What is DDoS Attack?

A Distributed Denial of Service (DDoS) attack is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources. They target a wide variety of important resources, from banks to news websites, and present a major challenge to making sure people can publish and access important information. DDoS attacks come in many different forms, from Smurfs to Teardrops, to Pings of Death. Below are 4 common categories of attacks :

TCP Connection Attacks - *Occupying connections*
These attempt to use up all the available connections to infrastructure devices such as load-balancers, firewalls and application servers. Even devices capable of maintaining state on millions of connections can be taken down by these attacks

Volumetric Attacks - *Using up bandwidth*
These attempt to consume the bandwidth either within the target network/service, or between the target network/service and the rest of the Internet. These attacks are simply about causing congestion.

Fragmentation Attacks - *Pieces of packets*
These send a flood of TCP or UDP fragments to a victim, overwhelming the victim's ability to re-assemble the streams and severely reducing performance.

Application Attacks - *Targeting applications*
These attempt to overwhelm a specific aspect of an application or service and can be effective even with very few attacking machines generating a low traffic rate (making them difficult to detect and mitigate).

What are the symptoms if your hotel's server is under a DDoS attack?

Your server's CPU usage will be extremely high and we will not be able to have any access to your server. There will be no internet traffic available for guests to access and they will not be able to login into the network as the whole WAN bandwidth will be used up for attacking the target.

XPossible's current solution to protect against any DDoS attack

DDoS is a new threat and uses a lot of techniques to hack/attack their target. It will require a period of time to fully understand and create a stable security patch to protect against all of it's attacks. As our team is continuingly researching for a permanent solution with the creation of a full fledged security patch, we advise our clients to follow the below mentioned to enable temporary protection against all DDoS attack. This will only allow access to the list of IP/MAC addresses to communicate with the server and devices outside of your network will not be able to harm your server.

- **LAN Admin Access**
  This will enable/disable access from LAN network to Admin/Guest Module and allow access only to MAC addresses included in this list (there should be at least one MAC address in the allow list for this function to work).

- **WAN Admin Access**
  This will enable/disable access from WAN network to the hotel server and allow access only to IP address included in this list.