



# How to order DDoS Hyper

DDoS Hyper mitigates DDoS attacks against your web assets and applications. This unlimited on-demand service requires an active internet IPv4 connection with Border Gateway Protocol (BGP) peering. Scrubbed traffic is returned to up to 10 locations via Generic Routing Encapsulation (GRE) and includes optional Flow-Based Monitoring for attack detection. For advanced DDoS mitigation features, please visit: [lumen.com/en-us/security/ddos-and-web-application.html](https://lumen.com/en-us/security/ddos-and-web-application.html).

## To quote and order DDoS Hyper, you will need the following information:

- **Customer Billing Account Number (BAN)**
  - For **current customers**, use Control Center to select your customer BAN before ordering DDoS Hyper.
  - For **new customers**, you will be asked to create an account by providing a company name, address, email and phone number with which to associate the service.
  - Both **new and current customers** will be asked to identify an order contact and a technical data contact who can provide the required information to place a DDoS Hyper order. The person ordering the service must be authorized to accept the quote, and terms and conditions of the service.
- **Service Address**

The primary address or place of use where the DDoS Hyper service will be received.
- **Total Bandwidth**

The bandwidth needed to support the aggregate level of traffic across all locations that is returned to you after mitigation.
- **Contract Term**

DDoS Hyper is offered on a month-to-month or 12-month term basis.
- **Professional Security Services Assistance**

Whether you want to add an optional service which provides a designated security consultant for configuration, runbooks, analysis and reporting that is tailored to your business needs. Options include 5 hours, 10 hours, 15 hours and 20 hours per month, on a month-to-month contract.

To [configure and activate your DDoS Hyper service](#), you will need the following information:

## What is being protected

- **IP Prefixes**

The group of IP addresses that will be protected. (NOTE: If your internet service is provided solely by Lumen, the Customer IP Prefix can be between /8 and /32. If some or all of your internet service is provided by a third party, the IP Prefix must be between /8 and /24.)
- **Autonomous System Number (ASN)**

An ASN is required in order to use Border Gateway Protocol (BGP). It can be obtained from your provider or from the regional internet registry (e.g. ARIN, APNIC, RIPE, AfriNIC, or LACNIC). If your internet service is provided solely by Lumen, use ASN 10753. NOTE: DDoS Hyper does not currently support internet service with static routing.

## Where Lumen sends scrubbed traffic

- **Clean Traffic Return Bandwidth**

Clean traffic return bandwidth supports legitimate traffic routed back to you after it is inspected and scrubbed. Bandwidth is selected for each clean traffic return path.
- **Customer IP Address**

The Customer IP is the IP address for the customer end of the GRE tunnel which receives the clean traffic from the Lumen scrubbing center.
- **Scrubbing Center**

The Lumen scrubbing center from where scrubbed traffic is returned to you. We recommend selecting a scrubbing center location closest to the customer end of the GRE tunnel to minimize latency.

## How Lumen monitors for attacks

- **NetFlow Export IP Address**

The customer router IP address from where NetFlow is originated. When Flow-Based Monitoring is established, it monitors for attacks against you using both NetFlow and SNMP information from your network router.
- **Simple Network Management Protocol (SNMP) Version**

The SNMP version that your router supports. (NOTE: Higher versions of SNMP provide advanced capabilities such as authentication and encryption.)
- **SNMP Polling IP Address**

The customer router IP address to be used for SNMP polling. When Flow-Based Monitoring is established, it monitors for attacks against you using both SNMP and NetFlow information from your network router.

---

- **Security Level**

For SNMP Version 3, you have an option to select: Polling Only, Polling with Authentication or Polling with Authentication and Privacy. If you select Polling with Authentication, you will need to make an additional selection for SNMP Authentication Protocol as described below. If you select Polling with Authentication and Privacy, you will need to make additional selections for SNMP Authentication Protocol and SNMP Encryption as described below.

- **SNMP Authentication Protocol**

The SNMP Authentication Protocol that is supported by your router. For SNMP Version 3, options include: None, Secure Hash Algorithm (SHA-1) and Message Digest Algorithm 5 (MD5).

- **SNMP Encryption Protocol**

The SNMP Encryption Protocol that is supported by your router. For SNMP Version 3, options include: None, Advanced Encryption Standard (AES) for 128-bit and Data Encryption Standard (DES).