Firewall Management

A White Paper published by Adept

Synopsis

With the relatively recent advent and subsequent explosive emergence of Managed Services, clients of ICT-centric organisations are increasingly opting for outsourced solutions in order to satisfy their technology-based requirements.

Firewall services are no exception to this trend, yet the potential for fully comprehensive products and services within this niche has yet to be extensively explored. This is partially explained by the lack of available in-depth case studies. In addition, the formation of firewall solutions that are ubiquitously successful while remaining flexible enough to function as bespoke deliverables is a highly innovative and lengthy process.

In addition, the human element forms a critical link in the security chain. While there are a number of solutions that protect networks, the skill to manage these solutions is a key point that is often lacking. One can have the best firewall that, if not set up and managed properly, can easily render its efficacy moot.

Adept herein presents the case of a large Enterprise client whose requirements inspired the development of a novel set of Firewall Management services, now available to all clients as a customised business solution.

Case Study - The Educational Institution

The client in question is an educational institution comprised of staff and students, with a mixed usage profile demographic of over 1000 unique users.

During the timeframe covered by Adept's investigations, the client had experienced several changes which affected their firewall services:

- Increased security requirements due to the addition of an on-site wireless network (a Bring Your Own Device shift can increase the amount of users by at least 1.5 to 2 times)
- A large expansion of intranet traffic caused by the rise in internal network communications and servers
- Expansion of Internet bandwidth, resulting in much larger data volumes for the firewall services to manage
- Ever-increasing numbers of Internet-capable devices (mobile phones, tablets and laptops) used by the client's personnel and student complements

When these factors were coupled to a proactive approach towards expansion and capacity planning, it became clear that the client's firewall services in their current form could potentially turn into a liability within less than 3 years.

Further investigation, including a set of comprehensive audit resolutions attended to by Adept, prompted a full review and optimisation of the client's firewall services. Over a staggered period of time, each change and optimisation to the firewall services was implemented, until the client was satisfied that their system was optimal, and hardware limitations became the sole limiting factor to further improvement.

Turning a Process Into a Solution

The case above highlighted the requirement for a niche product, in the form of an all-encompassing managed firewall service, built for universal application and customisable to every client's needs. The product would be available in varying iterations, to cater to all needs within the business spectrum.

Using insights gleaned from this and other cases, and with industry-specific best practises in mind, Adept's solutions architects devised a plan to create an offering matching these specifications.

Essential Requirements

A comprehensive solution encompasses a minimum set of specifications, and firewall services are no exception. Given the wide scope that these products are meant to work in, the key elements that were considered are summarised below.

Monitoring

A system that operates on security concerns should be actively monitored. Managed Firewall products should include active monitoring capabilities, with options for multiple items to be monitored, triggered and trended.

Technical Support

All Firewall Management products would enjoy support from dedicated personnel, the availability of up-to-date patching and support structures based on proactive monitoring.

Client Engagement

The argument for manages services includes a mandate for priority engagement as well as delivery, in order to facilitate Enterprise-level support as is likely necessary for high-end requirements.

All clients with Firewall Management services would thus be entitled to priority support, regardless of which package is selected. This means that a service provider would prioritise requests from these clients over clients without managed services portfolios. Furthermore, since a large proportion of managed services suffer from a lack of constant communication, an ideal provider would offer feedback not just when issues arise, but to confirm everything is in working order as well as offer optimisation information.

Device Compatibility

To ensure as broad an implementation capability as possible for potential clients who are already making use of their own firewalls, the Firewall Management products and associated services should be designed to be compatible with industry-leading vendors' firewalls.

Currently, models from the following device types are supported:
- Linux-based (IPtables)
- Mikrotik (RouterOS)
- SonicWALL
- Cyberoam
- Cisco ASA
- GTA

Service Level Agreement

A managed service at business level benefits from a well-structured SLA. Having such an agreement clearly defines the scope and responsibilities of the relationship to all parties. In addition, it sets out the performance and communication parameters which form an integral part of service delivery.

Conclusion

Firewall management is an integral component of any firewall solution. Based upon our findings and subsequent testing, we have taken the initiative and successfully "productised" the Firewall Management niche into a set of viable solution options. We are confident that all requirements are addressed across the product range and that our solutions are in line with evolving industry best practises and standards.

Our experiences with this and other practical case studies have resulted in a more formal approach to problem-based innovation, taking each case on its own merits and difficulties, while using information from all available instances to ensure a more diverse and flexible offering. In the applied environment, the Firewall Management service's primary aim will be to promote far less downtime, the bane of any client's network edge.

Bronze Firewall Management

Regarded as the starting point of a successful firewalling paradigm, the Bronze package is an entry-level product with no support engineer hours included, providing prioritisation and SLA-level service.

Feature	Details
Basic Setup	- Includes configuration of the most common firewall settings - LAN/WAN, NAT/route configuration, filter policies/rules, licensing - Up to 1 hour Tier 3 engineer time
Configuration Backup	- The saved configuration profile is backed up daily to a secure FTP location - Backups stored for 30 days - Accessible only by Adept engineers - Backup restoration on request (subject to contracted hourly rates)
Reactive Support	- Based upon proactive monitoring - Client requests follow standard support procedures - Communication to and from client is addressed by Tier 1 engineers - Actionable requests will be handled by Tier 2 engineers (subject to contracted hourly rates)
Low-level SLA	- Support during business hours only 2 hour response time via Tier 1 engineers - Escalation to Tier 2 engineers available regarding actionable requests
Basic Monitoring	- Up to 30 SMSs per month - Monitoring based on up to 5 predefined sensors
Documentation	Initial configuration settings as well as changes are recorded
Supported Devices (*SonicWALL and Cyberoam devices are not recommended for the Bronze service)	- Linux-based (IPtables) - Mikrotik (RouterOS) - SonicWALL* - Cyberoam*

Silver Firewall Management

Aimed at SMBs with intermediate firewall requirements, the Silver package fulfils the need for bundled monthly management. It also allows for higher escalation possibilities and direct lines of communication.

Feature	Details
Basic Setup	- Includes configuration of the most common firewall settings - LAN/WAN, NAT/route configuration, filter policies/rules, licensing - Up to 1 hour Tier 3 engineer time
Configuration Backup	- The saved configuration profile is backed up daily to a secure FTP location - Backups stored for 30 days - Accessible only by Adept engineers - Backup restoration on request (subject to contracted hourly rates)
Basic Tier 2 Support	- Includes 1 hour of Tier 2 engineer support per month - Managed by trained and equipped Tier 2 engineers - Any requirement for additional time will be communicated to the client and is subject to contracted hourly rates
Reactive Support	- Based upon proactive monitoring - Client requests follow standard support procedures - Communication to and from client is addressed by Tier 1 engineers - Actionable requests will be handled by Tier 2 engineers (subject to contracted hourly rates)
High-level SLA	1 hour response time, with Tier 3 engineer escalation available - Client may communicate directly with engineer attending to requests
Advanced Monitoring	- Up to 90 SMSs per month - Monitoring based on up to 50 sensors, agreed upon via communication with client and based on a pre-set sensor type array
Documentation	Initial configuration settings as well as changes are recorded
Supported Devices	- Linux-based (IPtables/Shorewall) - Mikrotik (RouterOS) - SonicWALL - Cyberoam

Gold Firewall Management

Designed to offer a hands-off, hassle-free experience, the Gold package places the entire scope and ownership of firewall device management in the capable hands of highly skilled experts.

Feature	Details
Advanced Setup	• Includes configuration of the most common firewall settings as well as multiple filter policies and rules, DMZ, bandwidth management, AD integration and HA • Up to 4 hours of combined Tier 2 and Tier 3 engineer time • Setup options agreed upon via communication with the client
Configuration Backup	• The saved configuration profile is backed up daily to a secure FTP location • Backups stored for 30 days • Accessible only by Adept engineers • Backup restoration on request (subject to contracted hourly rates)
Basic Tier 2 Support	• Includes 1 hour of Tier 2 engineer support per month • Managed by trained and equipped Tier 2 engineers • Any requirements for additional time will be communicated to the client and is subject to contracted hourly rates
Advanced Tier 3 Support	• Includes 1 hour of Tier 3 engineer support per month • Optimised support including Tier 3 engineer change control • Any requirements for additional time will be communicated to the client and is subject to contracted hourly rates
Proactive Support	• Scheduled maintenance measures • Business hours patch management • Performance optimisation • Reporting and additional documentation
Vendor Escalated Support	• Adept accesses direct vendor channels for bug analysis and resolution, as well as in cases of undocumented concerns • Vendor support based on vendor-supplied contract and T&Cs
High-level SLA	• 1 hour response time, with Tier 3 engineer escalation available • Client may communicate directly with engineer attending to requests
Advanced Monitoring	• Up to 90 SMSs per month • Monitoring based on up to 50 sensors, agreed upon via communication with client and based on a pre-set sensor type array
Documentation	• Initial configuration settings as well as changes are recorded
Tier 2 Engineer Meeting	• Up to 1 hour with Tier 2 engineer for revision of documentation, basic reporting and potential improvements • Either at Adept's or client's premises (travel time is excluded from the dedicated hour and is subject to contracted hourly rates)
24/7 Support Availability	• Based on the contracted hourly rates for Basic and Advanced support • Vendor support based on vendor-supplied contract and T&Cs
Supported Devices	• SonicWALL • Cyberoam • Cisco ASA • GTA

Platinum

As the pinnacle of the research and development initiative, the Platinum package incorporates the highest levels of management and resource allocation, meeting the needs of Enterprise clients.

Feature	Details
Advanced Setup	• Includes configuration of the most common firewall settings as well as multiple filter policies and rules, DMZ, bandwidth management, AD integration and HA • Up to 4 hours of combined Tier 2 and Tier 3 engineer time • Setup options agreed upon via communication with the client
Configuration Backup	• The saved configuration profile is backed up daily to a secure FTP location • Backups stored for 30 days • Accessible only by Adept engineers • Backup restoration on request (subject to contracted hourly rates)
Basic Tier 2 Support	• Includes 1 hour of Tier 2 engineer support per month • Managed by trained and equipped Tier 2 engineers • Any requirements for additional time will be communicated to the client and is subject to contracted hourly rates
Advanced Tier 3 Support	• Includes 1 hour of Tier 3 engineer support per month • Optimised support including Tier 3 engineer change control • Any requirements for additional time will be communicated to the client and is subject to contracted hourly rates
Proactive Support	• Scheduled maintenance measures • Business hours patch management, with after-hours availability • Performance optimisation • Reporting and additional documentation • Audit compliancy • HA failover testing (where applicable and based on client communication) • External port scan availability
Vendor Escalated Support	• Adept accesses direct vendor channels for bug analysis and resolution, as well as in cases of undocumented concerns • Vendor support based on vendor-supplied contract and T&Cs
High-level SLA	• 1 hour response time, with Tier 3 engineer escalation available • Client may communicate directly with engineer attending to requests
Advanced Monitoring	• Up to 90 SMSs per month • Monitoring based on up to 50 sensors, agreed upon via communication with client and based on a pre-set sensor type array
Documentation	• Initial configuration settings as well as changes are recorded
Tier 3 Engineer Meeting	• Up to 1 hour with Tier 3 engineer for revision of documentation, advanced reporting and potential improvements • Either at Adept's or client's premises (travel time is excluded from the dedicated hour and is subject to contracted hourly rates)
24/7 Support Availability	• Based on the contracted hourly rates for Basic and Advanced support • Vendor support based on vendor-supplied contract and T&Cs
Supported Devices	• SonicWALL • Cyberoam • Cisco ASA • GTA

Company Profile

Adept Internet was launched in January 1996 in Stellenbosch, and is today one of the oldest independent Internet Service Providers (ISPs) in South Africa. To be Adept is to be proficient and expertly accomplished. This is what we strive for and have achieved in all our services.

Many of our solutions are tailor-made, in order to perfectly suit each client's individual requirements. We thus ensure that our approach is personal and conforms to exactly what is needed in order to be successful.