17.8. Internet Protocol Security (IPSec)

Objective

17.8.1. Internet Protocol Security (IPSec) is correctly implemented.

Context

Scope

17.8.2. This section covers information on the conditions under which IPSec can be used as an Approved Cryptographic Protocol.

17.8.3. When using a product that implements IPSec, requirements for using approved cryptographic protocols will also need to be referenced from Section 17.3 Approved Cryptographic Protocols.

Modes of operation

17.8.4. IPSec can be operated in two modes: transport mode or tunnel mode.

Cryptographic algorithms

17.8.5. Most IPSec implementations can accommodate a number of cryptographic algorithms for encrypting data when the Encapsulating Security Payload (ESP) protocol is used. These include 3DES and AES.

Key exchange

17.8.6. Most IPSec implementations facilitate a number of methods for sharing keying material used in hashing and encryption processes. Two common methods are manual keying and IKE using the ISAKMP. Both methods are considered suitable for use.

ISAKMP authentication

17.8.7. Most IPSec implementations can select from a number of methods for authentication as part of ISAKMP. These can include digital certificates, encrypted nonces or pre-shared keys. All these methods are considered suitable for use.

ISAKMP modes

17.8.8. ISAKMP uses two modes to exchange information as part of IKE. These are main mode and aggressive mode.

References

17.8.9. Further information on IPSec can be found at:

Reference	Title	Publisher	Source
RFC 2401	**Security Architecture for the IP overview**	IETF	https://datatracker.ietf.org/doc/html/rfc2401
NIST 800-77 Rev. 1	**Guide to IPSec VPNs, June 2020**	NIST	https://csrc.nist.gov/publications/detail/sp/800-77/rev-1/final

Rationale & Controls

Mode of operation

17.8.10.R.01. **Rationale**

The tunnel mode of operation provides full encapsulation of IP packets whilst the transport mode of operation only encapsulates the payload of the

IP packet.

17.8.10.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:2842]

Agencies SHOULD use tunnel mode for IPSec connections.

17.8.10.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:2843]

Agencies choosing to use transport mode SHOULD additionally use an IP tunnel for IPSec connections.

Protocol

17.8.11.R.01. **Rationale**

In order to provide a secure VPN style connection both authentication and encryption are needed. ESP is the only way of providing encryption yet Authentication Header (AH) and ESP can provide authentication for the entire IP packet and the payload respectively. ESP is generally preferred for authentication though as AH has inherent network address translation limitations.

17.8.11.R.02. **Rationale**

If however, maximum security is desired at the expense of network address translation functionality, then ESP can be wrapped inside of AH which will then authenticate the entire IP packet and not just the encrypted payload.

17.8.11.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:2847]

Agencies SHOULD use the ESP protocol for IPSec connections.

ISAKMP modes

17.8.12.R.01. **Rationale**

Using main mode instead of aggressive mode provides greater security since all exchanges are protected.

17.8.12.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:2850]

Agencies using ISAKMP SHOULD disable aggressive mode for IKE.

Security association lifetimes

17.8.13.R.01. **Rationale**

Using a secure association lifetime of four hours or 14400 seconds provides a balance between security and usability.

17.8.13.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:2853]

Agencies SHOULD use a security association lifetime of four hours or 14400 seconds, or less.

HMAC algorithms

17.8.14.R.01. **Rationale**

MD5 and SHA-1 are no longer approved Cryptographic Protocols. The approved algorithms that can be used with HMAC are HMAC-SHA256, HMAC-SHA384 and HMAC-SHA512.

17.8.14.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:2856]

Agencies SHOULD use HMAC-SHA256, HMAC-SHA384 or HMAC-SHA512 as the HMAC algorithm.

DH groups

17.8.15.R.01. **Rationale**

Using a larger DH group provides more entropy for the key exchange.

17.8.15.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:2859]

Agencies SHOULD use the largest modulus size available for the DH exchange.

Perfect Forward Secrecy

17.8.16.R.01. **Rationale**

Using Perfect Forward Secrecy reduces the impact of the compromise of a security association.

17.8.16.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:2862]

Agencies SHOULD use Perfect Forward Secrecy for IPSec connections.

IKE Extended Authentication

17.8.17.R.01. **Rationale**

XAUTH using IKEv1 has documented vulnerabilities associated with its use.

17.8.17.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:2865]

Agencies SHOULD disable the use of XAUTH for IPSec connections using IKEv1.