Palo Alto Networks
UK Telecoms Security Framework – Alignment Statement & Security Declaration

Contents

Document Purpose

Overview

This document provides an overview of Palo Alto Networks alignment with the published UK Telecommunications Security Framework - Assessing the Security of Vendor Equipment (2021). Within this document Palo Alto Networks details how our focus and attention to engineering best practice and security detail help to ensure that we (Palo Alto Networks) continue to support and conform to the exacting demands for quality, transparency and partnership of both the Government and the Telecommunications Sector within the UK.

Capability Scope of Statement

This statement has been published based upon the features and functions of our current operating system, PAN-OS 10.0. We anticipate, but cannot assure, that the entirety of this statement will hold true for future versions of PAN-OS as well.

Structure of Document

This document has been constructed to align with the Vendor security assessment criteria of the Telecoms Security Framework - Assessing the Security of Vendor Equipment document published by NCSC:

- Product Lifecycle Management
- Product Security Management
- Product Development & Build Environments
- Exploitation Mitigation Approach
- Secure Updates & Software Signing
- Hardware Roots of Trust and Secure Boot
- Security Testing
- Secure Management & Configuration
- Vulnerability & Issue Management

Within each of the sections above this document provides either an overview of our approach or methodologies or a link to one of our public facing ‘living’ web resources that address the scope within the section.

Document Limitations & Legal Construct

As the reader will appreciate and understand, given the nature of some of these topics, the details we provide will be at a level that is acceptable from a security, confidentiality or commercial perspective to be made available via this medium. If further detail or clarification is required please contact your Palo Alto Networks representative and they will forward the request to the Palo Alto Networks Federal & Government Team who will provide further direction or details for those parties that are entitled and require this next level of detail within an appropriate framework.

Palo Alto Networks has and will continue to maintain close liaison and collaboration with the National Cyber Security Centre (NCSC) as we do with other key Government National Technical Authorities or International Standards boards to ensure that we maintain an enhanced awareness of our development controls and processes and thus are confident that all statements within this document are within both the spirit and the technical detail of the regulatory document.

Please note that the information provided with this document concerning technical or professional subject matter is for general awareness only, may be subject to change, and does not constitute legal

or professional advice, warranty of fitness for a particular purpose or any kind, or compliance with applicable laws.

V.A Product Lifecycle Management

Palo Alto Networks' approach to life cycle management has been designed to ensure that our Customers have the utmost visibility and awareness of the current status of our capabilities and services.

V.A.1,2 Lifecycle Process & Software Maintenance

For every software release we issue we also provide a comprehensive set of release notes that can be accessed, searched and referenced from our TechDocs website – All Release Notes.

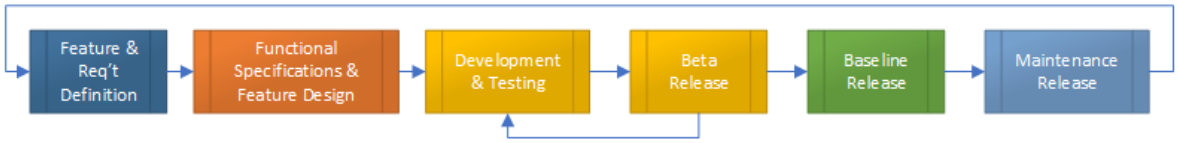
In addition to these release notes we also maintain a comprehensive information portal for all of our products as it applies to - End of Life - Software, and for our specific hardware the End of Life - Hardware can also be found on our public site.

In the event of a requirement for technical support, bug fixes, etc. this can be found within our Customer Support Portal of our public site.

V.A.3-5 Software Version Control (inc. release, development & forking)

As would be expected from a company such as Palo Alto Networks we have established and maintained a rigorous, well documented, trained and audited software version management and release process. Through this process and rigor it is possible to track all modifications, additions and removals from our source code, and link those changes to a specific developer. The following section provides an overview of how this is managed and achieved.

At the highest level Palo Alto Networks follows a six-step process for each major release.



It is useful to appreciate our approach to release numbering at this point.

PAN-OS **X.Y.Z-hN**

A major release is identified by the X.Y value, where Y is zero. A minor release is identified by the X.Y value where Y is greater than zero. A maintenance release is identified by the Z value and any interim release hot-fixes are identified by an hN designation. In this way the number of supported versions are kept to an absolute minimum for each 'in-service' version of PAN-OS. Note we do not diverge our codebase for different International versions.

V.A.6 Release Management & Documentation

The full list of all supported release versions, corresponding release notes and the checksums are available within the Updates section of our Customer Support Portal. Please note to access this site you need a Support account with MFA, which you can get after you have registered (available via the link if no existing account).

V.A.7 Software Tools Libraries & OS Licencing

For each release a complete list of all third-party components by release are provided within - PAN-OS OSS Listings. There are a number of internal quality and testing processes that help ensure

all third-party components are maintained and managed to minimise and mitigate any identified risks or vulnerabilities. This is a continuous process for all supported versions of PAN-OS. All libraries used are sourced and packaged from internal repositories, which are updated and maintained by the designated developers.

V.A.8 System & Software Documentation

Palo Alto Networks provides online documentation for all aspects of our product capabilities within our Documentation Portal. This includes the Administrator's Guide, New Features Guide and Release Notes to name but a few of the available resources. We also have comprehensive documentation of all features in our Administrator's Guides, and information about known and addressed issues and changes in default behaviour in our Release Notes. All documentation is kept up to date.

V.A.9 CPE Vendor Specific Security

It is not currently anticipated that the capabilities within this document qualify as CPE products. and thus this document provides no specific commitment as outlined in table B.1 of EN 303 645. The 13 key aspects within EN 303 645 are addressed for our capabilities and details of this can be found within this document or the relevant sections of the administration guide relating to the version of supported PAN-OS implemented and has been subjected to third party evaluation and certification (e.g Common Criteria).

V.B Security Management

Within Palo Alto Networks everybody is trained and made aware of our security culture and standards. Our ethos and respect for security by design is one of our key pillars for all. A summary of our Information Security Measures and Culture can be found within this published document – Palo Alto Networks – Information Security Measures.

V.B.1 Product Security Culture

Further to the company's security training, any developer or person with access to the product suite has additional training, assessment and reviews to help ensure the highest quality code development and the mitigation of vulnerability in code development by design. This posture is delivered, managed and maintained by the development leads in conjunction with our Cerberus Team. This Team (a branch of our Security Research Team) focuses on maintaining our internal product security and the associated toolkits to assure this.

V.B.2 Secure Development Lifecycle

As should be expected, security checks and balances are embedded and audited throughout our development lifecycle as illustrated and evidenced within the various sections of this document and the public resources referenced herein. As a best practice, Palo Alto Networks provides a set of 'safe' functions for use by all of our developers.

V.B.3 Internal Component Management

As can be understood from our version control processes and branching management introduced previously, Palo Alto Networks strives to maintain rigid management of all internal components within the codebase including the use of centralized approved library sources.

V.B.4 External Component Management

Management of external components and ensuring their usage, status and issues are reflected within our solution is and will remain an on-going activity. Palo Alto Networks has a programme to review and address any legacy issues in this area to help ensure all OSS packages are fully within long

term supported (LTS) versions once completed. As previously identified all external components are sourced from internally managed repositories.

V.B.5 Unsafe Functions

Palo Alto Networks ensures safe versions of key functions that we identify as critical during our development cycle. As stated previously within this section, Palo Alto Networks maintains an internal list of preferred functions that all developers are required/expected to use.

V.B.6 Redundant and Duplicate Code

Palo Alto Networks leverages our Coverity implementation (which triggers on unused code) to manage this process.

V.B.7,9 File Structure & Code Comments

Palo Alto Networks does and continues to maintain a logically structured, commented and documented file and code structure.

V.B.8 Debug Functionality

No code with development debugging flags is made available for a released version in the public domain.

V.C Product Development & Build Environment

V.C.1,2 Segregation of Development & Build Environments

Palo Alto Networks has deployed and maintains fully segmented and segregated development and build environments with dedicated resources and administrative/engineering teams. This segregation and segmentation utilise recognised best practices, enforce role-based access control and monitor and audit all access and session activity. This segregation utilises multiple additional measures including user-based access control with network-based MFA to enforce access and separately managed and administered development accounts for this role function.

V.C.3,6 Build Automation & Repeatability

Within this environment quality, repeatability, code reviews and managed regression processes are fully implemented and managed using automated and audited processes and procedures. These roles and duties are performed by a dedicated, discrete, and focused engineering tools team.

V.C.4 Role Based Access Controls

RBAC is achieved using a combination or a zero-trust NGFW-based configuration and our Perforce implementation and role management therein.

V.C.5 Code Reviews

Code control and review processes are automatically initiated as soon as code is checked into our source control via a Crucible based solution. This methodology, as users of Crucible will be aware, and tooling help ensure that heightened visibility, reviews and auditing of code changes are automatically enabled at the commencement of the process thus enabling better code quality and accuracy throughout the process.

All new code automatically generates a code review ticket in Crucible. The process dictates that no changes are allowed into the release branches without being code reviewed. The QA team validates that this is the case before allowing code to be integrated to release branches. If any anomalies are detected, then an audit is initiated which will identify where the anomaly was injected and how this can be mitigated earlier within the development lifecycle process.

V.D Exploit Mitigations

As would be expected, during the development process Palo Alto Networks leverages best practices to help ensure that any potential exposure from exploit mitigations are addressed using effective techniques at source to maximize efficiency. These automated mitigations include the following techniques as appropriate and applicable. The scope of these mitigations are continually reviewed and enhanced as would be expected within a continual service improvement environment.

- Heap & Stack Protection
- Data Execution Prevention
- ASLR
- Memory Mapping
- Least Privilege Methodologies

Furthermore, Palo Alto Networks continues to evaluate new methodologies and extend our existing coverage and practices to further enhance the protection of our capabilities across all expected or future deployment mediums that may have a limited trust or assurance value for the hosted capabilities.

V.E Secure Updates & Software Signing

V.E.1 Software & Firmware Signing

Palo Alto Networks digitally signs all of our PAN-OS software and updates. These signatures are checked and validated by the NGFW (appliance & software form factors) prior to installation. These checks are documented within our PAN-OS documentation – Device > Software.

V.E.2 Signature Verification

All of our firewalls and Panorama instances are designed to perform software integrity checks for tamper detection and software corruption. The software integrity check validates that the operating system and data file structure are intact and as delivered by Palo Alto Networks. When the check is successful, a System log of informational severity is generated. If the check detects a software corruption or possible appliance tampering, it generates a System log of critical severity on PAN-OS 8.1.1 and 8.1.2. Starting with PAN-OS 8.1.3, the appliance goes into maintenance mode when the check fails. For more details on how the software integrity check works both at boot time and periodically whilst operating, see the PAN-OS 8.1.1 Software Integrity Check article. Note as this function is available on all implementations (appliance & virtual) of our PAN-OS products thereafter.

Note that prior to 8.1.1 software integrity checks were performed upon image loading and installation and on boot when in FIPS/CC mode. With 8.1.1+, these checks are performed on boot regardless of system mode.

V.E.3 Secure Update

Palo Alto Networks also provides all updates via a validated secure channel. Using Verify Update Server Identity (enabled by default), the firewall or Panorama (which when set will make this an enterprise-wide default setting for all new devices introduced) will verify that the server from which the software or content package is downloaded has an SSL certificate signed by a trusted authority. This adds an additional level of security for the communication between firewalls or Panorama servers and the update server. This configuration is described within the Global Service Settings section of our documentation.

V.E.4 Downgrade Protections

Palo Alto Networks recognises the customers' requirement for flexibility of upgrade/downgrade. We provide multiple alerts and indicators thus making it easy to determine if the system has been downgraded.

V.F Roots of Trust & Secure Boot

Palo Alto Networks recognises the need for a strong root of trust thus this is another area within which continual service improvement and hardening is being addressed within our development lifecycles.

Given the wide range of supported hardware (age and underlying technologies) our approach and implementation vary based upon the selected platform and the evolving best practice and relevant standards. For example - NIST SP 800-193 - all new hardware platforms released post the publication of these standards are by design conformant with this standard.

As expected this functionality is performed transparently to the end-user. This capability when used in conjunction with other inherent capabilities such as our software integrity checker as introduced in V.E.2 above and expanded upon in the following article - PAN-OS 8.1.1 Software Integrity Check illustrate our continued and evolving commitment to help ensure the integrity of the PAN-OS capability both at boot and during operations.

V.G Security Testing

Palo Alto Networks takes the quality of our products very seriously, thus throughout the development process we retain an independent quality function that includes the security testing functions that are exercised for each security test for each update processed.

V.G.1 Automated Testing

Palo Alto Networks has and leverages an extensive automated test suite against our development cycle that we believe is commensurate to and exceeds that of a well-resourced aggressor. This includes both positive and negative testing.

V.G.2 Testing Rigour

Within our tooling and process it is not possible for our developers to make any changes to the build systems which would modify that which is checked in to the code repository or bypass other automatic tests.

V.G.3 Security Testing

This function is performed by leveraging the skills of both our internal resources and external penetration testing teams.

V.G.4 Negative Testing

Palo Alto Networks performs both negative and ad-hoc testing the scale of which is believed to be commensurate with the risk.

V.G.5 Fuzzing

Fuzzing is performed against our capabilities using a suite of specifically designed tools by our Security Team to help ensure suitable coverage is achieved. As identified above this, like all other tests, are included in each testing event and include but not limited to:

- CLI command line fuzzing

- DP traffic fuzzing tools per protocol
- Web fuzzer for XSS and other vulnerabilities
- MGMT interface fuzzer
- The static analysis + pseudo-symbolic execution tool for PAN-OS

V.G.6 External Testing

As previously identified external penetration testers are included as part of our major and minor release security QA process.

V.G.7 Dynamic Application Security Testing (DSAT)

As identified previously, the majority of our DSAT tooling has been specifically developed in-house. This tooling is complemented by such tooling as the Burp Suite of tools to ensure multi-axis and expansive coverage.

V.H Secure Management & Configuration

Palo Alto Networks recognises the importance of security by default and zero-trust solutions. To support this posture several measure and implementation guides have been provided for our capabilities:

V.H.1 Product Lockdown

Palo Alto Networks can be operated in a secure configuration utilising the FIPS/CC mode – details of this can be found in the Enabling FIPS & Common Criteria Support section of the Administrator's Guide which describes each aspect of the process for these modes. Alternatively to achieve a hardened implementation without invoking specific FIPS/CC attributes you can follow the practice guides within our documentation - an example of which is Best Practices for Securing Administrative Access

V.H.2,3 Secure Protocol Standardisation inc. Management Plane

By design all communications protocols are standards based where practical; if a custom communications channel is required then this is protected using TLS 1.2 or higher.

V.H.4-7 Management & Administrative Access

To ensure correct and controlled management and administrative access to our platforms, Palo Alto Networks provides a comprehensive delegated and audited administrative access capability. This is fully documented within the relevant sections of the Administrator's Guide found in the Documentation Portal. We also provide a specific section on the best practices for securing Administrative Access. All administrative accounts are visible within the management interface irrespective of the type of Admin account (human or system—there is no difference in PAN-OS—there is a common security model). This is further auditable using the relevant system logs.

V.H.8 Default Users and Credentials

At initial power-up, PAN-OS forces a complex password to be set.

V.H.9 Good Practice Guidance

Throughout our Administrator's Guides and knowledge base we provide configuration best practice guidance. Palo Alto Networks also provides guidance via a dedicated Best Practice Portal.

V.J Vulnerability & Issue Management (V.J.1-5)

Palo Alto Networks maintains a dedicated PSIRT Team to address any reported or identified Vulnerabilities or Issues; this is a public service and the full description of the service, our processes and contact details are available from our PSIRT Portal.