Sesiones Telnet seguras y confidenciales

SeguriTELNET

SeguriTELNET permite trabajar en un ambiente de confidencialidad y de autenticidad de los interlocutores.

SeguriTELNET ha sido diseñado pensando especialmente en los ambientes TELNET, que tanto predominaron y que hoy siguen teniendo presencia en un gran número de entidades. Las necesidades de seguridad son tan fuertes como en cualquier otro ambiente, sin embargo, los desarrollos enfocados a TELNET han disminuido sensiblemente en los últimos años.

El esquema de funcionamiento se basa en el uso de la tecnología de certificados digitales bajo el estándard X.509, así como de criptografía de llave pública para así asegurar la confidencialidad de la información que fluye entre un servidor y un cliente durante una sesión TELNET, y garantizar la autenticidad del servidor TELNET con el que se realiza la conexión. Esta posibilidad de autenticidad, puede ser extendida hacia los clientes, cerrando un círculo de seguridad.

SeguriTELNET asegura cada sesión de manera única e individual desde el inicio de la sesión, hasta que esta se da por concluida.

SeguriTELNET realiza sus funciones por medio de dos procesos simultáneos encaminados no sólo a la autenticación del servidor y de los clientes, sino también encriptando el canal de comunicación.

Cliente

Cuando un usuario se conecta a un servidor seguro usando SeguriTELNET, se incia el siguiente proceso:

1. Generación de una llave aleatoria simétrica de 128 bits para encriptar el canal. La llave es encriptada con la llave pública del servidor para su envío.
2. Se recibe un mensaje de reto que solo puede ser abierto con la llave privada del usuario para su autenticación.
3. La información es encriptada y desencriptada con el algoritmo RC4.

Servidor

Cuando el servidor detecta una conexión, se inician los siguientes servicios de seguridad.

1. Desencripción de la llave aleatoria con la llave privada del servidor.
2. Generación de un mensaje de reto para el usuario que es encriptado con la lave pública del usuario para su autenticación.
3. La información es encriptada y desencriptada con el algoritmo RC4.

SeguriPROXY utiliza los más altos niveles de seguridad y tiene como complemento SeguriSERVER, que genera y administra certificados digitales bajo estándares internacionales como Public Key Cryptography Standards y Edi for adminstration commerce and transport (Edifcat), sin limitaciones o restricciones legales de ningún tipo.

Plataformas

Solaris
HP-UX
Linux
Windows NT
Windows 95

Contáctenos

+(52)-5575-6385
info@seguridata.com
SeguriDATA
www.seguridata.com