

Insight Guide into Securing your Connectivity

Cyber Security threats are ever present in today's connected world. This guide will enable you to see some of the innovative ways Stream Networks are securing our customers' Internet connectivity – providing possibly the most secure Internet service from a UK business ISP ever.

Our intelligent network technologies can be rapidly deployed to deliver cost savings and provide multiple layers of protection from outside attack.



Don't I just need a good Firewall?



Businesses and organisations of all sizes are being challenged to extend their networks to more people, places and things than ever before. The rise of Cloud, SaaS, mobile devices, and Internet of Things (IoT) technologies are forcing more network traffic over the public Internet.

As a result, the threats posed to an organisations IT security are increasing exponentially and with the implementation of

DDoS Protection

A Distributed Denial of Service (DDoS) attack is when an overwhelming level of traffic is purposely channelled to an online service resulting in a negative performance. They are becoming more and more commonplace, and worryingly more and more sophisticated. This means there has never been a more relevant time to protect your networks.

GDPR legislation, the failure to protect your organisation from Cyber-attack is also costly.

This shift is being felt in IT across virtually every industry.

What's becoming increasingly clear is that securing your Internet Connectivity by an on premise Firewall alone no longer provides complete peace of mind.

Stream Networks have developed a unique proposition that incorporates DDoS protection alongside an additional highly resilient Cloud Firewall service that sits between the edge of our Core Network and the Customers network connection/s to ensure all connections are ultra-secure.

DDoS attacks use a network of botnets, which are infected computers to launch attacks against any target. Once infected, these botnets will try to overwhelm targets by sending high volumes of connection requests or random data.

A DDoS attack that can take down an SME for a week can be purchased for just \$150!

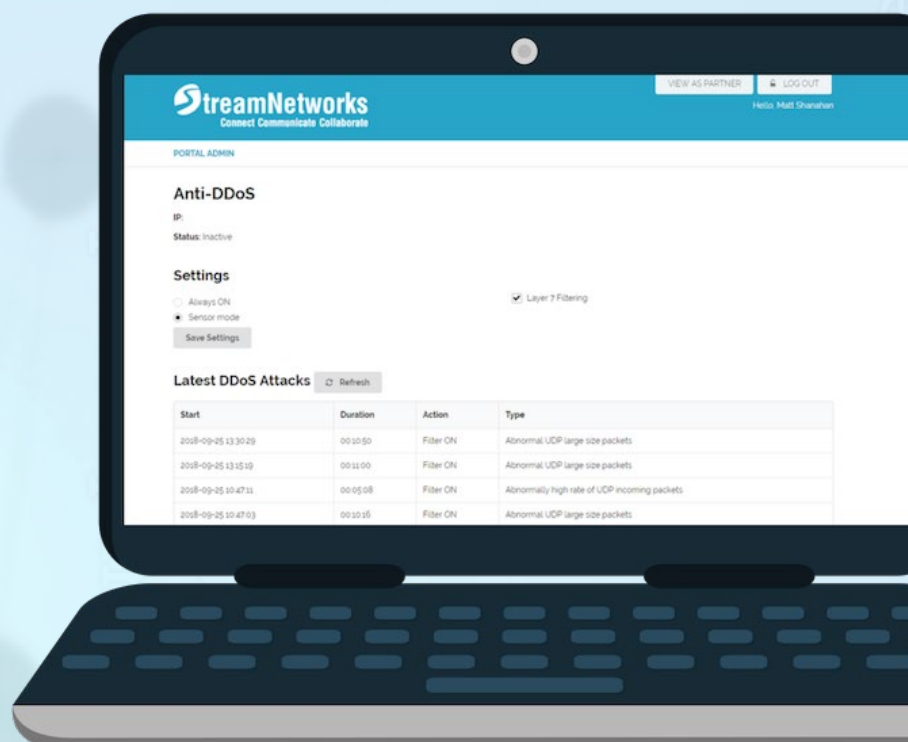
How the Stream network mitigates against DDoS

Using our peering partners, our connectivity and Cloud solutions come with default DDoS protection as standard. Our network advertises your public Facing Internet addresses via our DDoS Scrubbing Centres. DDoS Scrubbing means that your service stays online during an attack. Your incoming and outgoing traffic is analysed with malicious traffic being removed and filtered, clean traffic is then passed on for delivery to your network.

The Stream Scrubbing Centres are located in 9 Data Centres in 8 cities within the EU and US and have The ability to filter attacks up to 1TBS in size meaning that it its virtually impossible to flood a Stream Networks DDoS protected Internet connection or Cloud Server.

DDoS Features and Benefits

- + Attacks against your network are filtered up to 1Tbps in size
- + Analyse your DDoS protected traffic in real time via our innovative portal
- + Solution works in real time, 24x7x365
- + Keeps your business and key Internet services on at all times – we won't black hole your service.



Types of DDoS attacks that are filtered

- + IP non-existing protocol attacks
- + ICMP & IGMP attacks; ICMP Flood, SMark, Smurf Attack, ICMP Flood
- + Layer 7, HTTP attacks; Slowloris, RUDY, HTTP Object Request Flood
- + TCP attacks/floods; SYN, SYN-ACK, ACK, FIN, RST, TCP, EXE, TCT NULL, Fake session
- + Fragment attacks such as mangled IP fragments with overlapping and oversized payloads to target machines
- + UDP attacks; Fraggle, DNS query, DNS Amplification, SNMPv2, NetBIOS, SDP, CharGEN, BitTorrent, Stream protocol

Think you've got nothing to worry about?

FIFA, Uber, Google, Facebook, British Airways, Talk Talk, Pizza Hut, Yahoo, Bupa, Wonga, Sage, Three Mobile – the list goes on.

What do all these companies have in common? They have all been subject to cyber-attacks that have led to mass data breaches.

Another thing all these companies have in common, maybe something they have in common with you too... they all thought their network was secure – if only they were using Stream Networks.

How a Cloud Firewall provides additional security



Stream Networks operate and own two high availability Cloud platforms (OpenStack and VMware) within multiple UK Data Centres. Our primary site is located within a nuclear proof ex MOD bunker that meets multiple compliancy standards including ISO27001, PCI DSS and IGGSOC.

Our Cloud Firewall service sits at the edge of our Core Network providing an additional level of Firewalling between our core and your edge connectivity. Based on trusted firewalling technology) customers also have the choice of deploying a cloud firewall from the vendor of their choice be it Fortinet, Palo Alto, Sophos, SonicWall; any Firewall vendor that provides their platform as a Virtual appliance.

All customer Internet traffic incoming and outgoing passes through the Cloud Firewall ensuring that traffic is filtered within the Core network before arriving at the end point, where if required, traffic can be firewallled and filtered a second time via an on premise Firewall.

In addition to providing Firewall protection within the Core, our Cloud Firewall Service allows for any Stream Networks connection to terminate as a LAN connection on the Cloud Firewall allowing customers to build a hybrid MPLS/SD-WAN adding additional sites into the network with ease, whilst managing the IP addressing schemes and Firewall rules from a single interface.

Cloud Firewall Features

Firewall and Router

- + Stateful Packet Inspection (SPI)
- + GeoIP blocking
- + Anti-Spoofing
- + Time based rules
- + Connection limits
- + Dynamic DNS
- + Reverse proxy
- + Captive portal guest network
- + Supports concurrent IPv4 and IPv6
- + NAT mapping (inbound/outbound)
- + VLAN support (802.1q)
- + Configurable static routing
- + IPv6 network prefix translation
- + IPv6 router advertisements
- + Multiple IP addresses per interface
- + DHCP server
- + DNS forwarding

VPN

- + IPsec and OpenVPN
- + Site-to-site and remote access
- + VPN support
- + SSL encryption
- + VPN client for multiple Operating systems
- + L2TP/IPsec for mobile devices
- + Multi-WAN for failover
- + IPv6 support
- + Split tunnelling
- + Multiple tunnels
- + VPN tunnel failover
- + NAT support
- + Automatic or custom routing
- + Local user authentication or RADIUS/LDAPPPoE Server

Intrusion Prevention

- +Snort-based packet analyser
- +Layer 7 application detection
- +Multiple rules sources and categories
- +Emerging threats database
- +IP blacklist database
- +Pre-set rule profiles
- +Per-interface configuration
- +Suppressing false positive alerts
- +Deep Packet Inspection (DPI)
- +Optional open-source packages for application blocking

Stream Cloud Firewall Benefits

- + Attacks against your network are filtered within our core network before reaching the endpoint Firewall
- + Use free OpenSource technology or deploy vendor approved virtual appliances.
- + Add on additional network connections managing IP addressing and firewall rules from a single interface
- + Build a Hybrid MPLS/SD-WAN network providing greater control over your network



Next steps

To fast-track a conversation, simply click on the link below to send us an email and one of the team will call you back straight away.

[Call me now regarding ultra-secure connectivity](#)



Stream Networks Ltd
info@stream-networks.co.uk
01635 884170

About Stream

Stream Networks has been built for business use, enabling our customers to leverage the power of our 10GB network capacity and benefit from our peering agreements by lowering costs and increasing bandwidth.

Our core is built using Cisco and Juniper to provide a fully meshed network between four key UK Data Centres, at which point we extend our footprint with our peering agreements and connections into the major carriers. Our network is managed and monitored 24x7x365 to ensure your business stays connected.

With a significant capital investment in our high availability Cloud infrastructure (which continues to grow each year), businesses are able to realise the benefits of moving computing to the cloud whilst knowing their data is secure, UK-based, and available 24x7x365. Based in our core UK Data Centres, each cluster is designed to provide 100% uptime, and comprises the latest in replicated storage arrays, network capacity, and processing power, all built using VMware's HA HyperVisor.