

Managed Security Gateway: Guarding Your Business

It has often been said that the only way to ensure 100% security online is to cut your Internet connection.

Since that approach is hardly practical, the more realistic practice has been to secure your Internet gateway with a variety of purpose-built applications that enforce a series of checks and controls. These controls both manage your employees' access to the outside world, and more important manage the outside world's access to your employees.

Despite their crucial role in today's infrastructure, however, most security systems can be tricky to configure, require constant attention and frequent updating. As a result, many companies install security software they think will keep doing the trick well into the future, never realising that those tools may leave them vulnerable to attackers that show remarkable tenacity exploiting software vulnerabilities.

Why not let BlueFire worry about all that? After all, we've spent millions building a world-class enterprise infrastructure – and we've invested heavily in modern security solutions to protect that investment. Thanks to our Managed Security Gateway (MSG) service, all of our customers benefit from that same investment, getting a clean and safe Internet feed for their business.

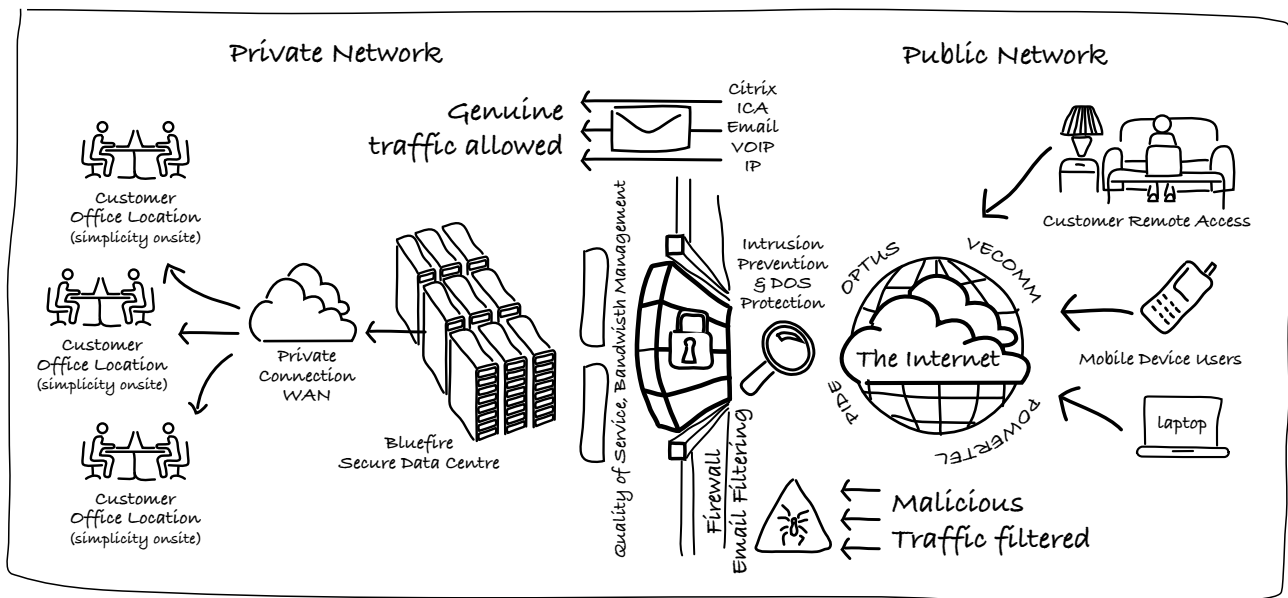
Using combinations of industry-leading security solutions from Cisco, Checkpoint and Allot networks, these core network security capabilities including managed multiple firewalls, intrusion prevention and quality of service systems that inspects every packet of information entering or leaving the datacentre. This is complimented by a full suite of content security services including virus scanning, spam detection, Web content filtering, anti-spyware checking, FTP content inspection, URL filtering, worm protection and filtering of applications such as peer-to-peer services, instant messaging and remote control. Remote access is supported via multiple secure options of Cisco VPN and SSL Access with RSA Dual Factor Authentication to provide travelling workers with totally secure access to your network resources.

These tools are available to any company, but MSG combines them with expertise that isn't. Our team of specially trained security professionals, working to the guidelines of the Banking Grade Security qualification for Information Security, monitor and manage our security infrastructure 24/7 and provide technical support, monitoring, reporting, and access to breaking security news.

Providing tight Internet security isn't easy, but we know how. By letting our experts take care of the hard part, you can rest easy that your corporate data and applications, hosted and run as part of BlueFire's comprehensive managed services portfolio, are totally protected with a multi-layered, scalable security gateway. It's the next best thing to cutting the cord – but a lot more useful.

"Blue Fire stood out from its competitors by understanding the nature of our business allowing for growth and expansion. This combination has instilled our confidence in Blue Fire's ability to ensure the security of our business. Blue Fire's standards were impressive with their highly detailed and professional data systems where all of our confidential data is protected and safely stored."

Tony Melvin. Managing Director, Chan Naylor



features...

description...

Highly Available Internet and WAN Services	<ul style="list-style-type: none"> Redundancy ensures availability of links between BlueFire customers' branch offices Fully redundant network infrastructure and environmental systems ensure internal resiliency
Managed Firewalls	<ul style="list-style-type: none"> Full firewall configuration and monitoring Multi-tiered firewall design allows segregation of networks with different security classifications
Managed Intrusion Prevention and Visibility	<ul style="list-style-type: none"> All inbound and outbound traffic is scanned for malicious content and surreptitious intrusion attempts in real time Accredited policies, response plans and operational procedures ensure a swift and appropriate protective response to new threats Customised reporting highlights each MSG customer's security profile and exposure
Content Filtering	<ul style="list-style-type: none"> Industry-leading content scanning identifies and isolates malicious and spam emails before they get a chance to congest your inbox or damage your systems URL and Web site filtering blocks offensive and harmful content according to policies that are set and enforced at the managed gateway – and, therefore, can't be circumvented by employees Scanning happens at BlueFire's data centre without the need for customer intervention; all they see is a safer, cleaner Internet experience without the hassles.
Internet Peering	<ul style="list-style-type: none"> BlueFire's Internet peering service enables free interchange of data between Internet service providers
Physical Security	<ul style="list-style-type: none"> Our highly secure physical environment has multiple layers of access control to ensure that only authorised personnel can get anywhere near our systems – and your data Highly granular access control is enforced across all of the digital assets in our environment, regardless of whether they're accessed from inside our network or outside it
Network Backbone	<ul style="list-style-type: none"> BlueFire operates a high-speed, switched Gigabit Ethernet network backbone that ensures optimal performance for all of our managed services
Monitoring and Reporting	<ul style="list-style-type: none"> Use of enterprise reporting tools such as Netflow provide trend analysis, Layer 7 packet screening and many other features to ensure communication services are managed as effectively as possible Open and transparent reporting to customers ensures service level agreements (SLAs) are met
Quality of Service	<ul style="list-style-type: none"> BlueFire's switched network infrastructure has been designed with full quality of service (QoS) capabilities QoS enables prioritisation of time-critical traffic such as voice over IP, Citrix thin-client desktop sessions, and other business critical applications – ensuring the most important functions perform at their best
Change Control	<ul style="list-style-type: none"> Stringent internal configuration and change control procedures ensure any requests are properly authorised Every change is assessed against potential risk to ensure nothing compromises client connectivity