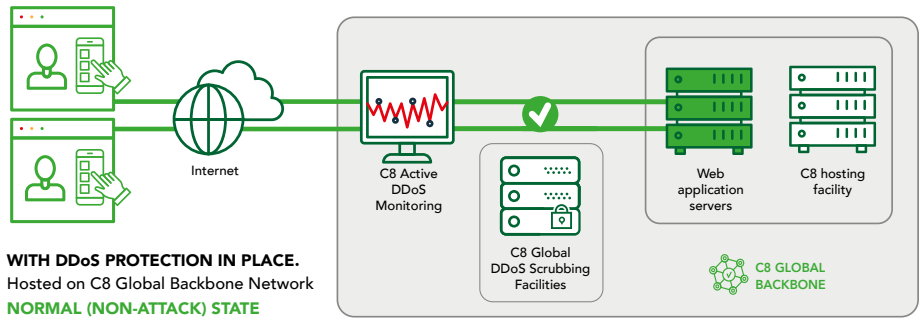# CONTINENT 8 technologies

DDOS | Secure

DDoS Protection | Platform Overview

The Continent 8 (C8) DDoS defence service is a mature, proven platform, built and developed over 16 years, using an optimised combination of technologies and our customised development layer. The key technology partners for our monitoring, detection and mitigation environments are Radware and Nokia.
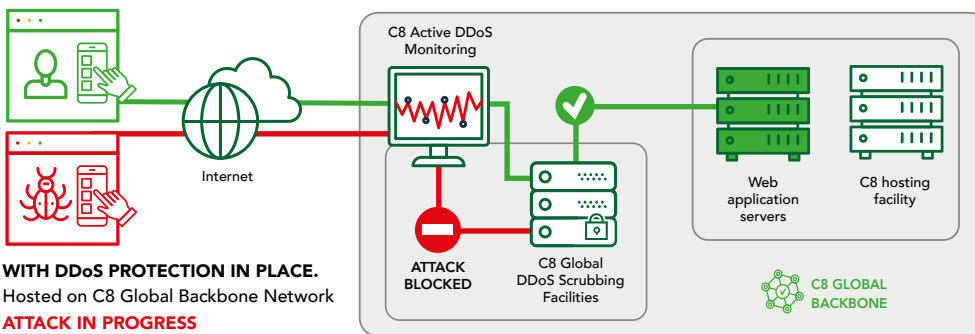
Typical time to mitigate a DDoS attack is 30-60 seconds

On-net protection

- On-net DDOS protection is for customers who are hosted within C8's data centres or utilise C8's IP bandwidth in third party locations.

- Customers can make use of C8 public IP address ranges or 'bring their own' Provider Independent ranges (subject to certain configuration criteria).

- On-Net mitigation of DDoS traffic is wholly under the control of C8 and will be achieved through automatic diversion using BGP route injection and dedicated VRF's.

Internet

C8 Active DDoS Monitoring

C8 Global DDoS Scrubbing Facilities

Web application servers

C8 hosting facility

C8 GLOBAL BACKBONE

WITH DDoS PROTECTION IN PLACE.
Hosted on C8 Global Backbone Network
NORMAL (NON-ATTACK) STATE

- Ingress traffic is distributed around the edge of the C8 network at a point closest to the source.

Internet

C8 Active DDoS Monitoring

ATTACK BLOCKED

C8 Global DDoS Scrubbing Facilities

Web application servers

C8 hosting facility

C8 GLOBAL BACKBONE

WITH DDoS PROTECTION IN PLACE.
Hosted on C8 Global Backbone Network
ATTACK IN PROGRESS

- Under DDoS attack conditions, traffic is diverted to the multi-node mitigation platform hosted within the C8 global backbone network. The platform selects to use the geographically closest scrubbing node to the source of the attack.

- In addition to scrubbing, network edge filtering can be achieved using BGP Flowspec. This can be deployed based on information shared by customers regarding their active ports and protocols.

- Real-time attack data can be seen by the customer in the C8 Portal, where custom whitelist configurations can also be created.

radware

Our Radware mitigation platform, which has been optimally integrated with our wider infrastructure, delivers a full suite of attack countermeasures that surgically remove attack traffic while maintaining legitimate traffic flow without interrupting network services.

Aggregate on-net scrubbing capacity of 1.2Tbps.

Total scrubbing capacity of 50Tbps+ is available through carefully designed upstream agreements and systems.

Global distributed architecture with four scrubbing centres in optimal geographic locations.

deepfield

Nokia Deepfield traffic monitoring and analysis delivers pervasive network visibility and actionable intelligence so we can proactively secure our customer network services, improve network performance and reduce costs.

Traffic is scrubbed at the closest entry point using our many Edge and IX locations in **Europe:** London, Dublin, Paris, Milan, Lisbon, Amsterdam, Marseille, Sofia, **North America:** New York, Newark, Los Angeles, Chicago, Dallas, Montreal, Toronto & **SE Asia:** Hong Kong, Singapore, Tokyo.

Off-net protection

- Off-net protection is available for customers that do not use C8's IP bandwidth.
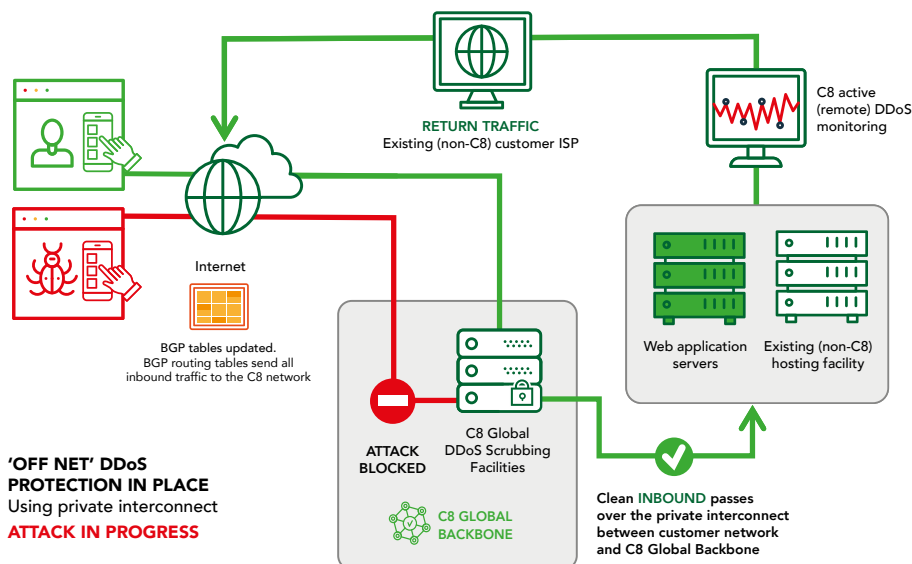- Customer Internet traffic can either be advertised permanently by C8 so that traffic is continually routed via our network for effective DDoS monitoring and automatic mitigation, or manually diverted to C8 in the event of a DDoS attack (subject to the customer's network configuration).

- C8 can assist with the remote monitoring of sites to identify any attacks and advise when our DDoS mitigation services are required.
- There are two options available for monitoring and returning traffic to the customer's hosted infrastructure: direct delivery via an encapsulated private circuit, or using a GRE tunnel across the Internet.

Off-net option 1: Direct delivery using a private circuit

- Physical connection installed between C8's global network and the border routers of the customers network (for resilience two separate circuits recommended).

- C8 will perform private monitoring and profiling of the customer traffic, via the private circuits, using NetFlow, BGP and SNMP information from the customer routing equipment.
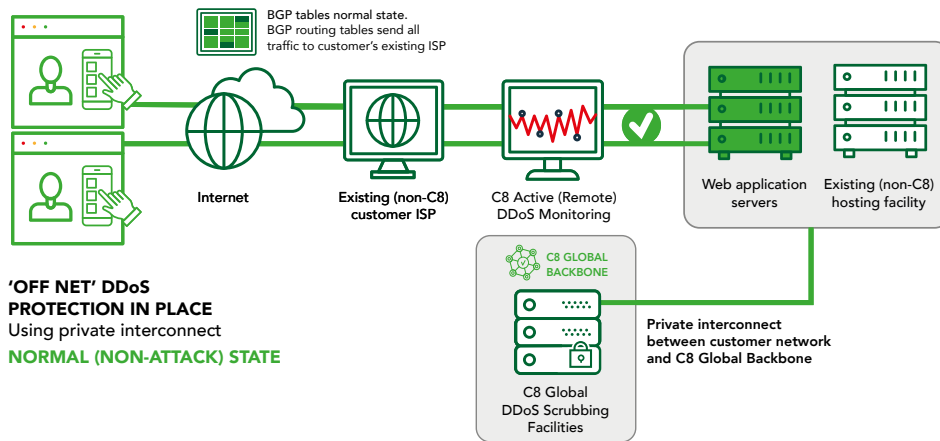
BGP tables normal state. BGP routing tables send all traffic to customer's existing ISP

Internet

Existing (non-C8) customer ISP

C8 Active (Remote) DDoS Monitoring

Web application servers

Existing (non-C8) hosting facility

'OFF NET' DDoS PROTECTION IN PLACE
Using private interconnect
NORMAL (NON-ATTACK) STATE

C8 GLOBAL BACKBONE

C8 Global DDoS Scrubbing Facilities

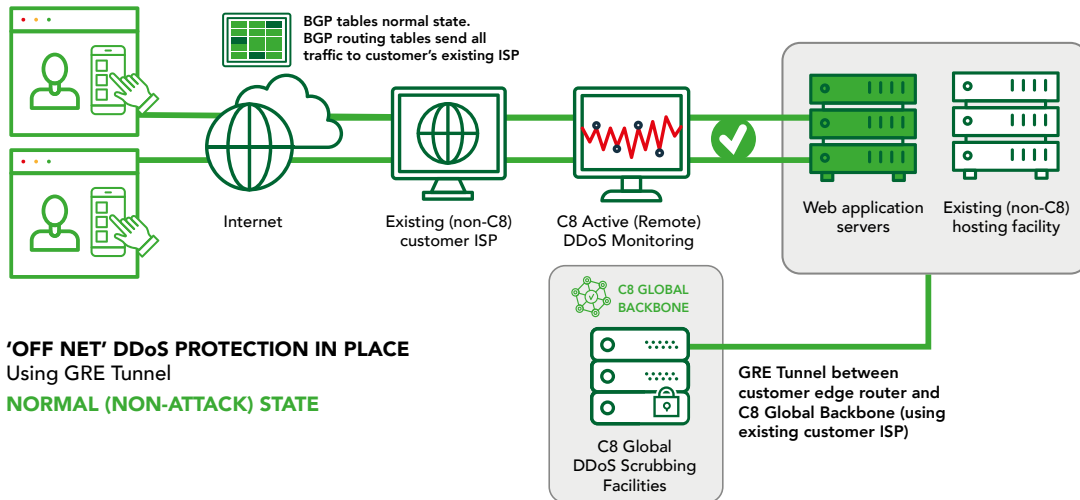Private interconnect between customer network and C8 Global Backbone

- When an attack is detected on a customer address range:
  - The address range will be advertised via BGP across C8's global network instead of with customer's existing ISP. (NB: the customer must have a minimum /24 provider independent public IP address space to subscribe to this service).

- All inbound traffic bound for the customer (both attack traffic and legitimate) will then be routed to the C8 network and 'scrubbed', with clean traffic passed to the customer over the private circuit(s). (Outbound traffic will still route from the customer to the Internet over their 'normal' ISP).

- This option is superior to using a GRE tunnel, as customer traffic is delivered over a private network on dedicated bandwidth, so backed by SLA.

RETURN TRAFFIC
Existing (non-C8) customer ISP

C8 active (remote) DDoS monitoring

Internet

BGP tables updated. BGP routing tables send all inbound traffic to the C8 network

Web application servers

Existing (non-C8) hosting facility

'OFF NET' DDoS PROTECTION IN PLACE
Using private interconnect
ATTACK IN PROGRESS

ATTACK BLOCKED

C8 Global DDoS Scrubbing Facilities

C8 GLOBAL BACKBONE

Clean INBOUND passes over the private interconnect between customer network and C8 Global Backbone
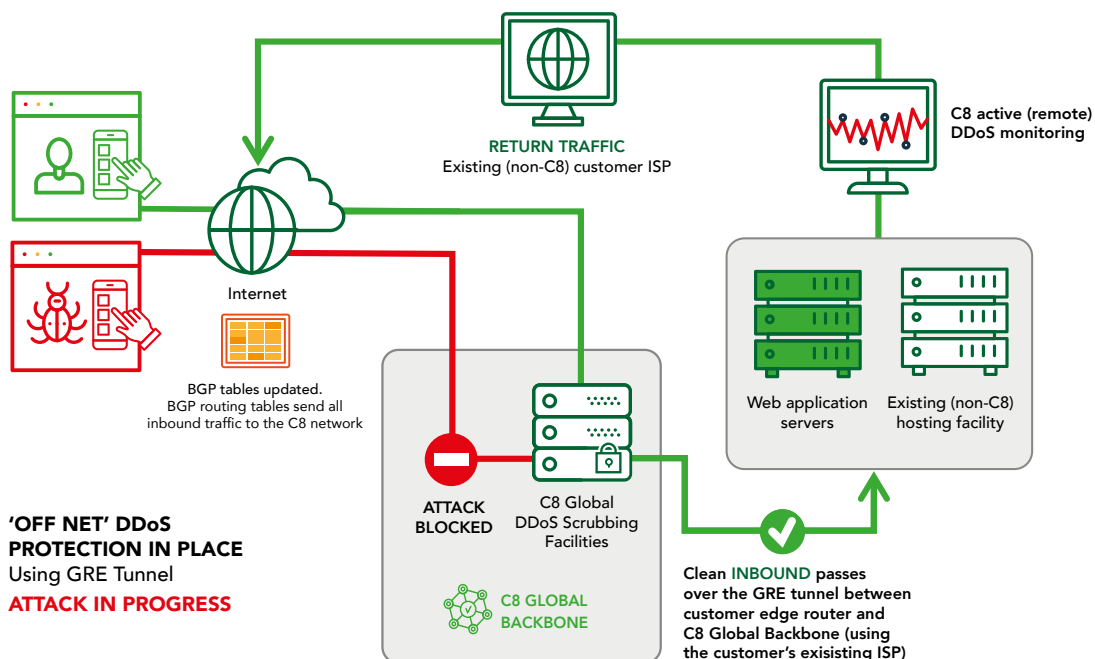
Off-net option 2 - IP Transit Delivery using a GRE Tunnel

- In this method, a GRE tunnel connection is established over the Internet between C8's core routers and customer's routers.

- When an attack is detected on a customer address range, the address range will be advertised via BGP across C8's global network instead of with customer's existing ISP. (NB: the customer must have a minimum 24 provider independent public IP address space to subscribe to this service).

BGP tables normal state. BGP routing tables send all traffic to customer's existing ISP

Internet

Existing (non-C8) customer ISP

C8 Active (Remote) DDoS Monitoring

Web application servers

Existing (non-C8) hosting facility

'OFF NET' DDoS PROTECTION IN PLACE
Using GRE Tunnel
NORMAL (NON-ATTACK) STATE

C8 GLOBAL BACKBONE

C8 Global DDoS Scrubbing Facilities

GRE Tunnel between customer edge router and C8 Global Backbone (using existing customer ISP)

- In the event of an attack, all inbound traffic bound for the customer (both attack traffic and legitimate) will then be routed to the C8 network and 'scrubbed', with clean traffic passed to the customer over the previously configured and tested GRE tunnel. (Outbound traffic will still route from the customer to the Internet over their 'normal' ISP).

- The GRE tunnel is able to retain all originating packet information, so the user's source IP and HTTP header info is all retained due to the encapsulation.

- This option is inferior to the direct delivery method, as delivery of traffic over the Internet cannot be guaranteed. Further, if the customer existing ISP (i.e. not C8) is being attacked, or has bandwidth volume issues, this method may not allow for successful mitigation.

RETURN TRAFFIC
Existing (non-C8) customer ISP

C8 active (remote) DDoS monitoring

Internet

Web application servers

Existing (non-C8) hosting facility

BGP tables updated. BGP routing tables send all inbound traffic to the C8 network

'OFF NET' DDoS PROTECTION IN PLACE
Using GRE Tunnel
ATTACK IN PROGRESS

ATTACK BLOCKED

C8 Global DDoS Scrubbing Facilities

C8 GLOBAL BACKBONE

Clean **INBOUND** passes over the GRE tunnel between customer edge router and C8 Global Backbone (using the customer's exisisting ISP)