SITUACIONES PRESENTADAS EN LOS SISTEMAS CONTPAQI CON EL FIREWALL DE WINDOWS

Antes de poder revisar la configuración de tu Firewall en tu equipo debemos empezar por definir ¿Qué es un Firewall? Y ¿Qué es un Puerto?

Empecemos por definir que son los **Puertos** en tu equipo de cómputo. Los puertos **dividen el tráfico de red y los servicios en segmentos**, así tu equipo es capaz de priorizar y procesar individualmente estos segmentos. **Al dividirlo de esta manera, una computadora puede enviar y recibir información de diferentes fuentes al mismo tiempo**, en donde estos **son controlados** y **administrados por el Firewall**.

Cada **Puerto de red** en actividad, **es capaz de enviar información directamente fuera del equipo en específico a la red local o a internet**. Para poner un ejemplo, si un proceso está funcionando sobre el puerto 1500, entonces este puerto puede enviar y recibir información específica o de forma exclusiva.

El Firewall es un proceso de seguridad en el equipo, que monitorea el tráfico de red (entrante y saliente) y **decide si permite o bloquea el tráfico en específico** o bien en función de un conjunto definido de reglas de seguridad.

Los firewalls han constituido una primera línea de defensa en seguridad de la red durante más de 25 años. **Establecen una barrera entre las redes internas protegidas y controladas en las que se puede confiar y redes externas que no son de confianza, como Internet.**

Tomando lo anterior en cuenta, **debes saber que en tu equipo con un sistema operativo Windows**, el Firewall es **administrado por "Firewall de Windows" o "Firewall de Windows Defender" a partir de la versión Windows 10** del Sistema Operativo.

Hay tres valores o estatus a configurar en la ficha General de Firewall de Windows:

1. **Activado.**

Esta opción está seleccionada de forma predeterminada. Cuando Firewall de Windows está activado **la mayoría de los programas quedan bloqueados para establecer comunicación.** Si desea **desbloquear un programa**, puede agregarlo a **la lista de excepciones**, permitiendo su conexión en las reglas del Firewall existentes o bien **creando una nueva regla de entrada y de salida** para el mismo.

2. **Bloquear todas las conexiones entrantes.**

Esta opción **bloquea todos los intentos no solicitados para conectarse a tu equipo**. Utilice este **ajuste cuando se necesita la máxima protección para su equipo**, como por ejemplo cuando se conecta a una red pública en un hotel o un aeropuerto, o cuando un "gusano" (virus) del equipo se está extendiendo a través de Internet. **Con esta configuración viene de forma "default" en el sistema y no se le notifica al usuario cuando Firewall de Windows bloquea programas y aun cuando estos están en la lista de excepciones, estas son ignoradas también**.

3. **Desactivado.**

Al desactivar **Firewall de Windows se permite la comunicación libre, sin ninguna restricción y validación de cualquier software en tu equipo**, así como cualquier mensaje entrante o saliente en él.

Si tu equipo cuenta con algún sistema CONTPAQi y presenta problemas deberás validar los siguientes puntos:

- Verifica que al entrar a tus sistemas CONTPAQi, no tengan errores de bloqueo de cualquier tipo ejemplo:
  - Ocurrió un fallo al intentar establecer la comunicación con el servidor de licencias. Servidor: localhost, Puerto: 9020 ¿Desea re-intentar la operación?
  -
  - Ocurrió un fallo al intentar establecer la comunicación con el servidor de licencias. Servidor: localhost, Puerto: 9047 ¿Desea re-intentar la operación?
  - Error al tratar de conectarse al administrador de documentos digitales. Verifique los siguientes puntos:

    *La configuración de conexión con el SACI es correcta.
    *La contraseña de SACI, en terminal y servidor, son iguales.
    *El servicio SACI esté iniciado.
    *Es posible comunicarse al puerto de servicios del SACI.

- Identifica quien administra el firewall en tu equipo ya sea tu programa antivirus o por el sistema operativo Windows.
- Revisa que en la configuración del firewall , las reglas de entrada y salida no tengan bloqueados o deshabilitados los puertos principales de CONTPAQi. (Recordando que estos sistemas utilizas los puertos para enviar información de los CDFIs)

¿Qué puedes hacer si caes en alguno de los puntos anteriores?

- Si tu equipo presenta algún mensaje de bloqueo, toma nota del puerto que indica el bloqueo y agrégalo a una nueva regla de entrada y salida en el Firewall de Windows.
- Si existe alguna regla bloqueada o deshabilitada en el Firewall de Windows deberás habilitarlos o activarlos.
- Si el Firewall es administrado por algún antivirus, la configuración deberás hacerla desde dicho antivirus, te recomendamos que la administración la lleve Windows pues el Firewall de los antivirus suele ser más riguroso y bloquea cualquier tipo de comunicación entre los puertos.
- En dado caso que el bloqueo persista, desactiva el Firewall de Windows para que permita la comunicación libre entre los puertos que los sistemas CONTPAQi utiliza. (No recomendado aquí te sugerimos el apoyo de nuestros expertos)

¿Qué puertos utiliza CONTPAQi?

Los necesarios para el correcto funcionamiento son:

- 9080 Corresponde al servidor de Aplicaciones (SACi).
- 9081 Corresponde al Administrador de documentos digitales.
- 9047 Puerto de Licenciamiento.
- 7653 Autorización remota y licenciamiento.
- 1099 Puerto que se utiliza para la conexión de terminales al servidor en red de CONTPAQi.
- 1138, 1139, 1775, 2003 Puertos Adicionales utilizados por CONTPAQi.

¡NO pongas en riesgo tu inversión, tus sistemas y tus equipos!

Nuestros expertos te asesoran donde y cuando lo necesites en soluciones de seguridad brindándote todo el apoyo en este tema de seguridad informática y antivirus . Por algo hemos sido reconocidos, durante tres años consecutivos, como una de las 50 empresas de consultoría TIC más importantes de México.

El mejor consultor de TI, cerca de TI.

También te invitamos a visitarnos en nuestra página:

http://www.gruponym.mx