Selecting and Hardening Remote Access VPN Solutions

Virtual Private Networks (VPNs) allow users to remotely connect to a corporate network via a secure tunnel. Through this tunnel, users can take advantage of the internal services and protections normally offered to on-site users, such as email/collaboration tools, sensitive document repositories, and perimeter firewalls and gateways. Because remote access VPN servers are entry points into protected networks, they are targets for adversaries. This joint NSA-CISA information sheet provides guidance on:

Selecting standards-based VPNs from reputable vendors that have a proven track record of quickly remediating known vulnerabilities and following best practices for using strong authentication credentials.

Hardening the VPN against compromise by reducing the VPN server's attack surface through:

Configuring strong cryptography and authentication

Running only strictly necessary features

Protecting and monitoring access to and from the VPN

Active Exploitation

Multiple nation-state Advanced Persistent Threat (APT) actors have exploited public Common Vulnerabilities and Exposures (CVEs) to compromise vulnerable VPN devices [1], [2], [3]. In some cases, exploit code is freely available online. Exploitation of these public CVEs can enable a malicious actor to perform:

- Credential harvesting
- Remote code execution of arbitrary code on the VPN device

- Cryptographic weakening of encrypted traffic sessions
- Hijacking of encrypted traffic sessions
- Arbitrary reads of sensitive data (e.g., configurations, credentials, keys) from the device

These effects usually lead to further malicious access through the VPN, resulting in large-scale compromise of the corporate network or identity infrastructure and sometimes of separate services as well.

Considerations for Selecting Remote Access VPNs

When choosing a remote access VPN, consider these recommendations:

- Avoid selecting non-standard VPN solutions, including a class of products referred to as Secure Sockets Layer/Transport Layer Security (SSL/TLS) VPNs. These products include custom, non-standard features to tunnel traffic via TLS. Using custom or non-standard features creates additional risk exposure, even when the TLS parameters used by the products are secure. NSA and CISA recommend standardized Internet Key Exchange/Internet Protocol Security (IKE/IPsec) VPNs that have been validated against standardized security requirements for VPNs.
    - Refer to the National Information Assurance Partnership (NIAP) Product Compliant List (PCL) for validated VPNs (Conformance Claim: EP_VPN_GW or MOD_VPNGW) [4]. NIAP-certified devices are rigorously tested by third-party labs against well-defined security features and requirements. Proprietary protocols may or may not have defined security requirements and may not have been analyzed and tested as much as standards-based protocols.
- Carefully read vendor documentation to ensure potential products support IKE/IPsec VPNs. Documentation for some products may not provide comprehensive information about the protocols they support when establishing VPN tunnels. Avoid products that do not clearly identify the standards they follow or claim to use proprietary methods to establish VPNs.
- Identify whether the product uses SSL/TLS in a proprietary or non-standards-based VPN protocol when unable to establish an IKE/IPsec VPN. Understand the circumstances that would cause the failure of IKE/IPsec negotiations. Disable the SSL/TLS proprietary or non-standards-based VPN fallback, if possible.

- Ensure that potential products use FIPS-validated cryptographic modules and can be configured to use only approved cryptographic algorithms [5].
- Check that a product supports strong authentication credentials and protocols and disables weak credentials and protocols by default. Plan to use multi-factor authentication and select products that support the credentials to be used [6].
- Research and select a vendor with a proven track record of supporting products via regular software updates and quickly remediating known vulnerabilities. Ensure support timeframes cover the entire expected usage lifetime of the product; replace the product before it becomes end-of-life.
- Request and validate a product's Software Bill of Materials (SBOM) so the risk of the underlying software components can be adjudicated [7]. Many vendors use outdated versions of open-source software in their products, including many with known vulnerabilities, so this risk is critical to manage.
- Ensure the product has a robust method to validate the integrity of its own code and regularly perform code validation. As a security device on a network's perimeter, VPN gateways are popular targets for an adversary. Without the ability to validate the integrity of a device, it is often impossible to detect intrusions.
- Ensure the product includes protections against intrusions, such as:
    - Use of signed binaries or firmware images
    - A secure boot process that verifies boot code before it runs
    - Integrity validation of runtime processes and files
- Understand the risk of not being able to inspect the product on your own. Some VPN vendors encrypt the devices in a manner that prevents timely incident response. Products that do not allow for full inspection of the device by the product owner introduce added risk and can result in the manufacturer being a product support choke point. Delays in the incident response process can allow sophisticated actors the time they need to cover their tracks.
- Review additional features of the prospective device against your organization's risk appetite. While many additional features, such as remotely accessible administrative pages or web-based access to internal services, can be useful, such features carry risk because they increase the product's attack surface and are often targeted and exploited by adversaries. Choose products that focus on protecting the core VPN functionality and do not have many additional features, or—at a minimum—ensure that additional features can be disabled and, preferably, are disabled by default.

U/OO/186992-21 | PP-21-1362 | SEP 2021 Ver. 1.0

Active Hardening

Once the selected VPN solution is deployed, the following actions will further harden the VPN against compromise.

Require only strong, approved cryptographic protocols, algorithms, and authentication credentials:

- National Security Systems (NSS) are required to use the algorithms in the NSA-Approved Commercial National Security Algorithm (CNSA) Suite (see Annex B of Committee on National Security Systems Policy (CNSSP) 15) [8]. Non-NSS U.S. Government systems are required to use the algorithms as specified by NIST, which includes the algorithms approved to protect NSS. NSA and CISA recommend that other systems also use the cryptographic algorithms included in the CNSA Suite.
- Configure the VPN to use IKE/IPsec and disable SSL/TLS VPN functionality and fallback options if feasible.
    - For IKE/IPsec VPNs, CNSSP 15-compliant cryptographic algorithms are required for IKE and Internet Security Association and Key Management Protocol (ISAKMP) for NSS [9], [10]. CNSSP 15 requirements are explained in the draft IETF document Commercial National Security Algorithm (CNSA) Suite Cryptography for Internet Protocol Security (IPsec) and NIST requirements for other U.S. Government systems are in SP 800-77rev1 [11], [12].
    - If SSL/TLS VPNs must be used, require the remote access VPN to only use strong TLS (i.e., TLS 1.2 or later) and reject all earlier versions of SSL and TLS [13]. Other CNSSP 15 requirements for NSS are explained in the draft IETF document Commercial National Security Algorithm (CNSA) Suite Profile for TLS and DTLS 1.2 and 1.3 and NIST requirements for other U.S. Government systems are in SP 800-52rev2 [14], [15].
- For server authentication, use trusted server certificates and update them periodically (e.g., every year). Discourage the use of self-signed and wildcard certificates because they should not be trusted or are trusted for an overly broad scope, respectively.
- If available, use client certificate authentication. Some VPN solutions may support client certificate authentication for remote clients attempting to access

the VPN—such as by use of a smartcard—which is a stronger form of authentication than using passwords. Whenever supported, use client certificate authentication so that the VPN prohibits connections from clients that do not present valid, trusted certificates.

- If client certificate authentication is not available, then use other supported forms of multi-factor authentication to prevent malicious actors from authenticating with compromised passwords [6].

Reduce the remote access VPN attack surface:

- Immediately apply patches and updates to mitigate known vulnerabilities that are often rapidly exploited (sometimes within less than 24 hours) [16], [17].
  - Explicitly follow all vendor patch guidance. For example, if a vendor, as part of regular patch guidance, recommends changing all passwords that are associated with the device, then the organization should be ready to change every single password within their infrastructure, without exception.
  - When performing a major update or updating from a vulnerable version that is known to have been exploited, consider:
    - Updating VPN user, administrator, and service account credentials.
    - Revoking and generating new VPN server keys and certificates, which may require redistributing VPN connection information to users.
    - Reviewing accounts to ensure that all accounts are expected and needed for remote access. Anomalous accounts can indicate a compromise.
- Restrict external access to the VPN device by port and protocol:
  - For IKE/IPsec VPNs, only allow UDP ports 500 and 4500 and Encapsulating Security Payload.
  - For SSL/TLS VPNs, only allow TCP port 443 or other necessary ports and protocols.
- If possible, allowlist known VPN peer IP addresses and block all others. Note: this may be difficult if it is expected that unknown peer IP addresses will be accessing the VPN.

- Disable non-VPN-related functionality and advanced features that are more likely to have vulnerabilities. Features such as web administration, Remote Desktop Protocol, Secure Shell, and file sharing are convenient, but not necessary for the operation of remote access VPNs.
- Restrict management interface access via the VPN. Malicious cyber actors that manage to compromise administrator credentials could try to authenticate into management interfaces and maliciously perform privileged operations. Do not allow VPN administrators to log into the management interface via the remote access VPN; instead, restrict administrative access to dedicated internal management networks. Investigate any attempts to use administrator credentials to access the remote access VPN [18].

Protect and monitor access to and from the VPN:

- Deploy an intrusion prevention system in front of the remote access VPN to inspect session negotiations and detect unwanted VPN traffic.
- Use Web Application Firewalls (WAFs). Some WAFs that are compatible with TLS VPN traffic may detect and block web application exploitation attempts, such as specially crafted Hypertext Transfer Protocol (HTTP) requests containing malformed strings that exploit VPN vulnerabilities. Work with WAF and VPN vendors to assess compatibility and deploy WAFs for protection, whenever supported.
- Enable enhanced web application security. Some remote access VPN solutions may provide features for enhanced web application security to prevent compromise attempts against the VPN web applications, such as malicious reuse of users' previous session information to bypass authentication. Enable these features whenever supported.
- Employ appropriate network segmentation and restrictions to limit access, so only services that are needed remotely are accessible via the VPN. Use additional attributes (such as device information, environment of originating access request, strength of credentials, and access path risks) when making access decisions [19], [20].
- Enable local and remote logging to record and track VPN user activity, including authentication and access attempts, configuration changes, and network traffic metadata. Continuously monitor and conduct analytics on all logs to look for

unauthorized access, malicious configuration changes, anomalous network traffic, and other indicators of compromise [21].

Secure the network entrance

Remote access VPNs are entryways into corporate networks and all the sensitive data and services they have. This direct access makes them prized targets for malicious actors. Keep malicious actors out by selecting a secure, standards-based VPN and hardening its attack surface. This is essential for ensuring a network's cybersecurity.▪

Works cited

[1] National Security Agency (2019), Mitigating Recent VPN Vulnerabilities. Available: https://www.nsa.gov/cybersecurity-guidance

[2] National Cyber Security Center, Cybersecurity and Infrastructure Security Agency, Federal Bureau of Investigation, and National Security Agency (2021), Advisory: Further TTPs associated with SVR cyber actors. Available: https://www.ncsc.gov.uk/files/Advisory Further TTPs associated with SVR cyber actors.pdf

[3] National Security Agency (2020), Chinese State-Sponsored Actors Exploit Publicly Known Vulnerabilities. Available: https://www.nsa.gov/cybersecurity-guidance

[4] National Information Assurance Partnership (NIAP) (2021), NIAP Product Compliant List (PCL). Available: https://www.niap-ccevs.org/Product/PCL.cfm

[5] National Institute of Standards and Technology (2021), Cryptographic Module Validation Program CMVP. Available: https://csrc.nist.gov/projects/cryptographic-module-validation-program

[6] National Security Agency (2019), Transition to Multi-factor Authentication. Available: https://www.nsa.gov/cybersecurity-guidance

[7] National Telecommunications and Information Administration (2021), Software Bill of Materials. Available: https://www.ntia.gov/SBOM

[8] Committee on National Security Systems (CNSS) (2016), CNSS Policy 15. Available: https://www.cnss.gov/CNSS/issuances/Policies.cfm

[9] National Security Agency (2020), Securing IPsec Virtual Private Networks. Available: https://www.nsa.gov/cybersecurity-guidance

[10] National Security Agency (2020), Configuring IPsec Virtual Private Networks. Available: https://www.nsa.gov/cybersecurity-guidance

[11] Corcoran, Jenkins, NSA (2021), Commercial National Security Algorithm (CNSA) Suite Cryptography for Internet Protocol Security (IPsec). Available: https://datatracker.ietf.org/doc/html/draft-corcoran-cnsa-ipsec-profile

[12] National Institute for Standards and Technology (2020), SP 800-77 Rev. 1: Guide to IPsec VPNs. Available: https://csrc.nist.gov/publications/detail/sp/800-77/rev-1/final

[13] National Security Agency (2021), Eliminating Obsolete Transport Layer Security (TLS) Protocol Configurations. Available: https://www.nsa.gov/cybersecurity-guidance

[14] Cooley, D, NSA (2021), Commercial National Security Algorithm (CNSA) Suite Profile for TLS and DTLS 1.2 and 1.3. Available: https://datatracker.ietf.org/doc/html/draft-cooley-cnsa-dtls-tls-profile

[15] National Institute for Standards and Technology (2020), SP 800-52 Rev. 2: Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations. Available: https://csrc.nist.gov/publications/detail/sp/800-52/rev-2/final

[16] National Security Agency (2019), Update and Upgrade Software Immediately. Available: https://www.nsa.gov/cybersecurity-guidance

[17] Cybersecurity and Infrastructure Security Agency (2020), Enterprise VPN Security. Available: https://us-cert.cisa.gov/ncas/alerts/aa20-073a

[18] National Security Agency (2020), Performing Out-of-Band Network Management. Available: https://www.nsa.gov/cybersecurity-guidance

[19] National Security Agency (2019), Segment Networks and Deploy Application-Aware Defenses. Available: https://www.nsa.gov/cybersecurity-guidance

[20] National Security Agency (2021), Embracing a Zero Trust Security Model. Available: https://www.nsa.gov/cybersecurity-guidance

[21] National Security Agency (2019), Continuously Hunt for Network Intrusions. Available: https://www.nsa.gov/cybersecurity-guidance

Disclaimer of endorsement

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

Purpose

NSA and CISA developed this document in furtherance of their respective cybersecurity missions, including their responsibilities to develop and issue cybersecurity specifications and mitigations. This information may be shared broadly to reach all appropriate stakeholders.

Contact

Client Requirements / Inquiries: Cybersecurity Requirements Center, 410-854-4200, Cybersecurity_Requests@nsa.gov

Media Inquiries / Press Desk:

- NSA Media Relations, 443-634-0721, MediaRelations@nsa.gov
- CISA Media Relations, 703-235-2010, CISAMedia@cisa.dhs.gov