Application Performance

An effective security solution needs not only to protect data and sensitive material, but also make websites open, load and work faster.

The speed with which websites function is critical to retaining users and preventing them from turning to competitors.

Key Benefits

- Accelerates application functionality
- Reduces apparent wait time for site visitors
- Reduces resource usage
- Optimizes the use of existing resources with no on-site installation, tuning, or server upgrades required
- Available in routed-proxy and reverse-proxy deployment modes

The need for speed

For businesses, speed with which websites function has considerable real-world commercial impact. For example, Google estimates the potential revenue impact gain from improving the speed a website loads by as little as one second at more than USD 760,000.

DoubleClick by Google research suggests that 53 percent of mobile site visits are abandoned if a page takes longer than three seconds to load.

How we ensure speed

Once undesirable traffic is removed, we deploy several techniques to ensure data security and optimize performance.

Our Application Performance measures are subdivided into four key areas: compression optimization, TCP optimization, multiplexing, and dynamic load balancing.

→

1. Compression optimization

We use compression algorithms supported by http, for example ".gz" to reduce the size of data packets sent to clients to 65kb. By reducing the size of the data packets, we increase the speed with which data can be sent, thereby making substantial efficiency improvements and service enhancements for end-users.

2. TCP optimization

The Transmission Control Protocol/Internet Protocol "stack" (TCP/IP) is the cornerstone of today's digital infrastructure and enables systems to communicate with each other. TCP ensures that the size of data packets is identical, and that recipient systems inform sender systems that data has been received. It also ensures that data packets arrive at their intended destination in the correct order. TCP also governs the flow of data between end-points, and between the IP layer below the TCP, as well as layers above it.

3. Multiplexing

As more clients access a server, that server needs to establish and maintain connections with those clients. This requires memory space on the server, and this increases as the number of sessions grow and existing sessions continue. Our Threat Protection Platform (TPP) helps reduce the effects of this by leveraging multiplexing.

Multiplexing is a technique that reduces the number of connections the protected server needs to maintain. Within our Threat Protection Centers™ (TPC™) we connect to the back-end server and establish single outbound connections from tens of thousands of inbound connections. This means that the back-end server is required to deal with a substantially smaller number of connections, thereby reducing memory use and CPU load. This also allows servers to maintain a greater number of page views at the same resource footprint. We effectively save resources on the back-end server, making it faster, safer and more cost effective.

4. Load balancing

We support static and dynamic load balancing.

Static load balancing evenly distributes connections across multiple servers. We use round robin load balancing, which distributes load to each node in circular order returning to the first node in the "circle" once the last node has been allocated load. Each node maintains its load index independent of allocations from the remote node.

Dynamic load balancing allows the allocation of load balance across multiple servers by measuring the relative load on each server and distributing load based on available capacity and server speed.

➞

This allows servers to be pooled with different configurations, (for example different amounts of memory or different CPUs), without the risk of overload.

With our dynamic load balancing service, we receive connections from the internet, which we then send back as requests to typically two or three servers. We monitor how many requests are made as well as the amount of time it takes for respective servers to respond by sending data back to us.

Threat Protection Centers™ (TPC)
Amsterdam, New York, Los Angeles, Singapore, Stockholm, Frankfurt, Dubai, Tokyo (2019), London (2019), Miami (2019)

RiverView™

Our RiverView™ portal monitors attacks in real-time. It provides statistics on all traffic and attempted attacks and a comprehensive reporting function allows clients to create daily, weekly and monthly reports.

You receive the best possible protection from fresh attacks with our Security Operation Center which monitors the constantly evolving threat landscape around the clock.

Regardless of where your assets are located – on premises, in cloud-based platforms, third party hosts – our Threat Protection Platform is equipped to provide multi-vector threat protection to all deployed assets.