**Fabricio Lima (Fab)**

[email@fabriciolima.com.br](mailto:email@fabriciolima.com.br)  
+64 (21) 088-12688

**Profile**

Network Security Engineer with 20 years of experience, performing troubleshooting and support combined with advanced skills on cloud, server side, open source tools and scripts for task automations.

Managing firewalls clusters for the last 10 years, but on last couple years I was more into security automation, dynamic scaling on the cloud, SIEM implementations with automatic response/remediation.

Providing security solutions for private/public sector in different countries, setting up Firewalls, VPN, Web filtering, anti-phishing and anti-ransomware protections based on Ethical Hacker experience from several purple-team exercises.

Nowadays, I’m focused in security automation / threat intelligence, while playing with cloud and containers on my spare time.

**Professional Experience**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Orion NZ** | | | | July 2023 – Ongoing | | |
| Industry: | | | Utilities | | | |
| Role: | | | DevSecOps Engineer | | | |
| Key Activities: | | |  | | | |
| * Security BAU – Vulnerability management, firewall and load balancer management. Nothing special or fancy, but owning the Security role, and getting it done. Alone in the security space, together with a small team of 2 others (one for network, other for servers/infra), leveraging all new features/knowledge to achieve desired security posture (focusing on Zero Trust Architecture); * Review current policies and practices - review / evolve them: Define new Windows update structure, review account management, revamp monitoring and SIEM to improve alerting and detection aiming self-healing network and automated incident response; * Security review of firewall rulebase, antivirus policies, web server protections and Internet access in order to improve security posture; * Infra-structure and service tidy up – automated scripts to generate server list => feed this into network monitoring, define escalation for security/monitoring incidents; * Increase security by server hardening, firewall IPS tuning, load balancer web protections; | | | | | | |
| **Otago University** | | | | April 2023 – Ongoing | | |
| Industry: | | | Education | | | |
| Role: | | | Contractor - Cloud Security Specialist | | | |
| Key Activities: | | |  | | | |
| * Consulting as second level escalation point for security incidents, enquiries and support; * While waiting for a large SIEM implementation by MSP, I deployed an Azure Sentinel instance to leverage Microsoft365 alerts including accounts compromised overseas (but still protected via MFA) and automated notifications for victims of phishing scams. In addition, dashboards to monitor our cloud billing, while bringing the university into automated incident response journey; * Increasing M365 phishing level protection due increased number of scams and users failing victims even losing their personal money; | | | | | | |
| **Kāinga-Ora (Housing NZ)** | | | | September 2021 – April 2023 | | |
| Industry: | | | Government | | | |
| Role: | | | Contractor - Senior Security Engineer – End User Solutions | | | |
| Key Activities: | | |  | | | |
| * Design and implementation of SIEM based on Azure Sentinel, creating security dashboards and alerts, automatic security feeds for importing new IOCs to increase agility on SOC and automatic Incident Response automation for Zero Trust model; * Microsoft365 E5 / Azure security technologies for automatic incident response and threat detection; * Over 100 Use Cases creation and implementation based on MITRE ATT&CK framework; * Deployment of a new Endpoint Security protection based on CheckPoint Harmony to replace old Antivirus and provide Web Filtering, Compliance, Threat emulation and Ransomware protection; * Responsible for AV deployment to 4,000 devices, support, training, processes and documentation; * Compliance checks for security baseline on desktops, and enforcing/restricting access based on these checks, implementing automatic remediating; * Advanced troubleshooting on Endpoint Security and new Antivirus issues, liaison with vendor and providing root cause and solution in outstanding issues where even the vendor was unable to figure out the culprit; * Consulting on security insights on several different projects towards Zero Trust Architecture; | | | | | | |
| **Foodstuffs South Island** | | | | April 2021 – September 2021 | | |
| Industry: | | | Grocery Retail | | | |
| Role: | | | Infrastructure Network & Security Engineer | | | |
| Key Activities: | | |  | | | |
| * Network/Security support to infrastructure comprised of 200 markets across South Island; * Managing Palo Alto firewalls, F5 load balancers and Meraki/Juniper network devices as BAU; * Support for network security incidents and troubleshooting connectivity and performance issues; * Over 50 major firewall changes raised in 6 months to uplift security posture and rule base tidy up (like enabling DoS protection, migrating to app based inspection, ban high risk apps, so on…); * SSL Inspection deployment using Palo Alto firewalls; * Health checks on VPN preventing access from non-compliant PCs (Network Admission Control); | | | | | | |
| **Victoria University** | | | | April 2019 – March 2021 | | |
| Industry: | | | Education | | | |
| Role: | | | Senior Security Engineer | | | |
| Key Activities: | | |  | | | |
| * Two large Firewall cluster migrations (from CheckPoint and Cisco ASA to Fortigate 6K chassis); * Level 3 support for network security incidents and troubleshooting advanced connectivity and performance issues, also providing guidance to team members and other teams; * UTM, IPS and SSL Inspection implementation/deployment; * Autonomous malware prevention and network protection based on security feeds integrated to firewall including creating custom IPS/Application signatures and external reputation lists; * Fortinet SIEM implementation with incident response automation based on malicious behaviours (integrating with firewall and AD for automatic ban/quarantine); | | | | | | |
| **Dimension Data NZ / NTT** | | | | March 2016 – April 2019 | | |
| Industry: | | | Telecommunication (ICT) | | | |
| Role: | | | Senior Security Engineer | | | |
| Key Activities: | | |  | | | |
| * Managed Firewall as a Service using a large deployment of Multi Domain CheckPoint VSX firewalls for several customers in government sector connected in the TaaS infrastructure; * Managed Cloud services – design, architecture, deployment (on Amazon AWS); * Level 3 support for network security incidents for several large customers and troubleshooting connectivity and performance issues on daily basis, also providing guidance to team members; * VPN, IPS/WAF, Proxies and f5 Load Balancer administration, on modules LTM/GTM/APM/ASM; * SIEM administration and support for Incident Response team at TransPower’s and ACC’s SOC; * Automating Firewall migrations from Fortigate and Checkpoint R77 to R80 using API; * Multi Domain HA firewall upgrade from R77 to R80 in large deployments; | | | | | | |
| **REANNZ – Research & Education Advanced Network NZ** | | | | September 2015 – March 2016 | | |
| Industry: | Telecommunication (ISP) | | | | | |
| Role: | Contractor - Security Engineer | | | | | |
| Key Activities: |  | | | | | |
| * Design of a Managed Firewall Service using Fortinet firewalls and management tools; * Implementation of multi-tenant redundant firewalls featuring VDOMs (virtualization); * Evaluation of firewall cluster technologies combined with BGP and OSPF for dynamic routing; * Definition of service description and processes, implementation of monitoring/alerting, reports customization and configuration of a central management system; | | | | | | |
| **Imprensa Oficial do Estado São Paulo - Brazil** | | | | April 2009 – June 2015 | | |
| Industry: | | Government (Printing Press and Certification Authority) | | | | |
| Role: | | Network Support and Security Analyst | | | | |
| Key Activities: | |  | | | | |
| * Clustered CheckPoint and FortiGate Firewalls installation/upgrade and troubleshooting; * TippingPoint IPS implementation review, enhancing the protection level of Web portals; * Local government’s web sites protection from DDoS and application attacks from Anonymous hacking group during FIFA World Cup when there were several manifestations on streets; * Several VPN SSL and IPSec implementations to secure connections and remote access; * Dynamic QoS policies design to allow thousands of customers to share a single 155Mbps link; * Over 300 Windows and Linux Virtual servers’ administration (Level 3 incident support); * Cloud provisioning for customers and publishing content over Internet using web accelerators, reverse proxies, and digital certificates for increased security and authentication purposes; * VMware Infrastructure and iSCSI storage support, Amazon Cloud infrastructure provisioning; * Network and servers monitoring implementation using Nagios and Cacti (SNMP); | | | | | | |
| **NET Serviços (outsourced by** **Capgemini Brazil)** | | | | June 2008 – March 2009 | | |
| Industry: | | Telecommunication (2nd Largest ISP in Brazil) | | | | |
| Role: | | Network Security Analyst | | | | |
| Key Activities: | |  | | | | |
| * Clustered CheckPoint Firewall and Web content filter implementation and support; * Level 4 support for Network, Windows and Linux teams (+200 servers); * Over 30 IPSec VPN tunnels implementation and support (CheckPoint and Cisco); * Security devices support: IronPort Antispam, TrendMicro VirusWall, Mcafee IPS, WebSense; * Development of VBScripts for user account management and auditing; * Vulnerabilities assessment, mitigation and control (on monthly basis); | | | | | | |
| **CPTM – Cia. Paulista de Trens (outsourced by Capgemini Brazil)** | | | | | | March 2007 – June 2008 |
| Industry: | | Public Transport (Train) | | | | |
| Role: | | Network Support and Security Analyst | | | | |
| Key Activities: | |  | | | | |
| * Windows and Linux servers’ administration (Level 3 support) (+200 servers); * Recreate server farm and network topology due several instabilities and misconfigurations; * LAN and WAN connectivity troubleshooting (+100 links); * Network monitoring using Nagios, Cacti and NetFlow open source implementations; * Development of a new IP network address plan to migrate desktops, servers and devices; * Creation of VBScripts for user account management and auditing, proxy reporting, server inventory, user synchronisation between ERP x AD; | | | | | | |
| **Proteus Security - Brazil** | | | | | August 2006 – February 2007 | |
| Industry: | | ICT Consulting (Security Auditing) | | | | |
| Role: | | Network Security Analyst | | | | |
| Key Activities: | |  | | | | |
| * Audit vulnerabilities and network misconfigurations of large local companies such as banks, factories, e-commerce, Telecom and Internet Service Providers (around 20~30 customers); * Development of scripts to collect/audit +1000 network devices’ configuration and firewall rules; * Analyse configurations which may involve security risks, suggest new approaches and write recommendations and reports about identified risks on a monthly basis; * Improve security baselines for routers, switches, firewalls and Windows and Linux servers; | | | | | | |
| **2M2B – Machine Building Bahia Brasil** | | | | | March 2004 – June 2005 | |
| Industry: | | Manufacturing (Electronics/Hardware) | | | | |
| Role: | | System Analyst | | | | |
| Key Activities: | |  | | | | |
| * Supporting to build gambling and vending machines; * Embedded Linux development with graphical interface using less than 50MB total size; * Hardware design for a custom motherboard, and custom cellular modem; * Linux device driver development for electronic LED displays using serial port; * Remote management of hundreds of gambling machines using a mobile 3G/GPRS network; * Secure communication protocol implementation in C, using RSA cryptography; | | | | | | |

**Other Projects**

Internet Service Provider design and implementation providing Wireless and Dial-up connections on ‘90s.

Nagios plug-in development using C for the largest WiFi hotspot in Latin America to integrate the CRM with network events in order to monitor hotspots status, using custom firmware on Linksys Wireless Routers.

Freelance support deploying Cloud environments. Consultancy services to enhance web servers’ security and fine tune for high performance mail/web servers and databases. Open source implementations for Web filtering and reports, VPN remote access and network monitoring.

Some bugfix contributions to RClone open source project – an utility to copy data to/from cloud storages.

Content for [tech-wiki.net](http://tech-wiki.net) website which is THE reference for Firewall CLI commands and several other network resources, such as hacks, tips, or scripts used for engineers all over the world, with +10k of monthly views.

**Technical Skills**

**Firewall:** CheckPoint, Fortinet, Palo Alto, pfSense

**Security Tools:** Azure Policy, F5 BIG-IP, VPN, IPS/WAF, Cloudflare CDN, Intune, Defender for Cloud/Endpoint

**Virtualisation**: Azure Hybrid Cloud, AWS Architect, Docker Containers, VMware ESX, Nutanix

**Azure Sentinel SIEM with SOAR - Incident Response automation** (Power Automate and Azure Logic Apps)

**Open Source tools and scripting**

|  |  |
| --- | --- |
| **General Information** | |
| Certifications | ISC² CISSP: Certified Information Systems Security Professional  ISC² CC: Certified in Cybersecurity  CEH – Ethical Hacker  CheckPoint CCSE R77 – Security Expert  Fortinet NSE5 – Network Security Expert (NSE7 trained)  F5 Big-IP Administrator  Azure Network+Security AZ-700/AZ-500, Security Operations Analyst SC-200  Amazon AWS Solutions Architect - Associate  Cisco CCNA  Microsoft MCSA – Security  ITIL Foundation |
| University | Bachelor in Computer Science – Brazil 2005 |
| Hobbies | Movies/TV Series, board games, electronics with Arduino and virtual labs: personal storage with private cloud in small SBC boards (Raspberry Pi); |
|  |  |
| Visa Status | NZ Citizenship |