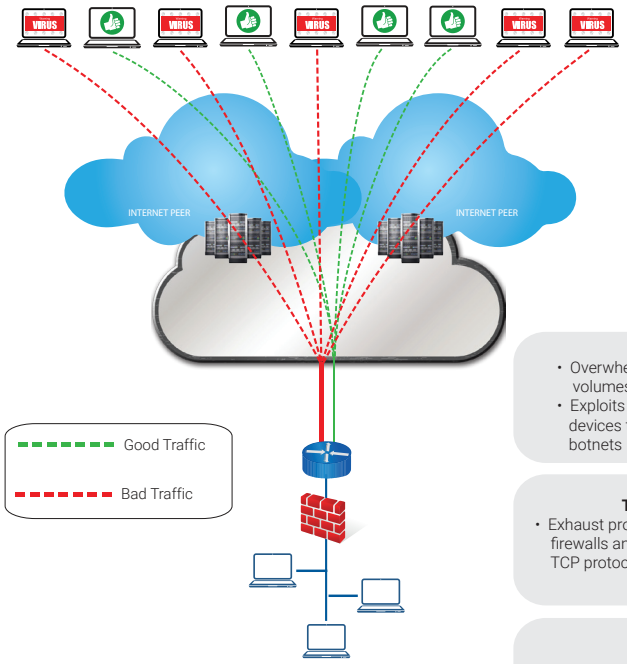
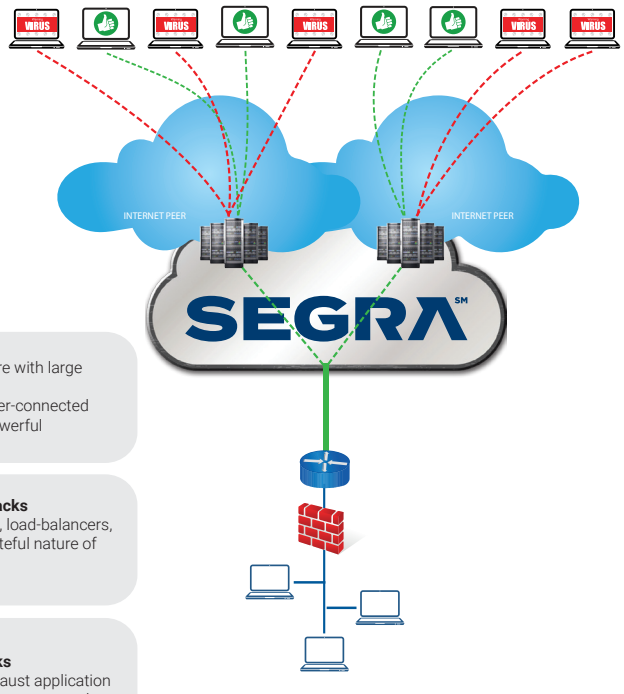
DDoS Edge Protect

Distributed Denial of Service (DDoS) attacks can strike at any time with potentially devastating effects to your network. At a minimum, these assaults compromise your user/customers' experience and can often shut down networks completely, resulting in lost productivity, revenue and costly bandwidth charges. With these attacks becoming a regular threat to the online business community, it pays to be prepared. Segra's DDoS Protection Service employs a multi-layered approach to DDoS defense to ensure your organization is safeguarded from both complex, stealthy DDoS attacks, and the very large attacks that can quickly saturate Internet connectivity.

ATTACK IN PROGRESS



ATTACK MITIGATED



Volumetric Attacks
- Overwhelms a targets infrastructure with large volumes of traffic (bps/pps)
- Exploits easily accessible and better-connected devices that create increasingly powerful botnets

TCP State-Exhaustion Attacks
- Exhaust protocol resources in servers, load-balancers, firewalls and routers by exploiting stateful nature of TCP protocol.

Application Layer Attacks
- 'Low & slow' attacks that stealthily exhaust application resources as opposed to flooding a targets network

DDoS ATTACKS DENIED AT INTERNET PEERING POINTS

- Network Traffic analyzed constant by Segra's SOC
- Automated attack alert email
- DDoS Protection for entire subnets
- Scrubbing service available, yet not needed

SPECIFICATIONS

- Types of Attacks Addressed - Volumetric, reflective and resource-exhaustion
- Availability - Only available in conjunction with Segra DIA service

DDoS Edge Protect

DDoS protection appliances are located at high-volume entry points on the Segra core network where attacks are most likely to occur, such as public transit connections. The appliances automatically inspect all traffic as soon as it arrives at an entry point, immediately discarding malicious packets while sending legitimate packets to their destination. During this process, other network services continue to operate without interruption, even latency-sensitive applications like voice and video.

FAST

The protection capability is purpose-built for speed and low latency, so attacks are detected and mitigated immediately without impacting network performance.

EFFECTIVE

The protection is comprehensive, identifying both existing and newly discovered attack types, and preventing direct attacks as well as their side effects.

RISK REDUCTION

The fast, effective protection included in the Segra DIA service significantly minimizes the risk of DDoS attacks from the public Internet.

REAL-TIME FILTERING

Inspection, detection and scrubbing occur as soon as traffic arrives at the Segra network.

AUTOMATIC PROCESSING

All filtering functions are performed automatically, without the requirement for regular human intervention and/or delay.

IN-LINE OPERATION

Traffic stays on the Segra network during filtering instead of being physically and/or logically diverted for processing, minimizing latency.

COMPREHENSIVE PROTECTION ANALYTICS

Inherent analytics detect a variety of attack types and are updated continually with the latest intelligence on DDoS threats.

CORE FUNCTIONALITY

DDoS protection is required as a standard, core function of the Segra DIA service. Taking this approach protects the entire Segra network path from DDoS attacks, and in turn, the entire Segra DIA customer base. The approach also complements any local DDoS solution a customer may implement since a local solution cannot protect the Segra network path.

SCALABILITY

The DDoS protection appliances are designed and located to easily keep pace with growth in the Segra footprint and the customer networks we serve. Any site a customer adds to the Segra network is automatically protected from DDoS attacks without configuration changes.