DDoS MITIGATION

Addressing DDoS at a Network Level

Businesses are moving ever more services to the Data Centre, or Cloud platforms located therein, making them highly dependent on network availability. The potential impact of any outage has increased correspondingly, an inability to connect to the Internet results in immediate revenue and reputation impact. Thus, a key consideration for all clients within the Data Centre environment is security, both physical security and also against one of the greatest threats to service uptime, Distributed Denial of Service (DDoS) attacks.

Industry professionals and business analysts report that DDoS attacks are occurring more frequently, with greater volumes and increased sophistication. Recognising this issue, C4L has ensured that the coreTX network offers the very best protection from DDoS, by deploying the A10 Networks Thunder TPS, into the fabric of our coreTX network. A10 TPS provides high-performance, network-wide protection from DDoS attacks, maintaining service availability against a variety of volumetric, protocol, resource, and other sophisticated application attacks.

DDoS Threat Montoring & Analysis

The A10 TPS solution operates in conjunction with sophisticated network traffic analysis which monitors every device across our entire network estate. This solution features high-speed detection and 'network forensics' on all coreTX network traffic, allowing C4L engineers to monitor in real-time so that they can detect and alert suspicious activity. Our DDoS solution can scale in parallel with our traffic growth, delivering a total solution both in terms of performance and security.

Our network monitoring software constantly learns and understands the patterns of behaviour over the entire network, when any traffic starts behaving unusually, both the C4L Network Operations Centre (NOC) and the A10 TPS platform are alerted instantly. The solution protects the network as a whole, whilst remaining granular enough to allow specific rules to be defined at a per customer IP level where requested.

C4L DDoS Monitoring solution is deployed in the core of the network, such that all traffic which is available to external IP, Internet Transit, exchange and peering points, is constantly analysed. In this way the system develops a highly accurate picture of what 'normal' looks like, thus, abnormal behaviour is identified quickly and 'false positive' readings are minimised. As a result all On-Net customers of C4L automatically benefit from the network level service, any DDoS attack which occurs is quickly identified and rerouted, so that normal operation can continue.

Key Security Features

Multi-Vector Application & Network Protection

- Detect and mitigate protocol, application and network attacks
- Flexible scripting and deep packet inspection (DPI) for rapid response

High Performance Mitigation

- Mitigate high volume attacks in excess of 100Gbps
- Processing millions of packets per second

Modular Scalability

- Multi-site deployment for resilience
- Capacity to cluster additional nodes as traffic rates increase

Rapid Traffic Analysis & Threat Identification

- Entire coreTX network monitored for instant protection
- Upgrade to enhanced traffic 'scrubbing' per client, service or IP

Visit the website **www.C4L.co.uk/DDoS**

Or call **08000 470 481** to discuss your requirements

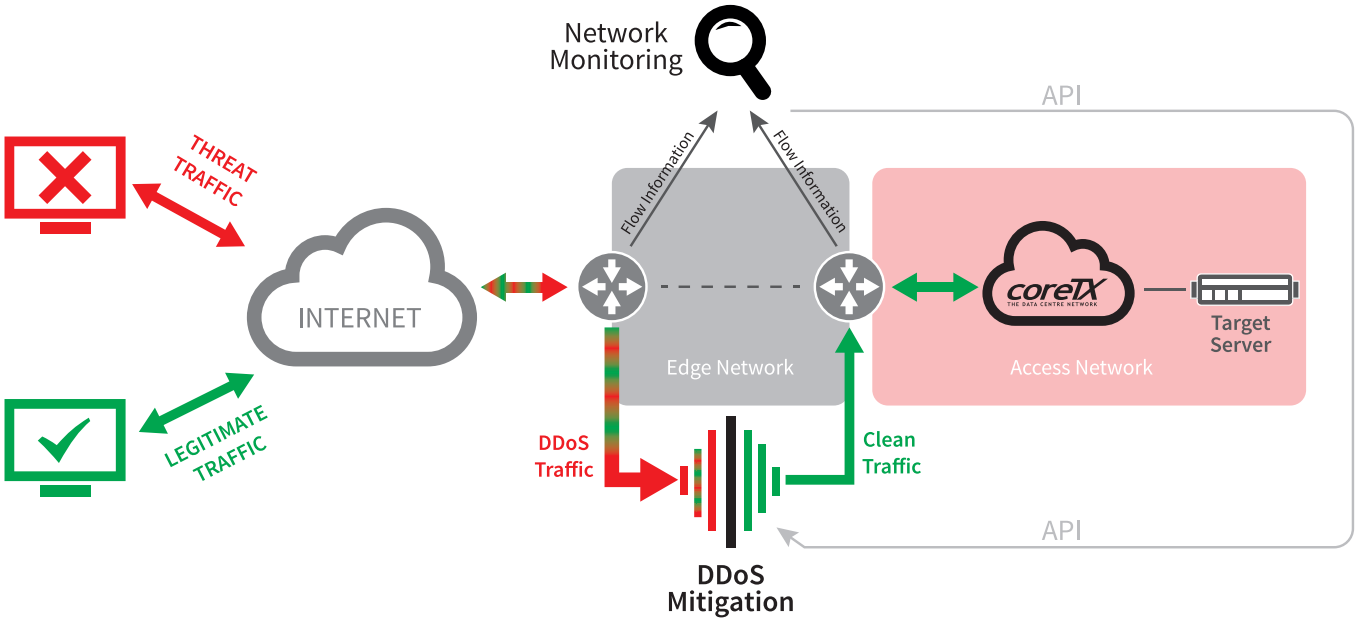
VIRTUS Data Centres

C4L Colocation • Connectivity • Cloud • Communications

DDoS Mitigation Service

In addition to highly effective network Monitoring which can quickly identify and reroute traffic, C4L offers a high performance DDoS Mitigation service, this premium service provides customers with clean IP traffic service which has passed through the A10 TPS solution prior to delivery. This service ensures that any DDoS attack which targets our customers critical Internet facing infrastructure will be 'scrubbed', ensuring that the DDoS threat is neutralised and normal service is maintained.

Because the C4L DDoS mitigation platform provides extremely large upstream capacity, we have the ability to receive very large amounts of DDoS traffic and still remain effective at cleansing the traffic and maintaining the service for our customers. Attacks in excess of 100Gbps can be successfully mitigated, with the platform processing millions of packets of data per second.



Service Definition

C4L DDoS mitigation provides a host of features to detect and mitigate multi-vector DDoS attacks with unprecedented performance scalability and deployment flexibility. The solution is able to detect and mitigate any level of attack, even if multiple attacks hit our network simultaneously. We support a vast set of features to validate, block or rate-limit the traffic entering our network, service availability is maintained by detecting and mitigating DDoS attacks of all types, whether they are pure volumetric, protocol / resource attacks, or even application-level attacks. The different styles of attack are defined below.

All C4L customers with equipment and services deployed 'On-Net' automatically benefit from 24x7x365 DDoS monitoring and analysis. In the event that an attack is identified, traffic will be routed away from the core network, ensuring that there is no loss or degradation of service as a result of an attack on a 'neighbour'. This is a standard benefit for all On Net customers, however, in the event that it is your specific server which comes under attack, then this will result in your traffic being dropped in order to protect the network.

The premium DDoS Mitigation solution ensures that your legitimate traffic will always be delivered to your platform even whilst under DDoS attack. In this solution, the DDoS traffic is routed through the A10 TPS platform and is 'scrubbed', to remove the DDoS traffic from the good traffic. The resultant clean traffic is delivered to your service at all times, ensuring that your solution is not impacted in any way. On Net customers can select standard IP transit, or DDoS mitigated IP transit at any time in order to take the benefit of this service.

C4L's commercial model offers a number of different DDoS Mitigation solutions. This allows our customers to choose if they wish to protect their entire IP transit commitment or focus the protection on specific devices, IP addresses or services only.

Detailed Feature List

Carrier-grade Hardware
- Advanced hardware architecture
- Redundant Power and Fans
- Access Control Lists (ACLs)
- MPLS traffic protection

Threat Detection & Analysis
- Manually controllable Thresholds
- Protocol Anomaly Detection
- IP/Port Scanning Detection
- Traffic indicator and Top-talkers

DDoS Actions & Redirection
- Drop packet & TCP Reset
- Dynamic Authentication
- Add to Black/White List
- Limit Concurrent Connections
- Limit Connection Rate
- Limit Traffic Rate (pps/bps)
- Forward to other device
- Remote Triggered Black Hole (RTBH)
- BGP Route Injection
- IPinIP (source and terminate)
- GRE Tunnel Termination

Protected Objects
- Source/Destination IP Address/Subnet
- Source and / or Destination Port
- HTTP, DNS, TCP, UDP, ICMP, URI and others
- DNS Query Type
- Class List/Geo Location

DDoS Protection: Flood Attacks
- SYN Cookies + Authentication
- ACK / DNS / SSL Authentication
- Spoof detection
- HTTP Challenge
- TCP/UDP/ICMP Flood protection
- Application (DNS/HTTP) Flood protection
- Amplification Attack Protection

DDoS Protection: Protocol Attacks
- Invalid Packets
- Anomalous TCP Flag Combinations (No Flag, SYN/FIN, SYN Frag, LAND attack)
- Packet size validation (Ping of Death)
- POODLE attack

DDoS Protection: Resource Attacks
- Fragmentation attack
- Slowloris
- Slow GET/POST
- Long Form Submission
- SSL Renegotiation

DDoS Protection: Application Attacks
- Regular Expression filter (TCP/UDP/HTTP)
- DNS / HTTP Request Rate Limit
- DNS Query Check
- HTTP Protocol Compliance
- HTTP Anomalies

DDoS Attack Definitions

Volumetric attacks: Typically DNS or NTP amplification attacks which are aimed to flood and saturate a victim's Internet connection, thus rendering services unavailable. C4L Mitigation service offers a variety of authentication techniques, amplification/flood attack mitigation and filter spoofed traffic. We apply highly granular, multi-protocol rate limiting to prevent sudden surges of illegitimate traffic to overwhelm our network and server resources. We can apply limits per connection, defined by bandwidth or packet rate on a per IP address basis.

Protocol attacks: For example SYN floods, ping of death, and IP anomalies which are aimed at exhausting a target system's protocol stack so it cannot respond to legitimate traffic. C4L detects and mitigates over 50 anomaly attacks in hardware to stop them before the system CPUs have to be involved. For example, SYN requests are validated, out of sequence segments are checked, TCP/UDP port scanning is activated and many more countermeasures are deployed.

Application attacks: Include more sophisticated attacks such as slowloris, HTTP GET flood or SSL-based attacks, these are specifically exploiting a weakness in an application's function or trying to make it unavailable. Though less frequent than Volumetric attacks, this style of attack is rapidly growing, increasingly complex and potentially devastating to target systems.

Visit the website **www.C4L.co.uk/DDoS**

Or call **08000 470 481** to discuss your requirements

VIRTUS Data Centres

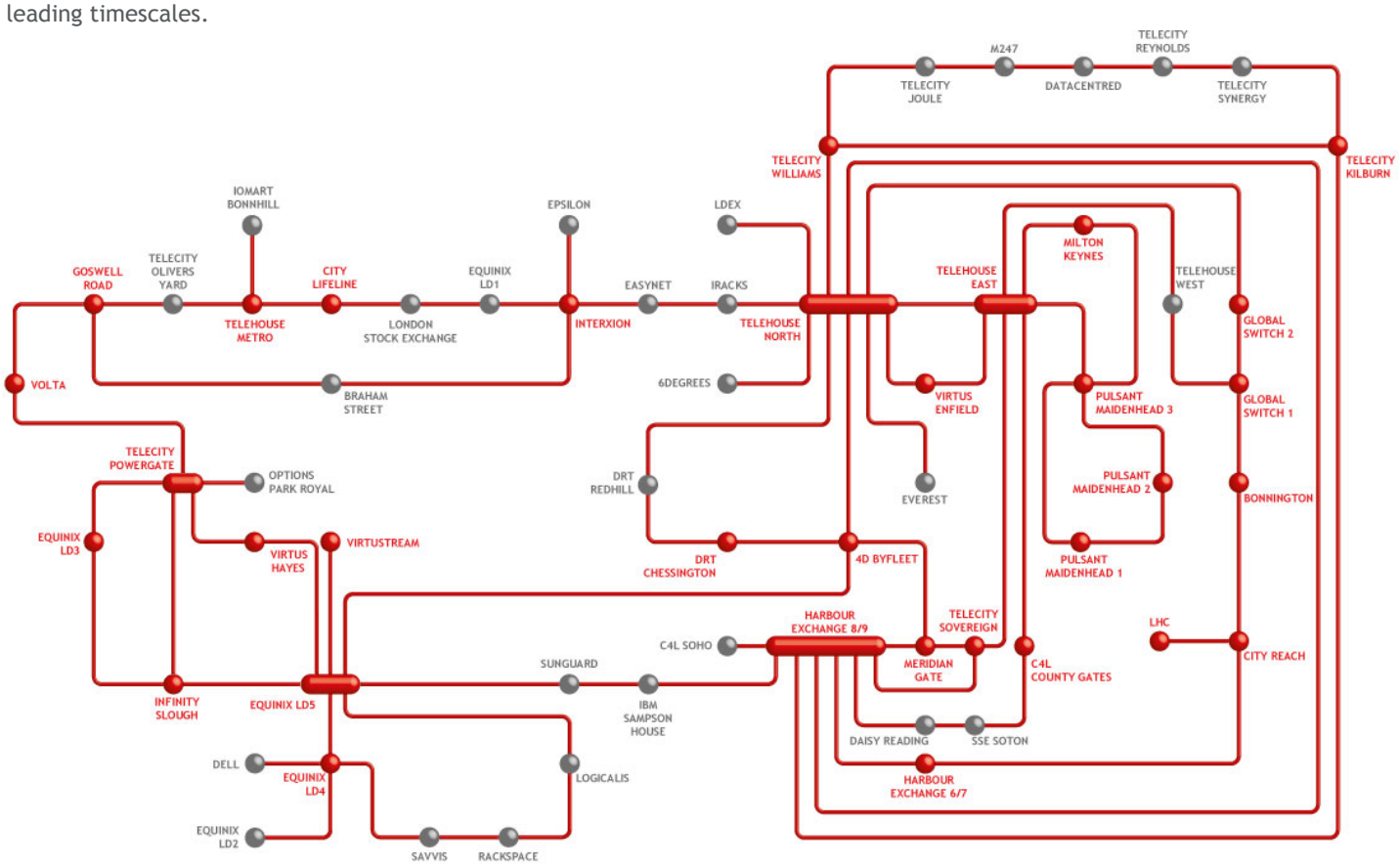
C4L Colocation • Connectivity • Cloud • Communications

coreTX
THE DATA CENTRE NETWORK

coreTX is C4L's high performance core transmission network, utilising privately owned fibre and spanning PoPs across the UK. coreTX delivers the highest capacity to the widest range of data centre locations within industry leading timescales.

Key:

- Primary coreTX network PoP, access to all products and services at 1GB/s and 10GB/s
- coreTX service access PoP, contact account manager to discuss requirements



C4L is a leading data centre colocation and connectivity solutions provider, with access to over 100 UK data centres and more than 300 globally. C4L offer a range of services including colocation, connectivity, cloud and communications. C4L own a data centre located on the South West coast and a fully privately owned, high-capacity, 1-100Gb fibre-optic network. This high performance MPLS network, called coreTX, links multiple data centres across the UK through a diverse fibre optic backbone, utilising routing and switching equipment from Juniper Networks, underpinned by A10 Thunder Protection System DDoS protection and mitigation appliances.

C4L clients include government agencies, FTSE 250 companies, international financial institutions, system integrators, top 100 VARs, resellers and many of the UK's network carriers. C4L's entire business is committed to customer satisfaction and quality of service and has achieved certifications such as ISO9001 & 27001 to demonstrate this. C4L is a Megabuyte Top 50 Company, HSBC South West Business Thinking initiative Winner, a Deloitte Technology Fast 50 and Fast 500 EMEA Company, as well as a Sunday Times Microsoft Tech Track 100 company.

megabuyte 50 company 2015
Revealing the UK's best-performing privately owned tech companies

2014 FINALIST SVC awards

The ISPAs FINALIST Best Dedicated Hosting 2014

INVESTORS IN PEOPLE

Visit the website **www.C4L.co.uk/DDoS**

Or call **08000 470 481** to discuss your requirements

VIRTUS Data Centres

C4L Colocation • Connectivity • Cloud • Communications