBP4 وBP5)

بالنسبة إلى الكثير من التطبيقات، من غير الضروري تعريض موارد AWS للإنترنت بشكل كامل. على سبيل المثال، قد لا يكون من الضروري أن يكون الوصول إلى مثيلات Amazon EC2 خلف ELB متوفرًا بشكل عام. في هذا السيناريو، قد تقرر السماح للمستخدمين النهائيين بالوصول إلى ELB على بعض منافذ TCP وتمكين ELB فقط من التواصل مع مثيلات Amazon EC2. ويمكن تحقيق هذا الأمر عن طريق تكوين مجموعات أمان وقوائم التحكم بالوصول إلى الشبكة (NACL) ضمن سحابة Amazon الخاصة الافتراضية (VPC). تسمح لك Amazon VPC بتزويد قسم معزول منطقيًا من سحابة AWS حيث يمكنك تشغيل موارد AWS في شبكة افتراضية تحددها أنت.

تُعد مجموعات الأمان وقوائم التحكم بالوصول (ACL) إلى الشبكة مماثلة من حيث أنها تسمح لك بالوصول إلى موارد AWS ضمن VPC. وتسمح لك مجموعات الأمان بالتحكم في عمليات النقل الواردة والصادرة على مستوى المثيل وتوفر قوائم التحكم بالوصول إلى الشبكة قدرات مماثلة، ولكن على مستوى شبكة VPC الفرعية. علاوةً على ذلك، لا يتم تطبيق الرسوم على عملية نقل البيانات الواردة على قواعد مجموعة أمان Amazon EC2 أو قوائم التحكم بالوصول إلى الشبكة. ويضمن لك ذلك عدم تكبد أي مصروفات إضافية لعمليات النقل التي تسجلها مجموعات الأمان أو قوائم التحكم بالوصول إلى الشبكة.

مجموعات الأمان (BP5)

يمكنك تعيين مجموعات الأمان عند تشغيل مثيل أو ربط المثيل بمجموعة أمان في وقت لاحق. يتم رفض كل عمليات النقل إلى مجموعة أمان من الإنترنت بشكل ضمني إلا إذا أنشأت قاعدة *السماح* للسماح بعملية النقل. على سبيل المثال، إذا كان لديك تطبيق ويب يتكون من ELB ومثيلات Amazon EC2 متعددة، فقد تقرر إنشاء مجموعة أمان لـ ELB ("مجموعة أمان ELB") ومجموعة أمان للمثيلات ("مجموعة أمان خادم تطبيق الويب"). ويمكنك عندئذٍ إنشاء قواعد *السماح* للسماح بعملية نقل من الإنترنت إلى مجموعة أمان ELB وللسماح بعملية نقل من مجموعة أمان ELB إلى مجموعة أمان خادم تطبيق الويب. ونتيجة ذلك، يتعذر على عملية النقل من الإنترنت التواصل بشكل مباشر مع مثيلات Amazon EC2، مما يزيد من صعوبة التعرف على تطبيقك من قِبل المهاجم.

قوائم التحكم بالوصول إلى الشبكة (ACL) (BP5)

من خلال قوائم التحكم بالوصول إلى الشبكة، يمكنك تحديد قواعد *السماح* و*الرفض* على حدٍ سواء. ويُعد هذا الأمر مفيدًا عندما تريد رفض بعض أنواع عمليات النقل إلى تطبيقك بشكل واضح. على سبيل المثال، يمكنك تحديد عناوين IP (مثل نطاقات CIDR) والبروتوكولات ومنافذ الوجهة التي يجب رفضها للشبكة الفرعية بكاملها. إذا تم استخدام تطبيقك لعملية نقل عبر بروتوكول TCP فقط، فيمكنك إنشاء قاعدة مهمتها *رفض* كل عملية نقل عبر بروتوكول UDP أو العكس بالعكس. وتكون هذه الأداة مفيدة عند الاستجابة لهجمات DDoS إذ يمكنها أن تسمح لك بإنشاء قواعدك الخاصة لتخفيف الهجمة إذا كنت تعرف عناوين IP المصدر أو أي توقيع آخر.

حماية الخادم الأصل (BP1)

إذا كنت تستخدم Amazon CloudFront مع خادم أصل يقع داخل VPC، فيجب استخدام وظيفة AWS Lambda لتحديث قواعد مجموعة الأمان بشكل تلقائي من أجل *السماح* بعمليات النقل فقط من Amazon CloudFront. من شأن ذلك أن يؤدي إلى تحسين أمان الخادم الأصل عن طريق المساعدة في ضمان عدم تجاوز Amazon CloudFront وAWS WAF.

لمعرفة المزيد عن كيفية حماية الخادم الأصل عن طريق تحديث مجموعات الأمان بشكل تلقائي، راجع كيفية تحديث مجموعات الأمان بشكل تلقائي لكل من Amazon CloudFront وAWS WAF باستخدام AWS Lambda[١٥].

قد تحتاج أيضًا إلى ضمان قيام توزيع Amazon CloudFront فقط بإعادة توجيه الطلبات إلى الخادم الأصل. من خلال رؤوس طلبات Edge-to-Origin، يمكنك إضافة قيمة رؤوس الطلبات الموجودة أو تجاوزها عندما تعيد Amazon CloudFront توجيه الطلبات إلى الخادم الأصل. يمكنك استخدام الرأس *X-Shared-Secret* للمساعدة في التحقق من أن إرسال الطلبات الموجهة إلى الخادم الأصل قد تم من Amazon CloudFront.

لمعرفة المزيد حول حماية الخادم الأصل بواسطة الرأس *X-Shared-Secret*، راجع إعادة توجيه الرؤوس المخصصة إلى الخادم الأصل[١٦].

حماية نقاط نهاية API (BP4)

عادةً، عندما توجد حاجة لعرض واجهة برمجة التطبيقات (API) أمام الجمهور، هناك خطر يتمثل في احتمال استهداف واجهة API الأمامية بهجمة DDoS. تسمح لك Amazon API Gateway، وهي خدمة مُدارة بشكل كامل، بإنشاء API تعمل بصيغة "بوابة أمامية" للتطبيقات التي يتم تشغيلها على Amazon EC2 أو AWS Lambda أو أي تطبيق ويب. باستخدام Amazon API Gateway، لن تحتاج إلى تشغيل خوادمك الخاصة لواجهة API الأمامية، ويمكنك إخفاء المكونات الأخرى لتطبيقك عن الجمهور. بإمكان ذلك أن يمنع استهداف موارد AWS من قِبل هجمة DDoS. تتكامل خدمة Amazon API Gateway مع Amazon CloudFront، مما يسمح لك بالاستفادة من مرونة DDoS المضافة الملازمة لهذه الخدمة. يمكنك أيضًا حماية الواجهة الخلفية من عمليات النقل المتزايدة من خلال تكوين حدود قياسية أو حدود لمعدل الاندفاع لكل أسلوب في REST API.

لمعرفة المزيد حول إنشاء واجهات برمجة التطبيقات (API) باستخدام Amazon API Gateway، راجع بدء استخدام Amazon API Gateway[١٧].

الأساليب التشغيلية

تسمح لك أساليب التخفيف التي ورد ذكرها في هذا المستند بتصميم تطبيقات تتمتع بمرونة متلازمة في التعامل مع هجمات DDoS. في حالات كثيرة، من المفيد أيضًا معرفة متى تستهدف هجمات DDoS تطبيقك وأن تكون قادرًا على اتخاذ الإجراء المناسب على هذه البيانات. قد تحتاج أيضًا إلى مشاركة موارد إضافية لتقييم تهديد أو مراجعة تصميم تطبيقك أو لطلب مساعدة أخرى. يصف هذا القسم أفضل الممارسات للحصول على قابلية رؤية السلوك الشاذ والتنبيه والتنفيذ التلقائي ومشاركة AWS للحصول على دعم إضافي.

قابلية الرؤية

يساعدك فهم السلوك العادي لتطبيقك في اتخاذ الإجراء المناسب بسرعة أكبر عندما تكشف عن وجود حالة شاذة. عندما ينحرف قياس أساسي بشكل ملحوظ عن القيمة المتوقعة، يمكن اعتبار ذلك بمثابة إشارة إلى أن المهاجم قد يكون بصدد محاولة استهداف توافر تطبيقك. باستخدام Amazon CloudWatch، يمكنك مراقبة التطبيقات التي يتم تشغيلها على AWS. وتسمح لك هذه الميزة بتجميع القياسات وتتبعها ومراقبة ملفات السجلات وتعيين التنبيهات والتفاعل بشكل تلقائي مع التغييرات في موارد AWS. للحصول على وصف لقياسات Amazon CloudWatch المستخدمة عادةً للكشف عن هجمات DDoS والتفاعل معها، راجع الجدول ٣.

الموضوع	القياس	الوصف
التكيف التلقائي	GroupMaxSize	الحد الأقصى لحجم مجموعة التكيف التلقائي.
Amazon CloudFront	الطلبات	عدد طلبات HTTP/S.
Amazon CloudFront	TotalErrorRate	نسبة جميع الطلبات التي تم تعيين رمز حالة HTTP لها إلى 4xx أو 5xx
Amazon EC2	CPUUtilization	نسبة وحدات حساب EC2 الموجودة قيد الاستخدام حاليًا
Amazon EC2	NetworkIn	عدد وحدات البايت المستلمة على جميع واجهات الشبكة بواسطة المثيل
ELB	SurgeQueueLength	عدد الطلبات الموضوعة في قائمة الانتظار من قِبل موازن الحمل، والتي تنتظر قيام مثيل خلفي بقبول الاتصالات ومعالجة الطلب.
ELB	UnHealthyHostCount	عدد المثيلات غير السليمة في كل منطقة توافر.
ELB	RequestCount	عدد الطلبات المكتملة التي تم استلامها وتوجيهها إلى المثيلات المسجلة
ELB	زمن الانتقال	الوقت المنقضي، بالثواني، بعد أن يغادر الطلب موازن الحمل إلى أن يتم استلام استجابة
ELB	HTTPCode_ELB_4xx HTTPCode_ELB_5xx	رقم رمزي الخطأ HTTP 4xx أو 5xx اللذين أنشأهما موازن الحمل
ELB	BackendConnectionErrors	عدد الاتصالات الفاشلة
ELB	SpilloverCount	عدد الطلبات المرفوضة بسبب امتلاء قائمة الانتظار
Amazon Route 53	HealthCheckStatus	حالة نقطة نهاية فحص السلامة

الجدول ٣: قياسات Amazon CloudWatch الموصى بها

بالنسبة إلى تطبيق مصمم وفقًا للتصميم المرجعي لمرونة مواجهة DDoS الذي تم توفيره في الشكل ٥، سيتم حظر الهجمات الشائعة على طبقة البنية التحتية قبل أن تصل إلى تطبيقك. ونتيجة لذلك، لن تظهر هذه الهجمات في قياسات Amazon CloudWatch.

قد يتسبب وقوع هجمة على طبقة التطبيق في حدوث ارتفاعات في الكثير من هذه القياسات. على سبيل المثال، قد يتسبب تدفق HTTP في حدوث ارتفاعات في الطلبات ومستوى استخدام CPU والشبكة لقياسات كل من Amazon CloudFront وELB وAmazon EC2 إذا تعذر على المثيلات الخلفية التعامل مع هذه الطلبات الزائدة، فقد تشهد أيضًا ارتفاعات في TotalErrorRate على Amazon CloudFront وSurgeQueueLength أو UnHealthyHostCount أو Latency أو BackendConnectionErrors أو SpilloverCount أو HTTPCode على ELB. وفي هذه الحالة، قد ينخفض حجم طلبات HTTP نظرًا لعدم قدرة التطبيق على التعامل مع المستخدمين النهائيين

العاديين. ويمكنك معالجة هذه الحالة عن طريق تكييف واجهة التطبيق الخلفية أو حظر عمليات النقل المتزايدة مع AWS WAF كما تمت مناقشته في قسم سابق من هذا المستند.

لمعرفة المزيد حول استخدام Amazon CloudWatch للكشف عن هجمات DDoS على تطبيقك، راجع بدء استخدام Amazon CloudWatch[١٨].

هناك أداة أخرى يمكنك استخدامها تسمح لك برؤية عمليات النقل التي تستهدف تطبيقك وهي سجلات تدفق VPC. على الشبكة التقليدية، يمكنك استخدام سجلات تدفق الشبكة لاستكشاف مشاكل الاتصال والأمان وإصلاحها، وللتأكد من عمل قواعد الوصول إلى الشبكة كما هو متوقع. باستخدام سجلات تدفق VPC، يمكنك التقاط معلومات حول عملية النقل إلى عنوان IP التي تذهب إلى واجهات الشبكة ومنها في VPC.

يتضمن كل سجل تدفق عناوين IP المصدر والوجهة ومنافذ المصدر والوجهة والبروتوكول وعدد الحزم ووحدات البايت المنقولة عبر نافذة الالتقاط. ويمكن استخدام هذه المعلومات للمساعدة في التعرّف على حالات الشذوذ في عمليات النقل إلى الشبكة وعلى موجه المهاجمة المحدد. على سبيل المثال، هناك منافذ محددة لمعظم هجمات انعكاس UDP (على سبيل المثال، المنفذ المصدر ٥٣ لانعكاس DNS). يمكنك اعتبار ذلك بمثابة توقيع واضح يمكن التعرّف عليه في سجل التدفق. وفي إطار الاستجابة، يمكنك أن تختار حظر المنفذ المصدر المحدد على مستوى المثيل أو إنشاء قاعدة تحكم بالوصول إلى الشبكة لحظر البروتوكول بكامله إذا لم يكن ضروريًا.

لمعرفة المزيد حول استخدام سجلات تدفق VPC للتعرّف على الحالات الشاذة في الشبكة وموجهات هجمات DDoS، راجع سجلات تدفق VPC[١٩] وسجلات تدفق VPC – تسجيل تدفقات عمليات النقل إلى الشبكة وعرضها[٢٠]

الدعم

من الضروري إنشاء خطة لمواجهة هجمات DDoS قبل وقوع حدث فعلي. تم وضع أفضل الممارسات المشار إليها في هذا المستند لكي تكون تدابير استباقية، ويجب تنفيذها قبل إطلاق تطبيق من المحتمل أن تستهدفه هجمة DDoS. باستطاعة فريق حسابك أن يساعدك في مراجعة حالة الاستخدام والتطبيق ومساعدتك عبر الرد على أي أسئلة معينة أو معالجة الصعوبات التي قد تواجهها.

في بعض الأحيان، قد يتبين لك أنه من المفيد التواصل مع AWS للحصول على دعم إضافي أثناء وقوع هجمة DDoS. وسيتم الرد على حالتك بسرعة وسيتم توجيهها إلى خبير قادر على مساعدتك. من خلال الاشتراك في خدمة الدعم على مستوى الشركة، ستحصل على إمكانية الوصول إلى مهندسي الدعم في السحابة عن طريق البريد الإلكتروني أو المحادثة أو الهاتف على مدار الساعة وطيلة أيام الأسبوع.

إذا كنت بصدد تشغيل أحمال عمل ذات مهام حرجة على AWS، فيجب الاستعانة بالدعم على مستوى المؤسسة. من خلال الدعم على مستوى المؤسسة، ستتلقى الحالات الملحة أولوية عليا ويتم توجيهها إلى كبار مهندسي الدعم في السحابة. علاوةً على ذلك، توفر لك خدمة الدعم على مستوى المؤسسة إمكانية الوصول إلى مدير فني للحسابات (TAM) يكون داعمًا لك ونقطة اتصال فنية مخصصة. وتوفر لك أيضًا خدمة الدعم على مستوى المؤسسة إمكانية الوصول إلى إدارة أحداث البنية التحتية، التي تتضمن الدعم التشغيلي في الوقت الحقيقي أثناء الأحداث المخطط لها وإطلاق المنتجات وعمليات الترحيل.

لمعرفة المزيد حول اختيار خطة دعم لملاءمة احتياجاتك الفريدة، راجع مقارنة خطط دعم AWS[٢١].

الخاتمة

باستطاعة أفضل الممارسات المشار إليها في هذا المستند أن تسمح لك ببناء تصميم مرجعي لمرونة مواجهة DDoS باستطاعته أن يحمي توافر تطبيقك من الكثير من هجمات DDoS الشائعة على طبقة البنية التحتية والتطبيق. سوف يؤثر مدى قدرتك على تصميم تطبيقك وفقًا لأفضل الممارسات هذه على نوع هجمات DDoS التي يمكنك تخفيفها وموجه هذه الهجمات وحجمها. تشجعك AWS على استخدام أفضل الممارسات هذه لتوفير حماية أفضل لتوافر تطبيقك في مواجهة هجمات DDoS الشائعة.

المساهمون

ساهم الأفراد والمؤسسات التالية في هذا المستند:

- Andrew Kiggins، مصمم حلول AWS
- Jeffrey Lyons، مهندس عمليات AWS DDoS

ملاحظات

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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