INTRODUCTION

Experts in Foresight Cyber has been working with Skybox Security products since 2011, becoming a Premium Partner and Service+ (fully certified SCPS+) in 2018. This document summarises accumulated knowledge in relation to formulating business benefits and justifying investment into the Skybox software and Foresight Cyber services.

SKYBOX MODULES

Modules that Skybox offers and relevant stakeholders:

- Firewall Assurance (FA) - functions useful for both cyber security, firewall service owner, and firewall admin team - analyse secure configuration, rules and access between firewall zones, optimise firewall rule base.
- Network Assurance (NA) - allows to build a network model, both on-premise and cloud, that is allows zone-based compliance assessments
- Change Manager (CM) - uses data from FA and NA to analyse planned firewall changes for technical implementation, and security policy compliance implications
- Vulnerability Controls (VC) - performs virtual attack simulations and shows which vulnerabilities should be remediate first, including compensating controls. This typically reduces number of actionable vulnerabilities in an organisation to just 1%

BENEFITS TO STAKEHOLDERS

FIREWALL SERVICE OWNER

- Increase internal customer satisfaction by shortening analysis of firewall changes through automation. Skybox together with our application management can provide semi or fully automated assessment of FW changes.
- Obtain assurance, through Foresight Cyber reporting, that only firewall changes that were requested through ServiceNow were implemented in Skybox, catching any 'unauthorised' ones
- Receive reports of the firewall platforms' secure configurations, and their compliance with the firewall secure configuration standards, across vendor products (Skybox support all major firewall vendors, such as but not limited to PaloAlto, FortiGate, Cisco ASA and, Checkpoint)
- Obtain reports of the firewall platforms' rules compliance with your firewall policy

- Save resources by getting proactive remediation orchestration support for non-compliance issues resolution discovered in above reports as Foresight Cyber issues remediation tickets to firewall service providers. My estimate is that you would need a full time PM/FW expert to handle the workload to remediate current non-compliance.

FIREWALL ADMINISTRATORS

- Change Manager allows firewall admins to understand better HOW to update a firewall rule-base to match the firewall change request. From experience this is one of the trickiest and error-prone activities. A misconfiguration can also lead to a security breach (consider an existing object being used in a new rule but the object contains more hosts than need access).
- Firewall Assurance allows firewall admins to see firewall compliance issues and possible optimisations for each firewall

SOLUTION ARCHITECTS

- See a network map and better analyse how their new system needs to communicate and if the connectivity is already there or needs to be requested. From my experience as a solution architect this is a time-saver.

NETWORK SERVICE OWNER

- There is huge benefit of seeing 'near-live' snapshot of the network configuration, topology and external connections. No amount of manual labour using Visio will deliver the same benefit.

3RD PARTY CONNECTIVITY SERVICE OWNER

- Specifically, for the 3rd party connectivity process, modelling all 3rd parties in the Skybox network model as individual connections gives an assurance that an external perimeter is protected - important for CIS Controls 9 and 14

IT SECURITY

- Get assurance that the Firewall policy, specifically zone to zone access restrictions, is being used in the configuration of firewalls, and any critical issues are discovered and pushed into a triage decision process
- Get assurance that firewall changes' compliance assessment is running as agreed with the firewall service owner

- Score vulnerabilities in line with the company's vulnerability management policy to allow for required variations
- By performing virtual vulnerability attack network simulations, greatly reduce number of vulnerabilities that need an urgent remediation attention

IT INFRASTRUCTURE OWNER

- Get assurance that all firewall and all network devices are correctly documented in ServiceNow CMDB - lifecycle, key attributes, resolver group – delivered by Foresight Cyber

PANORAMA BPA VS SKYBOX

If your organisation uses PaloAlto, you might be familiar with a PaloAlto BPA report, a paid for module in Panorama server. A few points on BPA compared to Skybox:

- BPA does have an overlap of checks with those in Firewall Assurance

- Where BPA delivers extra compared to Skybox:
  - L7 checks around App-ID, User-ID, decryption, Wildfire
  - BPA Device Configuration checks are the equivalent to Skybox Configuration Compliance; however, BPA has had more checks than Skybox, and it also looking at Panorama configuration in addition to individual firewalls

- Where Skybox FA module outperforms BPA:
  - Multi firewall vendor support
  - Zone to zone policy compliance - i.e. Should traffic from external zone going to internal zone be allows for this App-ID.
  - BPA does not include Anything to do with Optimisation and Clean-up especially Rule Usage Analysis. (However, rule hit counts are available in Panorama (updated every 5 minutes) but these don't go down to the object level.
  - Shadowed and Redundant analysis can't be done natively in Panorama retrospectively; however, you do get a warning in Panorama if you are about to commit a rule that will shadow another
  - BPA does not have network maps so does not understand connectivity between firewalls