Cifrado

- DES → 56bits . Es la más antigua . No usar
- 3DES →112 bits (en vez de los 168 bits del 3×56)
- AES →128,192,256

Protocolos de Cifrado

- ipsec.
- SSL. Nivel 4 OSI
- TLS
- SSH Combina protocolo de cifrado con una interfaz de línea de comandos

IPSEC

Nivel 3 OSI. Posee dos subprotocolos AH y ESP.

- AH encabezado de autenticación
- ESP carga de seguridad de encapsulación

AH se encarga de
* integridad del mensaje

- función antirepetición
- autenticación



AH no soporta NAT

ESP se encarga de

- integridad del mensaje
- función antirepetición
- autenticación
- cifrado del contenido

ESP si soporta NAT mediante NAT-T (NAT Transversal)

From:
https://wiki.intrusos.info/ - **LCWIKI**

Permanent link:
https://wiki.intrusos.info/doku.php?id=seguridad:cifrado

Last update: **182023/01/ 13:11**