Minecraft DDoS Protection - Why Is It Needed When I Have The Host?

Minecraft is a fantastic game with easy financial opportunities and and building brilliant communities, but it also has it's downfalls which you need to be aware of. Many malicious actors exist in the world who want nothing better than taking down your MC network when you are having a good player count online and that's no fun for anyone!

Basically, when you run an MC network, you need some sort of DDoS protection. Now, with hosting providers, when you buy from a Minecraft server host, you are putting your trust into them to keep your server online in case of an attack on their network. This is fine and all, but when you become a large network, you need to start thinking about getting a VPS or dedicated system and that's where Jasmeow.Systems comes in.

When you purchase one, you normally have the host say to you "Anti-DDoS Protection 10Tbps" or what have you in their features list. This is fine, but it's mainly for hosting applications and websites, not Minecraft. TCP and UDP connections can get flooded by bots in the Minecraft scene, malicious actors can do L7 attacks and circumvent typical protections put in place by the hosting provider. This is where external DDoS providers come in to serve you protection which isn't connected with the host. You can find them here - https://docs.jasmeow.systems/books/external-ddos-providers

You know providers like TCPShield, NeoProtect, Papyrus, InfinityFilter, CosmicGuard and more? Yep, these are all Anti-DDoS providers for Minecraft. In simple terms, you

put in your dedicated IP address from your VPS or Dedicated server and they route the traffic using their protected CNAME's, SRV's and A records so you don't get taken offline.

You should **NEVER** rely on your hosting providers protection as they will simply email you and state "You need to stop these attacks or we will null route your connection". This basically means you cannot access your SSH, control panels, players can't connect and more. This is why not exposing your IP is the most important step in the system administration community. Once it's shown and live on public tracking websites, you are practically screwed, needing to ask the provider to update your IP and get it replaced.

Providers like OVH and Bloom do make good efforts to protect your IP if it is attacked but for your own benefit of the doubt, don't share it. You can prevent this by having trusted people on your control panels, SSH delegated access to only trained individuals and using CloudFlare wherever possible with the proxy cloud turned on and not set to DNS only.

Hopefully this provides some context into why we state "Don't rely on your hosting providers protection". Any questions, feel free to ask one of the members of our team.

Revision #3
Created 31 January 2024 01:45:51 by JasmeowTheCat
Updated 2 February 2024 01:10:04 by JasmeowTheCat