DDoS 완화 서비스 공급자에게 해야 할 5가지 질문

DDoS 공격의 빈도와 복잡도가 증가하고 있어, 적절한 DDoS 완화 서비스를 선택하는 일이 네트워크와 사용자 보호에 매우 중요해졌습니다. 하지만 모든 서비스가 동일하지는 않습니다. 잘못된 서비스를 선택하면 예기치 않은 골칫거리, 성능 문제, 작동 중단 등이 발생할 수 있습니다.

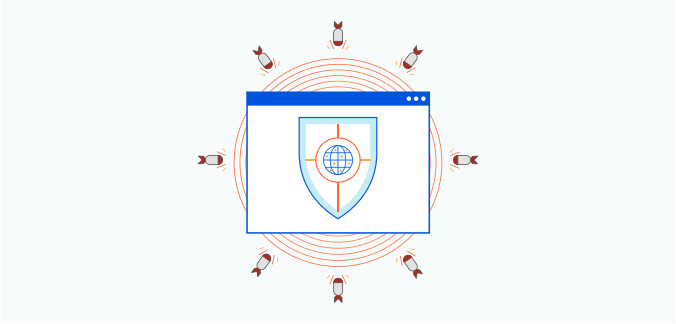
다음은 DDoS 완화 서비스 공급자를 평가할 때 고려해야 할 다섯 가지 질문입니다.

1. 서비스가 클라우드 네이티브입니까?

효과적인 DDoS 완화 서비스는 클라우드 네이티브여야 합니다. 온프레미스 기술을 클라우드 데이터 센터에서 가상화되고 호스팅하는 것이어서는 안 됩니다. 차이는 무엇일까요? 클라우드 네이티브 완화 서비스는 비즈니스의 필요에 따른 확장이 원활하여 인공적인 성능의 병목 현상이 발생하지 않지만, 클라우드로 호스팅되는 가상의 장치에는 온프레미스 하드웨어 관리의 복잡성이 여전히 남아 있다는 것입니다.

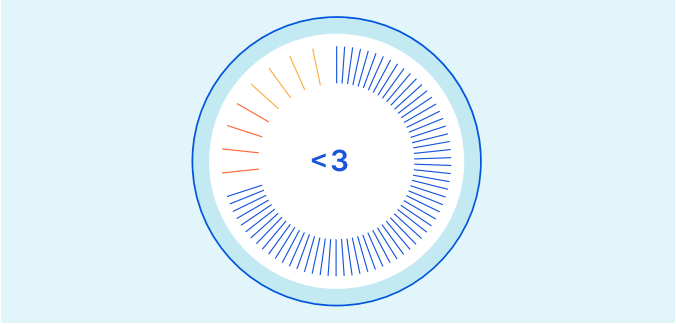
2. 공급자가 제공하는 네트워크 용량이 얼마나 됩니까?

대규모 DDoS 공격(예: 2020년 AWS 고객을 대상으로 했던 2.3 Tbps 공격)은 네트워크 용량이 부족한 서비스 공급자가 흡수할 수 없을 정도로 압도적입니다. 이러한 규모의 공격을 방지하려면 중단 시간 또는 성능 저하 없이 공격을 견딜 수 있을 만큼 충분한 네트워크 용량을 제공하는 공급자를 선택해야 합니다.



3. 서비스가 얼마나 신속하게 DDoS 공격을 감지하고 대응할 수 있습니까?

공격에 직면하면 완화 시간(공격을 감지하고 완화하는 데 걸리는 시간)이 짧아야 합니다. 중단 시간이 몇 초 이상 지나면 고객 경험, 브랜드 평판, 수익 등에 돌이킬 수 없는 손상을 초래할 수 있습니다.

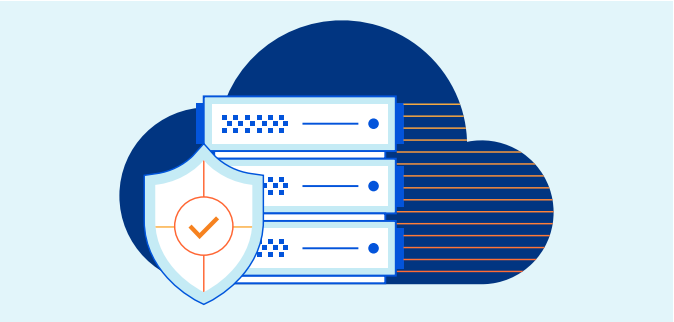


4. 모든 데이터 센터에서 서비스가 제공됩니까?

모든 데이터 센터에서 DDoS 스크러빙 기능을 사용할 수 없다면 트래픽을 전문 "스크러빙 센터"로 백홀해야 하는데 이 과정에서 대기 시간이 길어지고 응용 프로그램 성능이 영향을 받습니다. 트래픽을 최적의 경로에 유지하면서 모든 데이터 센터에서 완화 서비스를 제공할 수 있는 제공자를 선택해야 합니다.

5. 서비스가 자동화되었습니까?

강력한 DDoS 방어 서비스는 대시보드나 API 로에서 자동화 및 셀프 서비스 기능을 이용할 수 있어, 사용자가 신속하게 위협 보호를 켜고 관리할 수 있어야 합니다. 연락이 잘 되면서 신속하게 응답하고 적극적으로 위협을 감지하고 서비스의 중단 없이 예방하는 공급자를 찾아야 합니다.



Cloudflare Magic Transit은 네트워크 트래픽을 가속화하면서 전체 IP 서브넷을 DDoS 공격으로부터 보호합니다. 200개 이상 위치의 데이터 센터로 구성된 Cloudflare의 전역 네트워크는 역사상 가장 큰 디도스 공격들 몇 가지를 포함하여 하루 평균 700억건의 위협을 차단하고 있습니다.

Magic Transit을 시작하려면 지금 바로 무료 데모를 요청하세요.