Securing IPsec Virtual Private Networks

Many organizations currently utilize IP Security (IPsec) Virtual Private Networks (VPNs) to connect remote sites and enable telework capabilities. These connections use cryptography to protect sensitive information that traverses untrusted networks. To protect this traffic and ensure data confidentiality, it is critical that these VPNs use strong cryptography. This guidance identifies common VPN misconfigurations and vulnerabilities.[1]

Maintaining a secure VPN tunnel can be complex and requires regular maintenance. To maintain a secure VPN, network administrators should perform the following tasks on a regular basis:

- Reduce the VPN gateway attack surface
- Verify that cryptographic algorithms are Committee on National Security Systems Policy (CNSSP) 15-compliant
- Avoid using default VPN settings
- Remove unused or non-compliant cryptography suites
- Apply vendor-provided updates (i.e. patches) for VPN gateways and clients

Reduce the VPN gateway attack surface

VPN gateways tend to be directly accessible from the Internet and are prone to network scanning, brute force attacks, and zero-day vulnerabilities. To mitigate many of these vulnerabilities, network administrators should implement strict traffic filtering rules to limit the ports, protocols, and IP addresses of network traffic to VPN devices. If traffic cannot be filtered to a specific IP address, NSA recommends an Intrusion Prevention System (IPS) in front of the VPN gateway to monitor for undesired IPsec traffic and inspect IPsec session negotiations.

Verify only CNSSP 15-compliant algorithms are in use

All IPsec VPN configurations require at least two items: (1) the Internet Security Association and Key Management Protocol (ISAKMP) or Internet Key Exchange (IKE) policy; and (2) the IPsec policy. If the cryptography on either of these policies is configured to allow obsolete cryptographic algorithms, the entire VPN is at risk and data confidentiality may be lost. Annex B of CNSSP 15 provides guidance on using strong cryptography [1]. As the computing environment evolves and new weaknesses in algorithms are identified, administrators should prepare for cryptographic agility: periodically check CNSSP and NIST guidance for the latest cryptographic requirements, standards, and recommendations.

When configuring **ISAKMP/IKE**, many vendors support having several possible ISAKMP/IKE policies. The device then chooses the strongest matching policy between the remote and local ends of the VPN. Some vendors do this through priority numbers and others through explicit selection. NSA recommends configuring only those policies that strictly use CNSSP 15-compliant algorithms, and removing all others. Also, if priority numbers are used, the strongest ISAKMP/IKE policy should be the highest priority. Many vendors also support configuring multiple **IPsec** policies; however, these policies are normally explicitly configured for a specific VPN. NSA recommends utilizing the strongest FIPS-validated cryptography suites supported by the device.

The best way to verify that existing VPN configurations are using approved cryptographic algorithms is to review the current ISAKMP/IKE and IPsec security associations (SAs). NSA recommends using this approach when reviewing ISAKMP/IKE and IPsec configurations because it displays the exact cryptography settings that were negotiated. Otherwise, administrators may miss connections where a device is selecting a non-compliant algorithm that was a device default or left over from a previous VPN configuration.

If SAs are identified with non-compliant algorithms, administrators should immediately investigate why the VPN negotiated a lower cryptography standard and make appropriate configuration changes. Also, if utilizing pre-shared keys for VPN authentication, NSA recommends that all keys be replaced as they may be compromised.

[1] For detailed instructions on how to securely configure an IPsec VPN, please refer to the "Configuring IPsec Virtual Private Networks" guide at https://www.nsa.gov/cybersecurity-advisories.

Avoid using default VPN settings

Due to the complexity of establishing a VPN, many vendors provide default configurations, automated configuration scripts, or graphical user interface wizards to aid in the deployment of VPNs. These tools take care of setting up the various aspects of a VPN to include ISAKMP/IKE and IPsec policies. However, many will configure a wide range of cryptography suites to ensure compatibility with the remote side of a VPN. NSA recommends avoiding these tools as they may allow undesired cryptography suites. If these tools are used, evaluate all configuration settings that the tool deployed. Administrators should then remove any non-compliant ISAKMP/IKE and IPsec policies. As a best practice, administrators should not utilize any default settings and ensure that all ISAKMP/IKE and IPsec policies are explicitly configured for the CNSSP 15-compliant algorithms.

Remove unused or non-compliant cryptography suites

It is very common for vendors to include extra ISAKMP/IKE and IPsec policies by default. These extra policies may include non-compliant cryptographic algorithms. Leaving extra ISAKMP/IKE and IPsec policies as acceptable policies creates a vulnerability to downgrade attacks. In downgrade attacks, a malicious user or Man-in-the-Middle offers only obsolete cryptography suites and forces the VPN endpoints to negotiate non-compliant cryptography suites. In doing so, it leaves the encrypted VPN vulnerable to decryption. Verifying that only compliant ISAKMP/IKE and IPsec policies are configured and all unused or non-compliant policies are explicitly removed from the configuration mitigates this risk. NSA also recommends periodically validating that only compliant policies are configured as the use of automated tools, graphical interfaces, or user error could reintroduce these non-compliant policies.

Apply vendor-provided updates

After ensuring that all configuration settings are using compliant cryptography suites and removing all non-compliant suites, implement a robust patch management procedure. Over the past several years, multiple vulnerabilities have been released related to IPsec VPNs. Many of these vulnerabilities are only mitigated by routinely applying vendor-provided patches to VPN gateways and clients. Many network equipment vendors allow customers to sign up for notification emails for new security alerts. These notifications are an excellent way to stay up-to-date on relevant out-of-cycle patches.

Protect the essential

VPNs are essential for enabling remote access and securely connecting remote sites, but without proper configuration, patch management, and hardening, VPNs are vulnerable to attack. To ensure that the confidentiality and integrity of a VPN is protected, reduce the VPN gateway attack surface, always use CNSSP 15-compliant and FIPS-validated cryptography suites, avoid using vendor defaults, disable all other cryptography suites, and apply patches in a timely manner.

Works Cited

[1] "CNSSP 15 - Use of Public Standards for Secure Information Sharing." Committee on National Security Systems, 20 October 2016. [Online] Available at: https://www.cnss.gov/CNSS/issuances/Policies.cfm

Related Guidance

- "Mitigating Recent VPN Vulnerabilities." National Security Agency, 2019. [Online] Available at: https://media.defense.gov/2019/Oct/07/2002191601/-1/-1/0/CSA-MITIGATING-RECENT-VPN-VULNERABILITIES.PDF
- "Configuring IPsec Virtual Private Networks." National Security Agency, July 2020. Available at: https://www.nsa.gov/cybersecurity-guidance

Disclaimer of Endorsement

Contact

Client Requirements / General Cybersecurity Inquiries: Cybersecurity Requirements Center, 410-854-4200, Cybersecurity_Requests@nsa.gov
Media inquiries / Press Desk: Media Relations, 443-634-0721, MediaRelations@nsa.gov