CCEVS APPROVED ASSURANCE CONTINUITY MAINTENANCE REPORT

ASSURANCE CONTINUITY MAINTENANCE REPORT FOR PALO ALTO NETWORKS PA-200, PA-500, PA-2000 SERIES, PA-3000 SERIES, PA-4000 SERIES, PA-5000 SERIES, PA-7000 SERIES, VM SERIES, NEXT-GENERATION FIREWALL WITH PAN-OS V7.0.8 AND V7.1.3

Maintenance Update of Palo Alto Networks PA-200, PA-500, PA-2000 Series, PA-3000 Series, PA-4000 Series, PA-5000 Series, PA-7000 Series, VM Series, Next-Generation Firewall with PAN-OS v7.0.8 and v7.1.3

Maintenance Report Number: CCEVS-VR-VID10640-2016a

Date of Activity: November 22, 2016

References: Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 3.0, 12 September 2016;

Palo Alto Networks PA-200, PA-500, PA-2000 Series, PA-3000 Series, PA-4000 Series, PA-5000 Series, PA-7000 Series, VM Series, Next-Generation Firewall with PAN-OS v7.0.8 and v7.1.3 Impact Analysis Report, version 1.0, 2 November 2016;

Palo Alto Networks PA-200, PA-500, PA-2000 Series, PA-3000 Series, PA-4000 Series, PA-5000 Series, PA-7000 Series, VM Series, Next-Generation Firewall with PAN-OS v7.0.8 and v7.1.3 Security Target, version 1.2, 2 November 2016.

Introduction

The Leidos Common Criteria Test Laboratory, on behalf of Palo Alto Networks, submitted an Impact Analysis Report (IAR) to Common Criteria Evaluation Validation Scheme (CCEVS) for approval on 9 September 2016 and provided an updated version of the IAR on 2 November 2016. The IAR satisfied the requirements outlined in Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 3.0. In accordance with those requirements, the IAR described the changes made to the certified Target of Evaluation (TOE), the evidence updated as a result of the changes and the security impact of the changes.

Summary of Changes to the TOE

The IAR described changes made between PAN-OS v7.0.1-h4 and the following current PAN-OS releases: PAN-OS v7.0.8; and PAN-OS v7.1.3. The described changes constitute all changes made to the Palo Alto Networks Next-Generation Firewall since completion of the NIAP evaluation and validation of the Next Generation Firewall with PAN-OS v7.0.1-h4 (VID10640).

Since the completion of the evaluation of the Palo Alto Next Generation Firewall appliances and virtual appliances with PAN-OS 7.0.1-h4, Palo Alto Networks has produced the following maintenance releases in the 7.0.x line up to v7.1.3:

- 7.0.2—no new features; 90 issues addressed
- 7.0.3—no new features; 81 issues addressed
- 7.0.4—no new features; 65 issues addressed

- 7.0.5—no new features; 59 issues addressed
- 7.0.5-h2—no new features; 2 issues addressed
- 7.0.6—no new features; 43 issues addressed
- 7.0.7—no new features; 51 issues addressed
- 7.0.8—no new features; 44 issues addressed.
- 7.1—adds new features in the following areas:
    - Management features
    - App-ID features
    - Virtualization features
    - WildFire features
    - Content Inspection features
    - GlobalProtect features
    - User-ID features
    - Networking features
    - Decryption features
    - VPN features
    - Panorama features
    - Hardware features
- 7.1.0—no new features; 116 issues addressed
- 7.1.1—one new Content Inspection feature; 1 issue addressed
- 7.1.2—no new features; 60 issues addressed
- 7.1.3—no new features; 50 issues addressed.

The new features introduced in PAN-OS 7.1 and 7.1.1 are described in Appendix A, along with rationale justifying why they can be considered minor changes to the evaluated TOE.

Each of the issues addressed in PAN-OS releases were documented in the IAR and are also included in Appendix B of this Assurance Continuity Maintenance Report, including rationale why each issue is considered a minor change to the TOE. NIAP CCEVS Policy Letter #22 encourages end users to install vendor-delivered patches to ensure the latest security bug fixes are incorporated into operational products, while still maintaining system accreditation on the evaluated product. As part of Palo Alto's bug tracking and flaw remediation process, a number of issues were addressed between PAN-OS v7.0.1-h4 and the PAN-OS v7.0.8 and PAN-OS v7.1.3 releases. These bug fixes do not result in any changes to TSF platforms, SFRs, Assumptions or Objectives, Assurance Documents, Test Results or the TOE Environment; therefore, they are all considered minor changes. For a complete description and analysis of these bug fixes, please refer to Appendix B of this report.

Documentation Updated

Evidence Identification	Effect on Evidence/ Description of Changes
Security Target: *Palo Alto Networks PA-200, PA-500, PA-2000 Series, PA-3000 Series, PA-4000 Series, PA-5000 Series, PA-7000 Series, VM Series, Next-Generation Firewall with PAN-OS v7.0.1-h4 Security Target*, Version 1.0, 23 November 2015 was updated to Version 1.2, 2 November 2016	The ST title and TOE identification (Section 1.1) and all other references throughout the ST are updated to identify the revised PAN-OS versions (7.0.8 and 7.1.3). The ST is also updated as follows: • Section 2.2.2.2 was updated to identify the CMVP certificates covering all the physical and virtual appliances included in the TOE • Section 2.3 provides updated TOE documentation references • In Section 5.2.2, the statement of FCS_COP.1(4) was updated to remove HMAC-SHA-224 from the claimed HMAC algorithms (see next bullet point for why this was done) • Table 4 in Section 6.2 is updated with new CAVP certificate numbers for v7.1.3. In addition, the claim for HMAC-SHA-224 (and all other references to it) has been removed, since it is not covered by any of the HMAC CAVP certificates associated with the TOE.
Guidance: *Palo Alto Networks Common Criteria Evaluated Configuration Guide (CCECG)*, Version 1.0, November 23, 2015 *Palo Alto Networks PAN-OS Administrator's Guide*, Version 7.0, 9 June 2015 *Palo Alto Networks Web Interface Reference Guide*, Version 7.0, 29 May 2015	The PAN-OS Administrator's Guide for Version 7.0 is unchanged. The Web Interface Reference Guide for Version 7.0 is unchanged. Palo Alto Networks has produced a PAN-OS Administrator's Guide for version 7.1 of PAN-OS. The differences between Version 7.0 and Version 7.1 of the Administrator's Guide involve some reorganization or renaming of material and addition of descriptions of new management capabilities, all of which are deemed to be minor changes. Palo Alto Networks has produced a Web Interface Reference Guide for version 7.1 of PAN-OS. The differences between Version 7.0 and Version 7.1 of this guide involve some reorganization or renaming of material and addition of descriptions of new management capabilities, all of which are deemed to be minor changes. The CCECG is revised to reference the updated release of PAN-OS 7.0 covered by this IAR (version 7.0.8). Also, a second version of the CCECG has been created, based on the original evaluated version, which references the release of PAN-OS v7.1 and provides references into the Version 7.1 Administrator's Guide where they differ from the references in Version 7.0.

Conclusion

The CCEVS reviewed the description of the changes and bug fixes and reviewed the discussion of regression test results provided. A certificate check was performed against the cryptographic certificates to ensure continued validity. The Common Criteria Test Laboratory performed a vulnerability analysis, which was documented in the IAR and was reviewed by validators. All identified vulnerabilities were not applicable to the TOE or were addressed in bug fixes.   An analysis of all changes to the product determined that the changes were minor. The CCEVS agrees that the original assurance is maintained for the above-cited version of the product.

Appendix A. New Features and Security Relevance

The new features introduced in PAN-OS 7.1 and 7.1.1 are described below, along with rationale justifying why they can be considered minor changes to the evaluated TOE.

New Features in the TOE	Rationale
Commit Queues: The firewall and Panorama™ now queue commit operations so that the user can initiate a new commit while a previous commit is still in progress. This enables the user to activate configuration changes without having to coordinate commit times with other administrators.	Minor change because when an administrator changes the configuration of the TOE, a Commit operation needs to be performed in order for those configuration changes to take effect. The Commit operation is not in itself security-relevant, so adding a feature to enable commit operations to be queued is also not security-relevant. This feature does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.
Synchronization of SNMP Trap and MIB Information: When an event triggers SNMP trap generation (for example, an interface goes down), the firewall, Panorama virtual appliance, M-Series appliance, and WF-500 appliance now update the corresponding SNMP object in response (for example, the interfaces MIB) instead of waiting for the 10-second timer to expire and allowing SNMP queries to receive out-of-sync replies. This ensures that the network management system displays the latest information when polling an object to confirm the event.	Minor change because the use of SNMP is outside the scope of evaluation. This feature is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.
Banners and Message of the Day: For the firewall and Panorama, the user can now customize the web interface as follows: • Force administrators to acknowledge the login banner to ensure they see information they need to know before they log in, such as login instructions. • Add a message of the day that displays in a dialog after administrator log in to ensure they see important information, such as an impending system restart, that can affect their tasks. The same dialog also displays messages that Palo Alto Networks embeds to highlight important information associated with a software or content release. • Add colored bands that highlight overlaid text across the top (header banner) and bottom (footer banner) of the web interface to ensure administrators see critical information, such as the classification level for firewall administration.	Minor change because the evaluated TOE was tested to confirm it satisfies the PP requirements for an administrator-configurable advisory notice and warning message (FTA_TAB.1). The changes described above do not affect that evaluated functionality. The message acknowledgement function is not required by FTA_TAB.1, so does not impact the ST, guidance, or Assurance Activities testing. The Message of the Day is displayed after the administrator has logged on, so is not within the scope of FTA_TAB.1. Similarly, the colored bands overlaying the top and bottom of the web interface are not within the scope of FTA_TAB.1.
Support for Certificates Generated with 4,096-bit RSA Keys: The firewall and Panorama now support certificates generated with 4,096-bit RSA keys, which are more secure than smaller keys. The user can use these certificates to authenticate clients, servers, users, and devices in several applications, including SSL/TLS decryption, Captive Portal, GlobalProtect™, site-to-site IPsec VPN, and web interface access	Minor change because the evaluated TOE was tested to confirm it satisfies the PP requirements to support certificates generated with a minimum 2,048-bit RSA keys. The cryptographic operations of digital signature generation and verification are confirmed through cryptographic algorithm validation testing and the ST references the applicable CAVP certificates. This change does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.
Bootstrapping Firewalls for Rapid Deployment: The user can now fully provision (bootstrap) a firewall with or without Internet access. Bootstrapping reduces operational effort and service-ready time by eliminating manual configuration steps and user errors when deploying new firewalls. The user can now bootstrap the firewall using an external device—a USB flash drive or a virtual CD ROM/DVD—and accelerate the process of configuring and licensing the firewall. The bootstrapping process is supported on all hardware-based firewalls and on VM-Series firewalls in both the private cloud (KVM, ESXi, Hyper-V) and the public cloud (AWS, Azure).	Minor change because the functionality described in this change relates to a new means for initially configuring the TOE and is not related to any of the evaluated functionality. As such, this change does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

New Features in the TOE	Rationale
Web Interface Design Refresh: The web interface design on Panorama and the firewalls is redesigned with new icons and buttons and an updated font and color scheme. This modernization does not include any changes in layout or workflows.	Minor change because this change alters only the look of the management interface of the TOE and does not affect any evaluated functions or capabilities. As such, this change does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.
New API Request to Show PAN-OS Version: The user can now use the PAN-OS XML API to show the PAN-OS version on a firewall or Panorama. In addition to the PAN-OS version, this new API request type (type=version) provides a direct way to obtain the serial number and model number.	Minor change because the XML API is not covered within the scope of the evaluation.
Unified Logs: A new unified log view allows the user to view the latest Traffic, Threat, URL Filtering, WildFire™ Submissions, and Data Filtering logs on a single page.	Minor change because the ST does not specify any requirements for reviewing audit or log records. As such, this change does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.
AutoFocus and PAN-OS Integrated Logs: AutoFocus™ threat intelligence data is now integrated with PAN-OS logs, providing the user with a global context for individual event logs. The user can now click on an IP address, URL, user agent, filename, or hash in a PAN-OS log entry to display an AutoFocus threat intelligence summary of the latest findings and statistics for that artifact.	Minor change because AutoFocus is a Palo Alto subscription service, use of which is outside the scope of the evaluation. This feature is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.
Administrator Login Activity Indicators: To detect misuse and prevent exploitation of administrator accounts on a Palo Alto Networks firewall or Panorama, the web interface and the command line interface (CLI) now display the last login time and any failed login attempts when an administrator logs in to the interface.	Minor change because this feature provides the administrator with additional information at login, but does not otherwise alter the behavior of the TOE during the login process. As such, this feature results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.
PDF Report for Visibility into SaaS Applications: The new SaaS application usage PDF report provides visibility into the SaaS applications in the user's network. SaaS is a way of delivering applications where the service provider owns and manages the software and the infrastructure, and the user controls the data, including the rights to who can create, access, share, and transfer data. The new report helps identify the ratio of sanctioned versus unsanctioned SaaS applications in use on the network and includes details on the top SaaS application subcategories by number of applications, by number of users, and by volume of data transferred using these applications.	Minor change because the scope of the evaluation is limited to the packet filtering/stateful traffic filtering capabilities of the TOE, which were tested only for the following protocols: IPv4; IPv6; ICMPv4; ICMPv6; TCP; UDP; and FTP. Identification of SaaS applications on the network, sanctioned or unsanctioned, and the presentation of related information in a report, is outside the scope of evaluation. This feature is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.
VM-Series Firewall for Microsoft Azure: The VM-Series firewall can now be deployed in Azure, the Microsoft public cloud.	Minor change because the deployment of the VM-Series firewall in Azure is outside the scope of the evaluation. This feature is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.
Support for Multi-Tenancy and Multiple Sets of Policy Rules on the VM-Series NSX Edition Firewall: When using the VM-Series NSX edition solution for automated provisioning of VM-Series firewalls, the user can now create multiple service definitions on Panorama.	Minor change because the VM-Series NSX edition firewall is not covered in the scope of evaluation. In addition, management of firewalls via Panorama is excluded from the evaluated configuration. As such, this feature is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.
VM-Series Firewall for Microsoft Hyper-V: To expand support for deploying the VM-Series firewall in private cloud and hybrid cloud environments, a capability was added to deploy the VM-Series firewall on Hyper-V Server 2012 R2 (standalone edition) or Windows Server 2012 R2 (standard and datacenter editions) with the Hyper-V role that allows the user to create and manage virtual machines.	Minor change because deployment of the VM-Series firewall on Microsoft Hyper-V is outside the scope of the evaluation. This feature is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

New Features in the TOE	**Rationale**
Support for VMware Tools on Panorama and on VM-Series Firewalls on ESXi: For ease of administration, the VM-Series firewall and the Panorama virtual appliance are now bundled with a customized version of open-vm-tools. This bundle allows the virtual infrastructure administrator to: • View the management IP address and PAN-OS version of the firewall and Panorama on vCenter. • View resource utilization metrics for the hard disk, memory, and CPU. • Monitor availability and health status of the virtual appliance using a heartbeat mechanism. • Gracefully shutdown and restart the firewall and Panorama from the vCenter server	Minor change because this change provides a set of tools to assist the administrator manage the virtual environment in which VM-Series firewalls are installed. This change does not affect any of the behavior of the VM-Series firewall itself. This feature is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.
Support for Device Group Hierarchy in the VM-Series NSX Edition Firewall: Capability was added to assign the VM-Series NSX edition firewall to a template stack and a device group in a hierarchy so that the firewalls can inherit settings defined in the stack and the hierarchy.	Minor change because the VM-Series NSX edition firewall is outside the scope of the evaluation. This feature is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.
Support for Synchronizing VM Monitoring Information on Firewalls in HA: For a pair of firewalls (VM-Series and hardware-based firewalls) deployed in a high availability configuration, dynamic data such as information about virtual machine IP addresses and other monitored attributes, can now be synchronized between High Availability peers.	Minor change because High Availability configurations are not covered in the scope of the evaluation. This feature is not security relevant to the evaluated configuration and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.
Support for Amazon ELB on the VM-Series Firewalls in AWS: To use Amazon Elastic Load Balancing (ELB) for increased fault tolerance in anAWS deployment, the VM-Series firewall can be deployed behind the Amazon ELB.	Minor change because this feature is not covered in the scope of the evaluation. This feature is not security relevant to the evaluated configuration and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.
Wildfire Features: The vendor added a number of Wildfire features including Five Minute Wildfire updates, MAC OS X File Analysis, and new Wildfire API Features.	Minor Change because WildFire is outside the scope of the evaluation. This feature is not security relevant to the evaluated configuration and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.
Content Inspection Features: The vendor added a number of content inspection features, including enhanced security for application and URL Category-Based Policy, protection against LZMA compressed Adobe Flash files, Extended support for URLs and Domain Names in an External Dynamic List, and TCP Sessions and Content ID^{TM} Settings in the Web Interface.	Minor change because the scope of the evaluation is limited to the packet filtering/stateful traffic filtering capabilities of the TOE, which were tested only for the following protocols: IPv4; IPv6; ICMPv4; ICMPv6; TCP; UDP; and FTP. In particular, content inspection features are outside the scope of evaluation. Therefore, the changes listed here are not security relevant and result in no changes to the ST or guidance documentation and have no effect on the result of any Assurance Activity test.

New Features in the TOE	Rationale
GlobalProtect Features: The vendor added a number of GlobalProtect Features, including a GlobalProtect App for Chrome OS, simplified GlobalProtect Agent User Interface for Windows and Mac OS Clients, Dynamic GlobalProtect App customization, enhanced Two-Factor Authentication for GlobalProtect, Client Authentication Configuration by Operating System or Browser, Kerberos Single Sign-On for GlobalProtect, Customizable Password Expiry Notification Message for GlobalProtect, Enhance Authentication Challenge Support for Android and iOS Devices for Global Protect, Block Access from Lost or Stolen and Unknown Devices for Global Protect, Certificate Selection by OID for GlobalProtect, Save Username Only Option for GlobalProtect, Use Address Objects in a GlobalProtect Gateway Client Configuration, Transparent Distribution of Trusted Root CAs for SSL Decryption for GlobalProtect, Maximum Internal Gateway Connection Retry Attemps for GlobalProtect, GlobalProtect Notification Suppression, and Disable GlobalProtect without Comment.	Minor change because GlobalProtect is outside the scope of the evaluation. These features are not security relevant to the evaluated configuration and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.
User-ID Features: The vendor added a number of User-ID features, including User-ID Redistribution Enhancement, Ignore User List Configurable in Web Interface, and User Group Capacity Increase.	Minor change because the use of user identities in firewall rule sets is not covered by the scope of evaluation testing. Therefore, the changes described here are not security relevant and result in no changes to the ST or guidance documentation and have no effect on the result of any Assurance Activity test.
Failure Detection with Bidirectional Forwarding Detection (BFD): The firewall product support BFD, a protocol that defects failures in the bidirectional path between an interface on the firewall and a configured BFD peer.	Minor change because the scope of the evaluation is limited to the packet filtering/stateful traffic filtering capabilities of the TOE, which were tested only for the following protocols: IPv4; IPv6; ICMPv4; ICMPv6; TCP; UDP; and FTP. Therefore, this change is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.
LACP and LLDP Pre-Negotiation for an HA Passive Firewall: An HA passive firewall can now negotiate LACP and LLDP before it becomes active. This pre-negotiation reduces failover times by eliminating the delays incurred by LACP or LLDP negotiations	Minor change because this relates to High Availability configurations, which are not covered in the scope of the evaluation. Therefore, this change is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.
Binding a Floating IP Address to an HA Active-Primary Firewall	Minor change because this relates to High Availability configurations, which are not covered in the scope of the evaluation. Therefore, this change is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.
Multicast Route Setup Buffering: The user can now enable buffering of the first packet in a multicast session when the multicast route or forwarding information base (FIB) entry does not yet exist for the corresponding multicast group. By default, the firewall does not buffer the first multicast packet in a new session; instead, it uses the first packet to set up the multicast route. This is expected behavior for multicast traffic. A user needs to enable multicast route setup buffering only if the content servers are directly connected to the firewall and the custom application cannot withstand the first packet in the session being dropped.	Minor change because this is a performance-related change. This change is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.
Per VLAN Spanning Tree (PVST+) BPDU Rewrite: When an interface on the firewall is configured for a Layer 2 deployment, the firewall now rewrites the inbound Port VLAN ID (PVID) number in a Cisco per-VLAN spanning tree (PVST+) bridge protocol data unit (BPDU) to the proper outbound VLAN ID	Minor change because this change is related to Layer 2 switching behavior of the TOE and does not affect any security functionality. This change is not security relevant and results in no changes to

New Features in the TOE	Rationale
number and forwards it out. This new default behavior in PAN-OS 7.1 allows the firewall to correctly tag Cisco proprietary Per VLAN Spanning Tree (PVST+) and Rapid PVST+ frames between Cisco switches in VLANs on either side of the firewall. Thus, spanning tree loop detection using Cisco PVST+ functions properly. There is no behavior change for other types of spanning tree.	the ST or guidance documentation and has no effect on the result of any Assurance Activity test.
Configurable MSS Adjustment Size: The Maximum Segment Size (MSS) adjustment size is now configurable so that the user can adjust the number of bytes available for the IP and TCP headers in an Ethernet frame. The user can expand the adjustment size beyond 40 bytes to accommodate longer IP and TCP headers	Minor change because this is a performance-related change. This change is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.
DHCP Client Support on the Management Interface: The management interface on the firewall now supports DHCP client for IPv4, which allows the management interface to receive its IPv4 address from a DHCP server. The management interface also supports DHCP Option 12 and Option 61, which allow the firewall to send its hostname and client identifier, respectively, to a DHCP server.	Minor change because this change allows the management interface to receive its IPv4 address from a DHCP server, rather than having the administrator configure it manually. This change is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.
Increase in Number of DHCP Servers per DHCP Relay Agent: In a DHCP relay agent configuration, each Layer 3 Ethernet or VLAN interface now supports up to eight IPv4 DHCP severs and eight IPv6 DHCP servers. This is an increase over the previous limit of four DHCP servers per interface per IP address family.	Minor change because configuration as a DHCP relay is outside the scope of evaluation. This change is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.
PA-3000 Series and PA-500 Firewall Capacity Increases: The PA-3000 Series and PA-500 firewalls support more ARP entries, MAC addresses, and IPv6 neighbors than they supported in prior releases. Additionally, PA-3000 Series firewalls support more FIB addresses	Minor change because this is a performance-related change. This change is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.
The Session End Reason column in Traffic logs now indicates the reason for SSL/SSH session termination. For example, the column might indicate that a server certificate expired if you configured certificate expiration as a blocking condition for SSL Forward Proxy decryption. You can use SSL/SSH session end reasons to troubleshoot access issues for internal users requesting external services or for external users requesting internal services.	Minor change because the Traffic log does not contribute to the security audit log necessary to satisfy the audit requirements specified in the Security Target. As such, this change is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.
Fast Identification and Mitigation of Sessions that Overutilize the Packet Buffer: A new CLI command (show running resource-monitor ingress-backlogs) on any hardware-based firewall platform allows the user to see the packet buffer percentage used, the top five sessions using more than two percent of the packet buffers, and the source IP addresses associated with those sessions. This information is very helpful when a firewall exhibits signs of resource depletion and starts buffering inbound packets because it is an indication that the firewall might be experiencing an attack. Another new CLI command (request session-discard [timeout <x>] [reason <reason_string>] id <session_id>) allows the user to immediately discard a session without a commit.	Minor change because use of the CLI for administration of the TOE is outside the scope of evaluation. This change is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.
SSL Decryption Features: The vendor added a number of decryption features to the product, including Transparent Certificate Distribution for SSL Forward Proxy and Perfect Forward Secrecy (PFS) Support with SSL Forward Proxy Decryption.	Minor change because SSL Decryption Policy and SSL Forward Proxy functions are outside the scope of evaluation. Therefore, the changes listed here are not security relevant and result in no changes to the ST or guidance documentation and have no effect on the result of any Assurance Activity test.
DES Support for Crypto Profiles: IKE gateways and IPsec tunnels now support Data Encryption Standard (DES) as an encryption algorithm in crypto profiles for a site-to-site VPN connection. DES support provides backward compatibility with legacy devices that do not use stronger encryption methods.	Minor change because the evaluated configuration of the TOE operates in FIPS mode. In FIPS mode, unapproved algorithms, including DES, are unavailable options for cryptographic algorithms. Therefore, this change is not security relevant and

New Features in the TOE	Rationale
	results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.
Panorama Features: The vendor added a number of new Panorama features, including Role Privileges for commit types for custom Panorama administrator roles and 8TB Disk Support on the Panorama Virtual Appliance.	Minor change because Panorama is outside the scope of the evaluation, therefore the changes are not security relevant and result in no changes to the ST or guidance documentation and have no effect on the result of any Assurance Activity test.
PA-7000 Series Firewall Network Processing Cards with Double the Session Capacity: Two new Network Processing Cards (NPCs) are now available to double the session capacity of previously released NPCs. • PA-7000-20GXM—Doubles the memory of the PA-7000-20G NPC, enabling support for eight million sessions (up from four million). This NPC has twelve RJ-45 10/100/1000Mbps ports, eight SFP ports, and four SFP+ ports. • PA-7000-20GQXM—Doubles the memory of the PA-7000-20GQ NPC, enabling support for eight million sessions (up from four million). This NPC has twelve SFP+ ports and two QSFP ports. For example, installing ten PA-7000-20GXM NPCs in a PA-7080 firewall enables support for up to 80 million sessions. All PA-7000 Series NPCs are compatible with each other, so the user can install any combination of them in a PA-7050 or PA-7080 firewall.	Minor change because this change increases the capacity of PA-7000 Series devices, in terms of number of concurrent sessions that can be supported. This change is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test

Appendix B. Bug Fixes

Bug Fixes Addressed in the 7.0.8 Release

97313—Fixed an issue where the management plane of Panorama M-100 and M-500 appliances stopped responding when renaming objects or security policies due to memory corruption.

Minor Change – This applies to the Panorama M-100 and M-500 appliances, which are not part of the TOE.

96792—Fixed an issue where commits failed due to a memory leak related to HA sync of the candidate configuration that caused the passive Panorama peer to stop responding.

Minor Change – This is a Panorama issue. Panorama is not covered in the scope of the evaluation.

94757—Fixed a rare issue on firewalls where Security policy rules included empty dynamic block lists (0.0.0.0/0) after a Commit from Panorama with Force Template Values enabled.

Minor Change – This is a Panorama issue. Panorama is not covered in the scope of the evaluation.

93729—Fixed an issue where SSH decryption caused a dataplane memory leak and restart.

Minor Change – SSH Decryption policy is outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

93072—A security-related change was made to address an issue in the policy configuration dialog.

Minor Change – This is the fix made to address PAN-SA-2016-0014, which closes a cross-site scripting vulnerability in the PAN-OS web GUI. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

92763—Fixed an issue where commits failed due to a validation error that occurred when Panorama pushed Authentication Sequence profiles that included a virtual system that was not migrated properly during an upgrade from a Panorama 6.1 release to a Panorama 7.0 or later release.

Minor Change – This is a Panorama issue. Panorama is not covered in the scope of the evaluation.

92391—Fixed an issue where firewall Traffic logs displayed unusually large byte counts for sessions passing through proxy servers.

Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

92293—A security-related fix was made to address CVE-2016-1712.

Minor Change – This is the fix made to address PAN-SA-2016-0012 (CVE-2016-1712). The vulnerability can be exploited only by local users who obtain a shell on the device. Use of the CLI is excluded from the evaluated configuration. Therefore, this issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

91900—Fixed an issue where a Panorama validate operation followed by an FQDN refresh caused the validate config to commit to the firewall.

Minor Change – This is a Panorama issue. Panorama is not covered in the scope of the evaluation.

91886—A security-related fix was made to address CVE-2015-7547.

Minor Change – This is the fix made to address PAN-SA-2016-0021 (CVE-2015-7547). The vulnerability can be exploited only by an attacker controlling the DNS server configured for the device. Furthermore, the attacker must overcome additional anti-exploitation mitigations, such as ASLR, to mount a successful attack. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

91876—Fixed an issue where the passive firewall in a VM-Series ESXi configuration was processing and forwarding traffic.

Minor Change – In the evaluated configuration, a single active VM-Series virtual appliance must be the only guest running in a virtualized environment. Therefore, this issue is not relevant to the TOE in its evaluated configuration.

91799—Fixed an issue were a PA-7050 firewall did not display logs as expected and caused a process (logrcvr) to stop responding.

Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

91728—A security-related fix was made to address a Denial of Service condition related to the API.

Minor Change – This is the fix made to address PAN-SA-2016-0008 (SecurityFocus Bugtraq ID 91468). The XML API is not covered within the scope of the evaluation. Therefore, this issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

91724—Fixed an issue where an autocommit failed after a reload due to a corrupt virus signatures file and a failed incremental installation.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

91653—Fixed an issue where SSL decryption did not work as expected for resumed sessions.

> Minor Change – SSL Decryption policy is outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

91643—Fixed a rare issue where traffic that triggered an SSL decrypt URL proxy action caused a process (all_task) to restart.

> Minor Change – SSL Decryption policy is outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

91497—Fixed an issue where stale next-hop MAC entries persisted on the session offload processor after you modified a subinterface configuration, which caused SSH connections to fail. With this fix, the management plane cache no longer duplicates next-hop MAC entries, which prevents the stale entries that caused SSH connections to fail.

> Minor Change – Use of SSH is outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

91336—Fixed an issue where the packet processor stopped responding when proxy packets were switched to the fast path group on the dataplane.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

90982—Fixed an issue where upgrading from a PAN-OS 6.1 release to PAN-OS 7.0.3 or a later PAN-OS 7.0 release caused the GlobalProtect portal or gateway and SSL decryption processes to stop responding. This issue occurred because SSL/TLS Service Profiles (introduced in PAN-OS 7.0) were not created successfully if you did not enable multiple virtual system (multi-vsys) functionality on the firewall. With this fix, SSL/TLS Service profiles are now successfully created on non-multi-vsys platforms when upgrading to PAN-OS 7.0.8 or later releases or to PAN-OS 7.1 releases.

> Minor Change – GlobalProtect and SSL Decryption policy are outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

90857—Fixed an issue with a Panorama passive peer in an HA configuration where administrators were unable to configure the Dynamic Updates schedule for Applications and Threats updates.

> Minor Change – This is a Panorama issue. Panorama is not covered in the scope of the evaluation.

90856—Fixed an issue where the dialog for creating certificates and the dialog for editing certificates had different character limits for the certificate name. With this fix, the certificate name field in both dialogs allows up to 63 characters.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

90842—Fixed an issue where the firewall received an unencrypted empty ISAKMP packet in quick mode that caused a process (ikemgr) to stop responding.

> Minor Change – This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

90794—Fixed an issue where a log file (/var/log/wtmp) inflated and consumed the available disk space. With this fix, PAN-OS uses a log rotation function to prevent log files from consuming more disk space than necessary.

> Minor Change – The affected log file is not a component of the TOE's security audit trail. Therefore, this is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

90680—Fixed an issue on PA-500 firewalls where certain processes (l3svc and sslvpn) stopped responding after the firewall attempted a dynamic update.

> Minor Change – This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

90635— A security-related fix was made to address a cross-site scripting condition in the Application Command Center (ACC).

> Minor Change – This is the fix made to address CVE-2016-2219. The Application Command Center (ACC) is an interactive, graphical summary of the applications, users, URLs, threats, and content traversing the network. The ACC uses the firewall logs to provide visibility into traffic patterns and actionable information on threats. The ACC is not described in the ST and its use is not covered in the scope of evaluation. Therefore, this issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

90553—Fixed an issue where Data Filtering and WildFire Submissions logs for non-NAT sessions contained incorrect or invalid NAT information.

> Minor Change – Data Filtering profiles and WildFire are outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

90326—Fixed an issue on PA-7000 Series firewalls where botnet reports were not created consistently due to a log cleanup job that ran just prior to when the botnet reports were generated, which—on some days—resulted in empty or no botnet reports. With this fix, the botnet log cleanup job takes place after the daily generation of botnet reports so that daily reports are created and populated as expected.

> Minor Change – Botnet reporting is outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

90256—Fixed an issue where decrypted SSH sessions were not mirrored to the decrypt mirror interface as expected.

> Minor Change – SSH Decryption policy is outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

90249—Fixed an issue where upgrading from a PAN-OS 6.1 or earlier release prevented administrators from overriding LDAP group mappings that were pushed from Panorama.

> Minor Change – This is a Panorama issue. Panorama is not covered in the scope of the evaluation.

90044—Fixed an issue where log forwarding in Panorama failed when using syslog over TCP.

> Minor Change – This is a Panorama issue. Panorama is not covered in the scope of the evaluation.

89979—Fixed an issue where the Aggregate Ethernet (AE) interface port in virtual wire mode with link state pass through enabled came up after a commit; although its peer AE interface port was down. With this fix, the other AE interface port will come up after the commit and is then brought down in approximately 10 seconds. This causes both AE interfaces to stay down until the first AE interface recovers.

> Minor Change – This issue relates to Link Aggregation Control Protocol (LACP), which is not in the scope of the evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

89917—Fixed an intermittent issue where one or more interfaces on a VM-Series firewall deployed in the Amazon Web Services (AWS) cloud could not obtain IP addresses from a DHCP server after booting up.

> Minor Change – Deployment of VM-Series firewalls in AWS is outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

89910—Fixed an issue where all LLDP packets were sent with the source MAC address of the MGT interface instead of the dataplane interface from which they were transmitted. With this fix, LLDP packets are encapsulated with the source MAC address of the interface that transmitted the packet.

> Minor Change – This issue relates to Link Layer Discovery Protocol (LLDP), which is not in the scope of the evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

89743—Fixed an issue where commits failed due to processes (configd and mgmtsrvr) that stopped responding. This issue was caused by memory corruption related to the scheduling of WildFire dynamic updates.

> Minor Change – This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

89551—Fixed an issue where User Activity Reports delivered via the Email Scheduler did not include usernames that contained German characters.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

88646—Fixed an issue where predicted FTP sessions were not established as expected from the parent FTP session.

> Minor Change – This is an availability issue. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

88346—Fixed an issue where a firewall was sending BGP packets with the wrong MD5 authentication value.

> Minor Change – This issue relates to Border Gateway Protocol (BGP), which is not in the scope of the evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

88327—Fixed an issue where several valid country codes were missing in the Certificate Attributes section when generating a certificate from the web interface.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

88157—Fixed an issue with reduced throughput for traffic originating on the firewall and traversing a VPN tunnel.

> Minor Change – This is a performance issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

87851—Fixed an issue where high rates of fragmented packets caused the firewall to experience a spike in packet buffer, descriptor, and CPU usage.

Minor Change – This is a performance issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

87741—Fixed an issue on PA-3000 Series firewalls where the dataplane restarted after an upgrade.

Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

87179—Fixed an issue where a virtual system (vsys) in a Panorama template was assigned duplicate vsys numbers during commit to the firewall.

Minor Change – This is a Panorama issue. Panorama is not covered in the scope of the evaluation.

86623—Fixed an issue where a firewall in an HA active/passive configuration dropped FTP PORT command packets after a failover.

Minor Change – This relates to High Availability (HA) configurations, which are not covered in the scope of the evaluation.

86123—Fixed an issue where an M-100 appliance in an HA pair had a process (configd) repeatedly restart, causing HA sync to fail.

Minor Change – This applies to the M-100 appliance, which is not part of the TOE.

85160—Fixed an issue where a firewall lost members of a domain group after a failover from the primary to the secondary LDAP server when the last modified timestamp for the group was not the same on both servers.

Minor Change – Use of LDAP external authentication servers is outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

84115—Fixed an issue where virtual system administrators (full access or read-only) were unable to access settings under the Network tab (Panel for undefined not registered was displayed, instead).

Minor Change – The virtual system administrator role is excluded from use in the evaluated configuration.

83239—Fixed an issue where inbound SSL decryption did not work as expected when you enabled SYN cookies.

Minor Change – SSL Decryption policy is outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

80953—Fixed an issue on firewalls in an HA active/active configuration that included virtual wire interfaces where packets did not adhere to virtual wire forwarding paths and caused MAC address flapping on neighbor.

Minor Change – This relates to High Availability (HA) configurations, which are not covered in the scope of the evaluation.

77822—Fixed an issue on a VM-Series NSX edition firewall that sent Dynamic Address Group information only to the primary virtual system (VSYS1) on the integrated physical firewall at the data center perimeter. With this fix, a VM-Series NSX edition firewall configured to Notify Device Group sends Dynamic Address Group updates to all virtual systems on a physical firewall running PAN-OS 7.0.8 or a later PAN-OS 7.0 release.

Minor Change – This relates to VM-Series NSX edition firewalls, which are not covered in the scope of the evaluation.

Bug Fixes Addressed in the 7.0.7 Release

94912—Fixed an issue in PAN-OS 7.0.6 where WF-500 appliances returned false positive results—primarily for Microsoft Word (.docx) files.

Minor Change – This applies to the WF-500 WildFire Appliance, which is not part of the TOE.

93775—Fixed an issue where packet diagnostics failed due to an unnecessarily large debug log related to HA3 packet forwarding.

Minor Change – This relates to High Availability (HA) configurations, which are not covered in the scope of the evaluation.

93644—Fixed an issue on PA-3000 Series firewalls where processing jumbo frames that were larger than 7,000 bytes during a period of heavy traffic caused the FPGA to stop responding. With this fix, the FPGA thresholds are adjusted to correctly handle up to 9KB jumbo frames.

Minor Change – This is a performance-related issue that does not affect any of the SFRs claimed in the ST.

93228—Fixed an issue on PA-7050 firewalls in an HA active/active configuration where jumbo frames that included the DF (do not fragment) bit were dropped when crossing dedicated HA3 ports.

Minor Change – This relates to High Availability (HA) configurations, which are not covered in the scope of the evaluation.

91771—Fixed an issue where a firewall did not send TCP packets out during the transmit stage in the same order as those packets were received.

Minor Change –This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

91443—Fixed an issue where a Panorama M-100 appliance purged logs due to an incorrect quota size.

Minor Change – This applies to the Panorama M-100 appliance, which is not part of the TOE.

91079—Fixed an issue on a VM-Series firewall where an ungraceful reboot caused Dynamic IP address information to get out of sync.

> Minor Change –This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

91075—Fixed an issue where the LSVPN tunnel interface failed to pass traffic after upgrading a satellite firewall to a PAN-OS 7.0 release while the GlobalProtect firewall was still running a PAN-OS 6.1 or earlier release. Additionally, the tunnel interface flapped if you enabled tunnel monitoring. These issues occurred due to changes to the encryption algorithm names when introducing Suite B ciphers in PAN-OS 7.0. With this fix, satellite firewalls running PAN-OS 7.0.7 (or PAN-OS 7.1) or later releases successfully recognize the old names used in PAN-OS 6.1 and earlier releases so that LSVPN tunnels are established and pass traffic as expected.

> Minor Change –LSVPN (Large Scale VPN) is a GlobalProtect feature. GlobalProtect is not covered in the scope of the evaluation.

90433—Fixed an issue where overrides of the default rules in the Shared policy took precedence over the overrides of default rules in a device group. With this fix, override precedence now behaves as designed (overrides of default rules in the lowest level device group take precedence over those settings in the higher level device groups and Shared).

> Minor Change –Device groups and the Shared policy are Panorama features. Panorama is not covered in the scope of the evaluation.

90194—Fixed an issue where firewalls without any WildFire public signatures (had never downloaded any or old signatures had been deleted) did not properly leverage WildFire private cloud signatures when monitoring traffic.

> Minor Change –Use of WildFire signatures and interaction with the WildFire service is not covered in the scope of the evaluation.

90158—Fixed an issue on PA-7000 Series firewalls where aggregate outbound traffic was incorrectly limited by the chassis switch fabric switching capacity.

> Minor Change – This is a performance-related issue. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

90070—Fixed an issue where a memory leak associated with the authentication process (authd) caused intermittent access and authentication issues.

> Minor Change – This is an availability issue. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

90029—Fixed an issue where a GlobalProtect gateway rejected the same routes learned from different LSVPN satellites when the routes were destined for a different virtual router.

> Minor Change – LSVPN is a GlobalProtect feature. GlobalProtect is not covered in the scope of the evaluation.

89761— Fixed an issue where a scheduled log export failed to export the logs if the password in the configuration contained the dollar sign (“$”) character.

> Minor Change – In the evaluated configuration, the TOE forwards generated audit records to a configured syslog server over TLS, using digital certificates for mutual authentication. The scheduled log export capability relevant to this issue is a separate capability not covered in the scope of the evaluation. Therefore, this issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

89588—Fixed an issue where packets that had to be retransmitted during SSL decryption were not handled correctly, which resulted in a depleted software packet buffer.

> Minor Change – SSL Decryption policy is outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

89503—Fixed an issue where user-group mappings were not properly populated into the dataplane after a firewall reboot.

> Minor Change – This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

89413—Fixed an issue where Panorama template commits failed when the names of several certificates in the Default Trusted Certificate Authorities list changed. This occurred when Panorama was running a PAN-OS 7.0 release and pushed a template to a firewall running a PAN-OS 6.1 or earlier release.

> Minor Change – This is a Panorama issue. Panorama is not covered in the scope of the evaluation.

89385—Fixed an issue with firewalls in an HA active/active configuration where session timeouts for some traffic were unexpectedly refreshed after a commit or HA sync attempt.

> Minor Change – This relates to High Availability (HA) configurations, which are not covered in the scope of the evaluation.

89296—Fixed an issue where a commit failed after renaming a Panorama shared object that was already referenced in the rules on a local firewall.

> Minor Change – This is an issue related to Panorama. Panorama is not covered in the scope of the evaluation.

89108—Fixed an issue where a firewall did not advertise prefixes to some BGP peers when expected.

Minor Change – This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

88689—Fixed an issue where a memory leak associated with the authentication process (authd) caused commit attempts to fail.

Minor Change – This is an availability issue. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

88450—Fixed an issue where Layer 3 interfaces without defined IP addresses, zones, or virtual routers dropped LLDP packets, which prevented the firewall from obtaining and displaying neighbor information.

Minor Change – This relates to Link Layer Discovery Protocol packet handling. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

88421—Fixed an issue where WildFire reports were generated for files already blocked by the Antivirus profile SMTP decoder.

Minor Change – WildFire-related functions and capabilities are outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

88325— Fixed an issue where a PA-500 firewall running a PAN-OS 7.0.1 or later release and with DNS Proxy enabled failed to connect to User-ID agents using FQDN.

Minor Change – As stated in Section 2.5 of [CCECG], the use of user identities in firewall rule sets is not covered by the scope of evaluation testing. Therefore, whether or not the TOE can connect to a User-ID agent is irrelevant in the evaluated configuration. As such, this issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

88313— Fixed an issue where read-only device administrators were unable to view logs on the ACC tab.

Minor Change – The Application Command Center (ACC) is an interactive, graphical summary of the applications, users, URLs, threats, and content traversing the network. The ACC uses the firewall logs to provide visibility into traffic patterns and actionable information on threats. The ACC is not described in the ST and its use is not covered in the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

87911—Fixed an issue where scheduled dynamic updates to managed firewalls stopped functioning after migrating the Panorama VM to an M-500 appliance.

Minor Change – This is an issue related to Panorama. Panorama is not covered in the scope of the evaluation.

87880—Fixed an issue where the XML API request to test Security policy was not properly targeted to a specified virtual system (vsys), which made the request applicable only to the default vsys. With this fix, the XML API request to test Security policy is able to retrieve results for any previously targeted vsys.

Minor Change – The XML API is not covered within the scope of the evaluation.

87833— Fixed an issue where WildFire updates caused the interface to flap.

Minor Change – This is a WildFire issue. WildFire is not covered in the scope of the evaluation.

87729— Fixed an issue where the dataplane on the passive firewall in a synced HA configuration restarted due to a Decryption profile that didn't have any associated Decryption policy rules, which resulted in SSL proxy sessions that were dropped on the passive firewall when the active firewall became suspended during a failover.

Minor Change – This relates to High Availability (HA) configurations, which are not covered in the scope of the evaluation.

87594—Fixed an issue on M-Series appliances that caused the show ntp CLI command to time out.

Minor Change – M-Series appliances are not included in the evaluated configuration.

87094—Fixed an issue where committing a policy on Panorama that contained interfaces that were manually defined generated the error: [interface name] is not an allowed keyword.

Minor Change – This is an issue related to Panorama. Panorama is not covered in the scope of the evaluation.

86977—Fixed an issue where LDAP sessions sourced from Panorama, a firewall, or an M-100 appliance were kept open and not actively refreshed, which caused sessions to timeout when they traversed the peer firewall (or the dataplane on the same firewall) and, ultimately, caused authentication attempts to fail when requests could no longer reach the LDAP server. With this fix, a keep-alive mechanism is added that is triggered after 15 minutes of session inactivity and that allows a maximum of five failed probes before dropping a connection (probes occur in 60-second intervals).

Minor Change – Use of LDAP external authentication servers is outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

86821—Fixed an issue where the server process (devsrvr) stopped responding when attempting to access a URL with multiple nested children, which caused the dataplane to restart.

Minor Change – This is an availability issue. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

86686— Security-related fixes were made to address issues reported in the October 2015 NTP-4.2.8p4 Security Vulnerability Announcement.

Minor Change – The October 2015 NTP-4.2.8p4 Security Vulnerability Announcement reported 13 low- and medium-severity vulnerabilities that are fixed in the ntp-4.2.8p4 release. The use of NTP by the TOE to synchronize its internal clock was not covered in the scope of evaluation. As such, this issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test

86313— Fixed an issue where the failed to handle CONFIG_COMMIT error was displayed during a commit.

Minor Change – This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

86202—Fixed an issue where the management plane stopped responding if you modified an object referenced in a large number of rules.

Minor Change – This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

86189 — Fixed an issue where the firewall did not send SNMPv3 traps that used an IPv6 server address.

Minor Change – The use of SNMPv3 is not covered within the scope of the evaluation.

86122— Fixed an issue where an LACP Aggregate Ethernet (AE) interface using SFP copper ports remained down after a dataplane restart.

Minor Change – This is an availability issue related to the behavior of physical external network connectors and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

85344—Fixed an issue where scheduled dynamic update installation caused the HA link to flap.

Minor Change – This relates to High Availability (HA) configurations, which are not covered in the scope of the evaluation.

85265—Fixed an issue in the XML API that prevented a read-only superuser from downloading custom packet captures.

Minor Change – The XML API is not covered within the scope of the evaluation.

84997—Fixed an issue on PA-7000 Series firewalls where the first auto-commit attempt failed.

Minor Change – Immediately after restarting, every Palo Alto Networks firewall performs an auto-commit. This takes place in the background and can last up to 30 minutes. The firewall can be accessed from the management interface during that time, but the data plane will be down and the physical interfaces will be down. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

84461—Fixed a Panorama issue where the virtual memory for a process (configd) exceeded its allocation, which caused commit and HA sync attempts to fail.

Minor Change – This is an issue related to Panorama. Panorama is not covered in the scope of the evaluation.

84146—Fixed an issue in PAN-OS 7.0 releases where the source and destination field was no longer included as expected in error messages that were triggered when requests to delete address objects failed. With this fix, the source and destination information is again included in the error message.

Minor Change – This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

84027—Fixed an issue where a firewall allowed some HTTP GET packets to pass through even when the URL Filtering profile was configured to block packets in this URL category.

Minor Change – The scope of the evaluation is limited to the packet filtering/stateful traffic filtering capabilities of the TOE, which were tested only for the following protocols: IPv4; IPv6; ICMPv4; ICMPv6; TCP; UDP; and FTP. In particular, security profiles such as the URL filtering profile are outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

83564—Fixed an issue where a certificate Common Name (CN) containing UTF-8 characters caused commit requests to fail because the decoded CN string exceeded the 64-character limit.

Minor Change – This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

82918—Fixed an issue where re-entering an LDAP bind password through the CLI using a hash value (instead of a regular password) was rejected for having too many characters.

Minor Change – Use of the CLI for administration of the TOE and use of external authentication servers (such as LDAP) are both outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

82470—Fixed an issue with IPsec tunnel throughput performance caused by incorrect hardware tagging.

> Minor Change – This is a performance issue. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

77460—Fixed an issue on a firewall with an expired BrightCloud license where the specified vendor was unexpectedly and automatically changed from BrightCloud to PAN-DB when any feature auth code was pushed from Panorama to the firewall.

> Minor Change – This is a license issue. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

76661—Fixed an issue where voltage alarms were triggered incorrectly (voltage was within the appropriate range).

> Minor Change – This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

74443—A security-related fix was made to address CVE-2015-0235.

> Minor Change – This is the fix made to address CVE-2015-0235, which related to a heap buffer overflow in the 'glibc' open source library. Palo Alto issued a security advisory (PAN-SA-2015-0002) stating that there was no known exploitable condition in PAN-OS software enabled by the vulnerability at the time of the advisory. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

73082—Fixed an issue where a firewall process (all_pktproc) stopped responding due to an issue with NAT pool allocation.

> Minor Change – This is an availability issue. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

Bug Fixes Addressed in the 7.0.6 Release

92671—Fixed an issue where traffic that was offloaded to hardware was not forwarded properly. This occurred on PA-3050 and PA-3060 firewalls and primarily with SSL traffic.

> Minor Change – Off-loading traffic to hardware is outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

90992—Fixed an intermittent issue where the initial GlobalProtect client connection to a GlobalProtect portal or gateway failed with the error: Valid client certificate is required. This occurred when the certificate profile used CRL/OCSP to check certificate validity and was due to a problem with the certificate not being available in the dataplane cache. Subsequent connections worked because the certificate was added to the cache during the initial connection attempt.

> Minor Change – This is an issue related to GlobalProtect. GlobalProtect is not covered in the scope of the evaluation.

90904—Fixed a packet drop issue on PA-7000 Series firewalls in HA configurations running a PAN-OS 7.0.3 through PAN-OS 7.0.5 release. This occurred due to a MAC address lookup issue on interfaces in an Aggregate Ethernet (AE) interface group that were part of a VLAN.

> Minor Change – This relates to High Availability (HA) configurations, which are not covered in the scope of the evaluation.

89881—Fixed an issue where the User-ID™ agent truncated NetBIOS names with more than 14 characters. As a result, users with domain names longer than 14 characters were not granted access.

> Minor Change – This is an issue related to User-ID Agent. The User-ID Agent is not part of the TOE.

89880—Added a new CLI operational command (set authentication radius-auth-type <auto|chap|pap>) for M-Series appliances in Panorama™ mode to address an incompatibility issue between PAN-OS and some RADIUS servers. With this fix, you can manually override the automatic selection mechanism and choose between CHAP and PAP.

> Minor Change – M-Series appliances are not part of the TOE.

89317—Fixed an issue where improper data pattern ordering occurred after an administrator deleted data patterns from an existing Data Filtering profile, which subsequently caused an error (rule is already in use) when attempting to add a new data pattern. With this fix, you can add or delete data patterns in any order.

> Minor Change – Security profiles such as the Data Filtering profile are outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

88794—Fixed an issue where one-time password (OTP) RADIUS authentication failed when the domain selection field was used in the authentication profile.

> Minor Change – Use of external authentication servers such as RADIUS is outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

88696—Fixed an issue where, under certain conditions, a process (mpreplay) frequently restarted due to excessive internal messaging.

> Minor Change – This is a performance issue. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

88570—Fixed an issue where a Neighbor Solicitation (NS) packet—used to refresh IPv6 neighbor tables—was sent out through a VLAN interface without a VLAN tag. The NS packet was tagged correctly when the neighbor entry was initially created but the packet used to refresh the table was sent without the tag, which caused the table update to fail when the neighbor did not receive an appropriately tagged response.

> Minor Change – This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

88168—Fixed an issue where VM-Series firewalls running on an 8-core platform changed the passive firewall to active when a socket error occurred. The socket remained closed until an interface-related change was made.

> Minor Change – This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

88125—Fixed an issue where TCP segments for DNS queries were dropped when the segments were smaller than 12 bytes.

> Minor Change – This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

87482—A security-related change was made to management plane account restrictions to avoid service disruption.

> Minor Change – This is an availability issue. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

87285—Fixed an issue where a User Activity Report PDF for the last 30 days generated an error when the report contained more than 100,000 lines.

> Minor Change – This issue is not security relevant, results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

87257—Fixed an issue that caused a dataplane restart when the firewall was configured as a DHCP relay and received DHCP requests from a third-party DHCP server or client that exceeded the payload length specified in RFC-2132.

> Minor Change – Configuration as a DHCP relay is outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

87158—Fixed an issue where some packets were duplicated in the egress stage. This occurred on multi-dataplane firewalls when traffic flowed from virtual system to virtual system or from virtual system to a shared gateway. An update has been made to prevent packet duplication.

> Minor Change – This issue is not security relevant, results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

86980—Fixed an intermittent issue where commits failed due to invalid file permission warnings related to SSH authentication.

> Minor Change – Use of SSH is outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

86970—Fixed an issue where decryption on the firewall did not function when using Chrome to browse certain websites because Chrome eliminated insecure fallback to TLS 1.0.

> Minor Change – SSL Decryption policy is outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

86916—Fixed an issue where traffic bursts entering a PA-3000 Series firewall caused short-term packet loss even though the overall dataplane utilization remained low. This issue was typically observed when two firewall interfaces on the same firewall were connected to each other. With this fix, internal thresholds were modified to prevent packet loss in these conditions.

> Minor Change – This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

86671—Fixed an issue where Panorama did not recognize threat IDs generated by a WF-500 appliance, which prevented you from configuring an exemption for these threats in Panorama that could be pushed to managed firewalls.

> Minor Change – This is an issue related to Panorama. Panorama is not covered in the scope of the evaluation.

86633—Fixed an issue where the web interface indicated that a new DHCP relay configured in the CLI was enabled even though the relay was not, yet, enabled from the CLI.

> Minor Change – Configuration as a DHCP relay is outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

86321—Fixed an issue where SSH decryption caused a dataplane memory leak and restart.

> Minor Change – SSH Decryption policy is outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

86251—Fixed an issue where an administrator was unable to retrieve log partition utilization using SNMP after adding additional virtual disk space on Panorama.

Minor Change – This is an issue related to Panorama. Panorama is not covered in the scope of the evaluation.

85913—Fixed an issue where an administrator was unable to add more than one X-Auth GlobalProtect gateway on the same interface.

Minor Change – This is an issue related to GlobalProtect. GlobalProtect is not covered in the scope of the evaluation.

85880—Enhanced the syslog variable list to include cef-number-of-severity.

Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

85531—Additional X-Frame protections introduced in GlobalProtect and SSL VPN pages.

Minor Change – This is an issue related to GlobalProtect and to SSL VPNs. Neither GlobalProtect nor SSL VPNs are covered in the scope of the evaluation.

85110—Fixed an issue where the firewall sent gratuitous ARP (GARP) packets for an interface IP address used in a destination NAT rule from all interfaces in the zone where that interface belonged. With this fix, the GARP packets are sent only from the interface that owns the IP address.

Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

84949—Fixed an issue where M-100 appliances in an HA active/active configuration forwarded logs only to one syslog server, even though two syslog servers were defined. This issue occurred only on the primary-secondary appliance and was due to an HA sync issue.

Minor Change – M-Series appliances are not part of the TOE.

84665—Fixed an issue where the Commit icon incorrectly indicated pending configuration changes after an Applications and Threats update.

Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

84641—Fixed an issue where some DNS requests were forwarded to the wrong DNS server—the one previously but no longer configured on the firewall.

Minor Change – Configuration as a DNS proxy is outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

84339—Fixed an issue where a single session consumed the majority of the packet buffer resources. With this fix, you can use information in the output of the show running resource-monitor ingress-backlogs command to identify sessions that use an excessive percentage of the packet buffer and then use the request session-discard CLI operational command to manually discard sessions as needed. These commands are only available on firewalls that support hardware offload.

Minor Change – This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

84236—Fixed an issue where special characters in the SNMPv3 Users field caused encryption to fail and caused the firewall to restart.

Minor Change – The use of SNMPv3 is not covered within the scope of the evaluation.

83722—Fixed an issue where destination-based service routes did not work for RADIUS authentication servers.

Minor Change – Use of external authentication servers such as RADIUS is outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

83702—Fixed an issue on PA-7000 Series firewalls running PAN-OS 7.0.2 and later releases where WildFire™ Analysis reports did not display in the WildFire Analysis Report tab (Monitor > Logs > WildFire Submissions > Detailed Log View).

Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

83361—Fixed an issue where the DoS classification counter stopped at an abnormally high value. This caused flood type false positives in the Threat logs, causing the firewall to appear as if it reached maximum session capacity.

Minor Change – This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

83135—Fixed an issue where the initial redirect failed for some SSL sites. (The error—Bad Record MAC—appeared after the user clicked continue but the user could then refresh the page to successfully enter the website.)

Minor Change – This is related to Captive Portal functionality, which is outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

83100—Fixed an issue where Panorama HA synchronization failed when attempting to upgrade to a PAN-OS 7.0.1 through PAN-OS 7.0.5-h2 release.

Minor Change – This relates to High Availability (HA) configurations, which are not covered in the scope of the evaluation.

82756—Fixed an issue where custom reports were not sent out by the Email Scheduler.

Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

82443—Fixed an issue where unwanted characters were displayed on the login page after a failed login.

Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

80721—Fixed an issue where the XML API command show dos-protection rule statistics (used to retrieve DoS protection statistics) returned an error: invalid command option.

Minor Change – The XML API is not covered within the scope of the evaluation.

80507—Fixed an issue in Panorama where Threat and Content names for certain threats did not appear in ACC reports, predefined reports, and spyware reports. This issue occurred only on PA-7000 Series firewalls managed by Panorama and only during an Antivirus update.

Minor Change – This is an issue related to Panorama. Panorama is not covered in the scope of the evaluation.

79729—Fixed an issue with firewalls in an HA configuration where a commit operation aborted for all daemons and then the DHCP daemon stopped responding. This occurred when the set deviceconfig high-availability group {group-name} configuration-synchronization enabled option was set to no.

Minor Change – This relates to High Availability (HA) configurations, which are not covered in the scope of the evaluation.

78090—Fixed an issue where the User-ID process stopped responding on both peers in an HA active/passive configuration. This issue occurred after an upgrade and was due to a problem with the LDAP library.

Minor Change – This relates to High Availability (HA) configurations, which are not covered in the scope of the evaluation.

74333—Fixed an issue where incremental updates for new and updated registered IP addresses were failing when registration events were occurring through the XML API. With this fix, integrating the updates for registered IP addresses no longer fails when using the XML API (on either standalone firewalls and appliances or those in HA configurations).

Minor Change – The XML API is not covered within the scope of the evaluation.

Bug Fixes Addressed in the 7.0.5-h2 Release
89750—A security-related fix was made to address a stack underflow condition.

Minor Change – This is the fix made to address CVE-2016-3656, which related to a stack underflow in the GlobalProtect Portal. GlobalProtect is not covered in the scope of the evaluation.

89706—A security-related fix was made to prevent some CLI commands from improperly executing code.

Minor Change – This is the fix made to address CVE-2016-3654, which related to a vulnerability in the CLI. The CLI is not covered in the scope of the evaluation.

Bug Fixes Addressed in the 7.0.5 Release
89752—A security-related fix was made to address a buffer overflow condition.

Minor Change – This is the fix made to address CVE-2016-3657, which related to a buffer overflow in the GlobalProtect Portal. GlobalProtect is not covered in the scope of the evaluation.

89717—A security-related fix was made to ensure the appropriate response to special requests received through the API interface.

Minor Change – This is the fix made to address CVE-2016-3655, which related to a vulnerability in the XML API. The XML API is not covered within the scope of the evaluation.

88550—Fixed an issue on firewalls running in Common Criteria (CC) mode where seeding using an OpenSSL deterministic random bit generator (DRBG) caused a process (cryptod) to stop responding and resulted in commit failures.

Minor Change – This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

88439—Fixed an issue on a PA-3000 Series firewall where a dataplane constantly restarted due to a hardware content matching memory issue.

Minor Change – This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

88382—Fixed an issue in a high availability (HA) active/active configuration with unexpectedly short (20 second) timeouts that occurred when an HA2 session sync message failed. This issue was due to an ARP problem between dataplanes in the HA configuration when the HA2-backup was in use and using either IP or UDP transport mode. With this fix, unexpectedly short session timeouts no longer occur due to this issue.

Minor Change – This relates to High Availability (HA) configurations, which are not covered in the scope of the evaluation.

88191—A security-related fix was made to address information leakage in systems log that impacted the web interface.

> Minor Change – This is the fix made to address PAN-SA-2016-0016, which related to a vulnerability where a read-only user with CLI access could elevate web interface privileges. Use of the CLI for administration of the TOE is outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

87565—Fixed an issue where a firewall did not forward correlation events to the syslog server.

> Minor Change – This relates to the automated correlation engine functionality of the TOE, which is not covered in the scope of the evaluation. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

87170—Fixed an issue where a firewall did not filter groups using the filters applied in search parameters; instead, the firewall ignored filters and displayed all groups in search results.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

86947—Fixed a rare issue where an active firewall in a high availability (HA) configuration incorrectly synced to the configuration from the passive firewall when a second commit was performed on the active firewall before a previous commit was completed.

> Minor Change – This relates to High Availability (HA) configurations, which are not covered in the scope of the evaluation.

86723—Fixed an issue where a dataplane restarted when client-to-server traffic exceeded 4GB and included HTTP GET or POST requests that had the source IP address in the Origin header.

> Minor Change – This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

86664—Fixed an issue with IKEv2 that caused a child security association (SA) to install incorrectly on a firewall when the tunnel was connected to third-party equipment using PFS.

> Minor Change – This is an availability issue and is not security relevant. Perfect forward security (PFS) is enabled by default, which means a new DH key is generated in Phase 2 processing. This key is independent of the keys exchanged in Phase1 and provides better data transfer security. Both VPN peers must be enabled for PFS. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

86390—Fixed an issue where a virtual system (vsys) created in a Panorama template did not display where expected when the first two characters of the vsys name was “sg” (such as “sg01”). With this fix, Panorama no longer allows you to create a vsys with a name that begins with “sg” in a Panorama template.

> Minor Change – This is an issue related to Panorama. Panorama is not covered in the scope of the evaluation.

86319—Fixed an issue where a process (routed) on the firewall stopped responding and resulted in high CPU usage when applying a BGP autonomous system (AS) path filter.

> Minor Change – This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

86312—Fixed an issue where the last update time never exceeded 1 second after making a change to the update interval of a group mapping service.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

86193—Fixed an issue in a high availability (HA) configuration where LDAP group mappings did not properly refresh after a firewall became the active peer again after going through the passive state. This was due to a variable that was not initialized properly and was then used in an error case. With this fix, LDAP variables are properly initialized to avoid this LDAP group mapping issue.

> Minor Change – This relates to High Availability (HA) configurations, which are not covered in the scope of the evaluation.

86136—Fixed an issue where the GlobalProtect gateway sent an access-request packet with malformed data inside the Framed-IP-Address field to the RADIUS server.

> Minor Change – This is an issue related to GlobalProtect. GlobalProtect is not covered in the scope of the evaluation.

86126—Fixed an issue where a user with a custom role-based administrative account couldn’t preview rules listed as Combined rules.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

86091—Fixed an issue where a commit to configure a tunnel interface that used a string instead of an integer caused a process (routed) on the firewall to stop responding.

> Minor Change – This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

86075—Fixed an issue on a PA-3060 firewall where the size of the SML VM EmlInfo software pool was less than expected. With this fix, the size of the SML VM EmlInfo software pool is increased to the expected value.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

85888—Fixed an issue where the firewall ignored the session timeout value and automatically refreshed administrators who were still logged in to the firewall even when those sessions were inactive for a period longer than the configured timeout.

> Minor Change – Palo Alto advised that this issue related specifically to Panorama running on an M-100 appliance. Panorama and the M-100 appliance are not covered in the scope of the evaluation.

85879—Fixed an issue where a firewall in a high availability (HA) configuration generated a false positive event (Running configuration not synchronized after retries) 75 seconds after each HA sync. With this fix, this error is returned only for commits that take longer than 45 minutes to complete.

> Minor Change – This relates to High Availability (HA) configurations, which are not covered in the scope of the evaluation.

85878—In response to an issue where DNS queries sometimes caused a Log Collector to run too slowly and caused delays in log processing, the debug management-server report-namelookup disable CLI command is added to disable DNS lookups for reporting purposes.

> Minor Change – Use of the CLI for administration of the TOE is outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

85863—Fixed an issue where multicast traffic sent over a virtual wire (vwire) with Multicast Firewalling disabled (Network > Virtual Wires > <vwire>) caused high CPU and packet buffer depletion.

> Minor Change – This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

85821—Fixed an issue where a dataplane stopped responding due to memory corruption.

> Minor Change – This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

85754—Fixed an issue where a VM-Series disk was corrupted and went into maintenance mode after processing mutated traffic from third-party signature detection software.

> Minor Change – This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

85687—Fixed an issue where the system log entries displayed logged in via Web from 127.0.0.1 for administrators who logged in via XML API. With this fix, the system log displays the correct IP address for administrators who logged in via XML API.

> Minor Change – The XML API is not covered within the scope of the evaluation.

85675—Fixed an intermittent issue where a process (mprelay) restarted and, after multiple restarts, caused the firewall to restart. This issue was associated with the processing of add and delete events for IPv4 ARP and IPv6 neighbor updates. With this fix, IPv4 ARP and IPv6 neighbor updates no longer cause the mprelay process or firewall to restart.

> Minor Change – This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

85611—Fixed an issue where the number of fib entries for device FIB counter was inaccurate with ECMP enabled. With this fix, the firewall maintains an accurate count of entries in the FIB table for the number of fib entries for device FIB counter.

> Minor Change – This issue relates to Equal Cost Multiple Path (ECMP) processing, which is not in the scope of the evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

85484—Fixed an intermittent issue where the GlobalProtect portal used the cookie instead of the authentication information provided by the GlobalProtect client, which caused authentication to fail. With this fix, if a client connects using a cookie, the GlobalProtect portal ignores the cookie in favor of the authentication information provided by the GlobalProtect client so that authentication is successful.

> Minor Change – This is an issue related to GlobalProtect. GlobalProtect is not covered in the scope of the evaluation.

85358—Fixed an issue where SSL decryption sessions were not cleared after executing the clear session all filter ssl-decrypt yes CLI command (or any other session clearing command that used the ssl-decrypt yes filter). With this fix, SSL decrypt sessions are cleared as expected when executing session clearing commands that include the ssl-decrypt yes filter.

> Minor Change – SSL Decryption policy is outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

85245—Fixed an issue where a virtual system (vsys) configuration remained in the firewall configuration even after the vsys was deleted. This caused commits to fail when attempting to add a new vsys using the same ID as the vsys that was not successfully deleted.

Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

85193—Fixed an issue in a high availability (HA) configuration where multiple overlapping queries resulted in a race condition that caused HA sync jobs to fail.

Minor Change – This relates to High Availability (HA) configurations, which are not covered in the scope of the evaluation.

84963—Fixed an issue in Panorama templates where administrators could mark a certificate as Forward Trust or Forward Untrust but forwarding did not take place as expected when the template was configured to apply only to one virtual system (single vsys mode). With this fix, marking a certificate as Forward Trust or Forward Untrust works as expected even when the template is in single vsys mode.

Minor Change – This is an issue related to Panorama. Panorama is not covered in the scope of the evaluation.

84908—Fixed an issue where the logged session end reason for decrypted SSL sessions always displayed as aged out regardless whether that was the actual TCP session end reason. With this fix, the session end reason now displays correctly for decrypted SSL sessions.

Minor Change – SSL Decryption policy is outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

84729—Fixed an issue on M-Series appliances and with PA-7000 Series Log Processing cards where output of the show system logdb-quota CLI command didn't match the values in Logging and Reporting Settings in the web interface (Device > Setup > Management > Logging and Reporting Settings > Log (Card) Storage) due to a discrepancy in space calculation. With this fix, the values in the web interface accurately reflect available storage space and match the output from the show system logdb-quota CLI command.

Minor Change – Use of the CLI for administration of the TOE is outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

84552—Fixed an issue where the debug user-id reset ts-agent/user-id-agent CLI command did not work as expected.

Minor Change – Use of the CLI for administration of the TOE is outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

84538—Fixed an issue where a dataplane restarted unexpectedly on a firewall with SSL decryption enabled. This occurred during the SSL handshake when the firewall received a Hello packet from the server that had a higher SSL protocol version than the Hello packet received from the client.

Minor Change – SSL Decryption policy is outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

84496—Fixed an issue on PA-7000 Series firewalls where excessive or prolonged log queries caused a memory leak on the Log Processing Card (LPC).

Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

84239—Fixed an issue where a read-only Superuser was able to perform a commit when using XML API (but not via the web interface). With this fix, read-only Superusers cannot use XML API to perform commits.

Minor Change – The XML API is not covered within the scope of the evaluation.

83764—Fixed an issue where using web interface certificate authentication caused login failures.

Minor Change –This is a usability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

83731—Fixed an issue in a virtual wire configuration where a firewall incorrectly modified the MAC address for traffic when decryption was enabled. With this fix, the firewall no longer modifies the MAC address of traffic.

Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

83454—Fixed an issue with IPv6 traffic that had an extension header and caused jitter when passing through a PA-7000 Series firewall in a high availability (HA) active/active configuration.

Minor Change – This relates to High Availability (HA) configurations, which are not covered in the scope of the evaluation.

83362—Fixed an issue where a commit failed when a subinterface that was pushed from Panorama lost its reference to its associated VLAN after the subinterface configuration on the firewall was overridden and then reverted in the template. With this fix, after an interface is reverted, subinterfaces do not lose their mapping to VLANs.

Minor Change – The use of Panorama to manage TOE appliances is explicitly excluded in the evaluated configuration, as specified in Section 2.4 of [CCECG]. As such, this issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

83337—Fixed an issue where firewalls generated multiple core dumps after a reboot when incoming packets were forwarded to the dataplane while an autocommit was still processing. With this fix, packets are not forwarded to the dataplane until an in-process autocommit is complete.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

83328—Fixed an issue where an M-100 appliance experienced a memory limit condition. With this fix, the virtual memory for the management server process is increased to avoid this issue.

> Minor Change – This applies to the Panorama M-100 appliance, which is not part of the TOE.

83145—Fixed an issue on a PA-7000 Series firewall where an interface in tap mode unexpectedly transmitted traffic that was received on that interface.

> Minor Change – Tap mode deployment is not supported in the evaluated configuration, since in this mode the firewall is unable to block traffic. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

82916—Fixed an issue where the trusted CA store on the firewall was missing the QuoVadis root CA2 and root CA3 G3 certificates. With this fix, both these QuoVadis certificates are included in the trusted CA list.

> Minor Change –This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

82873—Fixed an issue with missing fields and inconsistencies in the Syslog format for Correlated Events that were exported to a syslog server.

> Minor Change – This relates to the automated correlation engine functionality of the TOE, which is not covered in the scope of the evaluation. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

82862—Fixed an issue where the device server process (devsrvr) restarted unexpectedly when Panorama pushed a template that contained a certificate with a corrupt public key.

> Minor Change – This is an issue related to Panorama. Panorama is not covered in the scope of the evaluation.

82667—Fixed an issue where the PAN-OS integrated User-ID agent failed to connect to a monitored server when the User-ID agent was configured to use the FQDN instead of the IP address for the server.

> Minor Change – As stated in Section 2.5 of [CCECG], the use of user identities in firewall rule sets is not covered by the scope of evaluation testing. Therefore, whether or not the integrated User-ID agent is able to connect to a monitored server is irrelevant in the evaluated configuration. As such, this issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

82358—Fixed an issue where, when using LDAP authentication, a GlobalProtect client incorrectly showed a Password expired message even when the password had not expired.

> Minor Change – This is an issue related to GlobalProtect. GlobalProtect is not covered in the scope of the evaluation.

81812—Fixed an issue where a firewall did not accurately check certificate revocation status via OCSP because the OCSP request did not include the HOST header option. With this fix, the firewall uses the HOST header option as expected and successfully retrieves the revocation status of the certificate in response to OCSP requests.

> Minor Change – This issue relates to the TOE operating as an OCSP responder (which it can be configured to do where the organization in which it is deployed has its own PKI. This mode of operation is not covered in the scope of the evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

81743—Fixed an issue where URL categorization failed for some URLs due to an issue with message buffer size.

> Minor Change – This relates to the URL Filtering profile. Security profiles such as the URL Filtering profile are outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

81425—Fixed an issue where IPsec renegotiation was not initiated as expected after a PPPoE interface received a new IP address.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

81424—Fixed an issue where the From column in the output of the show admins command was Console instead of the correct IP address when connected to the CLI via telnet or SSH.

> Minor Change – Use of the CLI for administration of the TOE is outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

81062—Fixed an issue where the email action for scheduled reports timed out due to reports that took too long to generate. With this fix, the email timeout is increased and report generation is enhanced to avoid this issue.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

80415—Fixed an issue where a firewall was not presenting the Captive Portal response page to users. This occurred when the URL category was marked not-resolved, such as when cloud servers were unavailable.

> Minor Change – This is related to Captive Portal functionality, which is outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

79596—Fixed an intermittent issue on PA-5000 Series firewalls where the dataplane stopped responding. With this fix, there are additional sanity checks and logging to avoid this issue.

> Minor Change –This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

73177—Fixed an issue where redistributed Not-So-Stubby Area (NSSA) type 7 routes converted to NSSA type 5 routes were not flushed from the OSPF database quickly enough after the redistributing NSSA router went down. With this fix, the OSPF is flushed within the expected period of time so that routes that go down are not advertised as still available.

> Minor Change – This is related to Open Shortest Path First (OSPF) functionality, which is outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

Bug Fixes Addressed in the 7.0.4 Release
88869—Fixed a performance degradation issue on a VM-Series firewall with 8 cores when threat scanning was enabled when attempting to process large transaction-specific SSL traffic types. Additionally, this fix addressed an intermittent issue where the GlobalProtect MSI file failed to download after a user authenticated to the portal page.

> Minor Change –This is a performance issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

87422—Fixed an issue where multicast traffic was dropped when the source started sending group traffic because there was not, yet, a corresponding multicast route or FIB entry on the firewall. With this fix, the multicast route is updated more quickly and packets are enqueued instead of dropped while the firewall waits for the updated route information.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

87410—Fixed an issue where an API call to add, delete, or modify a URL entry failed when the URL included a single (‘) or double (“) quote character as an XML attribute. With this fix to comply with XML Xpath 1.0, API instructions are completed successfully even when acting on a URL that includes a single or double quote used as an XML attribute.

> Minor Change – The XML API is not covered within the scope of the evaluation.

87385—Fixed an issue where all the widgets on the ACC tab of a managed firewall (and when exported in a PDF file) display Report Error when you access the firewall through a context switch from Panorama (whether virtual or M-Series appliance).

> Minor Change – This is an issue related to Panorama. Panorama is not covered in the scope of the evaluation.

87280—Fixed an issue where the number of SSL free memory chunks was depleted to 0, which caused a disruption in SSL decryption-related traffic.

> Minor Change – SSL Decryption policy is outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

87231—Fixed an issue where a PA-7000 Series firewall did not load-balance egress traffic on Aggregate Ethernet (AE) interfaces as expected.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

87078—Fixed an issue where the management server stopped responding where there was a high logging rate, which caused the Log Collector to disconnect from Panorama.

> Minor Change – This is an issue related to Panorama. Panorama is not covered in the scope of the evaluation.

86938—The client certificate used by PAN-OS and Panorama to authenticate to the PAN-DB cloud service, the WildFire cloud service, and to WF-500 appliances expired on January 21, 2016. The expiration results in an outage of these services. To avoid an outage, either upgrade to content release version 550 (or a later version) or upgrade PAN-OS and Panorama instances running a PAN-OS or Panorama 7.0 release to PAN-OS (or Panorama) 7.0.4 or a later release.

> Minor Change –This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

86895—Fixed an issue on M-Series and WF-500 appliances where the Ethernet1/2 interface unexpectedly broadcasted DHCP discover packets with the internal BMC IPMI LAN MAC address as the source MAC address when the internal BMC IPMI LAN was configured to use DHCP as the source address.

> Minor Change – This applies to the Panorama M-Series and WildFire appliances, which are not part of the TOE.

86803—Fixed an intermittent issue where the idle timer for GlobalProtect IPsec tunnels either did not expire appropriately (such as when the tunnel was torn down) or expired at the configured idle time expiration even when a user was actively using the connection. With this fix, the GlobalProtect IPsec tunnel idle timer behaves as expected.

> Minor Change – This is an issue related to GlobalProtect. GlobalProtect is not covered in the scope of the evaluation.

86467—Fixed an issue in PAN-OS 7.0.3 where firewalls did not check for superuser accounts that were pushed through a Panorama template, which caused an upgrade process error when all superuser accounts were pushed through a Panorama template (firewalls must have at least one superuser account in the configuration). With this fix, firewalls correctly recognize superuser accounts that are pushed through a Panorama template.

> Minor Change – The use of Panorama to manage TOE appliances is explicitly excluded in the evaluated configuration, as specified in Section 2.4 of [CCECG]. As such, this issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

86212—Added a new CLI operational command (set authentication radius-auth-type <auto|chap|pap>) to address an incompatibility issue between PAN-OS and some RADIUS servers. With this fix, you can manually override the automatic selection mechanism introduced with Challenge-Handshake Authentication Protocol (CHAP) support in PAN-OS 7.0 to select either CHAP or Password Authentication Protocol (PAP) as needed.

> Minor Change – Use of the CLI for administration of the TOE is outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

85801—Fixed an issue where a firewall that was forwarding logs to multiple Panorama management servers and Log Collectors stopped forwarding logs to any appliance after an administrator suspended log forwarding on the active primary Panorama server. With this fix, the firewall continues to forward logs to all Panorama management servers and Log Collectors except any appliance for which an administrator specifically suspends log forwarding.

> Minor Change – The use of Panorama to manage TOE appliances is explicitly excluded in the evaluated configuration, as specified in Section 2.4 of [CCECG]. As such, this issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

85721—Fixed an issue where firewalls with a specific OCZ Deneva hard disk (model DENCSTE251M21) configured in a RAID and running PAN-OS 7.0.1 or later releases experienced RAID errors.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

85514—Fixed an issue where a commit request failed due to processes (configd and mongod) with high memory usage.

> Minor Change –This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

85364—Fixed an issue where HTTP and HTTP Online Certificate Status Protocol (OCSP) management services were enabled only for the first IP address on an interface with multiple IP addresses. With this fix, when HTTP and HTTP OCSP management services are enabled on an interface, services are enabled for all IP addresses associated with that interface.

> Minor Change – This issue relates to the TOE's HTTP service and the TOE operating as an OCSP responder (which it can be configured to do where the organization in which it is deployed has its own PKI). The HTTP service and OCSP responder mode of operation are not covered in the scope of the evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

85285—Fixed an issue where output from the show ntp command did not always display the correct NTP status. Primarily, this issue occurred when there was only one NTP server configured and, even when correctly connected to the NTP server, the output of the show ntp status command displayed as rejected. With this fix, output from the show ntp command correctly displays NTP status as synchronized after the firewall successfully connects to an NTP server.

> Minor Change – Use of the CLI for administration of the TOE is outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

85166—Fixed an issue on a PA-7000 Series firewall where the first packet in a session was dropped when it arrived before the firewall freed up a previous session that used the same 5-tuple. With this fix, the firewall treats the previous session as an inactive flow and successfully creates the new session.

> Minor Change –This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

85091—Fixed an issue on a firewall where software packet buffers were being depleted. With this fix, the firewall will dynamically adjust the TCP receive window based on peer traffic to avoid software packet buffer depletion. Additionally, there is a fix for a memory leak in error handling of SSL Forward Proxy mode and the size of the software buffer pools is increased.

> Minor Change –This is a performance and availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

84851—Fixed an issue where the virtual system (vsys) ID on the firewall was computed incorrectly when Panorama pushed a template with Force template value enabled and containing virtual system information to the firewall.

> Minor Change – The use of Panorama to manage TOE appliances is explicitly excluded in the evaluated configuration, as specified in Section 2.4 of [CCECG]. As such, this issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

84811—Fixed an issue on a VM-Series firewall (KVM on Centos7/Redhat) where a process (vm-uuid) displayed as empty after boot. With this fix, the vm-uuid process is displayed correctly.

> Minor Change – This applies to VM-Series firewalls deployed in a KVM virtual environment, which is not part of the TOE.

84678—Fixed an issue with the way the management plane performed updates through HTTP and HTTPS calls, such as for block list and content updates.

> Minor Change – This issue relates to mechanisms that support the product's content inspection features. The scope of the evaluation is limited to the packet filtering/stateful traffic filtering capabilities of the TOE. In particular, content inspection features are outside the scope of evaluation. Therefore, this issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

84595—Fixed an issue with HTTP requests generated by the firewall when retrieving custom Dynamic Block Lists.

> Minor Change – This issue relates to mechanisms that support the product's content inspection features. The scope of the evaluation is limited to the packet filtering/stateful traffic filtering capabilities of the TOE. In particular, content inspection features are outside the scope of evaluation. Therefore, this issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

84495—Fixed an issue where, in some cases, generating output for the show running url-cache all CLI command caused a short delay in communication with the dataplane. With this fix, to avoid this communication delay, the output of the show running url-cache all command is no longer included when generating the tech support file.

> Minor Change – Use of the CLI for administration of the TOE is outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

84494—Fixed an issue where the session end reason for a single threat ID was reported differently depending on which decoder was used. With this fix, only one session end reason (threat) is reported for all blocked SMTP traffic regardless which decoder is used.

> Minor Change – The scope of the evaluation is limited to the packet filtering/stateful traffic filtering capabilities of the TOE, which were tested only for the following protocols: IPv4; IPv6; ICMPv4; ICMPv6; TCP; UDP; and FTP. The evaluation did not consider processing of SMTP traffic. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

84465—Fixed an issue where the external interface on an LSVPN satellite was unable to establish an LSVPN connection to the active-primary firewall in an HA active/active configuration that was acting as the GlobalProtect portal or gateway when the external interface of the satellite was configured as a DHCP client. (This failure occurred even though an LSVPN connection was successfully established with the active-secondary firewall.) With this fix, the LSVPN satellite (with the external interface configured as a DHCP client) successfully establishes an LSVPN connection to both firewalls (active-primary and active-secondary) after a reboot.

> Minor Change – This relates to High Availability (HA) configurations, which are not covered in the scope of the evaluation.

84454—Fixed an issue where attempts to load a partial configuration for a device group from an XML file resulted in an error message. With this fix, you can successfully load a partial configuration for a device group and merge it with an existing device group.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

84433—Fixed an issue where a web page would not load successfully without refreshing the browser multiple times when Open Certificate Status Protocol (OCSP) validation was enabled. This occurred when a block page message was presented within one second of the attempt to load an HTTPS site while decryption was enabled on the firewall with the OCSP validation timeout set to 60 seconds.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

84167—Fixed an issue where a firewall incorrectly reordered certain TCP traffic during transmit stage.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

84008—Fixed an issue where an LSVPN IPsec tunnel went down when the hard key lifetime expired during a re-key. With this fix, the soft key lifetime is adjusted so that the hard key lifetime does not expire before the re-key finishes.

> Minor Change –LSVPN (Large Scale VPN) is a GlobalProtect feature. GlobalProtect is not covered in the scope of the evaluation.

83907—Fixed an issue where administrators could not disable counters in system logs using the debug dataplane packet-diag set log counter <counter-name> CLI command when those counters had names longer than 31 characters.

> Minor Change – Use of the CLI for administration of the TOE is outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

83902—Fixed an issue where monitoring an SNMP OID (.1.3.6.1.2.1.25.2.3.1.5.41) for disk space resulted in incorrect values on volumes over 2TB in size.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

83898—Fixed an issue on Panorama M-Series and virtual appliances where exporting a report as a comma-separated value (CSV) file (Monitor > Reports) failed and resulted in a web interface error (Error enqueuing export job).

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

83889—Fixed an issue where a PA-7000 Series firewall incorrectly dropped non-TCP and non-UDP fragmented traffic, such as EtherIP traffic.

> Minor Change –This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

83844—Fixed an issue where a memory leak caused a PA-200 firewall to reboot.

> Minor Change –This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

83657—Fixed an issue where Panorama did not properly push device or template configurations for NTP, send-hostname-in-syslog, or WildFire settings to a device.

> Minor Change – This is an issue related to Panorama. Panorama is not covered in the scope of the evaluation.

83592—Fixed an issue where the User-ID process (useridd) went into a reboot loop and caused the passive firewall in a high availability (HA) configuration to restart. This was due to bulk and incremental updates of terminal services users.

> Minor Change – This relates to High Availability (HA) configurations, which are not covered in the scope of the evaluation.

83253—Fixed an issue where video calls failed when H.245 (openlogicalchannelack) packets referenced a pre-NAT address.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

82913—Fixed an issue where ToS headers were not set correctly in Encapsulating Security Payload (ESP) packets across VPN tunnels.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

82865—Fixed an issue with a PA-5000 Series firewall where sessions owned by dataplane 1 (DP1) or DP2 did not display in the output when executing the show session command on DP0.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

82710—Fixed an issue where unexpected dataplane restarts occurred due to out of memory errors and high resource usage on packet descriptors when SSL Forward Proxy was enabled. This fix also addresses a dataplane process memory leak.

> Minor Change –This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

82621—Fixed an intermittent issue on a PA-7000 Series firewall where traffic was dropped when the log interface and dataplane interfaces were both configured on the same Network Processing Card (NPC).

> Minor Change –This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

82605—Fixed an issue where policy-based forwarding (PBF) with Enforce Symmetric Return enabled (Policies > Policy Based Forwarding > pbf-rule > Forwarding) caused offloaded PBF sessions to fail when attempting to egress the firewall.

> Minor Change –This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

82424—Fixed an issue on a PA-5000 Series firewall where packets were dropped or the dataplane stopped responding when receiving specific ingress or egress traffic associated with offloaded sessions. With this fix, a field-programmable gate array (FPGA) change was made to address these issues.

> Minor Change –This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

82138—Fixed an issue where WildFire reports were not displayed on the web interface when proxy settings were configured for the management interface.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

82118—Fixed an issue on the QoS Statistics panel (Network > QoS) where data was displayed only on the bandwidth tab; all other tabs (Applications, Source Users, Destination Users, Security Rules, and QoS Rules) were empty.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

82095—Fixed an issue where a commit request did not finish processing due to a process (routed) that stopped responding.

> Minor Change –This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

81996—Fixed an issue where a HIP Profile did not sync between the active and passive firewalls in a high availability (HA) configuration, which caused the HIP Profile to no longer be in effect after a failover. With this fix, the HIP Profile is correctly synced between the active and passive firewalls and remains in effect after a failover.

> Minor Change – This relates to High Availability (HA) configurations, which are not covered in the scope of the evaluation.

81949—Fixed an issue where Dynamic Address Groups pushed from Panorama to a firewall were not displayed in the output of CLI show commands.

> Minor Change – The use of the CLI for administration of the TOE is outside the scope of evaluation. In addition, use of Panorama to manage TOE appliances is explicitly excluded in the evaluated configuration, as specified in Section 2.4 of [CCECG]. As such, this issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

81830—Fixed an issue where SSL Forward Proxy did not include the appropriate TLS 1.2 extension (Signature Algorithms) in Client Hello messages, which prevented successful interoperability with some Microsoft websites.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

81333—Fixed an issue where managed firewalls and appliances were unable to connect to Panorama using the master key after a factory reset (or RMA).

> Minor Change – The use of Panorama to manage TOE appliances is explicitly excluded in the evaluated configuration, as specified in Section 2.4 of [CCECG]. As such, this issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

81241—Fixed a rare issue where NAT traffic was dropped after a failed commit attempt.

> Minor Change –This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

80631—Fixed an issue in a high availability (HA) configuration where the ports on the passive firewall did not come up when the passive link state was set to auto (Device > High Availability > General > Active Passive Settings).

> Minor Change – This relates to High Availability (HA) configurations, which are not covered in the scope of the evaluation.

79917—Fixed an issue on a PA-3000 Series firewall where the dataplane stopped responding when receiving specific ingress or egress traffic associated with offloaded sessions. With this fix, a field-programmable gate array (FPGA) change was made to address this issue.

> Minor Change –This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

79531—Fixed an issue where an error was displayed (No Data to Display) in the Threat Monitor window (Monitor > App Scope > Threat Monitor) when selecting the Show Files filter.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

78624—Fixed an issue where the active-secondary firewall in an HA active/active configuration was incorrectly responding to ARP requests for the IP address used in the destination NAT rule with binding to the active-primary firewall.

> Minor Change – This relates to High Availability (HA) configurations, which are not covered in the scope of the evaluation.

78482—Fixed an issue where VM Information Sources bypassed proxy settings.

> Minor Change – This relates to VM Information Sources, which support monitoring of the underlying virtual environment (e.g., ESXi) on which the VM-Series firewall is deployed. This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

78317—Fixed an issue where the management plane in an HA active/passive configuration restarted due to a dataplane process (mprelay) that stopped responding when it experienced memory corruption and encountered unexpected behavior from the FIB pointer.

> Minor Change – This relates to High Availability (HA) configurations, which are not covered in the scope of the evaluation.

77236—Fixed an issue where importing a certificate more than once with different names caused the dataplane to stop responding when the certificate was used for SSL Inbound inspection.

> Minor Change –This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

76269—Fixed an issue where an active-primary M-100 appliance in an HA configuration was unable to establish a connection with the passive-secondary or active-secondary HA peer for log collection.

> Minor Change – This relates to High Availability (HA) configurations, which are not covered in the scope of the evaluation.

76197—Fixed an issue where firewall Traffic logs displayed unusually large byte counts for http-proxy and httpy-video counters due to frequent application shifts between those application-type packets within a single proxy session.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

76103—Fixed an issue where adding a threat exception to a Vulnerability Protection profile (Objects > Security Profiles > Vulnerability Protection > profile > Exceptions) resulted in an error (Schema node for Xpath was not found).

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

73187—Fixed an issue where the WildFire Analysis report (Monitor > WildFire Submissions > Detailed Log View > WildFire Analysis Report) did not display on versions 9 or 10 of Internet Explorer due to a script error.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

70719—In response to an issue where a dataplane restarted due to an incorrect flow ID, PAN-OS 6.1.4 and later releases included additional checks to help prevent the dataplane from restarting due to this issue. In PAN-OS 7.0.3, those PAN-OS 6.1.4 modifications were further modified to provide a more complete solution that avoids inadvertently dropping IPv4 traffic affected by this issue; in PAN-OS 7.0.4, the solution includes an additional fix to avoid inadvertently dropping IPv6 traffic related to this issue.

> Minor Change –These are availability issues and are not security relevant. They result in no changes to the ST or guidance documentation and have no effect on the result of any Assurance Activity test.

66285—Fixed an issue where the web interface certificate did not properly sync between HA peers, which led to a race condition that caused a commit request to fail.

> Minor Change – This relates to High Availability (HA) configurations, which are not covered in the scope of the evaluation.

Bug Fixes Addressed in the 7.0.3 Release

85065—Fixed a CLI input parsing issue that caused a process on the management plane to stop responding when processing unexpected input.

> Minor Change – The use of the CLI for administration of the TOE is outside the scope of evaluation. This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

84711—Fixed an intermittent issue where some packets incorrectly matched Security policy rules, which resulted in App-ID™ policy lookup errors and discarding of packets.

> Minor Change –This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

84599—Fixed an issue in PAN-OS 7.0 releases where a process (dhcpd) did not correctly handle DHCP padding Option 0 when receiving DHCP request from the DHCP client. This prevented the firewall that was acting as the DHCP server from allocating and committing the offered IP address to the DHCP client, which caused the firewall to be stuck in offered state. With this fix, the DHCP process correctly handles DHCP padding Option 0 and successfully commits IP addresses offered to DHCP clients.

> Minor Change – Configuration as a DHCP server is outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

84246—Fixed an issue where a PA-7050 firewall running PAN-OS 7.0 assigned the same MAC address to all interfaces on two different PA-7050 chassis when the chassis base MAC addresses differed only in the 10th bit. With this fix in PAN-OS 7.0.3, two such different PA-7050 chassis are assigned different interface MAC addresses as expected.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

84094—Fixed an issue where a user activity report (Monitor > PDF Reports > User Activity Report) contained no statistics for users with a domain+username string-length that exceeded 32 characters.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

84046—Fixed an issue where SSL decryption failed when a certificate was rejected due to a missing or empty basicConstraints extension. With this fix, an exception is added to allow a missing or empty basicConstraints extension for self-signed non-CA certificates.

> Minor Change – SSL Decryption policy is outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

84012—Fixed an issue where a process (ikemgr) stopped responding due to a missing IKE profile.

> Minor Change –This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

83907—Fixed an issue where the debug dataplane packet-diag set log counter <counter-name> CLI command did not accept counter names longer than 31 characters, which prevented administrators from adding such counters for logging in system logs.

> Minor Change – The use of the CLI for administration of the TOE is outside the scope of evaluation. This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

83867—Fixed a rare issue where one of the internal databases was corrupted after an improper shutdown (power off) of the firewall. When this happened, the firewall was unable to automatically restart and would not startup properly thereafter.

> Minor Change –This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

83819—Fixed an issue on an M-100 appliance running Panorama™ 7.0 where a custom report failed to run when setting the Database (Monitor > Manage Custom Reports) to Summary Databases > Remote Device Data > Threat and selecting Severity from the list of Available Columns when any remote firewall used for custom reporting was running a PAN-OS 6.1 or earlier release.

> Minor Change – This is a Panorama issue. Panorama is not covered in the scope of the evaluation.

83637—Fixed an issue where packet processing on a VM-Series firewall caused the firewall to stop forwarding traffic.

> Minor Change –This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

83574—Fixed a rare issue where, in some scenarios—such as when a firewall is restarted and IPsec security associations (SAs) are not established when a remote VPN peer is unreachable—the tunnel interface configured with IPsec tunnel monitoring is present in the routing table and status is Up.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

83519—A security-related fix was made to address CVE-2015-5600.

> Minor Change – CVE-2015-5600 relates to a vulnerability in OpenSSH (sshd). Use of SSH is outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

83293—Fixed an issue in Panorama where SNMPv3 settings were removed and could not be updated when modifying an existing SNMPv3 device template.

> Minor Change – This is a Panorama issue. Panorama is not covered in the scope of the evaluation.

83288—Fixed an issue where autocommit failed when the GlobalProtect gateway or Captive Portal certificate was pushed through Panorama after upgrading a firewall from a PAN-OS 6.1 release to PAN-OS 7.0.2.

> Minor Change – The use of Panorama to manage TOE appliances is explicitly excluded in the evaluated configuration, as specified in Section 2.4 of [CCECG]. As such, this issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

83256—Fixed an issue where the firewall did not block unsupported elliptic curve Diffie-Hellman (ECDH) exchange cipher suites during SSL forward proxy even when Block sessions with unsupported cipher suites was enabled (Objects > Decryption Profile > <decrypt-profile> > SSL Decryption > SSL Forward Proxy).

> Minor Change – SSL Decryption policy is outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

83149—Fixed an issue where a missing node (user) in the unlock command prevented administrators from using the Panorama web interface to unlock a locked LDAP user.

Minor Change – The use of Panorama to manage TOE appliances is explicitly excluded in the evaluated configuration, as specified in Section 2.4 of [CCECG]. As such, this issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

83142—Fixed an issue where triggering a DHCP release did not clear the original settings for a DHCP client that was in renew state.

Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

83113—Fixed an issue where attempts to regenerate metadata caused a process (update_vld_itvl_idx) to stop responding when encountering a corrupt log file (a log file that contained invalid data). With this fix, the metadata regeneration process skips log files that contain invalid data so that regeneration task is successfully completed.

Minor Change –This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

83102—Added functionality to allow commits to succeed even when there is no Network Processing Card (NPC) installed, yet, or when the NPC is not supported or recognized in the current PAN-OS release. With this fix, you can install PA-7000 Series cards that are not supported in the PAN-OS version shipped with or running on the firewall and then upgrade to the appropriate PAN-OS version.

Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

83041—Fixed an issue where adjustments to the width of columns in the web interface are not saved, causing columns to revert to previous settings when you view a different tab. With this fix, changes to the width of columns in the web interface are retained until changed again.

Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

83004—Fixed an issue where a Zone Protection profile with strict IP checking enabled resulted in incorrectly dropped packets. These drops were caused by an improper check of whether the source IP address was a broadcast address.

Minor Change –This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

83001—Fixed an issue on an M-100 appliance where available disk size was reported as 0 bytes during an upgrade. This incorrectly caused old logs to be purged from the other Log Collectors in the group in an attempt to adhere to the configured log quota for the group. Additionally, Panorama 6.1.8 and Panorama 7.0.3 (and later releases) on an M-100 appliance with zero disk space displays an error when attempting to commit to Collector Group (Failed to commit collector config) or a warning when attempting to commit to Panorama (Disk <disk-ID> on log collector <log-collector-id> in group <group-ID> has a size of zero bytes).

Minor Change – This applies to the Panorama M-100 appliance, which is not part of the TOE.

82887—Fixed an issue where authentication attempts against a local authentication profile within an authentication sequence failed when the local profile was not the first profile in the sequence.

Minor Change –This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

82853—Fixed an issue where role-based administrators were not allowed to perform API calls.

Minor Change – The XML API is not covered within the scope of the evaluation.

82849—Fixed an issue on a Panorama virtual appliance using a Network File System (NFS) storage partition where the file system integrity check incorrectly failed for the NFS directory, which caused the NFS mount to fail when rebooting Panorama after an upgrade to Panorama 7.0.

Minor Change – This is a Panorama issue. Panorama is not covered in the scope of the evaluation.

82838—Fixed an issue where the User-ID process (useridd) stopped responding when reading config messages from the Terminal Services (TS) agent.

Minor Change –This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

82778—Fixed an issue where failed authentication attempts were not cleared when the authentication attempt was eventually successful. With this fix, the failed authentication attempt counter for a given user is reset as expected after every successful login.

Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

82560—Fixed an issue where a passive VM-Series firewall in an HA pair with Use Hypervisor Assigned MAC Address enabled (Device > Management > Setup) was sending GARP requests without an established HA2 connection. With this fix, a passive VM-Series firewall no longer sends these GARP requests when you enable Use Hypervisor Assigned MAC Address without an HA2 connection.

Minor Change – This relates to High Availability (HA) configurations, which are not covered in the scope of the evaluation.

82534—Fixed an issue where a firewall incorrectly injected SSL messages into traffic on port 443.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

82533—Fixed an issue where the OSCP responder failed to check the validity of client certificates and showed status as unknown when unable to locate the custom root CA used in the certificate profile for the GlobalProtect portal configuration.

> Minor Change – This is an issue related to GlobalProtect. GlobalProtect is not covered in the scope of the evaluation.

82377—Fixed an issue where, in a Large Scale VPN (LSVPN) configuration, a GlobalProtect gateway incorrectly installed the previously allocated IP address for the GlobalProtect satellite as the next hop for the routes advertised by satellites. With this fix, the GlobalProtect gateway removes any old IP addresses allocated to the satellite and correctly installs the new IP address allocated to the satellite as the next hop for the routes advertised by satellites.

> Minor Change – This is an issue related to GlobalProtect. GlobalProtect is not covered in the scope of the evaluation.

82338—Fixed an issue where one-time password (OTP) RADIUS authentication failed when configured in the same authentication sequence as the domain selection. This issue was caused by the firewall incorrectly truncating the RADIUS challenge state. Also fixed OTP RADIUS authentication issues where the backslash (“\”) character was incorrectly removed from the username entry and where an incorrect password resulted in long delays before returning a password error message.

> Minor Change – Use of external authentication servers such as RADIUS is outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

82326—Fixed an issue where additional locked users are not displayed when you click More in the web interface (Devices > Authentication-Sequence > Locked Users).

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

82136—Fixed an issue where packets that matched a policy-based forwarding (PBF) rule with Action set to No PBF (Policies > Policy Based Forwarding > pbf-rule > Forwarding) were dropped when offloading was enabled. With this fix, offloaded sessions are passed as expected even when the traffic matches a PBF rule with Forwarding set to No PBF.

> Minor Change –This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

82109—Fixed an issue on a PA-7000 Series firewall where passive FTPS with inbound decryption failed after entering passive mode. This occurred when predict sessions did not merge as expected due to the predict queue. With this fix, proxy ingress executes before the predict queue so that all data sessions merge as expected and FTP transfer is successful over TLS.

> Minor Change –This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

82099—Fixed an issue where the remote host (From) IP address for the Panorama session displayed in reverse order—displayed the administrator IP address—in the Logged in Admins widget on the Dashboard.

> Minor Change – The use of Panorama to manage TOE appliances is explicitly excluded in the evaluated configuration, as specified in Section 2.4 of [CCECG]. As such, this issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

81944—Fixed an issue where patch management for a GlobalProtect host information profile (HIP) check failed to identify missing patches when the Check setting for patch management in HIP Objects criteria was set to has-all, has-any, or has-none (Objects > GlobalProtect > HIP Objects > Patch Management > Criteria).

> Minor Change – This is an issue related to GlobalProtect. GlobalProtect is not covered in the scope of the evaluation.

81927—Fixed an issue where a firewall stopped submitting files to a WildFire cloud (public or private) when a CPU process (varrcvr) stopped responding. This issue occurred when receiving an email with a subject line containing more than 252 characters.

> Minor Change –This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

81868—Fixed an issue with a packet buffer (FPTCP) leak and resolved a few dataplane-to-management plane connection issues, as well.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

81584—Fixed an issue in Panorama 7.0 where output from the show ntp command did not always display the correct NTP status. Primarily, this issue occurred when there was only one NTP server configured and, even when correctly connected to the NTP server, the show ntp status displayed as rejected. With this fix, output from the show ntp command correctly displays NTP status as synchronized.

> Minor Change – This is a Panorama issue. Panorama is not covered in the scope of the evaluation.

81581—Fixed an issue where a process (useridd) was unable to accommodate a large number of HIP reports during HA synchronization, which caused abnormally high CPU and memory utilization on the firewall.

> Minor Change – This relates to High Availability (HA) configurations, which are not covered in the scope of the evaluation.

81522—Fixed an issue where a firewall allowed commits to succeed even when there were no superuser administrator accounts included in the configuration. This would cause the firewall to be inaccessible (except when the firewall was managed by Panorama, which could still provide access to the firewall through Panorama context switching). With this fix, a commit succeeds only if there is at least one local superuser account in the configuration; if none exist, the commit fails.

> Minor Change –This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

81415—Fixed an issue on PA-7000 Series, PA-5000 Series, PA-3000 Series, and PA-500 firewalls where an Aggregate Ethernet (AE) interface was unable to transmit an ARP request on a tagged subinterface to the neighboring device.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

81408—Fixed an issue where shared address objects that are not used in security policy rules were pushed to firewalls even when Panorama Settings (Panorama > Setup > Management) was configured to not Share Unused Address and Service Objects with Devices.

> Minor Change – The use of Panorama to manage TOE appliances is explicitly excluded in the evaluated configuration, as specified in Section 2.4 of [CCECG]. As such, this issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

81383—Fixed an issue where the show routing route CLI command output was missing a comma (","). With this fix, the output displays correctly.

> Minor Change – The use of the CLI for administration of the TOE is outside the scope of evaluation. This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

81370—Fixed an issue where the firewall was unable to allocate a large memory block, which caused sessions to fail. This fix ensures adequate resources are available for a large memory block when needed.

> Minor Change –This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

81367—A security-related fix was made to address CVE-2015-4024.

> Minor Change – CVE-2015-4024 relates to a vulnerability in PHP, which PAN-OS uses to support the administrator GUI. The vulnerability, if exploited, results in a denial-of-service (CPU consumption). This issue is not security relevant in the context of the evaluated configuration and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

81301—Fixed an issue on a firewall with decryption enabled where insufficient buffer space resulted in discarded SSL sessions.

> Minor Change – SSL Decryption policy is outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

81170—Fixed an issue where the SNMP manager returned a warning (subtype-illegal) related to panVsysEntry OBJECT-TYPE (panVsysName) when adding the PAN-COMMON-MIB.my MIB file. With this fix, adding the current version of MIB files to the SNMP manager does not trigger a subtype-illegal warning.

> Minor Change – The use of SNMP is outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

81079—Fixed an issue where, in a Dynamic Updates schedule pop-up (Device > Dynamic Updates > <Schedule>), hovering over the override icons displayed incorrect values for the Recurrence setting for antivirus and content updates when the Recurrence setting on the firewall was overridden by a template push. With this fix, hovering over the Recurrence value override icon for a Dynamic Update schedule displays the correct information even when the Recurrence setting was pushed to the firewall through a template push.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

81058—Fixed an issue on PA-7000 Series firewalls where NAT Dynamic IP fallback did not correctly translate resources, which resulted in dropped packets.

> Minor Change –This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

80932—Fixed an issue where passwords for non-administrators entered in the GlobalProtect login window were truncated to 40 characters when using RADIUS authentication.

> Minor Change – The use of GlobalProtect and RADIUS authentication are outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

80831—Fixed an issue where SSL decryption failed for some sites when the size of the certificate was larger than 1.5KB.

> Minor Change – SSL Decryption policy is outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

80766—Fixed an issue where dataplane 0 (DP0) on the passive firewall in a high availability (HA) configuration restarted after a session was established on the active firewall interface when that same interface did not also exist on the passive firewall.

> Minor Change – This relates to High Availability (HA) configurations, which are not covered in the scope of the evaluation.

80753—Fixed an issue on a PA-3060 firewall where a network outage occurred when the number of active sessions reached 100,000. With this fix, the maximum number of detector threats (dthreats) is increased to avoid this issue.

> Minor Change –This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

80702—Fixed an issue in a high availability (HA) configuration where the ARP table synced with the primary peer but was refreshed only on dataplane 0 (DP0) of the passive peer, which caused ARP entries to expire prematurely on the passive firewall when their TTL reached 0.

> Minor Change – This relates to High Availability (HA) configurations, which are not covered in the scope of the evaluation.

80648—Fixed an issue where a device group commit failed when using the destination interface in a NAT rule configured on Panorama.

> Minor Change – The use of Panorama to manage TOE appliances is explicitly excluded in the evaluated configuration, as specified in Section 2.4 of [CCECG]. As such, this issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

80533—Fixed an issue where administrators could view addresses and usernames in the Application Command Center (ACC) view even when the Show Full IP Addresses or Show User Names In Logs And Reports option was disabled for the Admin Role profile associated with those administrators (Device > Admin Roles > <Admin Role Profile> > Web UI > Privacy settings).

> Minor Change – Fine-grained admin role restrictions are not covered in the scope of the evaluation. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

80463—Fixed an issue where a local commit on Panorama failed (invalid reference) on a template or template stack when a Log Forwarding profile was configured to send logs to syslog (Objects > Log Forwarding).

> Minor Change – The use of Panorama to manage TOE appliances is explicitly excluded in the evaluated configuration, as specified in Section 2.4 of [CCECG]. As such, this issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

80397—Fixed an issue where you could create a new Monitor profile when creating a policy-based forwarding (PBF) rule on Panorama even when the target template was unknown (the PBF rule is part of a device group and the Monitor profile is part of a template configuration). With this fix, you can no longer create a new Monitor profile when creating a PBF rule on Panorama.

> Minor Change – The use of Panorama to manage TOE appliances is explicitly excluded in the evaluated configuration, as specified in Section 2.4 of [CCECG]. As such, this issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

80389—Fixed an issue on a PA-5060 firewall where internal packet path monitoring failed when under a heavy load. With this fix, internal packet path monitoring is forwarded using a priority setting that prevents these failures even when experiencing high traffic conditions.

> Minor Change –This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

80086—Fixed an issue were a firewall displayed an incorrect location for the source or destination on the Traffic Map.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

79841—Fixed an issue where, in certain circumstances, there were discrepancies between a scheduled report and that same report generated using the run now option (Monitor > Manage Custom Reports > <Custom Report>).

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

79746—Fixed an issue on a PA-2000 Series firewall where an Aggregate Ethernet (AE) interface was unable to transmit an ARP request on a tagged subinterface to the neighboring device.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

79328—Fixed an issue where Applications and Security rules in QoS statistics view (Network > QoS > <interface>) were not displayed when the ingress interface was configured to use L2 VLAN.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

78848—Fixed a rare issue where a commit (such as an antivirus update or FQDN refresh) caused the firewall to stop processing traffic. This issue occurred after a high availability (HA) synchronization event when the autocommit triggered by the synchronization event was ignored. With this fix, a force commit request is automatically and repeatedly generated until successful.

> Minor Change – This relates to High Availability (HA) configurations, which are not covered in the scope of the evaluation.

78773—Fixed an issue where the debug dataplane flow-control enable port and debug dataplane flow-control disable port CLI commands failed to modify flow control settings as expected.

> Minor Change – The use of the CLI for administration of the TOE is outside the scope of evaluation. This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

78426—Fixed an issue where a CPU process (pan_dhcpd) spiked when DHCP NAK packets were received on the DHCP relay interface.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

78210—Fixed an issue in a high availability (HA) active/passive configuration where the multicast tree failed to converge non-offloaded multicast traffic as quickly as expected after a failover. With this fix, the multicast tree convergence time is reduced for non-offloaded multicast traffic after an HA active/passive failover.

> Minor Change – This relates to High Availability (HA) configurations, which are not covered in the scope of the evaluation.

78040—Fixed an issue where the output of the show zone-protection zone CLI command did not correctly display zone protection information for a defined virtual system (VSYS).

> Minor Change – The use of the CLI for administration of the TOE is outside the scope of evaluation. This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

77376—Fixed an issue where a gateway Config refresh on a satellite device (Network > IPSec Tunnels > Gateway Info (for a gateway) > select <gateway> > Refresh GW Config) caused a delay in tunnel installation and resulted in connectivity issues for the duration of the delay.

> Minor Change –This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

77299—Fixed an issue where WildFire analysis reports did not display Coverage Status for the sample when using a Firefox browser even when a signature was generated to identify the sample (Monitor > Logs > WildFire Submissions > Detailed Log View > WildFire Analysis Report). With this fix, you can view the correct Coverage Status for a sample when using a Firefox browser.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

76981—Fixed an issue where a certificate containing a space character (“ ”) in the Common Name field of the certificate failed to establish a secure syslog connection with the syslog server. With this fix, certificates establish syslog connections as expected even when containing space characters in the Common Name.

> Minor Change –This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

76811—Fixed an issue where packet loss could occur with asymmetric traffic when two PA-4060 firewalls were set up as peers in a high availability (HA) active/active configuration. This issue occurred with VLAN-tagged traffic when jumbo frames processing was disabled and large non-jumbo frames passed over the HA3 link and became jumbo frames.

> Minor Change – This relates to High Availability (HA) configurations, which are not covered in the scope of the evaluation.

76481—Fixed an intermittent issue where a Category for a session in the URL Filtering log did not match the actual categorization of that session. With this fix, the logic for removing expired or unresolved URL cache entries is improved so that a Category in the URL Filtering log stays in sync with the actual categorization of a session.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

72115—When the web interface was set to display in any language other than English, service routes to specify how the firewall communicates with other servers or devices could not be configured (Device > Setup > Services > Service Route Configuration). This issue has been fixed so that service routes can be configured and work correctly when the web interface is set to any language preference.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

70719—In response to an issue where a dataplane restarted due to an incorrect flow ID, PAN-OS 6.1.4 and later releases included additional checks to help prevent the dataplane from restarting due to this issue. With this fix in PAN-OS 7.0.3, those PAN-OS 6.1.4 modifications are further modified to provide a more complete solution that avoids inadvertently dropping IPv4 traffic affected by this issue.

Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

67254—Fixed an issue where an XML API call for system RAID failed with an attribute error for raid_handler object.

Minor Change – The XML API is not covered within the scope of the evaluation.

66607—Fixed an issue on a PA-200 firewall where administrators could configure a firewall directly or use Panorama to push external block lists (EBLs) with a total number of EBL lists or IP addresses that exceeded limitations and did not receive an error message. (Low-end platforms support a maximum of 10 lists and 50,000 IP addresses; high-end platforms support a maximum of 30 lists and 150,000 IP addresses; there is no per-list maximum for any platform.) With this fix, an error message is displayed as expected when configuring a PA-200 firewall directly or through a push from Panorama (or PAN-OS release downgrade) where the number of EBL lists or IP addresses exceeds the limitations of that firewall or of the current PAN-OS release.

Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

34340—Fixed an issue where a large number of informational logs for the key manager process (keymgr) were included in reports when log setting for keymgr logs was set to normal. With this fix, informational logs for keymgr are included only when you configure logging for keymgr messages to the debug setting using the debug keymgr on debug CLI command.

Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

Bug Fixes Addressed in the 7.0.2 Release

82724—Fixed an issue where old registered IP addresses in a Dynamic Address Group on a high availability (HA) active/passive pair were deleted from the passive firewall when that firewall switched from non-functional to passive state and received an incremental update of registered IP addresses from the active firewall. This fix also addressed a related issue in an HA active/active configuration where the active-secondary firewall retained old IP addresses in the Dynamic Address Group after switching to a functional state when the active-secondary firewall switched to non-functional state and all IP addresses in the Dynamic Address Group became unregistered on the active-primary firewall.

Minor Change – This relates to High Availability (HA) configurations, which are not covered in the scope of the evaluation.

82717—Fixed an issue where a dataplane stopped responding after a reboot due to an initialization issue on SFP+ ports.

Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

82675—Fixed an issue on an M-100 appliance where, after an upgrade to PAN-OS 7.0.1, an authentication process (authd) stopped responding when the LDAP binding password contained special characters.

Minor Change – This applies to the Panorama M-100 appliance, which is not part of the TOE.

82370—Fixed an intermittent issue where a dataplane process (mprelay) experienced a memory leak that caused the virtual memory to increase until it triggered a dataplane restart.

Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

82310—In response to a fragmentation issue, virus patterns are split into smaller chunks to reduce the possibility of memory allocation failure.

Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

82087—Fixed an issue where a firewall displayed an alert for low disk space. With this fix, the /opt/content directory was removed to improve the disk cleanup process.

Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

82009—Fixed an issue where a document file triggered an attempt to ping an IP address.

Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

81981—Fixed an issue where the LLDP System Name field displayed the firewall model number and could not be modified to differentiate from other similar firewalls. With this fix, the firewall populates the LLDP System Name field using the configurable hostname value.

Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

81970—Fixed an issue where some Active Directory (AD) servers were incorrectly displaying a Password expires in x days message even after selecting Password never expires on the AD server. With this fix, the AD server ignores the maximum password age (maxPwdAge) value when the Password never expires option is selected.

Minor Change – The use of external authentication servers, such as Active Directory, is outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

81955—Fixed an issue on a firewall where files were not sent to WildFire as expected when the first 8 bytes of the file were split across different packets or decrypted buffers.

Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

81941—Fixed an issue where a dataplane restarted when encountering resumed SSL sessions using inbound SSL decryption.

Minor Change – SSL Decryption policy is outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

81819—Fixed an issue where the System log reported that a firewall in a high availability (HA) active/active configuration Received conflicting ARP for the floating IP address of its HA peer. With this fix, duplicate IP address detection continues to log conflicts for non-floating IP addresses, as well as duplicate addresses detected for a floating IP address received from any other device that is not a member of the HA pair.

Minor Change – This relates to High Availability (HA) configurations, which are not covered in the scope of the evaluation.

81816—Removed support for SSLv3 on Panorama for connections to managed devices.

Minor Change – This is a Panorama issue. Panorama is not covered in the scope of the evaluation.

81797—Fixed an issue where ASCII and special characters were not supported in the user activity report username field.

Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

81783—Fixed an issue where a firewall picked the wrong decryption cipher when configured with multiple IPsec Crypto profiles for IKEv2 negotiation.

Minor Change – This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

81676—Fixed an issue where a firewall allowed administrators to configure subinterface with using invalid notation (such as ethernet1/1.1.1).

Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

81577—Fixed an issue where custom URL categories associated with a Decryption policy did not match traffic destined for a proxy server.

Minor Change – The use of Decryption policies (SSL or SSH) is outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

81572—Fixed an issue on a PA-7000 Series firewall that displayed incorrect timestamps in Traffic, Threat, and URL Filtering logs.

Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

81535—Fixed an issue where the group list was empty after pushing the group mapping configuration from Panorama to a multi-vsys firewall during an attempt to configure users in a Security policy rule even though the group mapping state was synchronized.

Minor Change – The use of Panorama to manage TOE appliances is explicitly excluded in the evaluated configuration, as specified in Section 2.4 of [CCECG]. As such, this issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

81510—Fixed an issue where Device Group and Template administrators were able to create and modify Shared objects. With this fix, Device Group and Template administrators are allowed to create and modify only objects specific to the device groups and templates to which they have access—not Shared objects.

Minor Change – Fine-grained admin role restrictions are not covered in the scope of the evaluation. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

81500—Fixed an issue where a VM-Series firewall in a VMware NSX configuration running on an ESXi server restarted when a process (all_task) stopped responding.

Minor Change – This relates to VM-Series NSX edition firewalls, which are not covered in the scope of the evaluation.

81485—Fixed an issue on PA-200 and VM-Series firewalls where local objects were not resolved in the Traffic log after selecting the Resolve hostname option (bottom of the Monitor > Logs > Traffic tab).

Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

81452—Fixed an issue where switching context from the Panorama web interface to a managed firewall did not indicate whether the administrator was logged in over an encrypted SSL connection; the System log message was always User admin logged in via Panorama from x.x.x.x using http regardless whether the connection was encrypted. With this fix, the System log now specifically reports User admin logged in via Panorama from x.x.x.x using http over an SSL connection when the administrator is connected through an encrypted SSL connection to differentiate from non-encrypted connections.

> Minor Change – The use of Panorama to manage TOE appliances is explicitly excluded in the evaluated configuration, as specified in Section 2.4 of [CCECG]. As such, this issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

81389—Fixed an issue where the output of the show admins all command displayed all administrator accounts on the firewall, including root accounts. With this fix, show admins all command output displays only local and non-local administrator accounts.

> Minor Change – The use of the CLI for administration of the TOE is outside the scope of evaluation. This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

81373—Fixed an issue where WildFire Analysis reports for samples analyzed in a WildFire cloud (public or private) were not displayed in the WildFire Submissions log (Monitor > WildFire Submissions) when the firewall was configured to communicate with the WildFire cloud through a proxy server.

> Minor Change – WildFire-related functions and capabilities are outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

81312—Fixed an issue where firewall Device administrators were unable to run and view output on a firewall for the show panorama-status CLI command. With this fix, Device administrator, Device administrator (read-only), Superuser, and Superuser (read-only) users (Device > Administrators > <administrator>) can run and view output for the show panorama-status command from the firewall.

> Minor Change – The use of the CLI for administration of the TOE is outside the scope of evaluation. This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

81271—Fixed an issue where the second attempt to access some websites over HTTPS failed when SSL Forward Proxy was enabled.

> Minor Change – SSL Forward Proxy is an aspect of operation of SSL Decryption policy, which is outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

81264—Fixed an issue where Threat logs were generated for Threat Name - IP fragment overlap, ID - 8705 after upgrading to a PAN-OS 7.0 release.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

81219—Fixed an issue with stability when adding Log Collectors to a Collector Group.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

81115—Fixed an issue where administrators experienced long delays when executing log queries consisting of multiple attributes.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

81110—Fixed a session reuse issue where an incoming SYN/ACK packet for an established session caused a failure in TCP reassembly, which resulted in a dropped packet even though the Reject Non-SYN TCP option was disabled (Network > Network Profiles > Zone Protection > <Zone Protection profile> > Packet Based Attack Protection > TCP Drop). With this fix, initiating session reuse with a SYN/ACK packet is successful regardless of the Reject Non-SYN TCP setting.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

80993—Fixed an issue in PAN-OS 7.0 (as well as in Panorama 5.1 and later releases) where XML API POST requests failed when including a QUERY_STRING but no content-length header. With this fix (in both PAN-OS and Panorama 7.0.2 releases), POST requests with a QUERY_STRING and a missing content-length header are successful.

> Minor Change – The XML API is not covered within the scope of the evaluation.

80960—Fixed an issue where attempting to Test SCP server connection (Device > Scheduled Log Export) created an unnecessary Config lock that prevented any additional changes to the running configuration.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

80933—Fixed a rare issue where a PA-7000 Series firewall experienced heartbeat failures on the HA1 and HA1 backup links that caused split brain in a high availability (HA) configuration.

Minor Change – This relates to High Availability (HA) configurations, which are not covered in the scope of the evaluation.

80924—Fixed an issue where a GlobalProtect Large Scale VPN (LSVPN) satellite configuration caused the satellite firewall to Proxy ARP for the defined access route subnets on all logical and physical interfaces.

Minor Change – The use of GlobalProtect is outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

80896—Fixed an issue where some actions that utilize the /opt/pancfg/ partition, such as dynamic updates and commits, were failing when that partition ran out of space due to a large number of HIP reports received from User-ID XML API. With this fix, HIP reports are no longer saved in the /opt/pancfg/ partition of the firewall.

Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

80840—Fixed an issue where the URL filter did not correctly parse the common name (CN) value when a MAC address was specified as the CN value in the server certificate.

Minor Change – This relates to the URL Filtering profile. Security profiles such as the URL Filtering profile are outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

80839—Fixed an issue where error is displayed for Tor status in the CLI output for both the show wildfire status and test wildfire tor CLI commands.

Minor Change – The use of the CLI for administration of the TOE is outside the scope of evaluation. This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

80767—In response to a very rare issue where the configured NAT pool or method was not utilized as expected, an enhancement was made to Tech Support file generation that includes additional data to help troubleshoot the issue.

Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

80720—Fixed an issue where a firewall experienced a dataplane restart when the packet processing daemon terminated due to a double free condition associated with a specific packet buffer (fptcp).

Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

80687—Fixed an issue on PA-7000 Series, PA-5000 Series, and PA-3000 Series firewalls where software packet buffers were depleted (although eventually recovered) when receiving TCP packets with large payloads. With this fix, modifications to processes for allocating software buffers and handling TCP congestion ensure that software packet buffers do not get depleted due to packets with large payloads.

Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

80669—Fixed an issue on firewalls in CCEAL mode where the management server would restart when the firewall attempted to send an SNMPv3 trap.

Minor Change – This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

80624—Fixed an issue where administrators experienced delays accessing the firewall web interface when the firewall reconnected to Panorama and had a large number of logs to send.

Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

80592—Fixed an issue where firewalls in a high availability (HA) active/passive configuration did not sync the Dynamic Address Group when one of the firewalls stopped functioning and then changed to a functional state.

Minor Change – This relates to High Availability (HA) configurations, which are not covered in the scope of the evaluation.

80567—In response to an issue where race conditions affecting Block IP table operations inadvertently caused some packets to be marked as drop ip block without any entry in the Block IP table.

Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

80532—Fixed an issue where files were not being forwarded as expected to the WildFire cloud (public or private) due to a terminated process (varrcvr). This issue occurred when the Subject field in forwarded emails contained non-ASCII characters.

Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

80404—Fixed an issue where PA-2000 Series firewalls experienced connectivity issues when auto-negotiating duplex and speed settings on the management interface connection to a third-party device. With this fix, a new driver is added to ensure that the management interface remains accessible and to provide a more reliable transition when speeds are changed (such as from 1,000 Mbps over full duplex—1000/Full—to 100/Full) when there is little or no traffic flowing through the firewall.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

80386—Fixed an issue where a configuration override failed when pushing system log settings to firewalls from Panorama resulting in the following error: edit failed, may need to override template object informational first.

> Minor Change – The use of Panorama to manage TOE appliances is explicitly excluded in the evaluated configuration, as specified in Section 2.4 of [CCECG]. As such, this issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

80318—Fixed an intermittent issue on a PA-7000 Series firewall where some packets were dropped during the initial session setup process. This issue occurred when two packets in the same session were sent almost simultaneously, causing the second of the two packets to get dropped.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

80251—Fixed an issue on a firewall where a dataplane restarted with multiple core files (all_pktproc, flow_ctrl, and flow_mgmt) after the firewall received percent-encoded HTTP requests from a proxy server when both the parsing of X-Forwarded-For (XFF) attributes and stripping of XFF from HTTP Headers were enabled (configured with the set system setting ctd CLI command). With this fix, you can enable both XFF actions without causing the dataplane to restart when the firewall receives percent-encoded HTTP request from a proxy server.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

80187—Fixed an issue where the test authentication authentication-profile command results in output that uses the management interface as the source regardless whether you configured a service route to provide a different source.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

80063—Fixed an issue on an M-100 appliance where the configuration daemon (configd) stopped responding when processing a null value.

> Minor Change – This applies to the Panorama M-100 appliance, which is not part of the TOE.

79960—Fixed an issue where the firewall sent an extra carriage return line feed (CRLF) in HTTP/1.1 POST packets when requesting an update from the BrightCloud URL database. This issue occurred when using a proxy server, which correctly rejects the packets and returns HTTP/1.1 400 Bad Request messages due to the extra CRLF (per RFC 7230).

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

79929—Fixed an issue where a process (mprelay) stopped responding and did not receive a refresh of the configuration when it restarted.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

79925—Fixed an issue where virtual wire (vwire) path monitoring failed and the firewall stopped sending ICMP packets over the vwire interface after a high availability (HA) failover.

> Minor Change – This relates to High Availability (HA) configurations, which are not covered in the scope of the evaluation.

79719—Fixed a rare issue where a dataplane restarted when multiple processes (flow_ctrl and mprelay) stopped responding due to a software buffer leak.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

79709—Fixed an intermittent issue where ZIP processing may cause the dataplane to restart.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

79535—Fixed an issue in a high availability (HA) configuration where the monitored destination IP address for Path Monitoring displayed as up even when unavailable, preventing the firewall from displaying as tentative as expected. With this fix, the monitored destination IP address correctly shows as down when unavailable, which results in the firewall correctly changing status to tentative.

> Minor Change – This relates to High Availability (HA) configurations, which are not covered in the scope of the evaluation.

79504—Fixed an issue where a passive M-100 appliance in a high availability (HA) configuration lost its device group and template configuration.

> Minor Change – This applies to the Panorama M-100 appliance, which is not part of the TOE.

79470—Fixed an issue where Panorama did not display WildFire Analysis reports correctly in the WildFire Submissions log for WF-500 appliances running PAN-OS 6.1 or earlier releases.

> Minor Change – This applies to the WF-500 WildFire Appliance, which is not part of the TOE.

79382—Fixed an issue where IP address registration through the XML API failed to populate the Dynamic Address Group following an AddrObjRefresh job failure during a template commit from Panorama when the Force Template Values option was checked, resulting in an Error: Failed to parse security policy.

> Minor Change – The XML API is not covered within the scope of the evaluation.

79347—Fixed an issue where a firewall stopped responding and triggered a dataplane restart when receiving incomplete and insufficient parameters in API calls. With this fix, checks are in place to prevent the dataplane restart when receiving API requests with invalid or insufficient parameters.

> Minor Change – The XML API is not covered within the scope of the evaluation.

79279—Fixed an issue that caused an error to be displayed (ntp-servers unexpected here. Discarding.) when pushing a device group configuration through templates after a Panorama upgrade.

> Minor Change – The use of Panorama to manage TOE appliances is explicitly excluded in the evaluated configuration, as specified in Section 2.4 of [CCECG]. As such, this issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

79046—Fixed an issue on an M-Series appliance running in Log Collector mode where log forwarding to an external syslog server stopped working after a Panorama commit when forwarding logs through TCP port 514 (default) instead of UDP port 514 (Device > Server Profiles > Syslog). With this fix, you no longer need to perform a Collector Group commit to resume log forwarding after a Panorama commit when the syslog server is configured to use TCP.

> Minor Change – This applies to M-Series appliances, which are not part of the TOE.

78891—Fixed an issue where the use of region-based objects in the Security policy caused consistently high dataplane CPU utilization.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

78803—Fixed an issue in Panorama where template settings that were global to every virtual system (vsys) on a firewall (for example, System log settings) were unable to reference configuration elements (for example, an Email server profile) when that element was added to a specific vsys instead of to the Shared location. With this fix, Panorama can push template and device group settings—even those that are not or can't be pushed to a specific vsys—regardless whether those settings refer to Shared elements or elements that are specific to a vsys.

> Minor Change – This is a Panorama issue. Panorama is not covered in the scope of the evaluation.

78571—Fixed an intermittent issue where a firewall received a Virtual Systems license that allowed for a higher number of virtual systems than the maximum amount supported for the platform. With this fix, the licensed virtual systems activated on a firewall cannot be higher than the maximum amount of virtual systems supported on the firewall.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

78568—Fixed an issue where PA-3000, PA-5000, and PA-7000 Series firewalls experienced a memory leak associated with improper purging of old, replaced entries in the ARP/ND table when the table reached capacity.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

78511—Fixed an issue where the DHCP relay agent incorrectly set the gateway IP address (giaddr) value to zero (instead of the IP address of the ingress interface as defined in RFC 1542) when responding to DHCP requests.

> Minor Change – Configuration as a DHCP relay is outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

78084—The output for the command show log collector serial number displayed different log data when executed on a primary-active Panorama than the output that was displayed when the command was executed from the secondary-passive Panorama. This issue is fixed so that the output for the command show log collector serial number correctly displays the latest log data for managed Log Collectors.

> Minor Change – The use of Panorama to manage TOE appliances is explicitly excluded in the evaluated configuration, as specified in Section 2.4 of [CCECG]. As such, this issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

78064—Fixed an intermittent issue where authentication failed in a two-phase authentication process when the login response contained customer data.

> Minor Change – This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

77816—Fixed an intermittent issue where some Windows 7 GlobalProtect clients using two-factor authentication (LDAP and certificate) lost connection to the portal or gateway and could not reconnect due to a failed authentication with the error Required client certificate is not found even when the certificate was available.

> Minor Change – The use of GlobalProtect is outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

77775—Fixed an issue where a validation error occurred when attempting to move an object from its current device group to a destination device group that was lower in the hierarchy even when the policy rules or objects that reference the object being moved were in the same destination or in a device group that should inherit the object.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

77103—Fixed an issue where a System log message (Failed to upgrade WildFire package to version <unknown version>) displayed on the firewall even when no WildFire license existed on the firewall.

> Minor Change – WildFire-related functions and capabilities are outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

76875—Fixed an issue where the dataplane rebooted when a process (brdagent) was terminated by the firewall in response to an out of memory condition. With the fix, dataplane reboots are no longer triggered by these out-of-memory events because the firewall no longer considers the brdagent process for termination when attempting to address an out-of-memory event.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

76781—Fixed an issue where a firewall incorrectly calculated packet length and TCP sequence due to a one-byte zero-window-probe packet when that packet was sent from one vsys to another.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

76631—Fixed an issue on PA-7000 Series firewalls where the Log Processing Card (LPC) failed to resolve the FQDN of the syslog server. With this fix, the firewall will re-initiate the DNS lookup request until the lookup succeeds.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

76561—Fixed an issue where the DHCP relay agent dropped DHCPDISCOVER packets that the agent could not process due to multiple BOOTP flags. With this fix, the DHCP relay agent recognizes the first BOOTP flag in a DHCPDISCOVER packet and ignores any additional BOOTP flags that may exist (per RFC 1542) so that multiple BOOTP flags do not cause DHCPDISCOVER packets to be dropped.

> Minor Change – Configuration as a DHCP relay is outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

76238—A security-related fix was made to address CVE-2015-1873.

> Minor Change – CVE-2015-1873 has been reserved. The details of the vulnerability have not been published. Palo Alto has advised this related to a cross-site scripting issue with one of the fields in the GUI. The issue was not fixed in some very old releases, so Palo Alto has not provided further details ion the public release notes.

75803—Addressed an issue regarding how often password API keys are regenerated.

> Minor Change – The XML API is not covered within the scope of the evaluation.

75344—Fixed an issue where a memory process restarted and caused an invalid memory reference; the invalid memory reference resulted in a management plane restart.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

74423—Fixed an issue where a firewall running PAN-OS 7.0.1 was incorrectly using the URL Updates service route when fetching a Dynamic Block List instead of using the service route attached to the Palo Alto Updates in the Service Route Configuration (Device > Setup > Services > Global).

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

73443—Fixed an intermittent issue that resulted in corrupted forwarding entries on the offload processor.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

71331—Fixed an issue on a PA-500 firewall where the firewall assigned a DHCP address for the management (MGT) interface even after the administrator configured a static IP address for that port. With this fix, DHCP initiation for the MGT interface is disabled.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

70887—Fixed an issue where clicking the More link to view the registered IP address under Object > Address Groups resulted in an error if the name of a Dynamic Address Group included a space. With this fix, spaces in Dynamic Address Group names no longer cause an error when displaying the IP address.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

70302—Fixed an issue where the autocommit process failed after upgrading a PA-7050 or PA-5000 Series firewall to a PAN-OS 6.1 or PAN-OS 7.0 release.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

69132—Fixed an issue where occasional dataplane restarts occurred due to a kernel memory allocation failure.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

64602—In response to an issue where a firewall generated core files for a process (pktproc) when a dataplane stopped responding, an additional check and associated error output is added to help troubleshoot an issue where an FPGA running the Aho-Corasick algorithm returns a session index mapped to a NULL pointer.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

64531—Fixed an issue where a high availability (HA) failover occurred due to insufficient kernel memory on a PA-5000 Series firewall. With this fix, PA-5000 Series firewalls include some cache-flushing events and increased kernel memory to ensure sufficient kernel memory remains available for ping requests and keep-alive messages to avoid these HA failovers.

> Minor Change – This relates to High Availability (HA) configurations, which are not covered in the scope of the evaluation.

64266—Fixed a rare issue where certain processes (l3svc and sslvpn) stopped responding when a Content update and FQDN refresh occurred simultaneously.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

Bug Fixes in 7.1.3 Release
Note: The following issues were also addressed in PAN-OS 7.0.8 and the rationale for their being minor changes is documented above in the following bug fixes: 9713; 96792; 93729; 91497; 90326; 89551. Similarly, Issue 82470 was also addressed in PAN-OS 7.0.7 and its rationale for being a minor change is documented above.

96634—Fixed an issue where a certificate signing request (CSR) using Simple Certificate Enrollment Protocol (SCEP) over SSL failed due to buffer limit (signing over non-SSL worked correctly).

> Minor Change – The use of SCEP was not covered in the scope of the evaluation. This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

96140—Fixed an issue where disabling and importing local copies of Panorama policies and objects resulted in exclusion of Log Forwarding profile imports on multi-virtual systems (multi-vsys).

> Minor Change – The use of Panorama to manage TOE appliances is explicitly excluded in the evaluated configuration, as specified in Section 2.4 of [CCECG]. As such, this issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

95747—Fixed an issue with VLAN tag translation where the firewall unsets the Priority Code Point value in VLAN tag field when forwarding the frame between different VLANs. With this fix, firewall preserves Priority Code Point value (802.1P) in Layer-2 VLAN tag field when receiving a frame on one VLAN Tag port and then forwarding it to another VLAN Tag port.

> Minor Change –VLAN tag translation was not covered in the scope of the evaluation. This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

95275—Fixed an issue where a role-based administrator could view unified logs under the Monitor tab, but could not export these logs.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

95133—Fixed an issue where firewall incorrectly applied Policy Based Forwarding (PBF) to sessions created via prediction (such as ftp-data sessions).

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

95047—Fixed an issue where PAN-OS log integration with AutoFocus did not use proxy server settings.

Minor Change – AutoFocus is a Palo Alto subscription service that is outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

94930—Fixed an issue where firewall running on VMware NSX had incorrect content of address-group objects pushed via Panorama updates.

Minor Change – This relates to VM-Series NSX edition firewalls, which are not covered in the scope of the evaluation.

94914—Fixed an issue where a firewall running a PAN-OS 7.1.0 or later release fails to block HTTP-Video application.

Minor Change – The scope of the evaluation is limited to the packet filtering/stateful traffic filtering capabilities of the TOE, which were tested only for the following protocols: IPv4; IPv6; ICMPv4; ICMPv6; TCP; UDP; and FTP. Identification of HTTP-Video applications on the network is outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

94790—Fixed an issue on PA-3050 firewall where dataplane CPU usage became excessive after upgrading from 7.0 to 7.1.

Minor Change – This is a performance issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

94765—Fixed an issue where the administrator deleted a virtual system (vsys) from a firewall with multiple virtual systems (multi-vsys) and NAT rules configured without first deleting NAT rules associated with the vsys, causing NAT translation to not work as expected. With this fix, when the administrator deletes a vsys, the firewall will delete NAT rules associated with the vsys.

Minor Change – This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

94573—Fixed an issue where a firewall dropped incoming PSH+ACK segments from the server.

Minor Change – This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

94570—Fixed an issue where role-based Panorama administrators were unable to perform commits because the Commit dialog opened and immediately closed without allowing administrators to modify, preview, or confirm their commit requests.

Minor Change – The use of Panorama to manage TOE appliances is explicitly excluded in the evaluated configuration, as specified in Section 2.4 of [CCECG]. As such, this issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

94533—Fixed an issue where Panorama pushed unused shared address objects to the firewall when the name of the object matched another pushed address object from the firewall’s device group, while the Share Unused Address and Service Objects with Devices option was unchecked.

Minor Change – The use of Panorama to manage TOE appliances is explicitly excluded in the evaluated configuration, as specified in Section 2.4 of [CCECG]. As such, this issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

94435—Fixed an issue on a PA-3000 Series firewall running a PAN-OS 7.0.1 or later release, where OSPF neighbors on aggregate Ethernet with maximum transmission unit (MTU) of 9216 failed to establish and got stuck in the exchange state.

Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

94282—Fixed an issue on PA-7000 Series firewalls configured as HA pairs where, after the active firewall failed over to become the passive firewall, the newly passive firewall restarted with the error message: internal packet path monitoring failure. With this fix, the firewall will not restart after becoming passive.

Minor Change – This relates to High Availability (HA) configurations, which are not covered in the scope of the evaluation.

94165—Fixed an issue where the firewall generated WildFire Submissions logs with an incorrect email subject and sender information when sending more than one email to a recipient in a POP3 session.

Minor Change – WildFire-related functions and capabilities are outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

94136—Fixed an issue where a PA-200 firewall reported an antivirus update job as successful when the update downloaded without installing. With this fix, a larger timeout value allows the installation to complete.

Minor Change – This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

94097—Fixed an issue where firewall does not log email sender, receiver and subject in WildFire Submissions log.

Minor Change – WildFire-related functions and capabilities are outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

93783—Fixed an issue on firewalls where autocommit failed if administrator configured an IPsec tunnel using the manual-key method.

Minor Change – This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

93778—Fixed a rare issue where a bind request from the firewall to the LDAP server failed. With this fix, the firewall will perform re-connection.

Minor Change – Use of LDAP external authentication servers is outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

93770—Fixed an issue where the firewall interpreted a truncated external dynamic list IP address (such as 8.8.8.8/) as 0.0.0.0/0 and blocked all traffic. With this fix, the firewall will ignore incorrectly formatted IP address entries.

Minor Change – This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

93667—Fixed an issue on firewalls where the Host Information Profile (HIP) report stalled and the firewall could not collect new HIP reports from GlobalProtect users.

Minor Change – The use of GlobalProtect is outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

93458—Fixed an issue where WildFire platforms experienced nonresponsive processes and sudden restarts under certain clients' traffic conditions.

Minor Change – WildFire-related functions and capabilities are outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

93276—Starting in 7.1.3, the Application Command Center (ACC) includes the following usability enhancements:

- You can Jump to Unified logs from an ACC widget; previously you could jump to all log types, except the Unified logs
- You can easily promote an IP address or a user as a global filter from a table within an ACC widget. The context drop-down that appears next to the value allows you to promote the users or IP address as a global filter.

Minor Change – The Application Command Center (ACC) is an interactive, graphical summary of the applications, users, URLs, threats, and content traversing the network. The ACC uses the firewall logs to provide visibility into traffic patterns and actionable information on threats. The ACC is not described in the ST and its use is not covered in the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

93218—Fixed an issue where an administrator (other than superuser) could not view detailed configuration changes using Logs > Configuration. With this fix, administrators of all types will be able to view detailed configuration changes.

Minor Change – This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

92934—Fixed an issue where firewall configured for DHCP relay (with multiple DHCP relays or in certain firewall virtual system configurations) rebroadcast a DHCP packet on the same interface that received it, causing a broadcast storm. With this fix the firewall will drop duplicate broadcasts rather than retransmitting them.

Minor Change – Configuration as a DHCP relay is outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

92912—Fixed an issue on Panorama where administrator observed a File not found error when attempting to view a threat packet capture (pcap).

Minor Change – This is a Panorama issue. Panorama is not covered in the scope of the evaluation.

92684—Fixed an issue on firewalls where the l3svc process stopped responding when processing a large number of user-authentication requests.

Minor Change – This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

92610—Fixed on issue on PA-200 firewall where, after an upgrade from PAN-OS 6.1.x to 7.0.x, the firewall stalled during boot-up.

Minor Change – This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

92467—Fixed an issue on Panorama where exporting the device state failed if a running-config.xml file already existed in the target location, which resulted in one or more Server error messages. With this fix, the new device state file exports as expected.

Minor Change – This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

91269—Fixed an issue where the firewall restarted the dataplane after a process stopped responding.

> Minor Change – This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

91202—Fixed a user interface issue on firewalls and Panorama where searches on Correlated Events logs using classless subnets (for example, /21 instead of /24) failed to give the correct results.

> Minor Change – This relates to the automated correlation engine functionality of the TOE, which is not covered in the scope of the evaluation. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

91171—Fixed the issue where, if the firewall processed a high volume of BFD sessions for routing peers that use BGP, OSPF or RIP, and the firewall also processed a high volume of packets belonging to existing sessions that were not offloaded, the BFD sessions to those peers flapped when the firewall received a content update.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

91086—Fixed an issue where the firewall experienced BGP disconnections due to firewall not sending keepalive messages to neighbors within specified timers.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

90691—Fixed an issue on firewalls running a PAN-OS 7.0 or later release where the web interface became inaccessible (502 bad gateway error) when sending a high rate of concurrent User-ID XML API POST requests.

> Minor Change – The XML API is not covered within the scope of the evaluation.

90618—Fixed an issue on Panorama where creating an exemption for a threat name from the Threat log caused the web interface to display the exemption multiple times depending on the number of sub-device groups. After the fix, the interface correctly displays only one profile name.

> Minor Change – This is a Panorama issue. Panorama is not covered in the scope of the evaluation.

90560—Fixed an issue where the firewall did not authenticate a syslog server's certificate signed by a trusted root certificate authority (CA) included in the predefined trusted root certificate list, which caused connection issues with syslog forwarding over SSL. With this fix, the firewall can authenticate the syslog server's certificate and can establish SSL connections.

> Minor Change – This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

90508—A security-related fix was made to address CVE-2016-0777 and CVE-2016-0778.

> Minor Change – This is the fix made to address PAN-SA-2016-0011, which addresses vulnerabilities in OpenSSH. These vulnerabilities affect PAN-OS only when initiating a connection to a malicious SSH server. The use of SSH in either client or server modes is not covered in the scope of the evaluation. Therefore, this issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

89007—Fixed an issue where VM-Series firewalls deployed in AWS firewalls used UDP port 24946 for HA2 keep-alive packets instead of UDP port 29281.

> Minor Change – Deployment of VM-series firewalls in AWS is outside the scope of the evaluation.

88334—Fixed an issue where the firewall restarted unexpectedly when trying to delete a tunnel interface configuration.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

88307—Fixed an issue where the dataplane restarted and dataplane processes stopped responding when passing SSH traffic using SSH decryption.

> Minor Change – SSH Decryption policy is outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

88194—Fixed an issue where Panorama did not log if the Force Template Values option was in the checked state when applying a Template or Device Group commit. With this fix, the Panorama logs will indicate if the Force Template Values option is in the checked state when doing a Template or Device Group commit.

> Minor Change – This is a Panorama issue. Panorama is not covered in the scope of the evaluation.

88029—Fixed an issue where, after an upgrade, the firewall did not use the previously configured system-wide proxy configuration (Device > Setup > Services) for accessing the WildFire public cloud (PAN-OS 7.0 introduced a separate WildFire proxy configuration Device > Setup > WildFire). With this fix, the upgrade process automatically uses the previous proxy configuration when creating the WildFire public cloud configuration.

> Minor Change – WildFire-related functions and capabilities are outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

Bug Fixes in 7.1.2 Release
Note:

- The following issues were also addressed in PAN-OS 7.0.8 and the rationale for their being minor changes is documented in Appendix B: 92763; 92391; 91724; 90856; 90044; 88157.
- The following issues were also addressed in PAN-OS 7.0.7 and the rationale for their being minor changes is documented in Appendix B: 93775; 93644; 93228; 91079; 90029; 77460; 76661; 74443.
- The following issues were also addressed in PAN-OS 7.0.6 and the rationale for their being minor changes is documented in Appendix B: 84641; 83722.

95120—Fixed an issue where authentication failed on the GlobalProtect gateway because the client tried to authenticate using cookies with domain\user specified in the agent configuration.

> Minor Change – GlobalProtect is outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

95021—Fixed an issue where the VLAN ID was added in the wrong location in the packet payload in Layer 2 deployments, which caused some applications to fail.

> Minor Change – This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

94990—Fixed an issue where the User-ID (useridd) process stopped responding when encountering a custom URL category that included a space (“ ”) character in the category name.

> Minor Change – This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

94939—Fixed an issue where strongSwan Linux VPN clients failed to connect to the GlobalProtect gateway because the firewall presented a server certificate that did not include a Common Name (CN) value.

> Minor Change – GlobalProtect is outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

94883—Fixed an issue on firewalls that were upgraded from a PAN-OS 7.0 release to a PAN-OS 7.1 release where GlobalProtect prevented third-party IPsec (X-Auth) clients from connecting to the GlobalProtect gateway. With this fix, you can now upgrade from a PAN-OS 7.0 release to a PAN-OS 7.1.2 or later release to prevent this issue.

> Minor Change – GlobalProtect is outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

94695—Fixed an issue where the firewall failed to connect to AutoFocus unless you manually re-entered the URL in the AutoFocus settings (Device > Setup > Management) even though the URL was correctly pre-configured. With this fix, the firewall connects to AutoFocus as expected using the prepopulated AutoFocus URL.

> Minor Change – AutoFocus is a Palo Alto subscription service that is outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

94571—Fixed an issue where commits failed if you configured two proxy IDs on a single tunnel using the same source, destination subnets, and protocol because the proxy IDs appeared to be duplicates of each other even though they were configured with different ports. With this fix, the firewall also uses the port value when determining whether proxy IDs are unique or duplicates.

> Minor Change – This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

94493—Fixed an issue where Panorama™ Device Group and Template administrators were unable to perform commits because the Commit dialog opened and immediately closed without allowing administrators to modify, preview, or confirm their commit requests.

> Minor Change – The use of Panorama to manage TOE appliances is explicitly excluded in the evaluated configuration, as specified in Section 2.4 of [CCECG]. As such, this issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

94437—Fixed an issue where configurations pushed from Panorama running a 7.1 release to a firewall running PAN-OS 7.0 or earlier release incorrectly deleted the gateway configuration even when address objects were not included in the pushed configuration. With this fix, the gateway configuration is deleted only when the pushed configuration includes address objects.

> Minor Change – The use of Panorama to manage TOE appliances is explicitly excluded in the evaluated configuration, as specified in Section 2.4 of [CCECG]. As such, this issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

94408—Fixed an issue where predefined URL categories were not populated in Security and Decryption policy rules as expected when using BrightCloud as the URL database.

> Minor Change – The scope of the evaluation is limited to the packet filtering/stateful traffic filtering capabilities of the TOE, which were tested only for the following protocols: IPv4; IPv6; ICMPv4; ICMPv6; TCP; UDP; and FTP. The use of URL categories in Security and Decryption policies is outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

93961—Fixed an issue were a process (configd or mgmtsrvr) restarted due to the use of special characters (such as a bracket character—“[” or “]”—in a search field (for example, in the Address section).

> Minor Change – This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

93882—Fixed an issue where you were unable to deploy a VM-Series firewall using a VHD exported from an existing VM-Series firewall in Azure.

> Minor Change – Deployment of VM-series firewalls in Azure is outside the scope of the evaluation.

93865—Fixed an issue on an M-100 appliance in Log Collector mode where locally-created proxy configurations were lost when a commit was performed from Panorama. With this fix, locally-created proxy configurations persist after a Panorama commit.

> Minor Change – This applies to the M-100 appliance, which is not part of the TOE.

93855—Fixed an issue where the DNS proxy template object that was pushed from Panorama did not override that object on the firewall as expected.

> Minor Change – The use of Panorama to manage TOE appliances is explicitly excluded in the evaluated configuration, as specified in Section 2.4 of [CCECG]. As such, this issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

93612—A security-related fix was made to address a privilege escalation issue.

> Minor Change – This is the fix made to address PAN-SA-2016-0015, which related to a vulnerability where a file locally created by an end user and placed in a specific directory could be executed in a higher privilege context. However, because no shell access is available to end users, exploitation of this issue is unlikely. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

93526—Fixed an issue where the web interface and CLI reported that configurations were out of sync between HA peers even when the peers were in sync. With this fix, sync status is reported correctly.

> Minor Change – This relates to High Availability (HA) configurations, which are not covered in the scope of the evaluation.

93508—Fixed an issue where a process (logrcvr) stopped responding and restarted repeatedly after an upgrade to content release version 571, which caused the firewall to reboot. Content release version 572 mitigated this issue but this fix ensures that firewalls running PAN-OS 7.1.2 or later releases will not be affected by this issue.

> Minor Change – This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

93449—Fixed an issue where the API browser displayed the incorrect XML API syntax for the show arp all command.

> Minor Change – The XML API is not covered within the scope of the evaluation.

93395—Fixed an issue on firewalls and Panorama running a 7.1.0 or 7.1.1 release where the firewall mgmtsrvr or Panorama reportd process stopped responding and caused the process to restart after displaying the following message: SYSTEM ALERT : critical : mgmtsrvr (or reportd) - virtual memory limit exceeded, restarting. This issue was caused by a memory leak that occurred when viewing logs of single log types (such as Traffic or Threat).

> Minor Change – This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

93367—Fixed an issue where ACC logs did not resolve IP addresses to FQDN under destination IP activity.

> Minor Change –The ACC is not covered in the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

93333—Fixed an issue where the firewall did not properly process active FTP data sessions if the FTP client reused—within a short period of time—the destination port number that was negotiated in the FTP control session.

> Minor Change – This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

93240—Fixed an issue where multiple SFP+ ports coming up at the same time caused a race condition that resulted in ports entering a re-initialization phase and that caused a several second delay before ports came up.

> Minor Change – This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

92979—Fixed an issue on Panorama where the Administrator Use Only option (Template > Device > Radius Profile) was not displayed in the web interface.

> Minor Change – This is a Panorama issue. Panorama is not covered in the scope of the evaluation.

92677—Fixed an issue where the Comodo® RSA certificate authority (CA) was not included in the default trusted root on the firewall, which caused SSL decryption to fail on sites using this as their CA.

> Minor Change – SSL Decryption policy is outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

92642—Fixed an issue on Panorama (virtual and M-Series appliances) where a process (configd) stopped responding when triggering a commit very soon after a reboot and before a database required for the commit process was ready for use. Additionally, administrators received an error message (Administrator does not have access to any device-group data) when they attempted to view Monitor > Logs information or ACC information on the Panorama web interface before the database was ready. With this fix, this database loads faster so that commits and attempts to view Monitor > Logs and ACC information are successful even when attempted immediately following a reboot of Panorama.

> Minor Change – This is a Panorama issue. Panorama is not covered in the scope of the evaluation.

92413—A security-related change was made to address a boundary check that caused a service disruption of the captive portal.

> Minor Change – This is the fix made to address PAN-SA-2016-0013, which closes a denial of service vulnerability in the PAN-OS Captive Portal functionality, which is outside the scope of evaluation. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

92082—Fixed an issue where an administrator with read-only privilege was unable to export Correlated Events logs in CSV format.

> Minor Change – This relates to the automated correlation engine functionality of the TOE, which is not covered in the scope of the evaluation. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

92050—Fixed an issue on a PA-3000 Series firewall running a PAN-OS 7.0.1 or later release with zone protection configured to drop fragmented traffic where outgoing OSPF DB Description packets were fragmented and subsequently dropped, which caused the OSPF neighbor status to get stuck in Exchange state.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

91998—Fixed an issue where the set application dump on rule CLI command did not work for Security policy rules pushed to firewalls from Panorama.

> Minor Change – The use of Panorama to manage TOE appliances is explicitly excluded in the evaluated configuration, as specified in Section 2.4 of [CCECG]. In addition, the use of the CLI for administration of the TOE is outside the scope of evaluation. As such, this issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

91785—Fixed an issue where a Panorama process (configd) stopped responding when trying to add tags to multiple firewalls at the same time.

> Minor Change – This is a Panorama issue. Panorama is not covered in the scope of the evaluation.

91395—Fixed an issue where the simultaneous transfer of large files from two different SMB servers over a GlobalProtect connection from a Windows 8 client caused the connection to fail. With this fix, you can enable heuristics on Windows 8 clients or set the tunnel interface MTU size to 1,300 to avoid this issue.

> Minor Change – GlobalProtect is outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

91379—Fixed an issue where an out-of-sequence packet was passed through the firewall.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

91156—Fixed an issue on Panorama where performing log queries and reports resulted in incorrect reporting of multiple Panorama logged-in administrators on PA-7000 firewalls.

> Minor Change – This is a Panorama issue. Panorama is not covered in the scope of the evaluation.

90826—Fixed an issue where unused shared objects were calculated incorrectly during a commit from Panorama due to address and service name overlaps.

> Minor Change – The use of Panorama to manage TOE appliances is explicitly excluded in the evaluated configuration, as specified in Section 2.4 of [CCECG]. As such, this issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

89925—Fixed an issue where PAN-OS 7.1 images failed to bootstrap a firewall if the bootstrapping tarball package was created using a Mac OS (BSD-based tar format). With this fix, you can bootstrap firewalls with PAN-OS 7.1.2 or later release images using a BSD-based tarball created using a Mac OS.

> Minor Change – This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

89620—Fixed an issue where SSL inbound decryption failed when a client sent a ClientHello with TLS 1.2 while the server supported only TLS 1.0.

> Minor Change – SSL Decryption policy is outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

89264—Fixed an issue where DNS resolution failed when message compression was disabled on the DNS server, which resulted in case mismatch between CNAME query and answer values in DNS server replies. With this fix, the firewall ignores case in CNAME values so that query and answer values match and DNS requests resolve successfully.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

89261—Fixed an issue where you could not display interface QoS counters when the CLI output mode was set to op-command-xml-output.

> Minor Change – The use of the CLI for administration of the TOE is outside the scope of evaluation. As such, this issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

86996—Fixed an issue where Traffic logs reported cumulative bytes for sessions with TCP port reuse, which caused custom reports to incorrectly report the byte count.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

86990—Fixed an issue on a firewall where a process (sslvpn) repeatedly restarted due to an internal thread synchronization issue.

> Minor Change – This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

83569—Fixed an issue where multiple QoS changes while under a heavy load caused the dataplane to restart.

> Minor Change – This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

83339—Fixed an issue with the web interface where uncommitted IPsec proxy ID details were unexpectedly deleted prior to commit.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

80177—Fixed an issue where the firewall did not present the URL block page as expected when proxied request from client used CONNECT method.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

40436—Fixed an issue where firewalls running PAN-OS 7.0 and earlier releases did not update FQDN entries unless you enabled the DNS proxy caching option (Network > DNS Proxy > <DNS Proxy config> > Advanced).

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

Bug Fixes in 7.1.1 Release
93710—Fixed an issue where the Pay-as-you-go (PAYG) hourly versions—Bundle 1 and Bundle 2 of the VM-Series firewall in Azure—were not available in the Azure Marketplace. These PAYG versions and solution templates are supported starting with PAN-OS 7.1.1.

> Minor Change – Deployment of VM-series firewalls in Azure is outside the scope of the evaluation.

Bug Fixes in 7.1.0 Release
Note:

- The following issues were also addressed in PAN-OS 7.0.8 and the rationale for their being minor changes is documented in Appendix B: 93072; 92293; 91900; 91876; 91728; 91653; 91336; 90982; 90857; 90794; 90635; 90553; 90249; 89979; 89910; 89743; 89551; 88346; 88327; 87851; 86623; 84115; 83239; 80953.
- The following issues were also addressed in PAN-OS 7.0.7 and the rationale for their being minor changes is documented in Appendix B: 91771; 91075; 90433; 90070; 89761; 89503; 89413; 89296; 88450; 88421; 88313; 87911; 87880; 87594; 87094; 86977; 86686; 86313; 86202; 86189; 86122; 85344; 85265; 84997; 84146; 84027; 82918.

- The following issue was also addressed in PAN-OS 7.0.6 and the rationale for its being a minor change is documented in Appendix B: 87482.
- The following issues were also addressed in PAN-OS 7.0.5-h2 and the rationale for their being minor changes is documented in Appendix B: 89750; 89706.
- The following issues were also addressed in PAN-OS 7.0.5 and the rationale for their being minor changes is documented in Appendix B: 89752; 89717; 88191.

92382—Fixed an issue where the firewall could not install PAN-OS or GlobalProtect agent software images on leap day (February 29). With this fix, the firewall can install these images regardless of the date.

> Minor Change – This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

91533—Fixed an issue where a firewall failed a commit after receiving a File Blocking profile from Panorama that contained a space at the end of the profile name. This issue occurred when the managed firewall was running an older version of PAN-OS (when File Blocking and WildFire™ Analysis profiles were merged into one profile) and Panorama pushed the config to a device group.

> Minor Change – The use of Panorama to manage TOE appliances is explicitly excluded in the evaluated configuration, as specified in Section 2.4 of [CCECG]. As such, this issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

91522—Fixed an issue where a cloned application name could not be edited after it was cloned from a Shared/Device Group location to a Shared location. With this fix, the cloned application names can be edited.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

91307—Fixed an issue where SSL decryption sessions failed for secure websites that used a certificate issued by the Entrust.net Certification Authority (2048).

> Minor Change – SSL Decryption policy is outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

90933—Fixed an issue where the firewall generated superfluous logs (for traffic that did not match the configured filters) after you enabled dataplane debugging.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

90742—Fixed an issue where you could not add WF-500 appliance signatures as exceptions in an Antivirus profile when the signature names contained more than 32 characters.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

90501—Fixed an issue where the firewall could not connect to a GlobalProtect portal or gateway after removing the LSVPN configuration.

> Minor Change – GlobalProtect is outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

90411—Fixed an issue where a global counter (flow_dos_pf_noreplyneedfrag) related to the suppress-icmp-needfrag Zone Protection profile displayed the action as drop even when configured to allow ICMP Fragmentation. This fix introduces a new global counter (Unsuprressed ICMP Need Fragmentation).

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

90260—Fixed an issue where a device administrator was unable to configure certain settings under Device > Setup > Operations.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

90141—Improved output of the command request batch license info on Panorama to include license expiration times.

> Minor Change – This is a Panorama issue. Panorama is not covered in the scope of the evaluation.

90106—Fixed an issue where a process restarted unexpectedly due to the reuse of a process ID (PID). The PID was associated with an old SSH session that the firewall intended to terminate because the SSH session had timed out but was never closed properly, which inadvertently resulted in a restart of the process currently associated with that PID.

> Minor Change – This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

89906—Fixed an issue where non-superuser administrators were unable to see Exempt Profiles and the Security policy rules in which the profiles are used when viewing a Threat log (Monitor > Logs > Threat > <Threat Name>).

Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

89723—Fixed an issue where IPsec tunnels using IKEv2 failed to establish a VPN if multiple remote gateways were behind a port address translation (PAT) setup. With this fix, the firewall can allow multiple devices behind PAT to set up security associations to the same IP gateway.

Minor Change – Evaluation testing of the TOE as a VPN gateway confirmed the ability of the TOE to establish IPsec tunnels using IKEv2 with single IPsec peers. Testing as specified in the Protection Profile does not extend to testing if multiple deices behind a PAT setup can establish security associations to the TOE. Therefore, this issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

89595—Fixed an issue where attempting to Hide Panorama background header (Panorama > Setup > Operations > Custom Logos) resulted in an error (Edit breaks config validity).

Minor Change – This is a Panorama issue. Panorama is not covered in the scope of the evaluation.

89467—Fixed an issue with exporting a botnet report where exporting to CSV returned the Missing report job ID error.

Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

89342—Fixed a rare condition where the root partition on a firewall or appliance ran out of space during device state generation.

Minor Change – This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

89284—Fixed a reporting issue on the ACC and SaaS Application Usage Report on managed firewalls. This issue occurred because the application information pushed from Panorama did not populate in a way or location that allowed the information to be used for reports generated on the firewalls.

Minor Change – The use of Panorama to manage TOE appliances is explicitly excluded in the evaluated configuration, as specified in Section 2.4 of [CCECG]. As such, this issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

89036—Fixed an issue where the delete user-file ssh known-hosts command was unavailable on an M-Series appliance in Log Collector mode.

Minor Change – M-Series appliances are not included in the evaluated configuration.

88651—Fixed an issue where the User-ID (useridd) process stopped responding when the running-config was missing the port number associations for the Terminal Services (TS) Agent.

Minor Change – This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

88585—Fixed an issue where DNS proxy rules didn't consistently match a domain name with the correct primary IP addresses. With this fix, matching logic favors results that do not include wildcards.

Minor Change – Configuration as a DNS proxy is outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

88561—Fixed an issue where the tunnel went down and began to renegotiate, causing traffic destined for the tunnel during that time to be dropped. This issue occurred when the configuration was pushed from Panorama to a firewall configured with IKEv2 preferred mode and that was connected to a firewall configured to use IKEv1 in an IPsec connection.

Minor Change – The use of Panorama to manage TOE appliances is explicitly excluded in the evaluated configuration, as specified in Section 2.4 of [CCECG]. As such, this issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

88408—Fixed an issue where the show logging-status device command used in the XML API caused the log daemon to stop responding when the device attribute was omitted.

Minor Change – The XML API is not covered within the scope of the evaluation.

88279—Fixed an issue where the debug dataplane packet-diag aggregate-logs command showed an incorrect target filename.

Minor Change – The use of the CLI for administration of the TOE is outside the scope of evaluation. As such, this issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

88225—Fixed an issue where the firewall could not register with the WildFire public cloud due to a problem with the log-cache size becoming too large. With this fix, a limitation mechanism is now in place to control the log-cache size.

Minor Change – WildFire-related functions and capabilities are outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

88142—Fixed an issue with time calculation when displaying statistics for more than a single day (Monitor > App Scope > Network Monitor) that caused data to be unexpectedly shifted (calculation used 12:00 A.M. GMT instead of local time and data was shifted accordingly). With this fix, graphs display data across multiple days as expected for the local time on the firewall.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

88141—Fixed an issue on Panorama where an administrator with an access-domain name longer than 31 characters received the following error when logging in: Login could not be completed. Please contact the administrator. With this fix, administrators with access-domain names of up to 63 characters can log in.

> Minor Change – This is a Panorama issue. Panorama is not covered in the scope of the evaluation.

88101—Fixed an issue where WildFire reports (web interface and PDF) were unable to display digital signer information.

> Minor Change – WildFire-related functions and capabilities are outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

87871—Fixed an intermittent issue in an HA active/active configuration where packets passed through a virtual wire were dropped due to a race condition that occurred when the session owner and session setup were not on the same HA peer.

> Minor Change – This relates to High Availability (HA) configurations, which are not covered in the scope of the evaluation.

87870—Fixed an issue where an OSPF route with a lower administrative distance than the static route should become the preferred route but was not installed and used as expected; the firewall continued to use the static route instead.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

87727—Fixed an issue where a virtual system custom role administrator could not add user to IP mappings using the XML API.

> Minor Change – The XML API is not covered within the scope of the evaluation.

87414—Fixed a cosmetic issue where the traffic log type was displayed in the severity column of the Log Forwarding profile.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

87207—Fixed an issue where the User-ID process (useridd) stopped responding, which caused the firewall to reboot.

> Minor Change – This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

87144—Fixed an issue where a change of an object name was not propagated in some parts of the configuration where the object was referenced.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

87066—Fixed an issue on Panorama virtual appliances and on M-Series appliances in Panorama mode where two correlation engine sub-objects on the Web UI tab (Correlation Objects and Correlated Events) were incorrectly excluded when adding or modifying an Admin Role profile (Template > Device > Admin Roles).

> Minor Change – This is a Panorama issue. Panorama is not covered in the scope of the evaluation.

86979—Fixed an issue where an incomplete IPsec tunnel configuration (one without an IKE gateway specified) caused the firewall server process to stop responding.

> Minor Change – This is an availability issue and is not security relevant. This issue results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

86944—Fixed an issue on Panorama where a commit to a device group caused the Panorama job to fail, but the job was successful on the managed device.

> Minor Change – This is a Panorama issue. Panorama is not covered in the scope of the evaluation.

86725—Fixed an issue where the SSL Certificate Errors Notify Page did not display values of some variables (such as certname, issuer, and reason) on web pages with expired certificates.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

86717—Fixed an issue where QoS statistics for a specific interface were empty after a device reboot.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

86613—Fixed an issue where the General Settings dialog for Device > Setup > Management did not resize correctly when the Login Banner contained a large amount of text.

> Minor Change – Testing associated with the login banner requirement (FTA_TAB.1) addresses the ability of the administrator to configure the banner and confirms the banner is displayed for each method of access specified in the TSS. Testing does not cover maximum lengths of login banner or issues displaying long banner messages. Therefore, this issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

86488—Fixed an issue where predefined Application Usage Risk Trend graphs (Monitor > Reports > PDF Summary Reports) did not display lines between contiguous dots as expected.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

86395—Fixed an issue where the administrator could not manually type the Ethernet interface name in a NAT policy in Panorama.

> Minor Change – This is a Panorama issue. Panorama is not covered in the scope of the evaluation.

85961—Fixed an issue that occurred when using the Panorama template stack where the configuration (gear) icon displayed in the wrong location (next to Panorama servers in the template stack).

> Minor Change – This is a Panorama issue. Panorama is not covered in the scope of the evaluation.

85882—Fixed an issue where improperly formatted API calls to Panorama caused one of the system daemons to stop responding.

> Minor Change – This is a Panorama issue. Panorama is not covered in the scope of the evaluation.

85602—Enhanced logging for events where long CLI system commands would timeout. For example, when generating a tech-support file.

> Minor Change – The use of the CLI for administration of the TOE is outside the scope of evaluation. As such, this issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

85426—Fixed a cosmetic issue where the log action for the interzone-default Security policy rule was incorrect in session detail (session to be logged at end) when the default log action was overridden by the user.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

85320—Fixed an issue where a process (cryptod) stopped responding when attempting to use SSH to access a firewall that rebooted into maintenance mode after the master key was allowed to expire. With this fix, administrators can use SSH to access the firewall without causing the cryptod process to fail even after a firewall reboots to maintenance mode after the master key expires.

> Minor Change – Use of SSH is outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

84911—Fixed an issue where an error was displayed when saving the NFS partition configuration on a Panorama virtual appliance.

> Minor Change – This is a Panorama issue. Panorama is not covered in the scope of the evaluation.

84695—Fixed an issue where GlobalProtect was not appropriately indicated on the interface tab when it is configured on a loopback interface.

> Minor Change – GlobalProtect is outside the scope of evaluation. This issue is not security relevant and results in no changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

84414—Fixed an issue on the PA-7050 firewall where after deleting a HIP log forwarding profile a false warning would appear during a commit.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

84143—Enhancement made to allow administrators to include the application field and URL field in custom response pages.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

83086—Fixed an issue where the output of the show dos-protection <zone-name> blocked source command didn't display the correct data for the requested zone.

> Minor Change – The use of the CLI for administration of the TOE is outside the scope of evaluation. As such, this issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

82524—Fixed an issue where a custom report with Group By Source User option did not include all data when the Source User field was empty.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

82493—Fixed an issue so that the firewall performs NAT translations on IP addresses in an SCCP packet by doing a second NAT policy lookup instead of using a NAT policy for the current session.

> Minor Change – The only aspect of NAT covered in the scope of evaluation is support for NAT traversal as part of IKEv2. Therefore, this issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

82322—Added an enhancement to the PAN-OS routing engine for BGP routing protocol to remove a varying AS number preceded by a static AS number in the AS_PATH attribute.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

82106—Fixed an issue where repetitive logging of inconsequential debug messages caused the snmpd.log file to reach its maximum file size and prevent further logging. With this fix, these inconsequential debug messages are no longer written to the log file.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

80336—Fixed an issue where Panorama custom report filenames that included a period (".") character resulted in empty reports. With this fix, reports are generated as expected for custom report filenames that include a period so long as the period is not the first character in the filename.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

77273—Fixed an issue where importing a certificate with the same subject name as an existing certificate failed. With this fix, you can import a certificate that uses the same subject name as an existing certificate.

> Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.

64717—Fixed an issue where an HA configuration did not correctly synchronize between firewalls when configured on Panorama and pushed to the firewalls.

> Minor Change – This relates to High Availability (HA) configurations, which are not covered in the scope of the evaluation.

42851—Fixed a performance issue with commit requests related to IKE configuration parsing. Also fixed cosmetic IKE validation messages displayed during the commit process, such as during a commit when the IKE gateway configuration was binded to an interface without an IP address. With this fix, the correct error message is displayed (IKE gateway <gw-name> used local interface <interface> which has no IP address. Configuration is invalid.)

Minor Change – This issue is not security relevant, does not result in any changes to the ST or guidance documentation and has no effect on the result of any Assurance Activity test.