voxility

voxility.com/shop/security/anti-ddos/tunnels

Anti-DDoS Tunnels

Expand your Anti-DDoS Solution Capacity with 500Gbps

Security is the #2 reason everyone wants to work with Voxility

We offer standard tunnel end-points to a nearby Voxility Security Cloud to connect your anti-DDoS equipment.

Through an encapsulated BGP session you will advertise end-user attacked subnet whenever downstream or equipment capacity is overwhelmed by an attack.

Security Cloud will "hijack" the affected subnet's incoming traffic, mitigated for DDoS with a 500Gbps capacity and sent to you through the tunnel.

Traffic exiting your network is never rerouted.

How to Order

This product is best suited to anti-DDoS Appliance makers and companies that have the knowledge to detect and stop small DDoS attacks.

Review prices and order online at
voxility.com/shop/security/anti-ddos/tunnels

Get answers to your questions 24/7
noc@voxility.com

Business Benefits

Save considerably on unwanted bandwidth cost

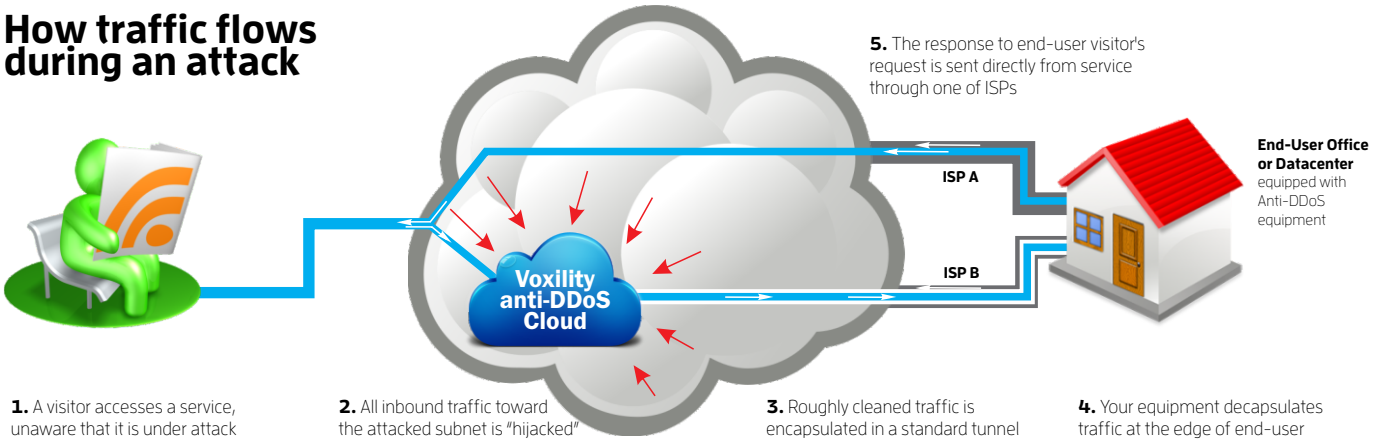
Protect investment in current Anti-DDoS equipment

Increase revenue through recurring charge

Attract new customers with enhanced protection

A truly affordable and unmatched price for massive Bandwidth

How traffic flows during an attack



How does Voxility's anti-DDoS in the Cloud work?

Whenever end-user overrun filtering or downstream capacity, inbound traffic for a specific IP subnet that would normally flow to him through ISP connections is globally "hijacked" by the Voxility Security Cloud.

Hijacking is achieved through BGP advertising using a more specific prefix (e.g., /24 instead of /23 you use on end-user existing ISPs) to prepend his AS number to ISP connections, or by completely withdrawing your prefix advertisement through your ISPs.

How we recommend to deploy

1. Add the following features to your anti-DDoS equipment:
   - establish a GRE tunnel
   - BGP session with Voxility and end-user
   - Thresholds when traffic will be redirected in Cloud
   - Intelligence of how is the best way to "hijack" traffic based on data collected from user and Voxility BGP sessions: advertise a more specific prefix, AS prepending, withdrawing an advertisement, BGP session reset.
   - End-user configured sequence of commands to be sent to his router for each case: advertising, prepending, withdrawing, BGP session reset
   - Intelligence to collect from BGP status of attack sent by Security Cloud
   - Test Cloud traffic hijacking for an IP
2. Order online a new tunnel end-point
3. Connect your anti-DDoS equipment to tunnel and establish sessions with end-user router.
4. The anti-DDoS cloud will notify the Appliance to restore initial configuration one hour after an attack stops.

Frequently Asked Questions

How quickly is the attack filtered?

Traffic hijacking is not instant. Our experience shows that you will stop receiving over 90% of attack traffic in less than 20 seconds, while the remaining traffic might take one minute.

How long will the "hijacking" last?

To avoid BGP "route dampening," route hijacking will remain active for 60 minutes after an attack ends.

It really stops any attack?

Yes, it does. If someone figures out how to crack it, we will know in seconds and our security team will update the algorithms immediately.

Why should I use Voxility anti-DDoS cloud?

Because it is affordable and protects your network from the biggest threat: overrunning downstream bandwidth and anti-DDoS equipment when your network is targeted.

Will my customers know I use Voxility anti-DDoS Cloud?

A traceroute from inside end-user network will not show any new additional hop. Tracerouting from outside network will show different hops during an attack, but most of them are hidden. There are no other indications.

Will latency increase during an attack?

Yes, it will increase at maximum with the latency between your service location and the nearby Security Cloud.
We run 7 Security Clouds (1 in Asia, 3 in the US, 3 in Europe) and you will be connected to the one that has the lowest latency. Still, routes will not be as direct as they are coming from end-user datacenter.

Get an answer 24/7 to your question at
noc@voxility.com