



Cloud-Based DDoS Protection for Expanded VPN Networks

Where It Came From; Where It's Going

Customer Challenges

For organizations urging their employees to work from home (WFH), the pattern of user connections to the enterprise network has turned upside down. Instead of most users connecting locally, now most are connecting remotely. Organizations are conducting critical business functions across the open Internet through dozens, hundreds or even thousands of individual VPNs.

This unexpected flood of WFH connections makes networks more vulnerable to the impact and damage of a distributed denial of service (DDoS) attack. Attackers can easily identify an organization's VPN endpoint, either by monitoring traffic or, even easier, because many enterprises use "vpn" in the URL or host name for their VPN server. From there an attacker can identify the IP address with a quick DNS lookup and launch a network protocol attack or rent a bot network for a conventional volumetric attack. Either way employees are effectively locked out, business grinds to a halt and assets are exposed.

With VPN Protect, your VPN server is protected against DDoS attacks by a purpose-built, cloud-based DDoS mitigation solution that is always on, ensuring your work-from-home workforce remains connected and productive and your business is uninterrupted.

BENEFITS

- **Fast.** Always-on cloud-based solution with the option of automated mitigation backed by a 24/7 SOC.
- **Flexible.** Tailored to your needs and your network, with the option to protect all enterprise traffic.
- **Capable.** Dedicated DDoS mitigation network with massive 12+ Tbps capacity covering layers 3-7.
- **Expert.** Best practices and countermeasures based on 15+ years of experience.

**ESSENTIAL FEATURES**

- Non-stop protection against non-stop threats: conventional flooding attacks, network protocol attacks and application layer attacks
- Available automation to quickly move any attack into mitigation
- Cloud deployment to protect with no hardware or software installation
- Massive network of dedicated scrubbing capacity for largest and most intense attacks
- Globally positioned scrubbing infrastructure for protection
- Multiple best-in-class DDoS mitigation vendor and proprietary technologies
- Multiple Tier 1 Internet Network Providers
- Fully IPv6 capable
- Supported 24/7 by senior-level DoS mitigation professionals

A Heightened Risk to Critical Resources Demands VPN Protect

Companies have inadvertently multiplied the potential impact of a DDoS attack by vastly increasing the use of VPN connections to allow more employees to work from home. Your VPN traffic and servers – and through them your network and digital assets and your ability to conduct business – have never been more vulnerable.

VPN Protect, from Neustar Security Services, is ready today to protect your VPN traffic with a VIP proxy strategy that can be quickly implemented and deployed with a minimum of disruption:

- VPN traffic is routed through our DDoS mitigation infrastructure;
- Malicious traffic is removed from the VPN traffic;
- Clean traffic can be returned directly via the internet, or sent through GRE tunnels if required;
- Your SSL certs are not required to protect the traffic

If your virtual workforce is frozen out by a DDoS attack, your enterprise will stop dead. Protect your business with VPN Protect.

FOR MORE INFORMATION

Visit: www.neustarsecurityservices.com

Call US: +1 (844) 929 - 0808

Call EMEA: +44 808 175 1189