Cloud Computing: Ensuring Availability for One and All

With cloud computing’s paradigm of shared infrastructure, DDoS attacks on a specific target can quickly affect many or all tenants. In this Arbor Insight, we explain why availability should be the top priority for cloud operators, and outlines best current practices for preventing and mitigating attacks.

The growing popularity of the cloud computing model has been accompanied by a great deal of discussion, and some concrete action, regarding security concerns related to the use of computing, storage, networking and services infrastructure which, by definition, is shared among multiple end customers. While the classic siloed, single-tenant server model quite often involves the use of shared networking and ancillary services infrastructure, such as DNS, bringing together the application logic and proprietary data of multiple organizations on the same computing/networking/storage substrate has highlighted these concerns, and brought them to the forefront for many IT professionals and executives worldwide.

Distributed denial of service (DDoS) attacks are launched with the intent of negatively impacting the availability of the targeted applications, data or services. While DDoS attacks launched against classic siloed systems often cause collateral damage due to their impact on shared resources—such as network infrastructure, DNS, etc.—the inherent and explicit multi-tenancy of cloud computing environments means that an attack against one tenant/customer is an attack against all end customers making use of the same shared infrastructure.

**Best practices for ensuring availability**

Ensuring availability in the face of DDoS attacks can be challenging. Fortunately, there is a large body of best current practices for maintaining availability which have been developed by the Internet operational community and successfully deployed by many service providers and data center operators with a good track record of maintaining availability. By properly assessing the risk to availability posed by the cloud computing model, operators and end users of cloud services can work to minimize their risks and maximize the security postures.

### Best Practices

- Maintain up-to-date communications plans
- Participate in online mitigation communities
- Implement scalable architectures
- Implement real-time detection, classification and traceback capabilities
- Deploy a source-based remotely triggered blackholing (S/RTBH) capability
- Avoid deploying firewalls and IDS/IPS in front of Internet-facing servers
- Deploy intelligent DDoS mitigation systems
- Employ infrastructure ACLs
- Filter irrelevant Internet protocols at network edges via ACLs
- Deploy additional network infrastructure best practices
- Make network infrastructure devices accessible only via designated management hosts
- Configure public-facing servers in a hardened manner
- Provide additional defensive capabilities with Apache modules
All organizations should implement the following as part of their organic cloud computing architectures and/or ensure their cloud providers have done so:

- **Maintain up-to-date communications plans**, including contacts for peers and upstream providers so established operational security teams can react quickly and effectively to DDoS attacks.

- **Participate in online mitigation communities** to increase the effectiveness of coordinated responses to attacks.

- **Implement strong, scalable architectures** that minimize state- and capacity-bound chokepoints, which can otherwise be exploited by attackers, leading to DDoS attacks that cripple public-facing properties.

- **Implement real-time detection, classification and traceback capabilities** to identify DDoS attacks, understand what is happening and take appropriate defensive measures. Flow telemetry such as Cisco NetFlow, Juniper cflowd and sFlow should be enabled at all network edges, and exported into a collection/analysis system such as Arbor Peakflow SP.

- **Deploy a source-based remotely triggered blackholing (S/RTBH) capability** which leverages existing network infrastructure in defending against simple packet-flooding attacks from a relatively small number of sources. S/RTBH leverages BGP as a control-plane mechanism to instantaneously signal edge devices to start dropping attack traffic at the edges of the network, based on the purported source IP addresses of the attack-related packets.

- **Avoid deploying firewalls and IDS/IPS in front of Internet-facing servers.** Even the largest devices are DDoS chokepoints; they degrade the operational security posture of the network and applications by making them more vulnerable to DDoS than the servers alone otherwise would be. Instead, policy should be enforced by stateless ACLs in hardware-based routers and switches, which are capable of handling millions of packets per second.

- **Deploy intelligent DDoS mitigation systems**, such as the Arbor Peakflow SP Threat Management System (TMS), in topologically appropriate cleaning centers to block attacking traffic on a more granular level, including sophisticated application-layer attacks and spoofed attacks.

- **Employ infrastructure ACLs (iACLs) at the relevant network edges—peering/transit, customer aggregation edge, etc.** to protect the network infrastructure itself. For traffic that is destined for Internet-facing servers, use additional service-specific sections to restrict the traffic to ports and protocols associated with the services and applications on those servers.

- **Filter irrelevant Internet protocols at network edges via ACLs.** There are 254 valid Internet protocols. Packet-flooding attacks based on protocol 0, ESP, GRE and other relatively uncommon protocols can be used by attackers to bypass ACLs that only contain policy statements relating to common protocols such as TCP, UDP and ICMP.

For more information about cloud-based DDoS protection services, visit the Arbor Web site.

**ARBOR INSIGHT**
By ensuring that availability is given the appropriate emphasis, organizations can ensure that stakeholders are able to properly assess the risks associated with the cloud computing model and successfully mitigate those risks in order to reap the benefits of cloud computing while ensuring continuity of operations.

- **Deploy additional network infrastructure best practices** such as control-and management-plane self-protection mechanisms (rACL, CoPP, GTSM, MD5 keying, etc.).

- **Make network infrastructure devices accessible only via designated management hosts.** During attacks, a dedicated, out-of-band (OOB) management network allows devices to be managed irrespective of conditions on the production network and ensures continuing visibility into attack traffic.

- **Configure public-facing servers in a hardened manner,** with unnecessary services disabled, service-specific configuration hardening, IP stack tuning and other relevant mechanisms.

- **For Web servers,** Apache modules such as mod_security and mod_evasive provide additional defensive capabilities.

Maintaining availability in the face of DDoS attacks can be challenging, but as the above list of best common practices demonstrates, it is neither impossible nor out of the reach of organizations of any size. By ensuring that availability is given the appropriate emphasis, organizations can ensure that stakeholders are able to properly assess the risks associated with the cloud computing model and successfully mitigate those risks in order to reap the benefits of cloud computing while ensuring continuity of operations.