

UNCLASSIFIED



VIRTUAL PRIVATE NETWORK (VPN) SRG REVISION HISTORY

Version 3, Release 1

24 July 2024

Developed by DISA for the DOD

UNCLASSIFIED

REVISION HISTORY			
Revision Number	Document Revised	Description of Change	Release Date
V3R1	- VPN SRG, V2R6	<ul style="list-style-type: none"> - SRG-NET-000145-VPN-000510, SRG-NET-000147-VPN-000520, SRG-NET-000147-VPN-000530, SRG-NET-000337-VPN-001290, SRG-NET-000337-VPN-001300, SRG-NET-000522-VPN-002320, SRG-NET-000345-VPN-002430, SRG-NET-000580-VPN-002431, SRG-NET-000580-VPN-002432, SRG-NET-000705-VPN-000110, SRG-NET-000715-VPN-000120, SRG-NET-000760-VPN-000160 - Updated based on NIST SP 800-53 Rev. 5 changes. - SRG-NET-000333-VPN-001250 - Changed status to NA 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
V2R6	- VPN SRG, V2R5	<ul style="list-style-type: none"> - SRG-NET-000019-VPN-002435 - Added new requirement to limit authenticated client sessions to initial session source IP. - SRG-NET-000230-VPN-002436 - Added new requirement to mandate use of Always On VPN connections for remote computing. - SRG-NET-000337-VPN-001290 - Clarified that the IPsec security association must be renegotiated after eight hours or less. - SRG-NET-000337-VPN-001300 - Clarified that the IKE security association must be renegotiated after eight hours or less. - SRG-NET-000345-VPN-002430 - Added new requirement to implement a local cache of revocation data to support path discovery and validation. - SRG-NET-000355-VPN-002433 - Added new requirement to accept only end entity certificates (user or machine) issued by DOD PKI or DOD-approved PKI Certification Authorities (CAs) for the establishment of VPN sessions. - SRG-NET-000512-VPN-002230 - Removed requirement. 	08 April 2024

REVISION HISTORY			
Revision Number	Document Revised	Description of Change	Release Date
		<ul style="list-style-type: none"> - SRG-NET-000580-VPN-002431 - Added new requirement for OCSP to ensure revoked user certificates are prohibited from establishing an allowed session. - SRG-NET-000580-VPN-002432 - Added new requirement to configure OCSP to ensure revoked machine certificates are prohibited from establishing an allowed session. - Rule numbers updated throughout due to changes in content management system. 	
V2R5	- VPN SRG, V2R4	<ul style="list-style-type: none"> - Rule numbers updated throughout due to changes in content management system. - SRG-NET-000525-VPN-002330 - Changed requirement to set minimum AES key size to 256. Updated to include FIPS 140-3. - SRG-NET-000074-VPN-000250 - Changed requirement to set minimum Diffie-Hellman group to 16. - SRG-NET-000063-VPN-000220, SRG-NET-000230-VPN-000780 - Changed requirement to set minimum SHA2 size to 384. - SRG-NET-000371-VPN-001640 - Changed severity to CAT I. Addressed issues of STIG style compliance. - SRG-NET-000400-VPN-001940 - Fixed misspelling in Rule Title. 	07 June 2023
V2R4	- VPN SRG, V2R3	<ul style="list-style-type: none"> - SRG-NET-000062-VPN-000200 - Updated reference to NIST SP 800-52 Rev 2. - SRG-NET-000063-VPN-000210 - Added TLS to the Requirement. - SRG-NET-000063-VPN-000220, SRG-NET-000371-VPN-001650 - Changed to require SHA-2. - SRG-NET-000074-VPN-000250 - Removed the example of DH implementation in the Fix text and corrected various typos. - SRG-NET-000168-VPN-000600, SRG-NET-000230-VPN-000780, SRG-NET-000400-VPN-001940 - Removed references to SHA-1 and updated to require SHA-2 or 	27 October 2021

REVISION HISTORY			
Revision Number	Document Revised	Description of Change	Release Date
		<p>above. Changed SP800-131Ar1 to SP800-131Ar2.</p> <ul style="list-style-type: none"> - SRG-NET-000213-VPN-000721 - Added requirement to perform risk assessment and document session inactivity termination period and document in the SSP. - SRG-NET-000234-VPN-000810 - Removed statement about mitigation to CAT III. - SRG-NET-000522-VPN-002320 - Added to Discussion: "NIST SP 800-52 Rev 2 provides guidance for using pre-shared keys with VPN gateways. PSKs may only be used in networks where both the client and server belong to the same organization." - SRG-NET-000550-VPN-002360 - Added acronyms in check and fix. - SRG-NET-000565-VPN-002390, SRG-NET-000565-VPN-002400 - Updated with NSS information. - SRG-NET-000585-VPN-002420 - Removed requirement. 	
V2R3	- VPN SRG, V2R2	<ul style="list-style-type: none"> - SRG-NET-000019-VPN-000040 -Changed finding statement to read: If the IPsec VPN Gateway does not use Encapsulating Security Payload (ESP) in tunnel mode for establishing secured paths to transport traffic between the organizations sites or between a gateway and remote end-stations, this is a finding." - SRG-NET-000375-VPN-001690 - removed "Encapsulating Security Payload" in fix text. 	23 April 2021
V2R2	- VPN SRG, V2R1	<ul style="list-style-type: none"> - SRG-NET-000375-VPN-001690 - Changed "must use" to "does not enable" in the Check to make a finding if the encapsulation is not enabled. 	22 January 2021
V2R1	- VPN SRG, V1R1	<ul style="list-style-type: none"> - DISA migrated the VPN SRG 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 number from V1R1 to V2R1. 	23 October 2020

REVISION HISTORY			
Revision Number	Document Revised	Description of Change	Release Date
		- SRG-NET-000341-VPN-001350, SRG-NET-000342-VPN-001360 - Clarified this requirement is for user connectivity using the VPN function of the product and uses CAC/PKI instead of PIV.	
V1R1	- NA	- Initial Release.	19 July 2019