AUTOMATIC DETECTION

STRONG PROTECTION

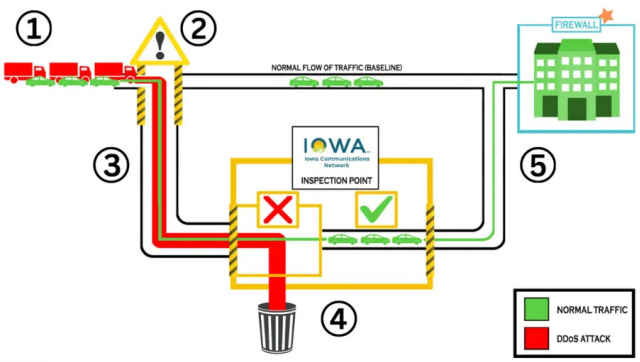
LAYERED DEFENSE

DDoS MITIGATION

Our mitigation service is a scalable and automated protection solution that manages a wide range of DDoS events which include volumetric, protocol, and application layer attacks. The on-premise solution is used to protect assets like our telecommunication networks, servers, and applications.

A SCALABLE AND AUTOMATED PROTECTION SOLUTION.

Our mitigation solution is easy to manage and deploy with a centralized management console, automated attack mitigation, and real-time reporting.



HOW DOES IT WORK?

Our solution includes: configuring multiple appliances to protect ICN assets and our customer's Internet services.

We typically mitigate using a variety of methods including: packet filtering, rate limiting, blackholing, geo-fencing, and challenge-response.

Service only available for ICN Internet customers.

WHY DO WE NEED MITIGATION?

DDoS attacks can be expensive. When you consider employee resources, potentially losing data, and the inability to access the Internet, the cost of being unable to do business can skyrocket.

IOWA™
Iowa Communications Network

Grimes State Office Bldg.
400 East 14th Street | Des Moines, IA 50319

icn.iowa.gov
(800) 572-3940 / ICN.info@iowa.gov

2025

A PLATFORM WITH GREATER FLEXIBILITY TO PERFORM SECURITY UPDATES.

	Automatic Detection & Mitigation
Design / The design consultation will include the development of customer requirements, an End User mitigation alert policy and appropriate response procedures.	●
Install / Our comprehensive installation includes a customer Internet access topology review and provisioning of the attack-detection system. End User will maintain an ICN Internet connection.	●
Configure / Our solution includes provisioning the detection and mitigation service and applying the security policy.	●
Monitor / Our advanced monitoring system incorporates automatic detection of attacks. End User traffic is monitored continuously.	●
Administration / Our service includes on-going evaluation and optimization of network and system performance.	●
Maintenance and Support / Incorporates software and hardware upgrades to maintain the latest version.	●
Mitigate / Mitigation (filtering) of traffic begins after the system determines that a DDoS attack is underway.	●
Cleanse / Once mitigation begins, traffic is routed to ICN Cleansing Center. The traffic immediately undergoes the stages to remove the malicious activity. Once cleansing is complete, traffic will be forwarded from the ICN Cleansing Center to its original destination.	●

EMERGENCY DDoS SERVICE

ICN offers emergency DDoS services to those in need. Here is how our process works:

STEP 1 / End User will contact ICN identifying that they believe they are under a DDoS attack.

STEP 2 / Network flow monitoring will be set up and customer will be informed of findings.

STEP 3 / End User will give approval to begin mitigation and traffic will be routed to ICN Cleansing Center. Once attack subsides traffic will be pointed back directly to End User.

PREMIUM & PROFESSIONAL SUPPORT

Our premium and professional support team is at your service 24/7 to assist you with your security needs.

*Event (one calendar day) fee is a flat rate daily charge that provides coverage from the first day mitigation is implemented.