ManageEngine
Access Manager Plus

Guía del administrador para **proteger el acceso remoto**

¿Qué es un acceso remoto seguro?

El acceso remoto seguro se refiere a una estrategia de seguridad de TI que permite el acceso autorizado y controlado a la red de una empresa, sistemas críticos de la misión o a cualquier dato confidencial. Permite a los equipos de TI suministrar varios niveles de acceso para empleados y terceros con base en sus roles y deberes laborales. Los métodos de acceso remoto seguro protegen los sistemas y aplicaciones, y garantizan su eficacia operativa continua.

¿Cuáles son los tipos de estrategias de acceso remoto seguro?

Algunos métodos notables de acceso remoto que permiten a las empresas acceder a su infraestructura de TI incluyen:

- **Red privada virtual (VPN):**

Las VPN son la forma más común de acceso remoto. Ellas usan autenticación y codificación para establecer una conexión segura a una red privada en la internet.

- **IPsec VPN**

IPsec es un grupo de protocolos de red usados para establecer conexiones codificadas, como VPN, en redes compartidas públicamente en la internet.

- **SSL VPN**

Las SSL VPN usan tecnología de autenticación y codificación para crear una conexión segura de VPN con un navegador web, lo que permite a usuarios remotos acceder a los recursos organizacionales desde fuera del entorno corporativo

- **Intercambio de desktop**

El intercambio de desktop o pantallas es un método de acceso y colaboración remotos que comparte una pantalla de desktop particular con otros dispositivos. Esto da al usuario control completo sobre el acceso en tiempo real a los datos de otro dispositivo.

- **Acceso remoto a Secure Shell (SSH)**

SSH es un protocolo de red que conecta usuarios a un equipo remoto sobre una conexión segura sin una contraseña. Un cliente de SSH da a los usuarios acceso a una terminal en modo de texto en un equipo remoto que ejecuta un servidor de SSH.

- **Control de acceso a redes (NAC)**

Las soluciones de NAC controlan y gestionan el acceso a toda la red de una organización—para sistemas on-premises o en la nube—mediante una combinación de autenticación, medidas de seguridad de endpoints y políticas de seguridad de red. Los sistemas de NAC pueden bloquear proactivamente amenazas antes de que se infiltren en la red.

- **Inicio de sesión único (SSO)**

SSO es un método de autenticación de usuarios que los autentica y les da acceso a varias aplicaciones y recursos a lo largo de la infraestructura de TI con solo un conjunto de credenciales para inicio de sesión.

- **Acceso a la red con confianza cero (ZTNA)**

Los sistemas ZTNA permiten el acceso seguro a aplicaciones privadas en la red solo después de la adecuada verificación. Es un modelo de acceso remoto seguro que no confía automáticamente en los usuarios y les da solo el acceso correcto con base en roles, privilegios mínimos y otros controles de seguridad detallados.

- **Acceso remoto con base en el contexto**

Esta estrategia aplica distintos controles de seguridad a distintos contextos de acceso, según los distintos niveles de seguridad. El control de acceso con base en el contexto da una gran flexibilidad y detalle, y define políticas basadas en quién accede a qué, cuándo, dónde, por qué y por cuánto tiempo.

- **Gestión de acceso privilegiado (PAM)**

La PAM es un conjunto de estrategias de seguridad informática que protege, gestiona y monitorea el acceso y los permisos privilegiados para usuarios, cuentas, aplicaciones, sistemas y procesos a lo largo del entorno de TI.

¿Por qué proteger el acceso remoto es importante?

La tendencia actual de trabajo remoto ha impactado a las estrategias generales de seguridad de muchas organizaciones y los administradores de TI ahora gestionan datos empresariales confidenciales y acceden a servidores sensibles desde ubicaciones remotas.
Los métodos tradicionales de seguridad de acceso ya no son suficientes para cubrir para las crecientes necesidades de acceso remoto.
Las organizaciones deben adoptar salvaguardas para dar a los empleados acceso remoto seguro en cualquier momento, desde cualquier dispositivo y ubicación.

- **Riesgos a partir del eslabón más débil de una empresa**

Los seres humanos son el eslabón más débil en la cadena de seguridad informática de una empresa, ya sea empleados internos descontentos o criminales cibernéticos externos que se hacen pasar por un infiltrado con privilegios. Con frecuencia, se da a los empleados más acceso del que requieren para sus roles. Los hábitos comunes de trabajo en casa como el uso de dispositivos corporativos para el trabajo personal, de dispositivos personales no gestionados desde una red casera para acceder a sistemas corporativos, la reutilización de contraseñas o el intercambio de dispositivos y datos sensibles con familiares pone los sistemas empresariales críticos en riesgo.

- **Los privilegios se dispersan en las redes corporativas**

Con la expansión del Internet de las cosas (IoT), muchos sistemas y aplicaciones requieren acceso privilegiado para garantizar la continuidad corporativa. Dichas entidades no humanas son más difíciles de gestionar, y la mayoría permanecen sin descubrir. Asimismo, a muchos empleados se les otorga acceso privilegiado extra para acelerar las operaciones, lo que da más oportunidades para que los atacantes se enfoquen en estas cuentas e instalen malware.

- **Los endpoints son uno de los objetivos clave de los ataques cibernéticos**

El creciente número de endpoints (equipos, laptops, servidores, smartphones, etc.) que requieren acceso a redes corporativas también amplían considerablemente la superficie de ataque. Los atacantes pueden explotar-cuentas administrativas predeterminadas, robar más credenciales, escalar privilegios y moverse lateralmente dentro de la red, vandalizando la cadena de seguridad.

- **Pirateo y estafas en el acceso remoto**

El trabajo remoto también presenta nuevos retos, especialmente empleados que son presa de sofisticadas estafas de phishing e intentos de pirateo. Los criminales cibernéticos aprovechan puntos débiles y vulnerables en métodos de acceso remoto no seguros y VPN para generar caos.

- **Aumento de la superficie de ataque**

El acceso privilegiado abarca toda la infraestructura de TI—en dispositivos endpoint, la nube, aplicaciones, sistemas de automatización y a lo largo de la línea de DevOps. Las malas prácticas de seguridad y el creciente panorama de amenazas ayudan a los criminales cibernéticos a explotar los activos corporativos más críticos.

- **Problemas con las VPN**

La mayoría de las organizaciones usa VPN para permitir el acceso remoto a sistemas remotos fuera de la red corporativa, lo que permite muchísimo movimiento lateral. Las VPN no dan controles detallados, y usarlas para facilitar el acceso administrativo remoto aumenta la vulnerabilidad a violaciones, amenazas internas y riesgos de credenciales comprometidas.

¿Cuáles son las ventajas de adoptar métodos de acceso remoto seguro?

Implementar una solución de acceso remoto seguro como parte de su programa de seguridad informática ayuda a las empresas a mitigar los riesgos de seguridad, reducir la complejidad operativa, mejorar la visibilidad del acceso privilegiado y adherirse a los estándares de cumplimiento.

- **Da un acceso centralizado a activos geográficamente restringidos**

De ahora en adelante, muchas organizaciones continuarán adoptando una cultura de trabajo en casa y tendrán a la mayoría de los empleados trabajando desde varias ubicaciones remotas. Un acceso remoto seguro permite a los líderes de TI y seguridad tener un punto de control central para gestionar recursos críticos desde cualquier lugar en el globo, tener controles detallados sobre rutas de acceso y definir cómo otros usuarios remotos privilegiados se conectan a sistemas críticos.

- **Permite el acceso detallado a terceros y sistemas externos**

Las soluciones de acceso remoto seguro ayudan a dar un acceso temporal basado en roles a terceros, como contratistas, proveedores y empleados subcontratados para acceder a sistemas o aplicaciones empresariales específicos sin la necesidad de credenciales privilegiadas. Compartir solo los datos suficientes con un tercero que depende de sus roles y deberes laborales puede ser muy ventajoso cuando se hace correctamente.

- **Aumenta la productividad y la facilidad de administración**

Implementar una solución de acceso remoto seguro facilita la administración centralizada de activos de TI distribuidos remotos mediante un solo punto de control. Los usuarios privilegiados pueden actualizar, resolver problemas y gestionar servidores remotos de forma centralizada, lo que facilita una administración rápida y eficaz. Esto también garantiza una mejora en la calidad laboral y una mejor rendición de cuentas mediante políticas estandarizadas y una supervisión eficaz.

- **Refuerza el gobierno general del acceso**

Además de dar acceso detallado, las soluciones de acceso remoto seguro también dan a los administradores los controles correctos para monitorear y gestionar activos distribuidos geográficamente. El monitoreo en tiempo real de sesiones remotas privilegiadas promueve la transparencia organizacional y da a los administradores de TI la capacidad de mitigar proactivamente ataques internos.

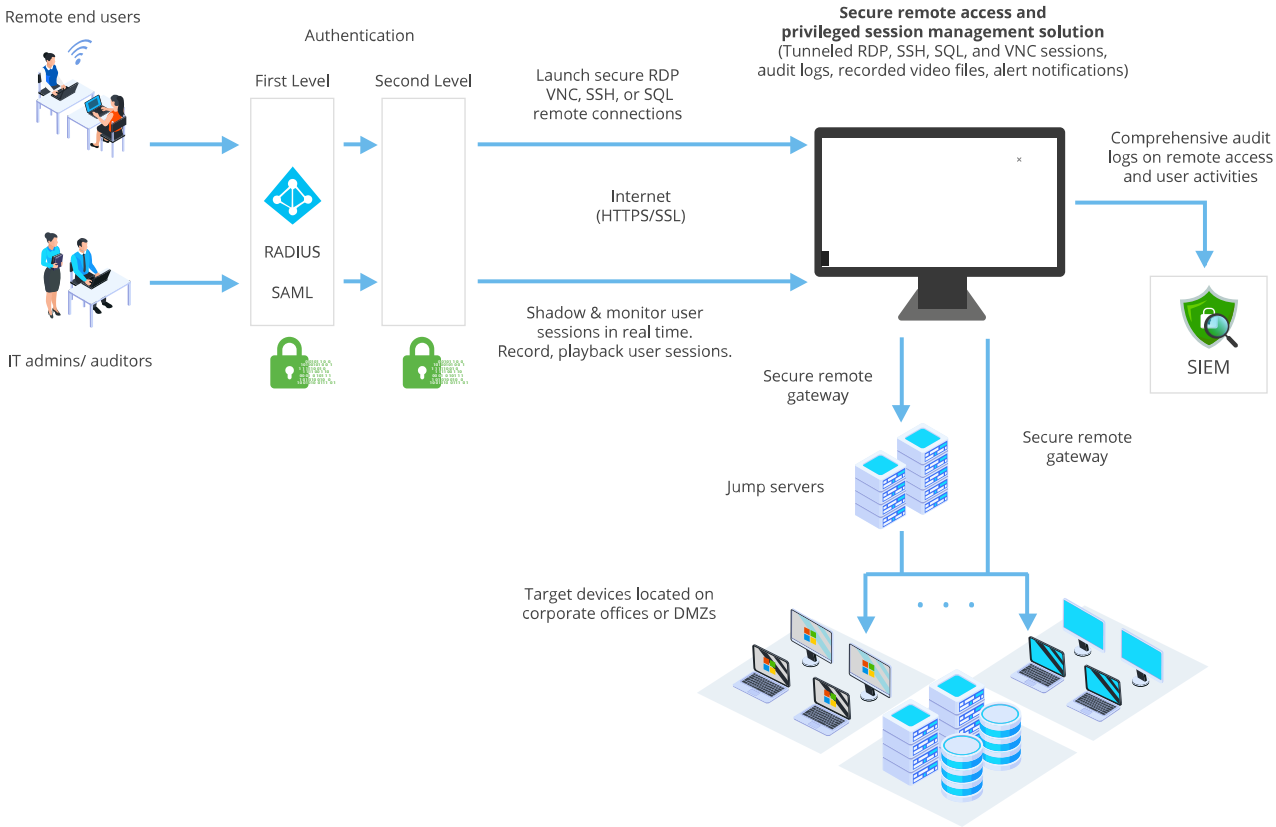
- **Ayuda a cumplir con varios estándares de cumplimiento para acceso remoto**

Un servicio de acceso remoto seguro cumple con los estándares de cumplimiento de la industria y permite a las organizaciones convencer a los clientes que confían en ellas de que mantienen sus datos tan seguros como sea posible. Implementar el acceso remoto seguro como parte de una estrategia integral de seguridad informática permite a las organizaciones registrar todas las actividades relacionadas con la infraestructura de TI y el acceso privilegiado críticos, lo que les ayuda a adherirse sin esfuerzo a los requisitos de auditoría y cumplimiento.

¿Cómo funciona el acceso remoto seguro?

Una herramienta de acceso remoto bien diseñada puede permitir conexiones seguras a sistemas objetivo y evitar el acceso no autorizado. Los siguientes pasos definen un proceso general de acceso remoto seguro y aplican para la mayoría de las arquitecturas de acceso remoto empresarial.

- Una sesión de acceso remoto empieza con la autenticación de usuarios u otras entidades, como sistemas o aplicaciones, mediante la identidad de la organización y el sistema de autenticación.
- Antes de autorizar una sesión remota, es obligatorio definir quién puede tener acceso a qué sistema, en qué momento, desde qué dispositivo y qué acciones específicas se pueden realizar.
- Luego de la autenticación exitosa, al usuario se le otorga un acceso controlado a los sistemas designados en la red empresarial, con base en los principios del control de acceso con menos privilegios o basado en roles (RBAC).



- Las sesiones remotas (RDP, SSH, SQL o VNC) se canalizan mediante rutas codificadas y seguras sin la necesidad de dar credenciales.
- Todas las sesiones remotas se graban como archivos de video para su revisión posterior a la sesión. Las sesiones también se monitorean en tiempo real.
- El equipo administrador puede bloquear o terminar una sesión remota sospechosa y la herramienta de acceso remoto seguro puede generar una alerta sobre actividades anómalas.
- Los logs de auditorías pueden también enviarse a sistemas SIEM para obtener mejor información sobre sesiones remotas privilegiadas.

Mejores prácticas para un acceso seguro

Incorporar las mejores prácticas y controles de seguridad para conexiones remotas es esencial, ya que una falta de seguridad en el acceso remoto podría permitir a los criminales cibernéticos obtener acceso a sistemas privilegiados, lo que resulta en violaciones de datos. Una solución eficaz de acceso remoto seguro incorpora las herramientas necesarias y las mejores prácticas para garantizar una seguridad informática y de acceso remoto completas. Si se consideran los retos que supone una carga laboral remota, es importante que los usuarios privilegiados tengan acceso remoto seguro a los sistemas e infraestructura críticos de la empresa.

- **Adoptar SSO y gestión de contraseñas**

Los empleados y terceros deben usar el acceso SSO para simplificar y centralizar el proceso de autenticación. Las empresas también deben considerar una bóveda central de credenciales que permita a los líderes de TI almacenar, gestionar y supervisar el uso de credenciales altamente sensibles y privilegiadas, y también reiniciarlas luego de una instancia de acceso único.

- **Exigir la autenticación multi factor (MFA)**

La MFA es imperativa para autenticar usuarios para un acceso remoto seguro. Muchas regulaciones y estándares de cumplimiento requieren MFA para el acceso remoto privilegiado.

- **Implementar una estrategia de seguridad de confianza cero**

Las empresas no deben confiar automáticamente en usuarios o aplicaciones que intentan acceder a la red interna. Es crucial conocer quién o qué solicita acceso, por qué, y desde dónde.

- **Adoptar políticas de acceso de privilegios mínimos**

La política de privilegios mínimos garantiza que a los empleados y terceros solo se les otorga el acceso mínimo y a tiempo requerido para realizar sus tareas, lo que evita que tengan acceso completo a toda la red corporativa por largos periodos de tiempo.

- **Aplicar controles de acceso detallados**

Garantice que solo usuarios privilegiados autorizados puedan acceder y gestionar recursos remotos. Establezca un conjunto de políticas que permita a los administradores controlar de forma remota las sesiones privilegiadas y obligar a los usuarios remotos a estar confinados a la actividad autorizada.

- **Gestionar activos de endpoints**

El mejor software de acceso remoto debe también suministrar una gestión eficaz de endpoints para proteger activos como laptops, teléfonos inteligentes y otros dispositivos de IoT de empleados. También debe ayudar a los administradores a monitorear los endpoints remotos, proteger proactivamente todos los dispositivos corporativos y proteger los datos corporativos.

- **Monitorear y auditar sesiones privilegiadas**

Monitoree el comportamiento de los usuarios en tiempo real para mitigar el riesgo de actividades no autorizadas. Una pista de auditoría integral ayuda a identificar vulnerabilidades y a rastrear una sesión anómala hasta la causa raíz. El monitoreo y registro de sesiones privilegiadas promueven la transparencia organizacional y permiten a los administradores de TI ver y, si es necesario, interrumpir y terminar una sesión privilegiada maliciosa.

- **Promover la conciencia de los empleados**

Capacite a sus empleados y garantice que siguen estrictamente los estándares de seguridad propuestos antes de conectarse a la red empresarial. Realice capacitaciones regulares sobre la importancia de políticas básicas de seguridad informática que involucren la integridad, confidencialidad, accesibilidad y disponibilidad de datos críticos, y explique la importancia de seguirlas.

Adoptar una estrategia de acceso remoto seguro

En el informe Market Guide for Zero Trust Network Access (ZTNA) de 2020, Gartner afirma que para el 2023, el 60% de las empresas reemplazará sus VPN con soluciones ZTNA. Una sólida solución de acceso remoto seguro da protección centralizada contra el abuso del acceso. Al fortalecer el acceso remoto privilegiado con una solución de confianza cero basada en privilegios, las organizaciones pueden tomar decisiones inteligentes y automatizadas mientras otorgan acceso privilegiado.

Se deben reemplazar las soluciones de acceso remoto seguro desactualizadas y tradicionales con las que cumplan con los modernos requisitos de acceso remoto para iniciar el acceso remoto seguro a cualquier sistema, o aplicación, desde cualquier ubicación, en cualquier momento. Las soluciones de acceso remoto seguro ayudan a las empresas a dar a los usuarios acceso detallado y obtener visibilidad de qué usuarios de los sistemas se conectan y qué acciones realizan durante toda la sesión remota.

ManageEngine Access Manager Plus es una solución de acceso remoto construida para ocuparse del acceso administrativo a endpoints remotos y otros sistemas críticos de TI. El servidor de gateway de la solución enruta todas las conexiones remotas mediante un canal codificado, lo que protege a las redes empresariales de malware y crímenes cibernéticos. Mediante una autenticación sólida, controles detallados y capacidades de gestión de sesiones, Access Manager Plus minimiza los riesgos de abuso de acceso deliberados y no intencionales mientras que a la vez permite a las empresas escoger y diseñar una estrategia utilitaria de acceso remoto.

Obtenga más información sobre ManageEngine Access Manager Plus y el software para el acceso remoto seguro de nuestros expertos.

Regístrese para una demo online gratuita

https://www.manageengine.com/latam/amp

Contáctenos
Correo electrónico: amp-support@manageengine.com
Phone: +1-925-924-9500

ManageEngine
Access Manager Plus