

UNCLASSIFIED



PALO ALTO NETWORKS STIG REVISION HISTORY

01 July 2026

Developed by DISA for the DOD

UNCLASSIFIED

REVISION HISTORY		
Document Revised	Description of Change	Release Date
- Palo Alto Networks NDM STIG, V3R3	Palo Alto Networks NDM STIG, V3R4: - PANW-NM-000144 - Rule number updated due to changes in content management system. - PANW-NM-999999 - Added unsupported software requirement to sunset the entire Palo Alto STIG.	01 July 2026
- Palo Alto Networks ALG STIG, V3R3	Palo Alto Networks ALG STIG, V3R4: - PANW-AG-000102 - Updated Rule, Vul Discussion, Check, and Fix.	02 April 2025
- Palo Alto Networks NDM STIG, V3R2	Palo Alto Networks NDM STIG, V3R3: - PANW-NM-000015, PANW-NM-000136 - Updated Check and Fix. - PANW-NM-000047 - Removed from STIG. LDAP is used and does not apply to account of last resort. - PANW-NM-000048 - Updated Vul Discussion, Check, and Fix. - PANW-NM-000046, PANW-NM-000059 - Rule numbers updated due to changes in content management system.	02 April 2025
- Palo Alto Networks ALG STIG, V3R2	Palo Alto Networks ALG STIG, V3R3: - PANW-AG-000120 - Updated the Check Text to provide an alternative to verifying the symbols exist.	30 January 2025
- Palo Alto Networks IDPS STIG, V3R1	Palo Alto Networks IDPS STIG, V3R2: - PANW-IP-000030 - Updated Discussion, Check Text, and Fix Text. - PANW-IP-000033 - Updated the CCI. - PANW-IP-000010 - Rule number updated due to changes in content management system.	30 January 2025
- Palo Alto Networks ALG STIG, V3R1	Palo Alto Networks ALG STIG, V3R2: - PANW-AG-000047 - Updated Check. - PANW-AG-000102 - Updated Title and Check. - PANW-AG-000121 - Updated Title, Discussion, and Check.	24 October 2024
- Palo Alto Networks NDM STIG, V3R1	Palo Alto Networks NDM STIG, V3R2: - PANW-NM-000048 - Added new requirement.	24 October 2024
- Palo Alto Networks ALG STIG, V2R4	Palo Alto Networks ALG STIG, V3R1: - PANW-AG-000047, PANW-AG-000049, PANW-AG-000060, PANW-AG-000065, PANW-AG-000102, PANW-AG-000107 -	24 July 2024

REVISION HISTORY		
Document Revised	Description of Change	Release Date
	<p>Updated based on NIST SP 800-53 Rev. 5 changes.</p> <ul style="list-style-type: none"> - Because this is a major revision, version numbers were incremented to the next whole number. - Rule numbers updated throughout due to changes in content management system. 	
- Palo Alto Networks IDPS STIG, V2R3	<p>Palo Alto Networks IDPS STIG, V3R1:</p> <ul style="list-style-type: none"> - PANW-IP-000018, PANW-IP-000024, PANW-IP-000029, PANW-IP-000041, PANW-IP-000043 - Updated based on NIST SP 800-53 Rev. 5 changes. - Because this is a major revision, version numbers were incremented to the next whole number. - Rule numbers updated throughout due to changes in content management system. 	24 July 2024
- Palo Alto Networks NDM STIG, V2R2	<p>Palo Alto Networks NDM STIG, V3R1:</p> <ul style="list-style-type: none"> - PANW-NM-000053, PANW-NM-000055, PANW-NM-000056, PANW-NM-000057, PANW-NM-000058, PANW-NM-000059, PANW-NM-000097, PANW-NM-000098, PANW-NM-000099, PANW-NM-000100, PANW-NM-000110, PANW-NM-000131, PANW-NM-000136 - Updated based on NIST SP 800-53 Rev. 5 changes. - PANW-NM-000114 - Removed based on NIST SP 800-53 Rev. 5 changes. - Because this is a major revision, version numbers were incremented to the next whole number. - Rule numbers updated throughout due to changes in content management system. 	24 July 2024
- Palo Alto Networks ALG STIG, V2R3	<p>Palo Alto Networks ALG STIG, V2R4:</p> <ul style="list-style-type: none"> - PANW-NM-000047 - Clarified that DOD requires zone protection on the egress interface to protect against the DOD system being used to launch an attack on external systems. - PANW-AG-000102 - Updated requirement to clarify compliance with PAN Zone Protection recommendations and clarified the difference 	24 January 2024

REVISION HISTORY		
Document Revised	Description of Change	Release Date
	between this requirement and PAN-AG-000047.	
- Palo Alto Networks NDM STIG, V2R1	Palo Alto Networks NDM STIG, V2R2 - PANW-NM-000075 - Corrected the check and fix to address the requirement that the neither the SA nor the Cryptographic Administrator can be the Audit Administrator.	27 October 2022
- Palo Alto Networks ALG STIG, V2R2	Palo Alto Networks ALG STIG, V2R3 - PANW-AG-000148 - Updated to reflect this is not a finding if the protocol is not used in the implementation.	27 October 2022
- Palo Alto Networks IDPS STIG, V2R2	Palo Alto Networks IDPS STIG, V2R3 - PANW-IP-000033 - Updated check and fix method for creating the vulnerability profile.	27 October 2022
- Palo Alto Networks NDM STIG, V1R4	DISA migrated the Palo Alto Networks NDM STIG to a new content management system. The new content management system renumbered all Groups (V-numbers) and Rules (SV-numbers). With the new Group and Rule numbers, DISA incremented the version numbers from V1R4 to V2R1. Palo Alto Networks NDM STIG, V2R1 - PANW-NM-000023, PANW-NM-000042, PANW-NM-000054, PANW-NM-000062, PANW-NM-000063 - Requirement was removed from parent SRG. - PANW-NM-000075, PANW-NM-000092, PANW-NM-000096, PANW-NM-000098, PANW-NM-000099, PANW-NM-000110, PANW-NM-000114, PANW-NM-000143 - Updated CCI information.	27 April 2022
- Palo Alto Networks ALG STIG, V2R1	Palo Alto Networks ALG STIG, V2R2 - PANW-AG-000102 - Updated discussion, added a new finding statement to check, and updated fix.	23 July 2021
- Palo Alto Networks IDPS STIG, V2R1	Palo Alto Networks IDPS STIG, V2R2 - PANW-IP-000007 - Removed FQDN as an option in the fix text for consistency with the check and discussion. - PANW-IP-000020 - Changed all AV PA STIGs to state: If the "Action" is anything	23 July 2021

REVISION HISTORY		
Document Revised	Description of Change	Release Date
	other than "drop" or "reset-both", this is a finding.	
- Palo Alto Networks ALG STIG, V1R5	<p>- DISA migrated the Palo Alto Networks STIGs to a new content management system. The new content management system renumbered all Groups (V-numbers) and Rules (SV-numbers). With the new Group and Rule numbers, DISA incremented the version numbers from V1R4 and V1R5 to V2R1.</p> <p>Palo Alto Networks ALG STIG, V2R1: PANW-AG-000062, PANW-AG-000063, PANW-AG-000073, PANW-AG-000074 - Changed check and fix action. Changed "Action" setting value to "drop" or "reset-both".</p>	23 October 2020
- Palo Alto Networks IDPS STIG, V1R4	<p>- DISA migrated the Palo Alto Networks STIGs to a new content management system. The new content management system renumbered all Groups (V-numbers) and Rules (SV-numbers). With the new Group and Rule numbers, DISA incremented the version numbers from V1R4 and V1R5 to V2R1.</p> <p>Palo Alto Networks ALG STIG, V2R1: PANW-AG-000062, PANW-AG-000063, PANW-AG-000073, PANW-AG-000074 - Changed check and fix action. Changed "Action" setting value to "drop" or "reset-both".</p>	23 October 2020
- Palo Alto Networks ALG STIG, V1R4	<p>Palo Alto Networks ALG STIG, V1R5: - V-62579, V-62581 - Revised content to use either Drop or reset-both.</p>	24 January 2020
- Palo Alto Networks IDPS STIG, V1R3	<p>Palo Alto Networks IDPS STIG, V1R4: - V-62651 - Changed the wording to allow the info level to be omitted when packet captures are needed. - V-62661, V-62647 - Revised to use either Drop or reset-both. - V-62663 – Modified requirement to replace SCA with SA in rule title.</p>	24 January 2020
- Palo Alto Networks NDM STIG, V1R3	<p>Palo Alto Networks NDM STIG, V1R4:</p>	24 January 2020

REVISION HISTORY		
Document Revised	Description of Change	Release Date
	- V-62765 - According to the NIST evaluation, if the Palo Alto is in Common Criteria mode (configured to use NIST FIPS 140-2 modules for cryptographic functions), it will use HTTP OCSP with TLS. Revised text to reflect this.	
- Palo Alto Networks IDPS STIG, V1R2	Palo Alto Networks IDPS STIG, V1R3: - V-62677 - Changed fix text to: In the "Source" tab, for "Zone", select the "External zone, for Source Address", select "Any". In the "Destination" tab, "Zone", select "Internal zone, for Destination Address", select "Any".	25 October 2019
- Palo Alto Networks ALG STIG, V1R3	Palo Alto Networks ALG STIG, V1R4: - V-62571 - Updated the Vulnerability Discussion, Check content, and Fix text removed incorrect steps with steps to add anti-spoofing for IP to each zone policy. - V-62579 - In the Check content and Fix text changed "block" to "drop". Block is not a selection on this screen. - V-62581 - In the Vulnerability Discussion, Check content, and Fix text changed "block" to "drop". Block is not a selection on this screen. - V-62585 - In the Rule, Vulnerability Discussion, Check content, and Fix text changed "block" to "drop". Block is not a selection on this screen. - V-62587 - In the Vulnerability Discussion, Check content, and Fix text changed "block" to "drop". Block is not a selection on this screen.	25 January 2019
- Palo Alto Networks IDPS STIG, V1R1	Palo Alto Networks IDPS STIG, V1R2: - V-62657 and V-62661 - In the Rule, Vulnerability Discussion, Check content, and Fix text change "block" to "drop". Block is not a selection on this screen.	25 January 2019
- Palo Alto Networks ALG STIG, V1R2	Palo Alto Networks ALG STIG, V1R3: - Updated V-62549, V-62551, V-62553, V-62633, and V-62635 – Updated fips-mode commands in check and fix to add a reference to fips-cc command, which is used in later version. These versions were not the tested versions that are in scope for this document. Please note that	28 July 2017

REVISION HISTORY		
Document Revised	Description of Change	Release Date
	minor updates cannot accommodate major changes in the software.	
- Palo Alto Networks NDM STIG, V1R2	Palo Alto Networks NDM STIG, V1R3: - Updated V-62721 fips-mode commands in check and fix to either add a note that they have changed in later version or change the commands to reflect current command sequence.	28 July 2017
- Palo Alto Networks ALG STIG, V1R1	Palo Alto Networks ALG STIG, V1R2: - Updated V-62603 fix to indicate that threat name field is a free-text entry field. - Updated V-62549, V-62551, V-62553, V-62633, and V-62635 to add a check and fix for PAN OS 7.0. - Updated V-62601 to remove second sentence in the vulnerability discussion and to correct fix (zones are reversed). - Updated V-62561 to correct the check, fix, and vulnerability discussion. - Updated V-62567 check and fix to correct the Packet Based Attack Protection options. - Updated V-62577 fix to include a manual process. - Updated V-62579 check to change "affects" to "allows" in the sentence, "For any Security Policy that affects traffic between Zones (interzone), view the "Profile" column." - Updated V-62593 to remove the last two sentences from the vulnerability discussion to improve clarity. - Updated V-62595 to remove the last two sentences from the vulnerability discussion to improved clarity. - Updated V-62597 in the check to state, "Go to Device >> Log Settings >> System". - Updated V-62627 to correct check and fix to include zone protection.	22 July 2016
- Palo Alto Networks NDM STIG, V1R1	Palo Alto Networks NDM STIG, V1R2: - Updated V-62773 check to exclude the emergency administration account.	22 July 2016
- Palo Alto Network STIG, V1R1	- Initial Release	01 December 2015