Actividad 4.

Implemente mecanismos que permitan dar soporte a la privacidad, integridad y control de acceso de manera de asegurar la comunicación segura entre los procesos involucrados en la situación problemática planteada en el Taller I.

Escenario.

El estacionamiento posee una computadora para elaborar reportes referidos al negocio (ingreso/ egreso de vehículos, movimientos de caja, etc) y periódicamente enviarlos vía e-mail al la organización propietaria del estacionamiento.

El estacionamiento posee una única conexión a internet solamente para enviar mensajes desde el servidor de correo local al servidor de correo de la organización propietaria.

Ninguna de las computadores posee interfaz grafica.

Existen dos tipos de usuarios, los empleados, que solo manejan el equipo para realizar las actividades de cobro y los administradores, que se encargan de la configuración y mantenimiento de los servidores.

Políticas que la organización impone sobre el manejo informatizado del estacionamiento.

Las políticas se implementan en un router que posee las siguientes funcionalidades a demas de router de primer salto.

- Firewall para filtro de paquetes que implementa las siguientes políticas

P.1. Ninguna computadora de la red local debe aceptar ninguna conexión TCP proveniente de internet.
F.1. Denegar: Paquetes con segmentos TCP flag = 0x0002 (solicitud de conexión), cualquiera sea su IP o Puerto origen/destino.

P.2. El servidor de correo local solo accede a internet para comunicarse al servidor de correo de la organización propietaria.
F.2.a Permitir: IP origen Servidor correo local; IP destino: Servidor correo de la organización; puertos origen y destino: puertos SMTP;

F2.b. Permitir: IP origen Servidor correo de la organización; IP destino: Servidor correo local; puertos TCP origen y destino: puertos SMTP;

P.3. Regla por defecto
F.3. Denegar: Cualquier IP origen/destino, cualquier Puerto origen/destino.

- NAT debe configurarse para redirigir el trafico que destinado al servidor de correo

Para aquellos paquetes que coincidan con el filtro F.2.a rescribir IP LAN del origen por la IP de la interfaz WAN del router.
Para aquellos paquetes que coincidan con el filtro F.2.b rescribir IP de la interfaz WAN del router del destino por la IP del servidor de correo local.

En ambos casos no se necesitan reescribir puertos porque se manejan solamente dos servidores en puertos bien conocidos.

Ademas se requiere que toda la información enviada por correo debe garantizar confidencialidad, integridad y autenticación.

Para cumplir este requisito, se utiliza software PGP que proporciona los servicios de confidencialidad e integridad de los mensajes de correo. Se requerirá generar un par de claves para Infraestructura de Clave Publica (PKI), uno asociado al servidor de correos local.

Por otra parte, añadimos servicios confidencialidad, integridad y autenticación a nivel de transporte, utilizando el paquete OpenSSL para generación de certificados entre el servidor los servidores de correo. Entre las funciones que permite el paquete es el de autenticación terminales (siempre que se dispongan de los certificados), cifrado de mensajes, verificación de la integridad de los mensajes enviados. Cada paquete incluye un numero de secuencia para evitar ataques por duplicado y cada conexión incluye un numero distintivo para prevenir ataques por reproducción de toda la conexión.

Finalmente, se establece como política que todo usuario de cualquier equipo debe poseer una contraseña al menos 64 bits (8 caracteres en ASCII). En el caso de los empleados, todos compartiran la misma cuenta y la misma contraseña. En el caso de los administradores, cada uno deberá poseer su propia cuenta y contraseña, y esta debe ser modificada cada mes por el departamento de sistemas de la organización.