

Mr. Stacy Scott Bean

PROFILE

A friendly and dependable security specialist contractor with 20+ years of experience within Information Technology. I learnt my craft in London when I moved there in 1999, and then continued to secure networks and information after returning to New Zealand in 2011.

Although I operate at architect and consultant level I still love to get hands-on especially around firewalls, proxies, network equipment and any of the latest security tools that appear in Kali Linux.

Key past workplaces: **Westpac NZ, healthAlliance, IBM, Unisys, BNP Paribas, BAA - British Aviation Authority, Royal Bank of Scotland, Centrica PLC, Price Waterhouse Coopers, Diageo, Microsoft, Reuters, and Rolls-Royce.**

I enjoy working in teams and can always be relied upon to provide help wherever I can to other team members and will go above and beyond to meet the most optimistic of deadlines.

Other's consider me a problem solver, I never back away from a challenge especially if there's a major incident or problem that needs to be solved and I enjoy the pressure of those situations.

Key areas of experience:

- Design or assess to NZISM, and internal Information Security policies/standards.
- Security assessment and endorsement of solution designs.
- Providing risk assessments to CISO.
- Visio - (Network Diagrams, traffic flows, etc)
- Broad range of firewalls: Checkpoint, Juniper, Fortinet, Cisco ASA Firewalls.
- IPsec VPN (Checkpoint, Nortel, Juniper)
- Bluecoat Internet Proxies.
- F5 Viprion, Alteon, Citrix Netscaler Load Balancers and gateways.
- Proficient with Cisco (up to 6500 series) IOS and CAT-OS
- Working in ITIL environments under strict change control.
- Reviewing and approving security related changes.
- Full understanding of TCP/IP routed and routing protocols

QUALIFICATIONS

My certifications below are old so I am actively pursuing an OSCP certification in an effort to keep my hands dirty and also to extend on my pen-testing skills.

Checkpoint Certified Security Expert (**CCSE - NGX**)

Checkpoint Certified Security Administrator (**CCSA - 2000 and NG**)

Cisco Certified Network Associate (**CCNA**)

Microsoft Certified Professional (**MCP x 4**) in the following:

- TCP/IP for Windows NT 4.0
- Networking Essentials
- Windows 95
- Windows NT Server 4.0

EMPLOYMENT HISTORY

April 2019 – Current

Westpac NZ

Security Architect / Consultant

During my time at Westpac I have led two major initiatives.

The first was to lead the insourcing of services provided by the 'Managed Security Services Tower' from IBM into a new internal Westpac team. This was driven by a Westpac requirement to become more agile and provide the ability to respond faster to business requirements where an opinion had been established that the current environment was too slow.

I recruited a new team of Westpac security engineers, defined their responsibilities, and ensured they had the tools available to take over the running of the insourced security services. This included support of Juniper firewalls and VPN concentrators, Bluecoat proxies, Datapowers proxies, and other ad-hoc pieces of security infrastructure.

In addition I negotiated new maintenance contracts with Juniper, Fujitsu, Origin-IT, and IBM covering hardware and software support for the new team to call upon if required.

Insourcing the MSS tower took just less than a year to complete and was a success both in terms of speed and cost.

Next, I was given the task of establishing an improved Privileged Access Management solution for Westpac.

This involved choosing a partner to work with (WebSecure), and going through high level, then detail level design phase, followed by the build out of a CyberArk platform.

I established processes by which infrastructure and applications could be "PAM'ed", provided training and gave demonstrations on how to use the new tool, and oversaw the on-boarding of thousands of privileged accounts.

I discovered that Privileged Access Management projects are by no means 'short term', and had to deal with very complex technical issues, such as on-boarding AIX servers already protected with eTrust, integrating into Linux OpenLDAP/Keberos directories, and 10 different Active Directory domains.

In my spare time, I acted as a sounding board for other members of the Information Security Group (ISG team), and played key parts in decisions to approve new technology and software within the bank.

I also taught members of the firewall team how to performance-test their firewalls using packet-generation tools, this allowed us to verify fixes supplied by Juniper were effective.

Oct 2017 – May 2018

healthAlliance

Senior Security Specialist

healthAlliance provides IT and Information Security services to the Northern Region District Health Boards, these being Auckland, Manukau, Waitemata, and Northland DHB's. The predominant infrastructure technologies are Microsoft, Cisco, Checkpoint, VMWare.

My role reports directly to the CISO and covers a number of responsibilities including the following:

Review of high level solution designs and detailed designs and providing direction to architects where healthAlliance standard controls or applicable NZISM related security controls have not been met.

Performing Cloud Risk Assessments based on the government provided CRAT template. As there is a 'Cloud First' design principle in place, SaaS solutions are very popular within the health sector. I have aided in simplifying the CRAT process at healthAlliance to make it faster and more efficient.

Provide security endorsements on solution designs after review where either the design meets all standards or has had the necessary security dispensations raised and risk accepted by the CISO / CIO.

I have authored an API Data Security Standard to facilitate a project implementing a new Mulesoft integration platform.

Attend 'Rough Order of Magnitude' meetings with portfolio managers, DHB stake holders, head of infrastructure and head of solutions to determine approximate cost of upcoming projects.

Attend Regional Technical Architecture Governance weekly meetings to provide endorsement of project-based solutions presented by solution architects.

In addition to the above, my previously used technical skills have helped identify areas in the current landscape where security improvements could be easily made.

May 2012 – Feb 2017

IBM New Zealand / Westpac NZ

Security Specialist

This role was project driven. The responsibility was to ensure that new projects being undertaken by IBM for Westpac were designed and implemented in a way that complied with Westpac's Information Security policies.

Taking high level design documents from Westpac Solution Architects, I would produce a Security Detailed Design document which would then be used by implementation teams to base their infrastructure related configuration changes on.

My responsibilities included:

Author of a security detailed design per project for the approval of Westpac Information Security Governance team. I worked on over 100 projects during this 5 year job.

Design Review: Identifying vulnerabilities or any poor design decisions made in the high level design and working with the architects to update their design.

Identifying all new systems being provisioned by the project and ensuring they reside in the correct network zones to suit their use.

Diagramming the solutions traffic flow requirements at a logical level using Visio.

Producing the configuration scripts required for Juniper Firewalls, VPN Concentrators, F5 & Alteon Load balancers and working with the implementation teams to schedule and make the changes on behalf of the project.

Identifying SSL certificate requirements, authentication methods, DNS updates, server-side static route updates, network related changes such as new VLAN's, routes and any other Infrastructure related changes

An example objective could be to connect Westpac via IPSec VPN to a third party in order for payment processing, or it could be to aid in the design and implementation of a project to meet new Government legislation, such as meeting AML (Anti Money Laundering) requirements.

Most recently it had been to introduce Skype for Business into Westpac in conjunction with Spark.

Sep 2011 – May 2012

UNISYS NEW ZEALAND (Wellington)

Network Security Analyst

Based in the Security Operations and Network team in Wellington, my responsibilities are to oversee and support various customer networks. These include the Ministry of Health, NZTA, VTNZ, and Parliamentary Counsel Office. This involves a degree of everyday support, and an element of consultancy depending on which client I'm working for at the time. The technologies supported in this role include Checkpoint Firewalls, Cisco ASA firewalls, Cisco routing and switching environments, and tuning of Arcsight event management alerting systems.

Apr 2011 – Sep 2011 BNP PARIBAS, COMMERCIAL INVESTMENT BANK (London)

Information Security Analyst

At BNP Paribas I work as part of the Information Security team which is responsible for reviewing and approving infrastructure changes from an IS security point of view, managing and implementing changes to the Checkpoint firewall estate and actively monitoring the network for security breaches using Arcsight, and McAfee anti-virus software.

My responsibilities are focussed on maintaining the firewall estate. This includes, reviewing and approving firewall changes, implementation of firewall changes, general house-keeping on the firewalls, and firewall management servers. I also liaise with other infrastructure teams to ensure their projects are sticking to the company's security policies.

The firewall estate consists of roughly 100 Nokia firewalls running Checkpoint R72, and all are centrally managed via a Checkpoint Provider-1 MDS server. Market Data networks, Internet Presentation DMZ's, Business to Business VPN, mail and browsing, and connectivity to other global offices environments are all secured by this firewall estate.

Oct 2009 – Dec 2010 ROYAL BANK OF SCOTLAND (London)

Network Security Analyst / Datacentre Consolidation

This is my second stint contracting at RBS. This time I was brought in to aid in a large scale datacentre consolidation and migration. The project involved the closure of 5 RBS datacentres, moving tens of thousands of servers to a new datacentre facility outside of London. My role was to ensure that all network and security infrastructure was in place and configured correctly to allow the migration to go smoothly with minimal loss of service. The server migrations were done weekly on Saturdays, and usually involved working into the wee hours of Sunday morning as we would often move up to 150 physical servers on one day. This was high pressure work as technical issues often crop up with migrations of this magnitude and I was often working with application owners, server teams, and project managers to investigate where issues lie (i.e. network, server, or application based problems)

Equipment configured:

- Checkpoint Firewall-1 (R-65) on Nokia
- Cisco 6500 series switches
- Cisco ASA firewalls
- Proteus DNS systems
- Cisco Load balancers
- Terminal Servers
- HP Blade Chassis'

Dec 2008 – Oct 2009 BAA (British Airport Authority) (London)

Network Security Analyst

Based at Heathrow Airport, as a member of the network security team responsible for maintaining the firewall, extranet, and Internet proxy services throughout Heathrow, Gatwick, Stansted, Edinburgh, and Aberdeen

airports. Typical systems that are protected are the networks running Baggage handling systems, Air Traffic Control networks, Queue management, plus the campus network serving thousands of BAA employees. There are also 100+ Extranet IPSEC VPN's / MPLS connections to various partner companies and airlines which are secured through a number of high end Fortigate 5000 series firewalls and Checkpoint / Nokia firewalls as well.

Sep 2007 – Sep 2008 ROYAL BANK OF SCOTLAND (London)

Security Analyst

A project-based role initially to design and build the firewall solution for RBS Global Banking and Markets IP telephony infrastructure. This was a Nokia / Checkpoint solution consisting of eight Nokia IP1220's running Checkpoint FW-1 R65 in a resilient network. The Avaya IPT solution was rolled out through Europe and Australasia consisting of thousands of handsets and high end Avaya servers based in London and Hong Kong hubs.

After completing the firewall installation and extensive rule base creation for this initial project I was then asked to carry out the security work for another Hong Kong based e-commerce project which involved building and installing another eight Nokia IP1220's.

I am now responsible for the upkeep of 100+ firewalls for the Global Banking and Markets division, including Reuters and Bloomberg market data feeds, VPN connectivity to various stock exchanges around the world, and the remote access solution for 5000+ staff.

This role is heavily focused on Checkpoint Firewalls, however some Cisco routing and switching work is also undertaken.

Mar 2007 – Aug 2007 CENTRICA PLC (London)

Security Analyst

Centrica is the parent company to British Gas, EON, and various other energy companies and electrical grids. This role involved design, implementation, and ongoing support of the network security infrastructure including Nokia, Checkpoint firewalls, and Bluecoat Internet proxies. Managing VPN connectivity between remote and central sites, remote workers and extranet business partners. An extremely fast moving environment working to very strict deadlines and doing whatever was required to get the job done during all hours of the day and night.

- 120 Nokia firewalls (IP330 – IP1220) within London, and many more around Europe, the US, and Africa.
- Checkpoint Firewall-1 R62 (upgraded from R-60)
- Checkpoint Provider-1 management
- Bluecoat Internet Proxy management

Mar 2005 – Jan 2007 PRICE WATERHOUSE COOPERS (London)

Security / Network Analyst

At PWC my responsibilities were all security and network related within a dedicated network team.

- Rogue host identification using NMAP and GFI Languard
- Administration of Nokia and Solaris based Checkpoint Firewalls (NG-AI) in a high availability 3-tier secured environment.
- Maintenance and monitoring of ISS Intrusion Prevention Systems using Proventia's and Siteprotector.
- Server Compliance (Identification of un-authorized servers on the network)
- Administration and fault fixing Cisco switches and routers (up to 10000 series)
- Site to site VPN solution using Nortel Contivity concentrator / routers.
- Liaise with BT on problems with BGP / IP Clear WAN circuits

- Wireless LAN deployment
- WAN Performance monitoring using, HP Openview, Concorde and Solarwinds
- Ciscoworks
- Maintenance of IP Addressing scheme and database.

Dec 2002 – March 2005 DIAGEO (London)

3rd Line Windows Server Support Engineer

Diageo is the largest producer of spirits and a key producer of beer in the world covering labels such as Smirnoff, Guinness, and Johnnie Walker

At Diageo I worked in the Windows Server team having technical implementation responsibilities through a number of projects.

May 2002 – Dec 2002 MICROSOFT CORPORATION (London)

Server / Network Support Analyst

At Microsoft's MSN data centre I was part of a team responsible for the running support of 700 servers and the various network equipment involved.

Build, support, operation, and monitoring of servers within the datacentre.

Aug 2000 – Jan 2002 REUTERS (London)

Network Support Analyst

At Reuters I was the sole local network support person for one of their inner-city offices. I was responsible for the day-to-day running of the Reuters LAN as well as supporting several complex development networks within the office.

Windows server/desktop, Solaris desktop support, as well as Cisco switch configuration, supporting the office WiFi solution.

Dec 1999 – Aug 2000 Rolls-Royce (London)

Network Engineer

I and one other contractor were responsible for the support of a completely new network for a small (100 staff) Rolls-Royce subsidiary that broke away from the main corporate Rolls-Royce network. This included support of:

3COM switches, Checkpoint Firewall, Web Sweeper, Mail Sweeper, Shiva RAS, Ace Secure Authentication Server (serur-id tags), an NT Domain / MS Exchange, and Arcserve Backups.

May 1999 – Dec 1999 SITA Equant

This was my first contract after moving to London where I was working a desktop support engineer in a large Windows NT based environment based at Heathrow Airport.

Jan 1998 – April 1999 The Internet Home User Group (IHUG)

I started my career at 20 on IHUG's helpdesk. After becoming certified in Windows 95 I was promoted to start installing Starnet, which was IHUG's high speed satellite internet solution for business and home users.

This included me installing a satellite dish at the customers premise roof, running coaxial cable to the server, installing a satellite receiver card into the server, and sometimes setting up proxy software to share the new high speed Internet connection throughout a LAN. This was before the days of ADSL / Broadband.