DDoS Auto-Mitigation FAQ

What is MCNC's Enhanced DDoS Protection service?

In response to the increased threat of Distributed Denial of Service attacks, MCNC has developed and implemented world-class DDoS protection capabilities for NCREN customers. MCNC has updated the NCREN backbone with advanced traffic routing capabilities and has deployed multiple DDoS scrubbing centers on the network. When customers face a DDoS attack, network traffic can be diverted into the nearest scrubbing center, where traffic can be analyzed and cleaned. DDoS attack traffic is removed from the flow, allowing legitimate network traffic to continue on to the targeted customer. In short, the scrubbing centers remove the bad traffic and allow the good traffic to continue on to the customer, ensuring that business services function normally while minimizing the negative impact of the DDoS attack.

What is DDoS Auto-Mitigation?

Auto-Mitigation is a new feature for MCNC's Enhanced DDoS Protection service. When a DDoS attack is detected, the impacted traffic flow can be directed into one of MCNC's DDoS scrubbing centers automatically, allowing attack mitigation to begin within a few seconds of attack detection. Once the attack has subsided, traffic flow will automatically return to its normal path on the network.

How is DDoS Auto-Mitigation different than Standard Mitigation?

With Standard Mitigation, MCNC generally will not modify any network traffic flow until conferring with the impacted customer. The normal process goes like this: DDoS attack is detected, MCNC network analyst is alerted to the attack and reviews pertinent attack data, Mitigation strategy is devised, MCNC contacts impacted customer to discuss details, DDoS mitigation is activated. Working through all of these steps can be time consuming, usually taking anywhere from 15 minutes to 45 minutes or more. Many DDoS attacks have already subsided before the mitigation can begin.

With Auto-Mitigation, the configuration and setup are done ahead of time. If the DDoS attack matches a pre-defined attack pattern (and most attacks do), attack mitigation can begin within seconds of detection, significantly reducing the negative impact of the attack.

How does Auto-Mitigation Work?

MCNC defines a template of common attack mitigations based on known, common attack patterns. When we enroll a customer in Auto-Mitigation, we create a template that that defines a customer's IP address space. When our DDoS attack detection system detects an incoming DDoS attack, it checks to see if the targeted IP address is in the Auto-Mitigation list. If so, traffic destined for the target IP address is automatically diverted to the nearest DDoS scrubbing center. Any traffic matching the already established mitigation profile (of well-known DDoS attacks) will be scrubbed. All other traffic (that does not match the mitigation profile) will pass through unmodified.

Why should I use Auto-Mitigation instead of Standard Mitigation

Standard Mitigation requires human intervention prior to starting the attack mitigation process. This intervention means that it may be anywhere from 15 - 45 minutes or more before mitigation can begin. Auto-Mitigation allows attack mitigation to begin within seconds of attack detection. With Standard Mitigation, many short-lived attacks are over before the mitigation process can even begin. Auto-Mitigation gives MCNC's customers the best chance for reducing the damaging impacts of a DDoS attack.

If attack mitigation is applied automatically, how will I know if I'm under a DDoS attack

Whenever Auto-Mitigation is activated, MCNC's response system will automatically open a support ticket and previously established customer contacts will be alerted via email. In cases where routine response measures appear inadequate, MCNC will attempt to contact customers via phone to discuss attack details and response strategies.

Is all of my network traffic impacted when Auto-Mitigation is enabled?

No. As a customer, you define the network address space that is enrolled in Auto-Mitigation. But even if Auto-Mitigation is enabled for your entire address space, most of the time your traffic flow is unmodified. Traffic is only routed to the scrubbing center if an active DDoS attack is detected. And even when an attack is detected, only traffic destined for the specific victim IP address will be diverted to the scrubber. All other network traffic will remain unmodified. And as the traffic for the specific victim IP address flows through the scrubber, only traffic matching the well-known DDoS traffic profiles will be scrubbed. Other traffic destined for the victim IP will not be modified by the scrubber. Traffic modification only occurs during active DDoS attacks, and even then only for traffic that is destined to thevictim IP address and that matches well-known DDoS traffic profiles.

Will Auto-Mitigation make my network run slower?

Network traffic sent through the DDoS scrubbing center may experience additional latency as compared to normal traffic flow. In MCNC's testing however, this additional latency is generally negligible and is not noticeable by most customers. However, any additional latency introduced by attack mitigation is generally preferable to negative performance impacts caused by unmitigated DDoS attacks.

What do I do if I think Auto-Mitigation is causing a problem on my network?

If you ever believe that Auto-Mitigation is causing an issue for your network traffic, you should contact the MCNC Network Operations Center (NOC) at 877-GO-NCREN (877-466-2736). Our NOC staff members are available 24x7 to assist with NCREN connectivity issues.

How much does MCNC charge for DDoS protection services?

MCNC's Enhanced DDoS Protection service is provided to all NCREN network customers as part of the standard NCREN network service. If you get network connectivity from MCNC, you get the Enhanced DDoS Protection service included at no additional cost.

Does Auto-Mitigation Cost more than Standard Mitigation?

No. Both Auto-Mitigation and Standard Mitigation are provided as part of MCNC's Enhanced DDoS Protection service, which is available to all NCREN network customers at no additional cost.

Does the Enhanced DDoS Protection service guarantee that I'll never have another DDoS issue on my network?

No. It is possible that you may face an attack that MCNC's solution cannot easily mitigate. However, MCNC's Enhanced DDoS Protection service provides a significantly improved capability to protect against the negative effects of DDoS attacks.