perspecta LABS

DDoS Defender

Protect your critical infrastructure and resources

Value and benefits:

- Disperses attack surface and reduces or eliminates dependence on centralized servers
- Significantly extends cyber defense capability by deceiving attackers and enabling a wide set of defensive and deceptive maneuvers
- Hides and provides deceptive information to attackers about critical network resources
- Dynamically maximizes service availability and responsiveness for legitimate users
- Improves efficiency of transporting traffic flows
- Minimizes latency in navigating severely degraded networks

Introducing DDoS Defender

Distributed Denial of Service (DDoS) attacks are among the most malicious cyberattacks made against military enterprise and public network infrastructure. DDoS attackers disrupt, delay and deny legitimate users' access to critical computer, communications and network resources.

DDoS Defender, the Perspecta Labs suite of DDoS defense solutions, delivers breakthrough cyber defense capabilities to protect infrastructure, provide resilience and maintain critical services.

Using a multimodal approach to thwart even the most sophisticated attacker, our novel techniques can dynamically obscure high-value cyber assets; detect stealthy, low-volume intrusions; perform defensive maneuvers to mislead and confuse adversaries; and launch mitigation steps to repel both widespread and targeted attacks. Combining multiple, proven innovations—each designed, developed and extensively tested on U.S. government cyber research projects—our suite of DDoS defense solutions delivers superior defensive capacity to detect and deter DDoS attacks.

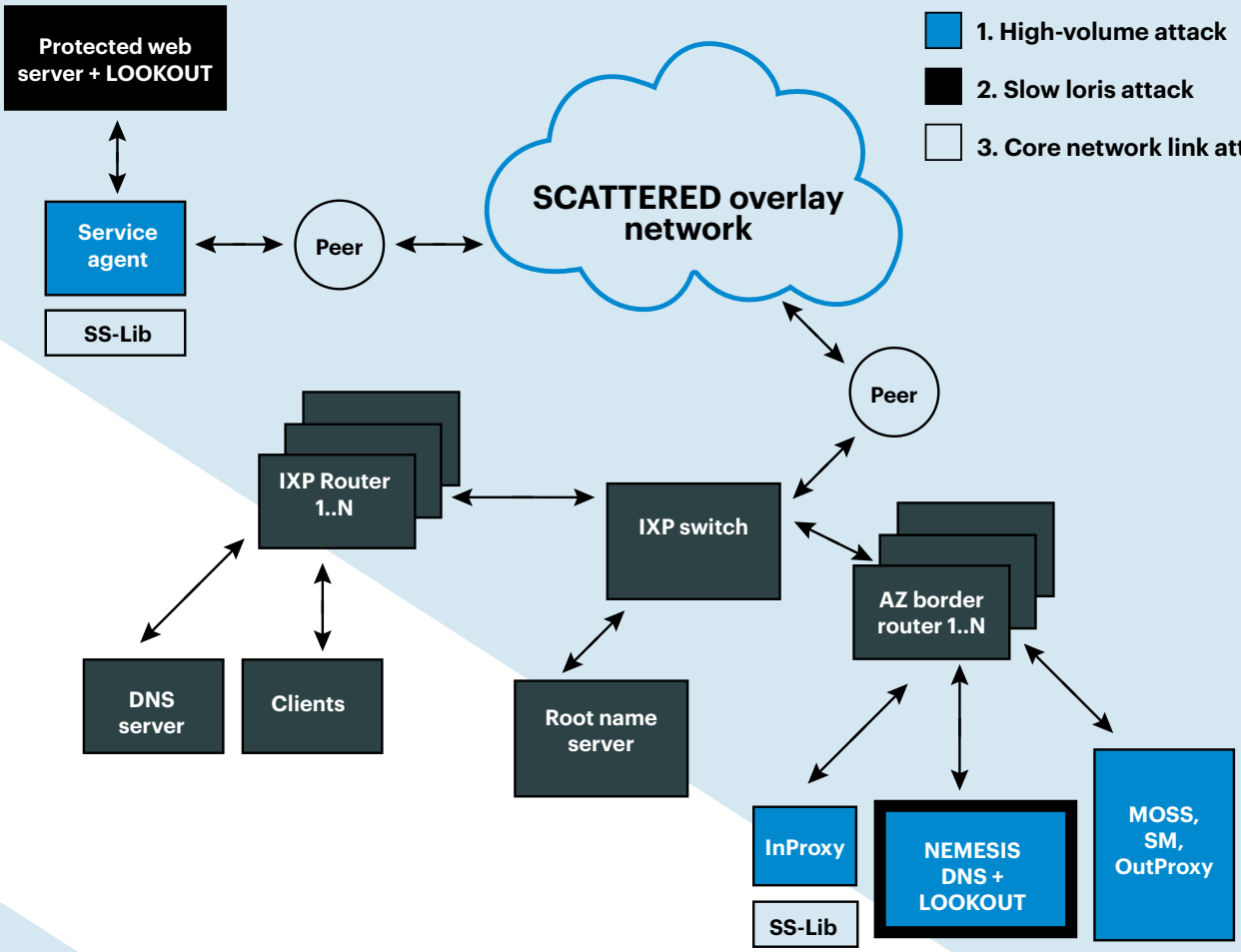
Three leading-edge cyber technologies create the foundation for DDoS Defender:

- **SCATTERED (SCalable Network-Aware Technologies for TunablE ResistancE to DDoS):** leverages a novel combination of artificial intelligence planning, peer-to-peer dispersion of cyber resources, and agile, resilient data transport to logically and/or physically disperse network resources to complicate adversarial targeting and minimize the impact of attacks
- **NEMESIS (NEtwork ManEuvering for Survivable Internet Services):** uses an innovative combination of techniques, including game-theoretic planning, real-time analytics, cloud-based maneuvers and randomized maneuver control to confuse adversaries and disrupt cyberattacks
- **LOOKOUT (Low Overhead Observations Keeping Operational Under Threats):** employs a sense-detect-correlate-remediate architecture to identify and mitigate attacks, especially the precision low-volume attacks that exhaust targeted server computing capacity while flying under the radar of traditional in-line detection and scrubbing techniques

DDoS Defender enables network operators to effectively identify and defend against a wide variety of attack scenarios and to deliver significantly enhanced network and service resilience. With our groundbreaking techniques, cyber opponents misidentify high-quality targets, are forced to disperse their resources and are fooled about the success of the attack.

perspectalabs.com | info@perspectalabs.com
150 Mount Airy Road
Basking Ridge, NJ 07920

perspecta LABS



DDoS Defender harnesses the following Perspecta Labs' innovations:

- Hierarchical network architecture, combined with our distributed peer-to-peer protocol extensions and enhancements, can incorporate real-time system awareness to navigate around compromised cyber assets and links in the network while also delivering superior scalability, performance and flexibility
- Network performance estimator performs passive and active measurements of available bandwidth, latency, and loss metrics to provide the critical network and application awareness
- Mission-aware dispersal offline strategic and online tactical planning tools work cooperatively to devise, control and manage the distributed architecture
- Advanced analytics provide real-time network maneuver direction and situational awareness
- Service-agnostic maneuver playbook presents a wide selection of network maneuvers for both proactive and reactive defense
- Mission-aware maneuver orchestrator determines the most effective defense against changing adversary tactics and mission activities. It leverages:
- Game-theoretic course of action planner to model the adversarial relation between a strategic attacker and a defender of cyber assets
- Dynamic maneuver controller to provide runtime stochastic control for selected network maneuvers
- Attack isolation techniques, through the use of containers, isolate the effect of attacks by separating malicious from benign traffic flows
- Robust, scalable detectors spot legitimate and illegitimate protocol usage, resource exhaustion and starvation, network tomography-based events and other anomalies to identify DDoS attacks
- Correlation and remediation decision engines serve to correlate attack alert evidence and launch mitigation responses

perspectalabs.com | info@perspectalabs.com
150 Mount Airy Road
Basking Ridge, NJ 07920