securus detection • connection • protection

Service Description — DDoS

The Securus Shield Distributed Denial of Service (DDoS) solution is a network tool to prevent DDOS attacks from overwhelming customer environments.

1. Setting Up Securus Shield

When a customer subscribes to Securus Shield, Securus will confirm back to the customer the IP addresses being protected and the level of protection they are subscribed to. The protection levels are:

Tier	Description of Service
Basic	DDoS protection is provided on the core network, but not individual customer assets. If a customer's IP address(es) are targeted in a DDoS attack and if the attack starts to compromise the Securus network, Securus will mitigate this by blocking the IP address for the duration of the attack.
Monitor	The customer's IP addresses are subscribed into the Securus Shield platform. If an attack occurs, then Securus can manually trigger a response, subject to the customer agreeing to the mitigation fees.
Protect	The customer's IP addresses are subscribed into the Securus Shield platform. If an attack occurs, the system will automatically mitigate the effect by scrubbing malicious traffic. Should volumetric attacks occur, Securus will implement cloud scrubbing to return clean traffic to the customer.

2. Configuring Securus Shield

As part of the onboarding process, Securus will need to evaluate customer traffic to determine the normal traffic mix / patterns. This is because Securus Shield starts the DDoS mitigation when higher than normal traffic levels are observed. The process will involve:

- Relevant IP addresses being enrolled into Securus Shield (as confirmed back to the customer).
- Securus Shield will start to evaluate customer traffic to determine the baseline of traffic — this process takes 2–3 weeks.
- The customer will confirm to Securus if the evaluation period has higher or lower traffic than usual, or any other activity going on that would change the base traffic profile.
- At the conclusion of the evaluation process, Securus will agree with the customer the mitigation thresholds. These will usually be:
    - In-line mitigation threshold — 3x observed traffic.
    - Cloud scrubbing — 5x observed traffic.
- These thresholds can be amended by the customer if required, either through the setup process or by raising a ticket with Securus once the service is live.
- In-line mitigation has a nominal capacity of 200 Gbps. Cloud Scrubbing has a nominal capacity of 200+ Tbps.

3. Managing Securus Shield

In normal operation, there is little management from the customer's perspective. However, in order that a mitigation isn't undertaken by accident, the following processes will need to be followed:

- Securus will re-evaluate customer traffic every six months in order to re-assess the baseline traffic profile.
- The customer MUST inform Securus if they are aware of any temporary or permanent increase to their baseline traffic profile. This is so Securus can increase the thresholds to avoid a mitigation being applied erroneously.

4. What does Securus Shield Protect from?

Securus Shield protects customer environments from:

- Significant increases in bandwidth towards the customer environment.
- Application level attacks, such as TCP syn floods, UDP floods.
- Volumetric attacks designed to overwhelm firewalls and routers.

5. How quickly does Securus Shield mitigate attacks

Securus Shield is constantly evaluating traffic for subscribed customers. Should an attack occur, then in-line mitigation is triggered in approximately 30 seconds. If a volumetric attack occurs, Securus will initiate cloud scrubbing for the affected block of IP addresses. This will take approximately 5 minutes to fully initiate, as it requires routing changes to be announced across the internet.

6. Attack alerting

Securus will alert the customer, as soon as is practicable, if a DDOS attack is detected. Securus will communicate the tyoe and origin of the attack, along with confirmation that the mitigation is being deployed correctly. Once the attack has stopped, Securus will communicate this to the Customer and provide a post-incident report if the customer wishes to receive one.