nScrub

DDoS Mitigation System

nScrub is a DDoS mitigation engine able to operate at multi 10 Gbps line-rate on a low-end machine, relying on commodity hardware and Open Source high-performance technologies for processing traffic.

nScrub can be deployed as bump-in-the-wire (transparent bridge) or as router, to be used with BGP diversion techniques. It can run both in asymmetric mode (mitigating inbound traffic only) or symmetric mode (inspecting traffic from Internet to the protected network as well as outbound traffic).

nScrub has been designed as an open platform, meaning that it can be easily extended, defining new plugins in addition to the built-in algorithms for traffic mitigation.

nScrub provides a RESTful API Over SSL for configuring the engine, in addition to a CLI console with auto-completion.

Web-based RRD-style historical graphs, combined with PCAP dump on request triggered by an event-driven scriptable engine, guarantee full visibility in case of attack. nScrub is able to export sampled/full good/bad/all traffic to external virtual devices for analysis using even third-party tools.

Performance

nScrub has been benchmarked with both synthetic line-rate traffic to simulate the worst case scenario as well as with real attacks in production environments, to verify its reliability in any attack condition. nScrub clusters are mitigating hundreds of Gbit/s attacks today, including UDP-based amplification attacks and SYN floods.

Key Features

- Active sessions verification for protocols including TCP and DNS.
- Flexible subnet blacklists and whitelists.
- ACL-like policies based on UDP/TCP/ICMP fields.
- Signature-based filtering, HTTP requests filtering for L7 attacks.
- Anomaly detection based on traffic behavior.
- Rate limiting based on source, destination, protocol.
- Traffic checkers implemented as plugins, third parties can define their own checkers for specific protocols.
- Multi-Tenancy: ingress traffic is split towards several virtual mitigators based on destination, with the ability to specify custom traffic policies based on service type.
- Transparent bridge mode (Bump-In-The-Wire).
- Routing mode: mitigate attacks on demand and on remote locations using BGP diversion.
- Hardware bypass support: when supported by the underlying hardware it ensures that nScrub will have no impact in the infrastructure in case of system failures.
- Software bypass: temporarily disable any protection policy with the desired granularity.
- Attack recording: sampled, raw traffic export in case of attack by means of scriptable events.