MAZEBOLT

7 Tips to Configuring Your Network and Preventing DDoS Attacks

Why do enterprises that already invest heavily in DDoS protection solutions still suffer damaging DDoS downtime? Part of the answer is that network configuration requires DDoS expertise – insight into the requirements and potential pitfalls, so that damaging DDoS attacks will be blocked successfully.

Companies Spend More but Still Suffer Damaging DDoS Attacks

Here are 7 tips for effectively configuring the network and building up your DDoS resilience.

Tip 1: Develop a Strategy for Eliminating DDoS Risk

The only way to eliminate the risk of damaging DDoS attacks is to adopt a strategy that includes the following steps:

- Regularly fine-tune security policies in DDoS protection tools, a crucial step to eliminate DDoS vulnerabilities
- Address misplaced confidence on the part of corporate management that can lead to DDoS downtime
- Work with experts in network architecture, as incorrect configuration leaves you exposed to attack
- Validate DDoS protections by means of continuous, nondisruptive DDoS attack simulation

Tip 2: Ask In-Depth Questions About the Configuration

As the network consists of many different mechanisms and layers, it's important to ask questions such as:

- Where is your organization blocking layer 3, layer 4, and layer 7 attacks?
- If an HTTPS flood comes at the network, where will it be stopped?
- Will a PSH ACK flood be stopped before or after reaching your firewall?
- Can your current network handle the attack traffic for long enough to allow the mitigation to kick in?

Tip 3: Keep Volumetric Attacks Away from the Firewall

Layer 3 and 4 attacks must be blocked before they reach a stateful device. As a firewall is a stateful device, layer 3 and 4 attacks should be blocked prior to reaching the firewall.

Sample Network Architecture

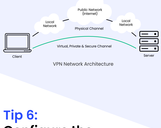
Tip 4: Configure Your Network to Identify HTTPS Traffic

When you activate layer 7 DDoS mitigation, typically it covers just HTTP by default – not HTTPS. Specific configuration work is necessary to ensure a device covers HTTPS vectors as well.

HTTP vs. HTTPS

Tip 5: If You're Using a VPN, Identify Expected Behavior

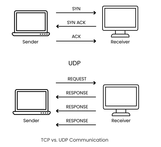
VPN traffic should be allowed only from legitimate sources – and directed only to the VPN server. VPN traffic shouldn't be sent from IoT devices, for example.



VPN Network Architecture

Tip 6: Configure the Network to Identify UDP Traffic

If a team hasn't specifically configured the network to recognize malicious traffic on UDP, a DDoS attack using UDP won't be identified by the network. This creates a high level of vulnerability, as most volumetric attacks go through UDP.



TCP vs. UDP Communication

Tip 7: For On-Premises Deployments – Check Pipeline Bandwidth

For organizations that are not using the Cloud or any off-prem. capabilities, the pipeline bandwidth needs to be considered – regardless of mitigation efficiency. If the pipeline capability is 1 GB, for example, when there is over 1 GB of traffic, the network will be saturated:

Pipeline	Traffic	Result
1 GB	100 MB legitimate traffic	Legit. traffic passes unimpeded
1 GB	100 MB legitimate traffic + 100 MB attack traffic	Legit. traffic passes unimpeded Attack traffic is blocked
1 GB	200 MB legitimate traffic + 2 GB attack traffic	Damaging DDoS attack – network goes down

MAZEBOLT

Avoid Damaging Downtime by Building Your Network's DDoS Resilience

Download the eBook