Dedicated Firewall

High-performance Network Security Solution

[COMPANY NAME]’s Dedicated Firewall solution ensures the safeguarding of your corporate network against unauthorised access and emerging internet security threats. With ever-evolving risks, our dedicated network security solution continuously adapts to incorporate the latest advancements in security measures, effectively countering targeted attacks. By implementing our dedicated network security solution, you can mitigate threats like hacking and exploitation attempts, fortifying your network and protecting the sensitive data it holds.

Operating without a firewall leaves you vulnerable to such attacks and leaves your system exposed to virus infections from malicious websites. Traditional firewalls may struggle to keep up with advancing Cloud technologies and bandwidth-intensive applications, compromising their effectiveness and leaving you susceptible to breaches.

Implementing a Dedicated Firewall

Our Dedicated Firewall solution is particularly suitable for single-site locations, especially those experiencing an increase in bandwidth demands. It is also an excellent choice for multi-site locations that rely on centralised internet connections, ensuring comprehensive protection against the latest security threats.

The solution encompasses a comprehensive array of technologies, providing the necessary flexibility to safeguard your corporate network. Each dedicated network security solution includes core security components such as an Intrusion Prevention System (IPS), antivirus protection, web and email filtering, as well as IPSec and SSL VPNs.

As part of our commitment to delivering exceptional service, our dedicated service desk team provides round-the-clock support, 365 days a year. Additionally, we regularly perform software patching and upgrades to maintain peak performance. Following industry best practice and our ISO 27001 accreditations, we also conduct routine configuration backups and changes.

Key Features

* Anti-Virus: Defends against viruses, worms, Trojans, spyware, and malware.
* Email Filtering: Identifies spam from known domains and websites, preventing inboxes and email servers from being inundated with unwanted messages.
* Web Filtering: Enforces acceptable user policies, blocking malware and viruses from malicious websites.
* Intrusion Prevention System (IPS): Prevents attacks by hackers utilising known vulnerability techniques.
* Application Control: Identifies and controls applications, particularly those known to circumvent firewall port blocking.

Benefits

* High-Performance Protection: Safeguards against a wide range of advanced threats prevalent today.
* Expert Management and Maintenance: Accredited security experts oversee security operations, ensuring constant monitoring and timely updates to counter the latest threats.
* Secure Remote Access: Enables secure remote access through encrypted VPNs, catering to home-based workers and remote sites.
* Stringent SLA Agreement: Provides maximum availability and peace of mind with a robust service level agreement.
* ISO27001: Professionally managed according to the highest security standards.

Deployment Options

Single Managed Dedicated Firewall: This common deployment method is suitable for customers with a direct internet connection who choose to position the firewall at their site. It establishes a barrier between trusted and untrusted networks and is ideal for small and noncritical sites.

Resilient Site Managed Dedicated Firewalls: For sites running critical business networks and applications that require minimal downtime due to network or firewall failures, a resilient solution is provided. This includes high-performance connectivity over diverse routes combined with high-availability firewalls.

Resilient Centralised Internet Breakout Managed Dedicated Firewalls: This solution consolidates internet access for multiple sites by employing a resilient pair of high-availability firewalls with comprehensive threat management capabilities.

Multi-tiered Firewalls: For the utmost security, multi-layered firewalls are deployed at various levels within the network. This approach allows for the optimisation of different firewall vendors, further reducing the risk of hackers exploiting vulnerabilities. The solution also facilitates the addition of supplementary threat management capabilities.

Resilient Centralised Internet Breakout – Diverse Sites: Building upon the Centralised Internet Breakout Managed Dedicated Firewall solution, diverse sites are used to locate each high-availability firewall.