Dedicated Firewall

Our Dedicated Firewall services protect your corporate network from unauthorised access and other Internet security threats. Such threats are ever evolving and so is our Dedicated Firewall to ensure that it offers the latest generation of advanced security measures to counter targeted attacks. Avoid threats such as hacking and attempts to exploit vulnerabilities of your system by implementing a Dedicated Firewall to protect your network and the data it contains.

Without a firewall in place you face the risk of such attacks, alongside virus infections from malicious websites. Legacy firewalls may not have the capability to cope with advancing technology, such as Cloud and bandwidth hungry applications, meaning that it may suffer and leave you vulnerable.

Implementing a Dedicated Firewall

A Dedicated Firewall is ideal for single-site location, particularly those that as constantly increasing the bandwidth they require to use. Similarly Dedicated Firewalls are an option for multi-site locations that use a centralised Internet connection, enabling the Network to remain protected against the latest security threats.

Our Dedicated Firewall solution includes a broad range of technologies to provide the flexibility required to protect your corporate network. Each Dedicated Firewall supports core security technology, such as an Intrusion Prevention System (IPS) ant-virus, web filtering, email filtering, IPSec and SSL VPNs.

Our service desk team offers 24 / 7 x 365 support, and as part of our Dedicated Firewall service we undertake regular software patching and upgrading to ensure that our service is operating at the highest levels. In line with industry best practise and our ISO 27001 accreditations we also run routine configuration backups and changes.

DEDICATED FIREWALL FEATURES

• Control access to your Network.
• High availability as Standard.
• Stateful inspection.
• Control TCP port access.
• Health monitoring.
• Configuration backup.

UNIFIED THREAT MANAGEMENT FEATURES

• Anti-Virus
• Email Filtering
• Web Filtering
• Intrusion Prevention System (IPS)
• Application Control

DEDICATED FIREWALL BENEFITS

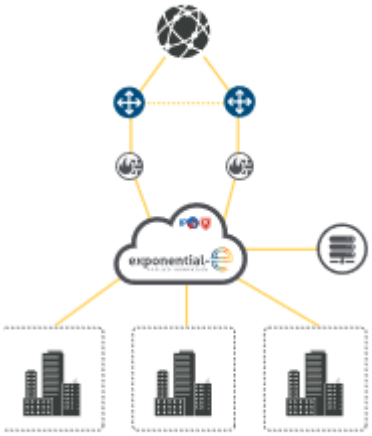
• High-performance protection against today’s wide range of advanced threats.
• Security is enhanced, managed and maintained by accredited security experts. Constantly monitored and regularly updated to protect against the latest threats.
• Secure remote access using encrypted VPN’s for home workers and remote sites. Stringent SLA Agreement for maximum availability and peace of mind.
• Professionally managed to ISO27001 security standards.

Single Managed Dedicated Firewall
This is a common deployment method when the customer takes a direct Internet connection and has the firewall located at their site to provide the barrier between trusted and untrusted Networks, and is suitable for small and non-critical sites.

Resilient Site Managed Dedicated Firewalls
For sites running critical business Networks and applications and needing to minimise outages from a Network or firewall failure. A resilient solution can be provided using both, resilient Connectivity over diverse routes, combined with High Availability firewalls.

Resilient Centralised Internet Breakout Managed Dedicated Firewalls
The Centralised Internet Breakout Dedicated Firewall solution provides a solution to consolidate Internet access for multiple sites through a resilient HA (High Availability) pair of firewalls with multiple threat management capabilities.

Multi-tiered Firewalls
For the most secure design multi-layered firewalls are deployed at various levels in the Network and can optimise a mix of firewall vendors to further minimise the possibility of hackers attempting to exploit vulnerabilities. The solution also provides the ability for additional threat management capabilities to be added.



Resilient Centralised Internet Breakout - Diverse Sites
The Centralised Internet Breakout Dedicated Firewall solution can be further enhanced to use diverse sites for the location of each of the High Availability pair of firewalls, providing further protection against a disaster failure impacting the active site, and causing the passive site to take over.