Managed next generation firewall.

Visibility and control over applications, users and threats.

The old model of security was simple. There was good traffic (business applications) and bad traffic (threats) and all you had to do was stop the threats and allow application traffic.

Today, the number, types and nature of applications have changed tremendously. Many applications are hosted outside the enterprise, with enterprise users employing a mix of business-focused and consumer-focused applications for a variety of reasons. All of these applications carry risk and some carry threats, but in most cases they are necessary for business. Blocking them will slow business down, while allowing them can mean taking on too much risk.

It all means network and information security professionals need to shift their focus from treating applications as threats, to working towards enabling them safely.

TELUS Managed Next Generation Firewall service allows you to safely enable modern applications, without taking on the unnecessary risks that accompany them. By focusing on applications, users, and content – in addition to ports and protocols like traditional firewalls – it gives you visibility and control. Your organization can:

- **See** what applications are running on the enterprise network
- **Decide** which applications are desirable from a risk/benefit perspective
- **Exert** fine-grained control over application traffic, allowing beneficial applications for the right users, disallowing risky applications or functions and mitigating the threats associated with beneficial, high-risk applications
- **Protect** your enterprise network against malicious/questionable activity

Best of all, you can do this without sacrificing network performance, thanks to parallel processing hardware delivering multi-gigabit performance.

Application visibility

Application visibility is critical to understanding network risks and achieving application control. With the TELUS Managed Next Generation Firewall solution, you can see streaming audio and video, file sharing, collaboration, and social networks – just a few of the applications that are capable of hopping from port to port, using encryption and non-standard ports to evade traditional firewalls. The business value these applications provide varies widely, but without application visibility and control, they all introduce a range of risks that includes loss of productivity, compliance issues, threat propagation and data leakage.

Application control

The ability to control applications is just as critical as identifying them. The traditional approach is to layer intrusion prevention systems (IPS), URL filtering or proxies onto the existing port-based firewall. However, none of these can see all the traffic on the network, nor are they designed to act as the most strategic security element on the network – the firewall. Our Managed Next Generation Firewall solution restores the firewall's strategic importance as the centre of the security infrastructure, by identifying and controlling applications, users and content.

The TELUS Managed Next Generation Firewall solution can be deployed in a wide range of network locations, including the perimeter, the DMZ, internally for network segmentation and in the datacentre. It can solve the kind of problems that lack of visibility and application control can introduce by giving you:

Managed next generation firewall.

- **P2P and streaming media control**. Stopping the use of P2P file sharing applications
- **Secure enabling of Web-based applications**. Removing the threats while still allowing the applications you need to do business
- **URL filtering**. Perfectly complementing application control to positively control model security policies
- **PCI compliance**. Reducing the complexity of PCI compliance, with control over applications, users and content, all combined with network segmentation
- **Threat and intrusion prevention**. Delivering security without sacrificing network performance and throughput

Threat prevention

Security threats to enterprises continue to evolve as threat developers become more sophisticated, both in their motivation and techniques. Applications have become the front line, with application-level threats now comprising about 80% of the leading threats impacting organizations.

Threats are also more complex in their structures and more sophisticated in their procedures, resisting traditional definitions (e.g., virus, exploit, or worm). They can take many forms, targeting an application, or being carried by an application. The traditional defence mechanisms – firewalls and IPS/IDS – cannot effectively control applications, and can't recognize the variety of threats targeting the applications since IPS/IDS only look at threats formally defined as "exploits".

Next-generation firewalls

In order to prevent threats effectively, you must first reduce the avenues of attack, beginning with controlling which applications run on the enterprise network. Then, you need to scan allowed application traffic more broadly, not limiting your system to a strict definition of a particular type of threat (e.g., "virus" or "exploit"). Finally, in today's economic environment, you need to do it without increasing complexity and cost, and without impacting the network's performance.

TELUS Managed Next Generation Firewall solution delivers a high performance threat prevention solution. With a low-latency, multi-Gbps platform, it:

- Limits traffic to approved applications while avoiding risks from unnecessary applications
- Scans "good" applications for a wide variety of threats – exploits, viruses, spyware, even confidential data leaks – with a single pass, stream-based scan
- Integrates intelligence, policies and reporting between the firewall and threat prevention functions
- Maintains network performance and throughput while providing IPS and threat prevention
- Simplifies infrastructure with a single policy, as well as high port-count and high performance
- Improves upon older forms of perimeter protection
- Provides clearer visibility to the Internet

Managed service features:

- **Design and implementation**
- **Confirmation of requirements**
- **Equipment and vendor maintenance package procurement**
- **Device(s) configuration**
- **VPN Tunnel creation**
- **Device installation**
- **Acceptance testing**
- **Warranty and support registration**
- **On-demand reporting**

Management and alert monitoring:

- **24/7 health monitoring of firewall devices and applications**
- **Ongoing device security and maintenance updates**
- **Defective hardware replacement**
- **Implementation of rules changes**
- **24/7 monitoring of real-time alerts**
- **24/7 proactive response on critical threats and alerts**
- **24/7 incident handling guidance**
- **Event viewing and reporting**

10_sm_048. 5/11

GET THE BEST FOR YOUR BUSINESS.

See how the TELUS Managed Next Generation Firewall service can help your organization by arranging for a demo or an on-site evaluation. Contact your TELUS Account Executive, call **1-866-GO-TELUS** or visit **telus.com/businesssecurity**