**Política de Seguridad de Router y Switch** (enrutador y conmutador).

**Exención de responsabilidad:** *Esta política fue creada por o para el SANS Institute para la comunidad de Internet. Toda o parte de esta política se puede utilizar libremente para su organización. No se requiere aprobación previa. Si desea contribuir con una nueva política o una versión actualizada de esta política, envíe un correo electrónico a [policy-resources@sans.org](mailto:policy-resources@sans.org).*

**Último estado de actualización:** *actualizado junio 2014*

# Visión general

Ver propósito.

# Propósito

Este documento describe una configuración de seguridad mínima requerida para todos los routers y switches que se conectan a una red de producción o que se utilizan en una capacidad de producción o en nombre de <Nombre de Empresa>.

# Alcance

# Todos los empleados, contratistas, consultores, trabajadores temporales y otros de <Nombre de la Empresa> y sus subsidiarias deben cumplir con esta política. Todos los enrutadores y conmutadores conectados a las redes de producción de <Nombre de la empresa> se ven afectados.

# Política

Cada enrutador debe cumplir con los siguientes estándares de configuración:

1. No hay cuentas de usuarios locales configuradas en el Router. Los Routers y los Switches deben usar TACACS + para toda la autenticación de los usuarios.
2. La enable password (contraseña de habilitación) en el Router o Switch debe mantenerse en una forma cifrada segura (secure encrypted form). El Router o Switch debe tener la enable password establecida en la contraseña de Router o Switch de producción actual desde la organización de soporte del dispositivo.
3. Los siguientes servicios o características deben estar deshabilitados:
   1. Emisiones dirigidas IP
   2. Los paquetes entrantes en el router/switch con direcciones no válidas, como las direcciones RFC1918
   3. Pequeños servicios TCP
   4. Pequeños servicios UDP
   5. Todo el enrutamiento y conmutación de origen
   6. Todos los servicios web que se ejecutan en el router
   7. <Nombre de la empresa> protocolo de descubrimiento en interfaces conectadas a Internet
   8. Servicios de Telnet, FTP y HTTP.
   9. Autoconfiguración

4. Los siguientes servicios deberían desactivarse a menos que se proporcione una justificación de negocio:

a. <Nombre de la empresa> protocolo de descubrimiento y otros protocolos de descubrimiento

b. Trunking dinámico

c. Entornos de script, como el shell TCL

5. Los siguientes servicios deben estar configurados:

a. contraseña-cifrada

b. NTP configurado a una fuente estándar corporativa

6. Todas las actualizaciones de routing se realizarán utilizando actualizaciones de routing seguras.

7. Utilice cadenas (texto, strings) de comunidad SNMP estandarizadas corporativas. Deben eliminarse las cadenas predeterminadas, como públicas o privadas. SNMP debe configurarse para utilizar la versión más segura del protocolo permitida por la combinación del dispositivo y los sistemas de administración.

8. Las listas de control de acceso deben utilizarse para limitar la fuente y el tipo de tráfico que puede terminar en el propio dispositivo.

9. Los controladores de acceso para transitar el dispositivo se agregarán a medida que surjan las necesidades comerciales.

10. El enrutador debe estar incluido en el sistema de gestión empresarial corporativo con un punto de contacto designado.

11. Cada enrutador debe presentar la siguiente declaración para todas las formas de inicio de sesión, ya sea remota o local:

“EL ACCESO NO AUTORIZADO A ESTE DISPOSITIVO DE RED ESTÁ PROHIBIDO. Debe tener permiso explícito para acceder o configurar este dispositivo. Todas las actividades realizadas en este dispositivo pueden estar registradas, y las violaciones de esta política pueden resultar en medidas disciplinarias y tal vez informarse a las autoridades policiales. No hay derecho a la privacidad en este dispositivo. El uso de este sistema constituirá un consentimiento para la supervisión “.

12. La red no puede usarse nunca en ninguna red para administrar un enrutador, a menos que exista un túnel seguro que proteja toda la ruta de comunicación. SSH versión 2 es el protocolo de gestión preferido.

13. Los protocolos de enrutamiento dinámico deben usar la autenticación en las actualizaciones de enrutamiento enviadas a los vecinos. El hashing de contraseña para la cadena de autenticación debe estar habilitado cuando sea compatible.

14. El estándar de configuración del enrutador corporativo definirá la categoría de dispositivos de enrutamiento y conmutación sensibles, y requerirá servicios o configuración adicionales en dispositivos sensibles, incluidos:

a. Contabilidad de la lista de acceso IP

b. Registro de dispositivos

c. Los paquetes entrantes en el enrutador provistos de direcciones no válidas, como las direcciones RFC1918, o las que podrían usarse para falsificar el tráfico de red, se eliminarán.

d. El acceso a la consola de enrutador y al módem debe estar restringido por controles de seguridad adicionales

# Cumplimiento de la Política

* 1. Medición de cumplimiento

El equipo de INFOSEC verificará el cumplimiento de esta política a través de varios métodos, incluyendo, pero no limitado a, Walk-thrus periódico, monitoreo de video, informes de herramientas de negocios, auditorías internas y externas, y retroalimentación a la propietario de la póliza.

# Excepciones

Cualquier excepción a la póliza debe ser aprobada por el equipo INFOSEC por adelantado.

# Incumplimiento

Un empleado que haya violado esta política puede estar sujeto a medidas disciplinarias, incluyendo la terminación del empleo.

# Normas, políticas y procesos relacionados

Ninguno.

# Definiciones y términos

Ninguno.

# Historial de revisión

|  |  |  |
| --- | --- | --- |
| **Fecha de cambio** | **Responsable** | **Resumen de cambio** |
| Junio 2014 | El equipo de políticas SANS | Actualizado y convertido a nuevo formato. |
|  |  |  |