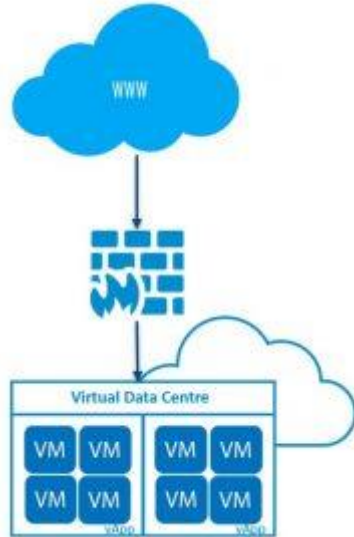


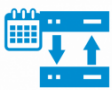
Shared Firewall

All Cloud Servers and Virtual Data Centres are protected through our shared managed firewall appliances. There is no need for you to configure or manage a guest operating system based firewall on your server, such as IP Tables on Linux and Windows Firewall for Windows Server. The shared firewall is for perimeter security and is used to filter network traffic to protect your servers from external threats.



The shared firewall service is based on next generation firewalls and includes advanced security features including Intrusion prevention system (IPS), web filtering, secure sockets layer (SSL) inspection, application control and automated threat protection. The shared firewall service is enabled by default and allows for customized policies for incoming and outgoing traffic to meet application(s) access requirements.

The shared firewall also allows for the configuration of a virtual DMZ to allow the separation of front-end and back-end systems. An SSL VPN software client is provided at no charge for up to 20 users who require access secure remote access. The service also includes up to 5 site to site IPSEC VPN tunnels

 Secure access to your servers with next generation firewall features	 Intrusion prevention & anti-virus scanning	 1 free DMZ	 5 x free IPSEC tunnels
 Managed by Security Experts	 Customised Policies	 Up to 20 VPN users	 Cost effective monthly OPEX fee

Shared Firewall – Virtual Domain

Should you require multiple DMZ's, dedicated internet access, we recommend our Shared Firewall Virtual Domain Service.

This Virtual Domain service provides a virtual instance of a Firewall appliance. The Virtual Domain is managed by security experts and requires no capital outlay for a firewall appliance.

 Secure access to your servers with next generation firewall features	 Intrusion prevention & anti-virus scanning	 Multiple DMZ	 5 x free IPSEC tunnels
 Managed by Security Experts	 Customised Policies	 Up to 20 VPN users	 Cost effective advanced firewall service

Dedicated Firewall

We offer a Dedicated Firewall service for customers who require hardware based firewall appliances for single tenant use. The Dedicated Firewall service is co-located within the hosted environment and can be combined with our Cloud Server, Virtual Data Centre or Dedicated Server services. The service includes management by security experts and is offered as a monthly fee. A range of Dedicated Firewall options are available based on your requirements.

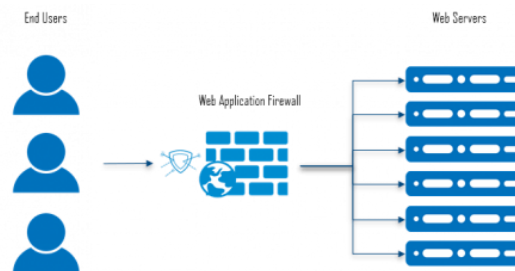
 Secure access to your servers with next generation firewall features	 Intrusion prevention & anti-virus scanning	 Multiple DMZ	 Multiple IPSEC tunnels
 Managed by Security Experts	 Customised Policies	 Free VPN software clients	 Monthly OPEX fee (cost per VM & GB per month)

Web Application Firewall

Web applications are often business critical and require specialised security to protect the service and information contained within. Dynamic web applications typically require additional security than standard firewall services.

Our Web Application Firewall service includes Web Application Firewall functionality as well as load balancing and web acceleration to ensure websites or application services perform optimally and are secured.

The Web Application Firewall filters, monitors and blocks malicious web traffic as well as protects against application vulnerabilities.



 Web application firewall to keep your website safe	 HTTP/S web acceleration, caching and optimization	 Load balance application servers
 Rate controls	 Layer 7 protection	 Monthly fee

Anti-Virus

Ensate offers a managed anti-virus service for your servers hosted with us. We use industry leading anti-virus software that provides malware, spyware, phishing, trojan, rootkit protection and detection.

Anti-virus policies are applied to each of your servers to ensure definitions are up to date and the servers are scanned regularly to identify any security threats. The service is offered as a monthly fee per server.

Network Private Access

Network Private Access (NPA) is a next-generation zero trust remote access technology which allows seamless connectivity to private and public resources whilst removing the exposure of VPN, gateways and applications to the internet.

Dissolving the concept of dial up VPN, our private access technology simplifies remote access management for operations and end users whilst strengthening security posture through conditional based access to applications and services with high availability architecture.

 Provide zero trust network access for private applications	 Connect directly to hosted cloud applications	 Protect private applications and resources	 Provide a seamless and transparent user experience
 Granular trust access configurations	 Encrypted	 Cost Per User	