NEXUSGUARD
DDoS Protection Made Simple

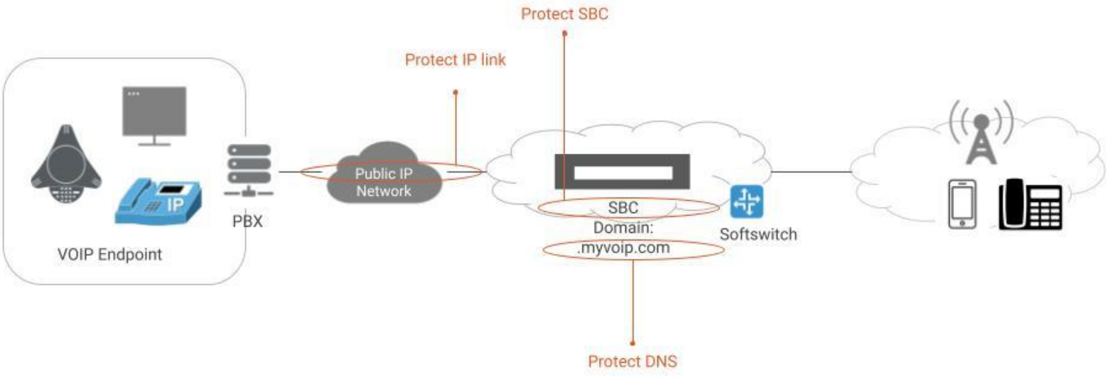
VoIP Protection Solution

VoIP Service Under Intensive DDoS Attacks

The past few months have been hectic for VoIP providers and users due to the recent rise in DDoS attacks aimed at VoIP providers. Attackers adopted a combination of TCP, UDP, SIP and DNS attacks to bring down targeted VoIP services. Attacks were seen over 100Gbps with high packet rate over millions per second, resulting in network congestion, call failure and poor call quality. Wireless Internet Service Providers with VoIP services could be at risk of the same type of DDoS attacks and a well planned defense strategy will help WISPs to avoid unnecessary service issues.

Critical VoIP Elements Needed Protection

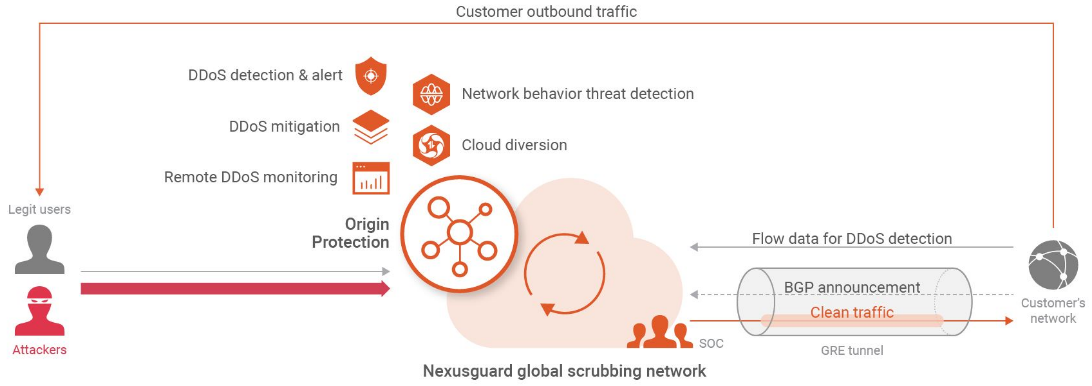
A Session Border Controller (SBC) is an important component in the SIP network, which acts like a firewall to govern call admission at the border. It filters calls, manages connectivity, controls call quality and protects against malicious attacks. It will control how calls are started, conducted, and terminated – and all the necessary media streams and data transfer to allow calls to occur [1]. Attackers recognized the importance of SBC and to bring down SBC, they sent multi-vector attacks towards the target using a mixture of TCP, UDP and SIP attacks. The side effects of the attacks are link congestion and service outage. In addition to SBC's and IP links being targeted, SIP domains are also targeted. SIP domains are domains authorized to send and receive SIP traffic, and are used when assigning SIP addresses to users. When SIP domains become unavailable, users are unable to register themselves for SIP calls. To ensure uptime availability of VoIP services, IP link, SBC and DNS are the critical elements that require protection.



[1] Reference: What is Session Border Controller (SBC)?, https://getvoip.com/library/session-border-controller/

Protect IP Link and SBC using Nexusguard Origin Protection

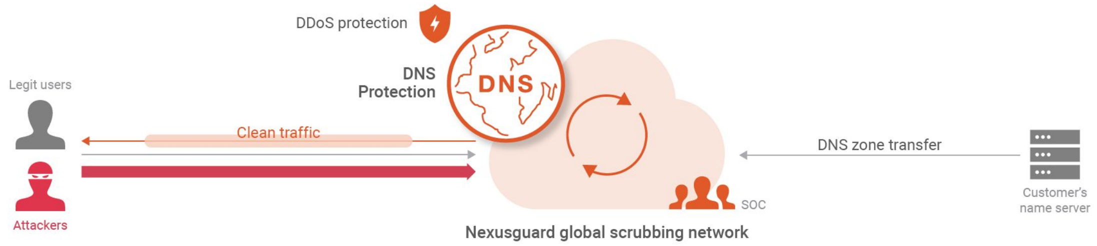
Nexusguard's Origin Protection is designed to protect mission-critical services across a network from L3/4 and L7 attacks. It is able to deliver up to 2.24Tbps of attack protection and provide real-time monitoring on an integrated portal with dynamic dashboard and analytics. It utilizes deep learning to observe and analyze the pattern of traffic of the protected network, delivering low false positives and fast detection. Hierarchical mitigation profiles provide protection to each service group with surgical precision. With the new Cloud Diversion App you can effortlessly and automatically divert traffic to the Nexusguard network when the service identifies anomalies so that attack mitigation can take place, ensuring that only legitimate traffic enters your network at all times.



When VoIP is under attack, Cloud Diversion App will trigger auto-announcement of VoIP service block. A /24 BGP route will be announced through Nexusguard, diverting attacks to Nexusguard's globally distributed network of scrubbing centers. Clean traffic can be returned to customers through Direct Connect/GRE.

Protect SIP Domain using Nexusguard DNS Protection

Nexusguard DNS Protection service protects mission-critical online services from all DNS attacks and malicious queries. The solution leverages Nexusguard's highly scalable, fully redundant and globally distributed DNS platform with sufficient capacity to absorb large DNS-based DDoS attacks while responding to legitimate user requests.



VoIP providers can implement Nexusguard DNS as their authoritative or secondary DNS, either by replacing or augmenting their existing DNS infrastructure. In either case, organisations receive a scalable and secure DNS network to ensure the best possible experience for their users.

To learn more about the VoIP Protection Solution or Nexusguard's managed DDoS protection services, visit www.nexusguard.com or contact the solution team at contact@nexusguard.com.