NETCONNECT PRIVATE™

Secure your network and safely enable applications with our managed network security service.

Network security is becoming vital for business communications and therefore the network must remain available and highly secure at all times. But the traditional port-based network security systems cannot address today's challenges of modern day attacks such as targeted and new unknown variants of malware. Also, fundamental shifts in the application usage, user behaviour, and network infrastructure create a threat landscape that exposes weaknesses in traditional port-based network security. File sharing, social networking, personal email, and streaming media are just a few of the applications that can evade the traditional firewall by hopping ports, using SSL, or non-standard ports. Blocking the applications outright may solve the problem temporarily, but may hurt your business objectives by placing too many limitations on user access. However, blindly allowing them invites business and security risks.

OUR SOLUTION

Using our managed network security service built on a next-generation firewall platform, you can strike the right balance between blocking all personal-use applications and safely allowing all of them. Secure application enablement begins with knowing exactly which applications are being used by whom and when. This information allows you to create effective security-control policies that extend well beyond the traditional 'allow or deny' approach. Our solution gives you the ability to securely enable applications without degrading your network performance.

SERVICE OVERVIEW

Netconnect Private includes bundled high speed symmetrical uncontended Internet service and a next generation firewall that provides you with a secure IP transit. We cover three aspects of enterprise security:

KNOWN THREAT PREVENTION

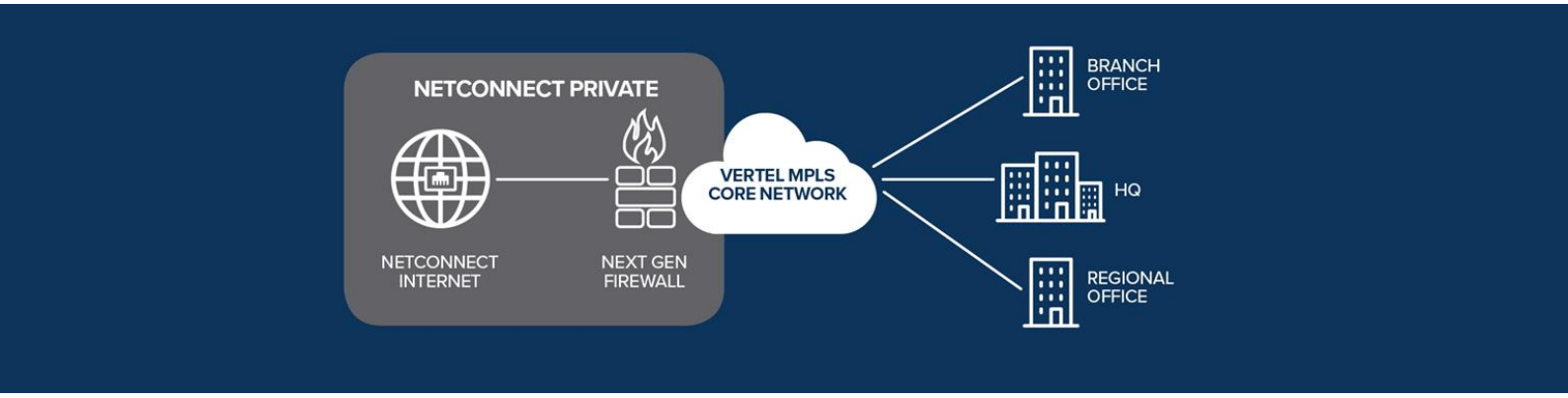
- Visibility into applications, web traffic, threats and data patterns.
- Gain visibility based on applications, users and user groups and not just by IP addresses.
- Control the policy definition based on users and groups (integration with active directory services). Flexible and policy based control over web usage through URL and content filtering capabilities.
- Enable bandwidth control for designated URL categories via QoS policies.
- Full IPS and threat prevention while maintaining performance.
- Antivirus to protect against a wide range of malware, spyware and exploits.
- Protection from DoS attacks.

UNKNOWN THREAT PREVENTION

- Identification and protection against unknown malware, zero-day exploits, and Advanced Persistent Threats (APTs).
- Sandbox analysis of unknown threats in a scalable virtual environment.
- Automatically generates and distributes protections globally in approximately an hour.
- Block a wide range of known and unknown vulnerability exploits.
- Gain full protection to your environment with automatic threat discovery and delivery based on signatures.
- Behavioural botnet analysis which co-relates traffic anomalies with user behaviours to identify the devices that are targets of botnet.

VPN AND MOBILE SECURITY

- Secure site-to-site connectivity through IPsec VPN.
- Configure security settings for your key VPN tunnels for multi-site VPN deployments.
- Consistent security policies for users everywhere including remote users through SSL or IPsec based VPN.
- Safely enable your mobile devices to access business applications and data in accordance with the same security policies as desktop users.
- Protect mobile devices from latest exploits and malware.
- Enforce policies based on apps, users and content on the mobile devices.



SERVICE EDITIONS

We offer three editions of the service to suit your business requirements:

Features	Standard	Premium	Advanced
Application Visibility	Yes	Yes	Yes
User and User Group Visibility	Yes	Yes	Yes
Intrusion Prevention and Anti-Virus	Yes	Yes	Yes
DOS Attack Protection	Yes	Yes	Yes
URL and Content Filtering	Yes	Yes	Yes
Unknown Threat and APT Prevention		Yes	Yes
SSL Remote Access VPN		Yes	Yes
Secure Site-to-Site VPN		Yes	Yes
Mobile Security			Yes

BENEFITS

The following are the benefits of a fully managed security service:

- Network traffic is secured before it hits your network.
- Single solution for known and unknown threat prevention, mobile security, remote access VPN and secure B2B VPN.
- Get protection from unknown malware, zero-day attacks and APTs in about an hour.
- Purpose-built platform with multi-Gbps performance.
- Designed, built and managed by our security specialists.
- Quick to deploy – with cloud based solution.
- Gain operational efficiencies by moving from Capex to Opex.
- Focus on your core business while we take the risk of securing your network.

SECURITY ASSESSMENT

We can provide an assessment on your network security by running application visibility and risk analysis on your network for four weeks. At the end of the four weeks, we can provide you with insights on your network security. You can find out which applications and threats are on your network some of which might not be detected using traditional firewalls.

CONTACT US TO GET A FREE ASSESSMENT OF YOUR NETWORK SECURITY.

Contact us on 1300 837 835 (1800 VERTEL) or info@vertel.com.au.
Visit us at www.vertel.com.au.

vertel