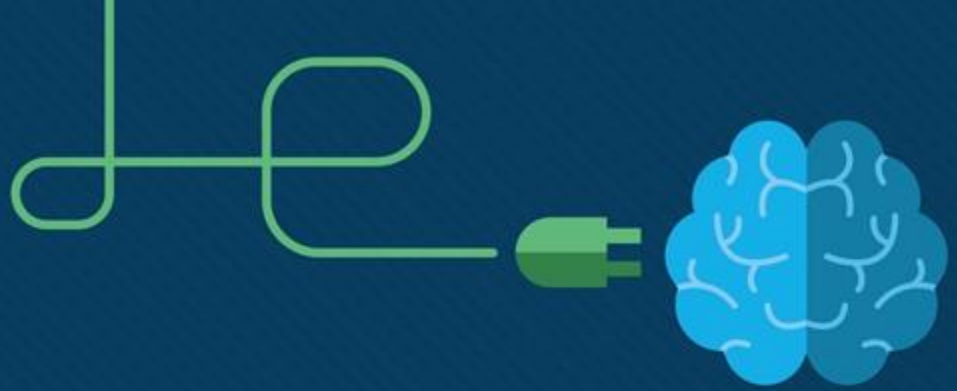


Fundamentos de seguridad de red

Introducción a Redes v7.0 (ITN)

16.1 Amenazas y vulnerabilidades de seguridad

Tipos de amenazas

Los ataques a una red pueden ser devastadores y pueden resultar en una pérdida de tiempo y dinero debido a daños o robo de información o activos importantes. Los intrusos pueden obtener acceso a una red a través de vulnerabilidades de software, ataques de hardware o adivinando el nombre de usuario y la contraseña de alguien. Los intrusos que obtienen acceso modificando software o explotando vulnerabilidades de software se denominan actores de amenazas.

Una vez que el actor de la amenaza obtiene acceso a la red, pueden surgir cuatro tipos de amenazas:

- Robo de información
- Pérdida y manipulación de datos.
- Robo de identidad
- Interrupción del servicio

Tipos de vulnerabilidades

La vulnerabilidad es el grado de debilidad en una red o un dispositivo. Algún grado de vulnerabilidad es inherente a los enrutadores, conmutadores, equipos de escritorio, servidores e incluso dispositivos de seguridad. Por lo general, los dispositivos de red que sufren ataques son las terminales, como los servidores y las computadoras de escritorio.

Existen tres vulnerabilidades o debilidades principales:

Las vulnerabilidades tecnológicas pueden incluir debilidades del protocolo TCP/IP, debilidades del sistema operativo y debilidades del equipo de red.

- Las vulnerabilidades de configuración pueden incluir cuentas de usuario no seguras, cuentas de sistema con contraseñas fáciles de adivinar, servicios de Internet mal configurados, configuraciones predeterminadas no seguras y equipos de red mal configurados.
- Las vulnerabilidades de política de seguridad pueden incluir la falta de una política de seguridad escrita, la política, la falta de continuidad de autenticación, los controles de acceso lógico no aplicados, la instalación de software y hardware y los cambios que no siguen la política, y un plan de recuperación ante desastres inexistente.

Las tres fuentes de vulnerabilidades pueden dejar una red o dispositivo abierto a varios ataques, incluidos ataques de código malicioso y ataques de red.

Seguridad física

Si los recursos de la red pueden verse físicamente comprometidos, un actor de amenazas puede negar el uso de los recursos de la red. Las cuatro clases de amenazas físicas son las siguientes:

- **Amenazas de hardware -** Esto incluye daños físicos a servidores, routers, switches, planta de cableado y estaciones de trabajo.
- **Amenazas Ambientales -** Esto incluye temperaturas extremas (demasiado calor o demasiado frío) o humedad extrema (demasiado húmedo o demasiado seco).
- **Amenazas eléctricas -** Esto incluye picos de voltaje, voltaje de suministro insuficiente (caídas de voltaje), energía no condicionada (ruido) y pérdida total de energía.
- **Amenazas de mantenimiento -** Esto incluye un manejo deficiente de los componentes eléctricos clave (descarga electrostática), falta de repuestos críticos, cableado deficiente y etiquetado deficiente.

Se debe crear e implementar un buen plan de seguridad física para abordar estos problemas.

16.2 Ataques de red

Tipos de malware

Malware es la abreviatura de software malicioso. Es un código o software diseñado específicamente para dañar, interrumpir, robar o infligir acciones "malas" o ilegítimas en los datos, hosts o redes. Los siguientes son tipos de malware: Los siguientes son tipos de malware:

- **Virus -** Un virus informático es un tipo de malware que se propaga insertando una copia de sí mismo y formando parte de otro programa. Se propaga de una computadora a otra, dejando infecciones a medida que viaja.
- **Gusanos -** Los gusanos informáticos son similares a los virus en que replican copias funcionales de sí mismos y pueden causar el mismo tipo de daño. A diferencia de los virus, que requieren la propagación de un archivo host infectado, los gusanos son software independiente y no requieren de un programa host ni de la ayuda humana para propagarse.
- **Trojan Horses -** Es un software dañino que parece legítimo. A diferencia de los virus y gusanos, los caballos de Troya no se reproducen al infectar otros archivos. Se autoreplican. Los caballos de Troya deben extenderse a través de la interacción del usuario, como abrir un archivo adjunto de correo electrónico o descargar y ejecutar un archivo de Internet.

Ataques de reconocimiento

Además de los ataques de código malintencionado, es posible que las redes sean presa de diversos ataques de red. Los ataques de red pueden clasificarse en tres categorías principales:

- **Ataques de reconocimiento -** El descubrimiento y el mapeo de sistemas, servicios o vulnerabilidades**.**
- **Ataques de acceso -** La manipulación no autorizada de datos, acceso al sistema o privilegios de usuario**.**
- **Denegación de servicio -** La desactivación o corrupción de redes, sistemas o servicios**.**

Para los ataques de reconocimiento, los actores de amenazas externas pueden usar herramientas de Internet, como las herramientas de **nslookup** y **whois**, para determinar fácilmente el espacio de direcciones IP asignado a una determinada corporación o entidad. Después de determinar el espacio de direcciones IP, un actor de amenazas puede hacer ping a las direcciones IP disponibles públicamente para identificar las direcciones que están activas.

Ataques de acceso

Los ataques de acceso explotan las vulnerabilidades conocidas de los servicios de autenticación, los servicios FTP y los servicios Web para obtener acceso a las cuentas Web, a las bases de datos confidenciales y demás información confidencial.

Los ataques de acceso se pueden clasificar en cuatro categorías:

- **Ataques de contraseña:** implementados usando fuerza bruta, troyanos y rastreadores de paquetes
- **Explotación de confianza -** Un actor de amenazas utiliza privilegios no autorizados para obtener acceso a un sistema, posiblemente comprometiendo el objetivo.
- **Redireccionamiento de puertos -** Un actor de amenaza utiliza un sistema comprometido como base para ataques contra otros objetivos. Por ejemplo, un actor de amenaza que usa SSH (puerto 22) para conectarse a un host A comprometido. El host B confía en el host A y, por lo tanto, el actor de amenaza puede usar Telnet (puerto 23) para acceder a él.
- **Man-in-the middle -** El agente de la amenaza se coloca entre dos entidades legítimas para leer o modificar los datos que pasan entre las dos partes.

Ataques de denegación de servicio

Los ataques de denegación de servicio (DoS) son la forma de ataque más publicitada y una de las más difíciles de eliminar. Sin embargo, debido a su facilidad de implementación y daño potencialmente significativo, los ataques DoS merecen especial atención por parte de los administradores de seguridad.

Los ataques DoS tienen muchas formas. Fundamentalmente, evitan que las personas autorizadas utilicen un servicio mediante el consumo de recursos del sistema. Para prevenir los ataques de DoS es importante estar al día con las actualizaciones de seguridad más recientes de los sistemas operativos y las aplicaciones.

Los ataques de DoS son un riesgo importante porque pueden interrumpir fácilmente la comunicación y causar una pérdida significativa de tiempo y dinero. Estos ataques son relativamente simples de ejecutar, incluso si lo hace un agente de amenaza inexperto.

Un DDoS es similar a un ataque DoS, pero se origina en múltiples fuentes coordinadas. Por ejemplo, un agente de amenazas construye una red de hosts infectados, conocidos como zombies. A una red de zombies se le conoce como botnet. El actor de amenazas utiliza un programa de comando y control (CNC) para instruir a la botnet de zombies para llevar a cabo un ataque DDoS.

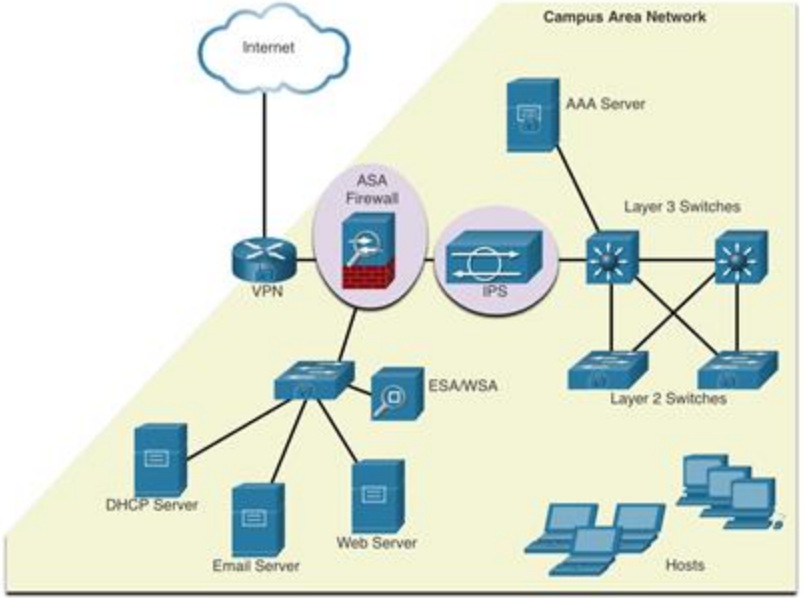
16.3 Mitigaciones para ataques de red

El enfoque en profundidad de la defensa

Para mitigar los ataques de red, primero debe proteger los dispositivos, incluidos enrutadores, conmutadores, servidores y hosts. La mayoría de las organizaciones emplean un enfoque de defensa en profundidad (también conocido como enfoque en capas) para la seguridad. Esto requiere una combinación de dispositivos y servicios de red que funcionen en conjunto.

Se implementan varios dispositivos y servicios de seguridad para proteger a los usuarios y activos de una organización contra las amenazas de TCP / IP:

- VPN
- ASA Firewall
- IPS
- ESA/WSA
- AAA Server



Mantener copias de seguridad

Hacer una copia de seguridad de las configuraciones y los datos del dispositivo es una de las formas más efectivas de protección contra la pérdida de datos. Las copias de seguridad se deben realizar de forma regular tal como se identifica en la política de seguridad. Las copias de respaldo de datos suelen almacenarse externamente para proteger los medios de copia de respaldo en caso de que ocurra algo en la instalación principal.

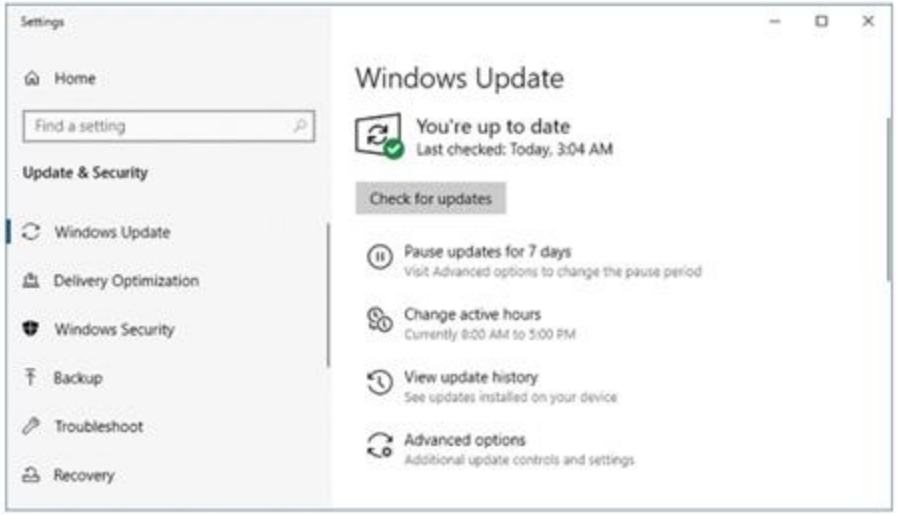
La tabla muestra las consideraciones de copia de seguridad y sus descripciones.

Consideración	Descripción
Frecuencia	• Realice copias de respaldo con regularidad, como se identifica en la política de seguridad. • Las copias de seguridad completas pueden llevar mucho tiempo, por lo tanto, realice copias de seguridad mensuales o semanales con frecuentes copias de seguridad parciales de los archivos modificados.
Almacenamiento	• Siempre valide las copias para garantizar la integridad de los datos y valide los procedimientos de restauración de archivos.
Seguridad	• Las copias de respaldo deben trasladarse de forma diaria, semanal o mensual, según lo que exija la política de seguridad, a una ubicación de almacenamiento externa aprobada.
Validación	• Las copias deben protegerse con contraseñas seguras. La contraseña es necesaria para restaurar los datos.

Mejorar, Actualizar y Parchear

A medida que se publica nuevo malware, las empresas deben mantenerse al día con las versiones más recientes del software antivirus.

- La manera más eficaz de mitigar un ataque de gusanos consiste en descargar las actualizaciones de seguridad del proveedor del sistema operativo y aplicar parches a todos los sistemas vulnerables.
- Una solución para la administración de parches de seguridad críticos es asegurarse de que todos los sistemas finales descarguen actualizaciones automáticamente.

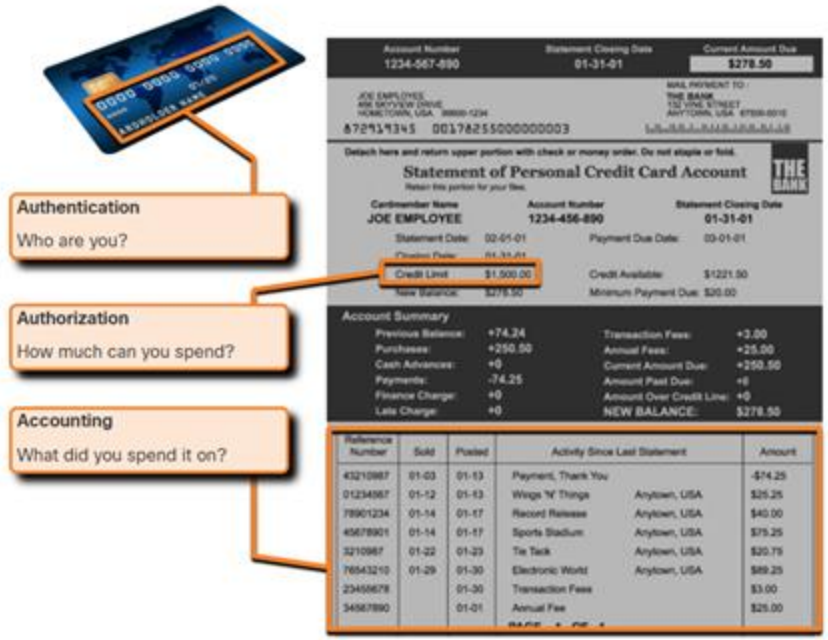


Autenticar, Autorizar y Contabilizar

Los servicios de seguridad de red de autenticación, autorización y contabilización (AAA o "triple A") proporcionan el marco principal para configurar el control de acceso en dispositivos de red.

AAA es una forma de controlar quién tiene permiso para acceder a una red (autenticar), qué acciones realizan mientras acceden a la red (autorizar) y hacer un registro de lo que se hizo mientras están allí (contabilizar).

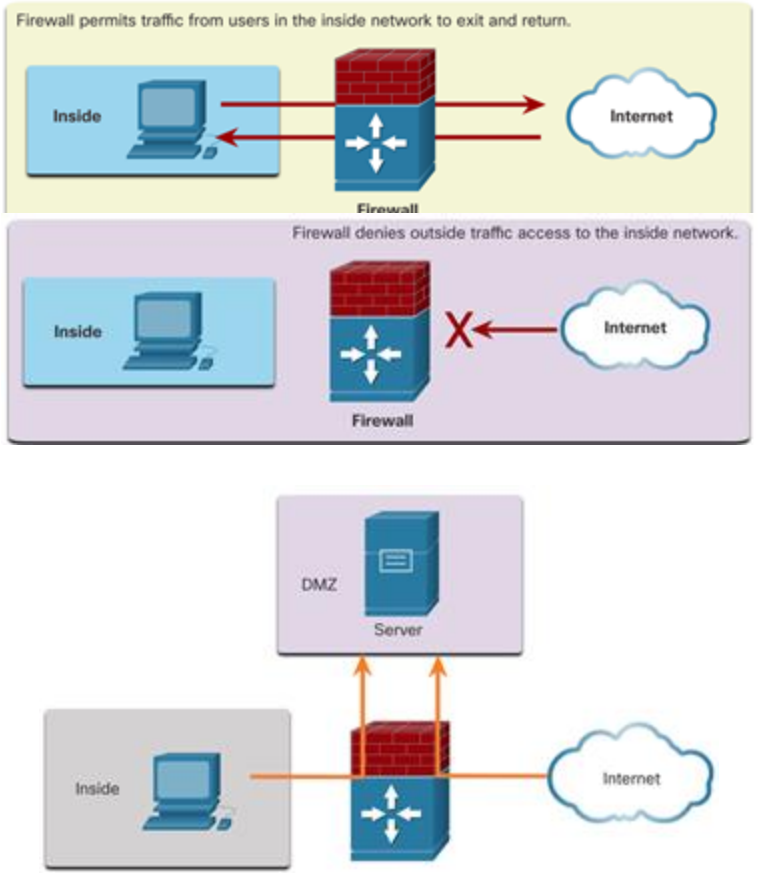
El concepto de AAA es similar al uso de una tarjeta de crédito. La tarjeta de crédito identifica quién la puede utilizar y cuánto puede gastar ese usuario, y lleva un registro de los elementos en los que el usuario gastó dinero.



Cortafuegos (Firewall)

Los firewalls de red residen entre dos o más redes, controlan el tráfico entre ellas y evitan el acceso no autorizado.

Un firewall podría brindar a usuarios externos acceso controlado a servicios específicos. Por ejemplo, los servidores accesibles para usuarios externos generalmente se encuentran en una red especial denominada zona desmilitarizada (DMZ). La DMZ permite a un administrador de red aplicar políticas específicas para los hosts conectados a esa red.



Tipos de cortafuegos

Los productos de firewall vienen empaquetados en varias formas. Estos productos utilizan diferentes técnicas para determinar qué se permitirá o negará el acceso a una red. Entre otros, se incluyen:

- **Filtrado de paquetes -** Evita o permite el acceso basado en direcciones IP o MAC**.**
- **Filtrado de aplicaciones -** Evita o permite el acceso a tipos de aplicaciones específicos según los números de puerto.
- **Filtrado de URL -** Evita o permite el acceso a sitios web basados en URL o palabras clave específicas**.**
- **Inspección de paquetes con estado (SPI)** - Los paquetes entrantes deben ser respuestas legítimas a las solicitudes de los hosts internos. Los paquetes no solicitados son bloqueados, a menos que se permitan específicamente. SPI también puede incluir la capacidad de reconocer y filtrar tipos específicos de ataques, como la denegación de servicio (DoS).

Puesto final de Seguridad

Una terminal, o un host, es un sistema de computación o un dispositivo individual que actúa como cliente de red. Las terminales comunes son PC portátiles, computadoras de escritorio, servidores, teléfono inteligentes y tabletas.

La seguridad de los dispositivos terminales es uno de los trabajos más desafiantes para un administrador de red, ya que incluye a la naturaleza humana. Las empresas deben aplicar políticas bien documentadas, y los empleados deben estar al tanto de estas reglas.

Se debe capacitar a los empleados sobre el uso correcto de la red. En general, estas políticas incluyen el uso de software antivirus y la prevención de intrusión de hosts. Las soluciones más integrales de seguridad de terminales dependen del control de acceso a la red.

16.4 Seguridad de dispositivos

Seguridad en Sistemas Operativos

La configuración de seguridad se establece en los valores predeterminados cuando se instala un nuevo sistema operativo en un dispositivo. En la mayoría de los casos, ese nivel de seguridad es insuficiente.

Además, existen algunos pasos simples que se deben seguir y que se aplican a la mayoría de los sistemas operativos:

- Se deben cambiar de inmediato los nombres de usuario y las contraseñas predeterminados.
- Se debe restringir el acceso a los recursos del sistema solamente a las personas que están autorizadas a utilizar dichos recursos.
- Siempre que sea posible, se deben desactivar y desinstalar todos los servicios y las aplicaciones innecesarios.
- A menudo, los dispositivos enviados por el fabricante pasaron cierto tiempo en un depósito y no tienen los parches más actualizados instalados. Es importante actualizar todo el software e instalar todos los parches de seguridad antes de la implementación.

Contraseñas

Para proteger los dispositivos de red, es importante utilizar contraseñas seguras. Las pautas estándar que se deben seguir son las siguientes:

- Use una contraseña de al menos ocho caracteres, preferiblemente 10 o más caracteres.
- Cree contraseñas complejas. Incluya una combinación de letras mayúsculas y minúsculas, números, símbolos y espacios, si están permitidos.
- Evite las contraseñas basadas en la repetición, las palabras comunes de diccionario, las secuencias de letras o números, los nombres de usuario, los nombres de parientes o mascotas, información biográfica (como fechas de nacimiento), números de identificación, nombres de antepasados u otra información fácilmente identificable.
- Escriba una contraseña con errores de ortografía a propósito. Por ejemplo, Smith = Smyth = 5mYth, o Seguridad = 5egur1dad.
- Cambie las contraseñas con frecuencia. Si una contraseña se ve comprometida sin saberlo, la ventana de oportunidad para que el actor de la amenaza use la contraseña es limitada.
- No anote las contraseñas ni las deje en lugares obvios, por ejemplo, en el escritorio o el monitor.

En los routers Cisco, se ignoran los espacios iniciales para las contraseñas, pero no ocurre lo mismo con los espacios que le siguen al primer carácter. Por lo tanto, un método para crear una contraseña segura es utilizar la barra espaciadora y crear una frase compuesta de muchas palabras. Esto se conoce como frase de contraseña. Una frase de contraseña suele ser más fácil de recordar que una contraseña simple. Además, es más larga y más difícil de descifrar.

Seguridad de contraseña adicional

Hay varios pasos que se pueden tomar para ayudar a garantizar que las contraseñas permanezcan secretas en un enrutador y conmutador Cisco, incluidas estas:

- Cifre todas las contraseñas de texto sin formato con el comando **service password-encryption**.
- Establezca una longitud mínima de contraseña aceptable con el comando **security passwords min-length** .
- Detente los ataques de adivinación de contraseñas de fuerza bruta con el***comando block-for # attempts # within # # .***
- Deshabilite un acceso en modo EXEC privilegiado inactivo después de un período de tiempo especificado con el comando **exec-timeout** .

```
Router(config)# service password-encryption
Router(config)# security password min-length 8
Router(config)# login block-for 120 attempts 3 within 60
Router(config)# line vty 0 4
Router(config-line)# password cisco
Router(config-line)# exec-timeout 5 30
Router(config-line)# transport input ssh
Router(config-line)# end
Router#
Router# show running-config | section line vty
line vty 0 4
 password 7 03095A0F034F
 exec-timeout 5 30
 login
Router#
```

Habilitar SSH

Es posible configurar un dispositivo Cisco para admitir SSH mediante los siguientes pasos:

Configure un nombre de host de dispositivo único. Un dispositivo debe tener un nombre de host único distinto del predeterminado.

Configure el nombre de dominio IP. Configure el nombre de dominio IP de la red utilizando el comando de modo de configuración global **ip-domain name**.

Generar una clave para cifrar el tráfico SSH. SSH cifra el tráfico entre el origen y el destino. Sin embargo, para ello, se debe generar una clave de autenticación única mediante el comando de configuración global **crypto key generate rsa general-keys modulus** *bits* . Los *bits* del módulo determinan el tamaño de la clave y se pueden configurar de 360 bits a 2048 bits. Cuanto mayor sea el valor de bit, más segura será la clave. Sin embargo, los valores de bits más grandes también tardan más en cifrar y descifrar la información. La longitud mínima de módulo recomendada es de 1024 bits.

Compruebe o cree una entrada de base de datos local. Cree una entrada de nombre de usuario de base de datos local utilizando el comando de configuración global **username.**

Autenticar contra la base de datos local. Utilice el comando de configuración de línea local **login** para autenticar la línea vty en la base de datos local.

Habilite las sesiones vty SSH entrantes. De forma predeterminada, no se permite ninguna sesión de entrada en las líneas vty. Puede especificar varios protocolos de entrada incluyendo Telnet y SSH mediante el comando transport input [ssh | telnet].


CISCO