National Security Agency | Cybersecurity Information

Configuring IPsec Virtual Private Networks

The recent NSA publication “Securing IPsec Virtual Private Networks” [1] lays out the importance of IP Security (IPsec) Virtual Private Networks (VPNs) and outlines specific recommendations for securing those connections. It is critical that VPNs use strong cryptography. This guidance goes deeper, providing device administrators with specific instructions.[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:

- Limiting access to UDP port 500, UDP port 4500, and ESP.
- When possible, limit accepted traffic to known VPN peer IP addresses. Remote access VPNs present the issue of the remote peer IP address being unknown and therefore it cannot be added to a static filtering rule.
- If traffic cannot be filtered to a specific IP address, NSA recommends an Intrusion Prevent System (IPS) in front of the VPN gateway to monitor for malformed IPsec traffic and inspect IPsec session negotiations. Examples of recommended ACLs and IPS signatures for anomalous ISAKMP/IKE traffic can be found in Appendices A and D.

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. These policies determine how an IPsec tunnel will negotiate phase 1 and phase 2 respectively when establishing the tunnel. If the cryptography on either of these phases is configured to allow weak cryptography, the entire VPN may be at risk, and data confidentiality will be lost.

When configuring ISAKMP/IKE, many vendors support having several possible ISAKMP/IKE policies. The device is then trusted to choose 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 only configuring 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 (for many vendors a priority of “1” is the highest priority). Each ISAKMP/IKE policy includes at least three key components. These components are the Diffie-Hellman algorithm/group, encryption algorithm, and hashing algorithm.

The following is an example of a recommended ISAKMP/IKE setting per CNSSP 15 as of June 2020[2]:

- Diffie-Hellman Group: 16
- Encryption: AES-256
- Hash: SHA-384

[1] For proprietary application layer VPN best practices, refer to NSA’s Cybersecurity Advisory “Mitigating Recent VPN Vulnerabilities.”

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. Similar to ISAKMP/IKE, the IPsec policy contains three key components: (1) the encryption algorithm; (2) hashing algorithm; and (3) the block cipher mode. The following is an example of a recommended IPsec setting per CNSSP 15 as of June 2020[2]:

- Encryption: AES-256
- Hash: SHA-384
- Block Cipher Mode: CBC

The best way to verify that existing VPN configurations are utilizing approved cryptographic algorithms is to review the current ISAKMP/IKE and IPsec security associations (SAs). Appendix B provides a set of common vendor commands to show the current SAs and what cryptographic algorithms were negotiated.

NSA recommends using this approach when reviewing ISAKMP/IKE and IPsec configurations because it will display the exact cryptography settings that were negotiated. On the other hand, if this approach is not followed, reviewing a device's configuration file may miss 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 as to 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 have been compromised due to weak cryptography standards.

Many organizations can detect or even block the use of certain common outdated cryptographic algorithms in IPsec within their networks, such as the Data Encryption Standard (DES), Triple DES (3DES) and Diffie-Hellman groups 1, 2, and 5. For examples on configuring the ISAKMP/IKE and IPsec policies on multiple common vendors, see Appendix C.

Cryptography standards continue to change over time as the computing environment evolves and new weaknesses in algorithms are identified. Administrators should prepare for cryptographic agility and periodically check CNSSP and National Institute of Standards and Technology (NIST) guidance for the latest cryptography requirements, standards, and recommendations.

NSA has observed scanning activity that includes anomalous malformed ISAKMP packets, which most customers should be able to block. The signature for these packets is in Appendix C.

Avoid using default 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 that administrators try avoiding these tools as they may allow more than the desired cryptography suites. If these tools are used, then 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

As previously described, many vendors support having several ISAKMP/IKE and IPsec policies configured on a single device. It is also very common for vendors to include extra ISAKMP/IKE and IPsec policies for compatibility by default or when using automatic configuration tools; however, these extra policies may include non-compliant cryptographic algorithms. Leaving extra ISAKMP/IKE and IPsec policies as acceptable ISAKMP/IKE and IPsec policies creates a vulnerability known as a downgrade attack. This type of attack is where a malicious user or Man-in-the-Middle only offers weak cryptography suites and forces the VPN endpoints to negotiate non-compliant cryptography suites.

In doing so, it leaves the encrypted VPN vulnerable to exploitation, including potential decryption, data modification, and adversarial system access. To mitigate against this vulnerability, administrators should validate that only compliant ISAKMP/IKE and IPsec policies are configured and all unused or non-compliant policies are explicitly removed from the configuration. 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 utilizing compliant cryptography suites and all non-compliant suites are removed, a robust patch management procedure must be implemented. Over the past several years, multiple vulnerabilities have been released related to IPsec VPNs. Many of these vulnerabilities are only mitigated by applying vendor-provided patches. Applying patches to VPN gateways and clients need to be a part of a regular routine. 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 connecting remote sites securely. However, without the proper configuration, patch management, and hardening, VPNs are vulnerable to many different types of attacks. To ensure that the confidentiality and integrity of a VPN is protected, always use CNSSP 15-compliant and FIPS validated cryptography suites, disable all other cryptography suites, and avoid using vendor defaults. Following the steps identified in this paper will ensure the most secure VPN configurations.

Publication Information

Works Cited

[1] “Securing IPsec Virtual Private Networks.” National Security Agency, June 2020. [Online] Available at: https://www.nsa.gov/cybersecurity-guidance

[2] “CNSSP 15 - Use of Public Standards for Secure Information Sharing.” [Online] Available at: https://www.cnss.gov/CNSS/issuances/Policies.cfm

Related Guidance

[1] NSA (2019). Mitigating Recent VPN Vulnerabilities. [Online] Available at: https://media.defense.gov/2019/Oct/07/2002191601/-1/-1/0/CSA-MITIGATING-RECENT-VPN-VULNERABILITIES.PDF

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. This guidance shall not be used for advertising or product endorsement purposes.

Purpose

This document was developed in furtherance of NSA’s cybersecurity missions, including its responsibilities to identify and disseminate threats to National Security Systems, Department of Defense, and Defense Industrial Base information systems, and to develop and issue cybersecurity specifications and mitigations. This information may be shared broadly to reach all appropriate stakeholders.

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

Appendix A: Reducing VPN Gateway Attack Surface Examples

ACL example to limiting ISAKMP traffic to only known peers

Cisco ASA:

```
Access-list deny-ike extended permit udp <source_peer_ip> <destination_peer_ip> eq isakmp
Access-list deny-ike extended permit udp <source_peer_ip> <destination_peer_ip> eq 4500
Access-list deny-ike extended permit esp <source_peer_ip> <destination_peer_ip>
Access-list deny-ike extended deny udp any <destination_peer_ip> eq isakmp
Access-list deny-ike extended deny udp any <destination_peer_ip> eq 4500
Access-list deny-ike extended deny esp any <destination_peer_ip>
```

Juniper SRX:

```
[edit security policies from-zone untrust to-zone trust]
Policy <permit-policy-name> {
        Match {
                source-address <source-peer-ip>;
                destination-address <destination-peer-ip>;
                Application [junos-ike junos-ike-nat];
        }
        Then {
                Permit;
        }
}
Policy <deny-policy-name> {
        Match {
                source-address any
                destination-address <destination-peer-ip>;
                Application [junos-ike junos-ike-nat];
        }
        Then {
                deny;
        }
}
```

Palo Alto Firewalls:

```
[edit rulebase security]
Security {
        Rules
                <permit-rule-name> {
                        From untrust;
                        To trust;
                        Source <source-peer-ip>;
                        Destination <destination-peer-ip>;
                        Service application-default;
                        Application [ike ipsec-esp-udp]
                        Action allow;
                }
                <deny-rule-name> {
                        From untrust;
                        To trust;
                        Source any;
                        Destination <destination-peer-ip>;
                        Service application-default;
                        Application [ike ipsec-esp-udp]
                        Action deny;
                }
        }
}
```

IPS Signature to block all IKEv2 traffic to devices that do not use IKEv2

```
alert udp any any -> any [500,4500] ( msg:"All IKEv2";  content:"|00 00 00 00 00 00 00 00 21 20 22
08 00 00 00 00 |"; offset: 8; sid:9800028;   rev:1;)
```

Appendix B: Security Association "show" Commands Examples

This appendix lists several common vendors and the available commands to show ISAKMP/IKE and IPsec connection details. For the purpose of this appendix, only common vendors that provide the cryptographic algorithms negotiated are listed.

Cisco IOS Routers and ASAs:

ISAKMP/IKE:

```
show crypto isakmp sa detail
```

IPSEC:

```
show crypto ipsec sa
```

Juniper SRX:

ISAKMP/IKE:

```
show ike security-associations details
```

IPSEC:

```
show security ipsec security-associations detail
```

Palo Alto Firewalls:

ISAKMP/IKE:

```
show vpn ike-sa
```

IPSEC:

```
show vpn ipsec-sa
```

Aruba:

ISAKMP/IKE:

Aruba provides the following command to show isakmp SAs however it does not provide cryptography details

```
show crypto isakmp sa
```

IPSEC:

```
show crypto ipsec sa
```

Appendix C: ISAKMP/IKE and IPsec Configuration Examples

In an effort to provide clear guidance on implementing strong IPsec VPNs, this document includes examples of the ISAKMP/IKE and IPsec, also known as phase 1 and 2, configurations for multiple vendors and devices. When deploying a remote access IPsec VPN, administrators must also ensure that all VPN clients are also configured properly. For further guidance on deploying VPNs on specific devices or VPN clients, appropriate vender documentation should be followed.

CISCO IOS ROUTERS

ISAKMP:

IKEv1:

```
no crypto isakmp default policy
crypto isakmp policy 1
encryption aes 256
group [16|20]
hash [sha384|sha512]
```

IKEv2:

```
crypto ikev2 proposal <proposal name>
encryption aes-cbc-256
integrity [sha384|sha512]
group [16|20]
```

IPsec:

```
crypto ipsec transform-set <transform name> esp-256-aes [esp-sha-hmac|esp-sha384-hmac|esp-sha512-hmac]
```

CISCO ASA

ISAKMP:

For Cisco ASA devices, NSA recommends IKEv2, since the IKEv1 implementation only supports SHA1.

IKEv2:

```
crypto ikev2 policy 1
encryption [aes-256|aes-gcm-256]
integrity [sha384|sha512]
group [16|20]
```

IPsec: `crypto ipsec ikev2 ipsec-proposal <proposal name>`

```
protocol esp encryption [aes-256|aes-gcm-256]
protocol esp integrity [sha-384|sha512]
```

Juniper SRX

ISAKMP/IKEv1 and IKEv2:

```
[edit security ike]
proposal ike-proposal {
        dh-group [group16|group20];
        authentication-algorithm [sha-384|sha512]
        encryption-algorithm [aes-256-cbc|aes-256-gcm]
}
policy ike-policy {
        mode main;
        proposals ike-proposal;
}
gateway <gw name> {
        ike-policy ike-policy;
        version v2-only;    #For IKEv2 otherwise SRX defaults to IKEv1
}
```

IPsec:

```
[edit security ipsec]
proposal <proposal name> {
        protocol esp;
        authentication-algorithm [hmac-sha-384|hmac-sha-512]
        encryption-algorithm [aes256-cbc|aes256-gcm]
}
```

Palo Alto Firewalls

ISAKMP/IKEv1 and IKEv2:

```
[edit network ike crypto-profiles]
ike-crypto-profiles <profile name>{
        dh-group group20;
        encryption aes-256-cbc;
        hash [sha384|sha512];
}
[edit network ike]
gateway <gw name>{
        protocol version [ikev1|ikev2|ikev2-prefered];
}
```

IPsec:

```
[edit network ike crypto-profiles]
```

```
ipsec-crypto-proiles <profile name> {
        dh-group group 20;
        esp;
        authentication [sha384|sha512];
        encryption [aes-256-cbc|aes-256-gcm];
}
```

Aruba

ISAKMP/IKEv1 and IKEv2:

```
crypto isakmp policy 1
encryption aes256
group 20
version [v1|v2]
hash sha2-384-192
```

IPsec:

```
crypto ipsec mtu <max-mtu> transform-set <transform-set-name> [esp-aes256|esp-aes256-gcm]
```

Apriva

Apriva does not provide extensive documentation for configuring their devices online. The following snippet was created using NIAP configuration guidance. Based on documentation provided, the ISAKMP/IKE and IPsec configuration is co-located.

```
vpn-suite <suite name> copy suiteb-rsa{
        algorithm [AES-256|AES-GCM-256]
        algorithm ike sha2 [SHA-384|SHA-512]
        algorithm ipsec sha2 [SHA-384|SHA-512]
        group ike [16|20]
```

Appendix D: Examples of ISAKMP/IKE Traffic Signatures

IPS Signatures for Weak Diffie-Hellman Groups (1, 2, or 5)

These signatures can be used to detect weak IKEv1 connections. From a defensive perspective, this can be used to identify VPN endpoints using weak Diffie-Hellman groups or to outright block these connections thereby ensuring policy compliance.

```
alert udp $HOME_NET 500 -> $EXTERNAL_NET any (msg:"Weak IKE group detected"; content:!"|00 00 00 00
00 00 00 00|"; offset: 36; depth: 8; content:"|80 02 00 01 80 04 00 01|"; within: 80; sid: 1; rev:
1;)

alert udp $HOME_NET 500 -> $EXTERNAL_NET any (msg:"Weak IKE group detected"; content:!"|00 00 00 00
00 00 00 00|"; offset: 36; depth: 8; content:"|80 02 00 01 80 04 00 02|"; within: 80; sid: 2; rev:
1;)

alert udp $HOME_NET 500 -> $EXTERNAL_NET any (msg:"Weak IKE group detected"; content:!"|00 00 00 00
00 00 00 00|"; offset: 36; depth: 8; content:"|80 02 00 01 80 04 00 05|"; within: 80; sid: 3; rev:
1;)

alert udp $HOME_NET 500 -> $EXTERNAL_NET any (msg:"Weak IKE group detected"; content:!"|00 00 00 00
00 00 00 00|"; offset: 36; depth: 8; content:"|80 02 00 02 80 04 00 01|"; within: 80; sid: 4; rev:
1;)

alert udp $HOME_NET 500 -> $EXTERNAL_NET any (msg:"Weak IKE group detected"; content:!"|00 00 00 00
00 00 00 00|"; offset: 36; depth: 8; content:"|80 02 00 02 80 04 00 02|"; within: 80; sid: 5; rev:
1;)

alert udp $HOME_NET 500 -> $EXTERNAL_NET any (msg:"Weak IKE group detected"; content:!"|00 00 00 00
00 00 00 00|"; offset: 36; depth: 8; content:"|80 02 00 02 80 04 00 05|"; within: 80; sid: 6; rev:
1;)
```

IPS Signatures for DES/3DES

These signatures can be used to detect devices attempting to use weak encryption.

```
alert udp $HOME_NET 500 -> $EXTERNAL_NET any (msg:"IKE DES Encryption Used";content:"|00 00 08 01
00 00 02|";offset:41; depth: 7; sid: 7; rev: 1;)

alert udp $HOME_NET 500 -> $EXTERNAL_NET any (msg:"IKE DES Encryption Used";content:"|00 00 08 01
00 00 03|";offset:41; depth: 7; sid: 8; rev: 1;)

alert udp $HOME_NET 500 -> $EXTERNAL_NET any (msg:"IKE DES Encryption Used";content:"|00 00 08 01
00 00 09|";offset:41; depth: 7; sid: 9; rev: 1;)

alert udp $HOME_NET 500 -> $EXTERNAL_NET any (msg:"IKE DES Encryption Used";content:"|00 00 08 01
00 00 11|";offset:41; depth: 7; sid: 10; rev: 1;)

alert udp $HOME_NET 500 -> $EXTERNAL_NET any (msg:"IKE DES Encryption Used";content:"|00 00 08 01
00 00 21|";offset:41; depth: 7; sid: 11; rev: 1;)
```

IPS Signatures of Anomalous ISAKMP/IKE Traffic

NSA has identified scanning activity that generates malformed ISAKMP traffic. The following rule is designed to block that malformed traffic.

```
alert udp any any -> any 500 ( msg:"Anomalous Malformed ISAKMP";  content:"|00 00 00 00 00 00 00 00
21 20 22 08 00 00 00 00 |"; offset: 8; content:"|03 00 00 0e 01 00 00 00 00 00|"; distance:16;
sid: 12;   rev:1;)
```

Appendix E: Frequently Asked Questions

Q1: How does NSA define “obsolete cryptography?”

A1: NSA defines “obsolete cryptography” as those algorithms that do not meet NIST recommendations for protecting sensitive-but-unclassified federal systems. (See NIST SP 800-131A rev2 and SP 800-56A rev3 for further details on NIST’s recommendations).

Q2: Can the WireGuard protocol be configured to use CNSSP 15 or NIST approved cryptography?

A2: WireGuard is not an implementation of IKE/IPsec and supports neither CNSSP 15 nor NIST approved cryptography.

Q3: Is AES-128 approved for use on National Security Systems (NSS)?

A3: CNSSP 15 specifies AES-256 for use on NSS. Although AES-128 is not approved for use on NSS, AES-128 does achieve a security strength consistent with NIST recommendations for protecting sensitive-but-unclassified federal systems.

Q4: Does the cryptographic strength of Diffie-Hellman groups increase as the group number increases?

A4: Not always. There are cases where Diffie-Hellman groups with lower group numbers (e.g., Groups 15 and 16) will possess greater cryptographic strength than a Diffie-Hellman group with a higher group number (e.g., Group 24).

Q5: Which Diffie-Hellman groups comply with CNSSP 15 guidance and are commonly available in commercial products?

A5: Diffie-Hellman groups 20, 16, and 15 are CNSSP 15-compliant and are currently available in many products.