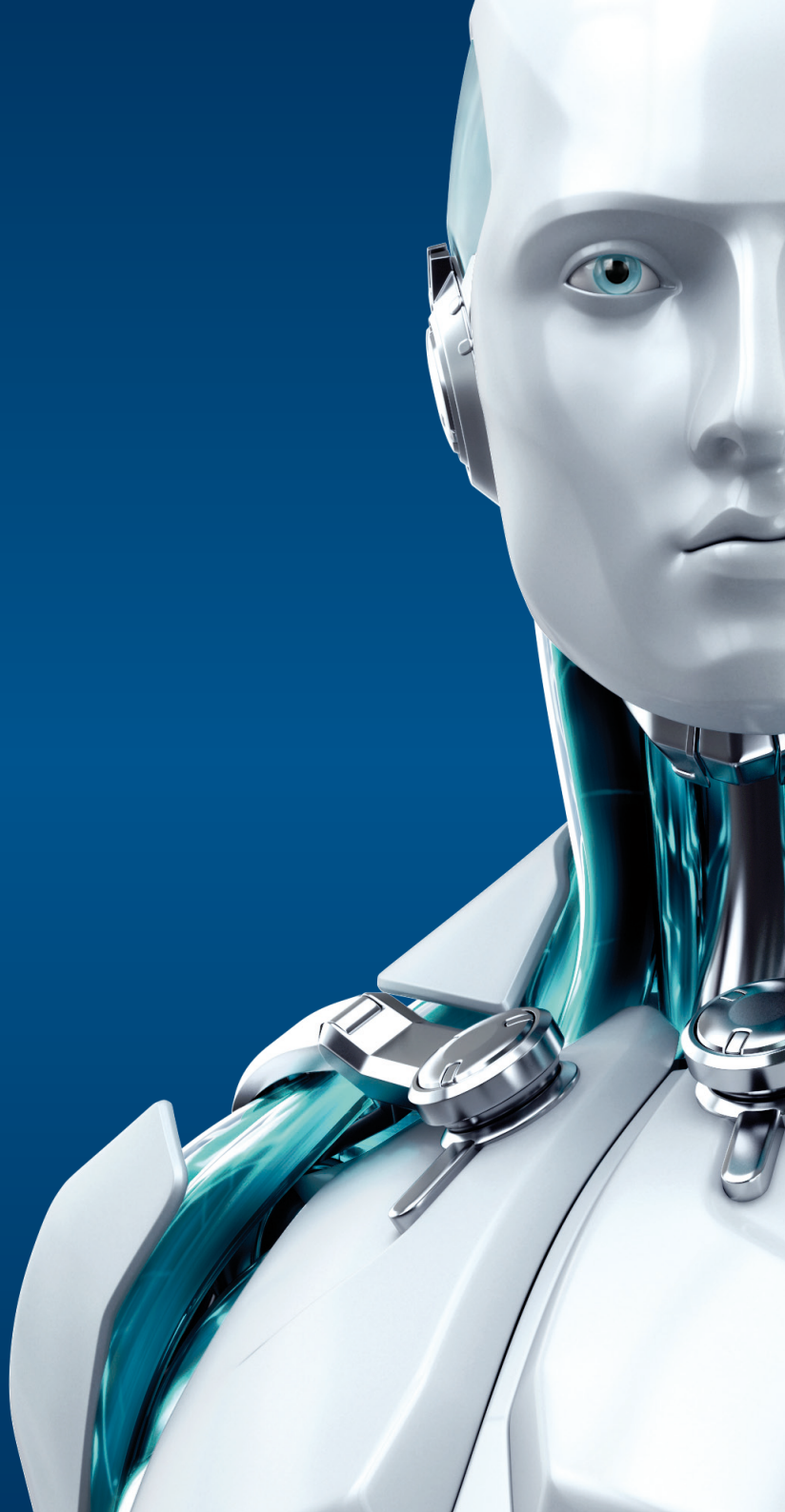
SECURE AUTHENTICATION

Mantiene la VPN protegida



ENJOY SAFER TECHNOLOGY™

Características generales

El creciente uso del acceso remoto está llevando a las empresas a buscar una solución segura y fácil de administrar para suministrar acceso a los bienes confidenciales corporativos.

Cada vez hay más cantidad de soluciones VPN económicas fáciles de administrar que ofrecen el acceso remoto y, en algunos casos, la Gestión unificada de amenazas a empresas de todos los tamaños, desde PYME hasta grandes corporaciones.

ESET, con su tecnología NOD32®, protege la infraestructura de TI corporativa en todos los sistemas operativos principales.
Ahora ofrece una forma de suministrar una autenticación fuerte a través de esta clase de dispositivos VPN, mediante el uso de Contraseñas de un solo uso (OTP, por sus siglas en inglés) generadas por una aplicación fácil de usar instalada en el teléfono móvil del usuario.

ESET Secure Authentication, en combinación con la VPN, le otorga un acceso remoto SSL-VPN fácil y seguro, sin clientes: en todas partes y en cualquier momento.

El problema

Los trabajadores móviles, las sucursales pequeñas o los partners y clientes les solicitan cada vez más a las empresas que habiliten el acceso remoto a las aplicaciones y recursos corporativos. La verdadera seguridad de red requiere varios elementos, muchos de los cuales son provistos mediante la creciente gama de dispositivos VPN.

Sin embargo, como ya es de conocimiento general que las contraseñas estáticas son inseguras y fáciles de verse comprometidas, muchos expertos en seguridad recomiendan suplementar la autenticación de usuarios integrada en estos dispositivos añadiendo un segundo factor de autenticación.

ESET Secure Authentication se integra con todos los dispositivos VPN para proporcionar autenticación en dos fases de los usuarios, asegurando una fuerte protección de la red corporativa y los recursos centrales.

La autenticación en dos fases (2FA) es un método de autenticación que requiere dos tipos de información independientes para comprobar la identidad del usuario. La 2FA es mucho más segura que la autenticación tradicional por contraseña, que requiere un solo factor.

Este documento sobre las características generales muestra lo rápido y fácil que es la configuración para dichos dispositivos.

Puede encontrar las guías detalladas de integración individuales para cada dispositivo VPN siguiendo los vínculos al final del presente documento o buscando en la Base de conocimientos de ESET por el nombre del dispositivo VPN.

La solución

ESET Secure Authentication se puede desplegar fácilmente para suplementar los dispositivos VPN existentes; de este modo, agrega una autenticación fuerte sin necesidad de realizar cambios significativos en la configuración de la VPN.

El método estándar de autenticación para la mayoría de los dispositivos VPN se basa en LDAP, RADIUS o autenticación local. ESET Secure Authentication usa RADIUS como método de autenticación externo para su dispositivo VPN.

Tras configurar ESET Secure Authentication y la VPN correctamente, habrá eliminado el punto más débil de toda infraestructura de seguridad: el uso de contraseñas estáticas, que se pueden robar, adivinar, reutilizar o compartir fácilmente.

Beneficios

ESET Secure Authentication ofrece los siguientes beneficios en combinación con el dispositivo VPN que haya elegido:

- Mejora considerablemente la seguridad, ya que requiere dos tipos de información independientes para la autenticación
- Reduce el riesgo por el uso de contraseñas débiles
- Requiere un tiempo mínimo para capacitación y soporte de los usuarios
- Se implementa fácilmente en la red

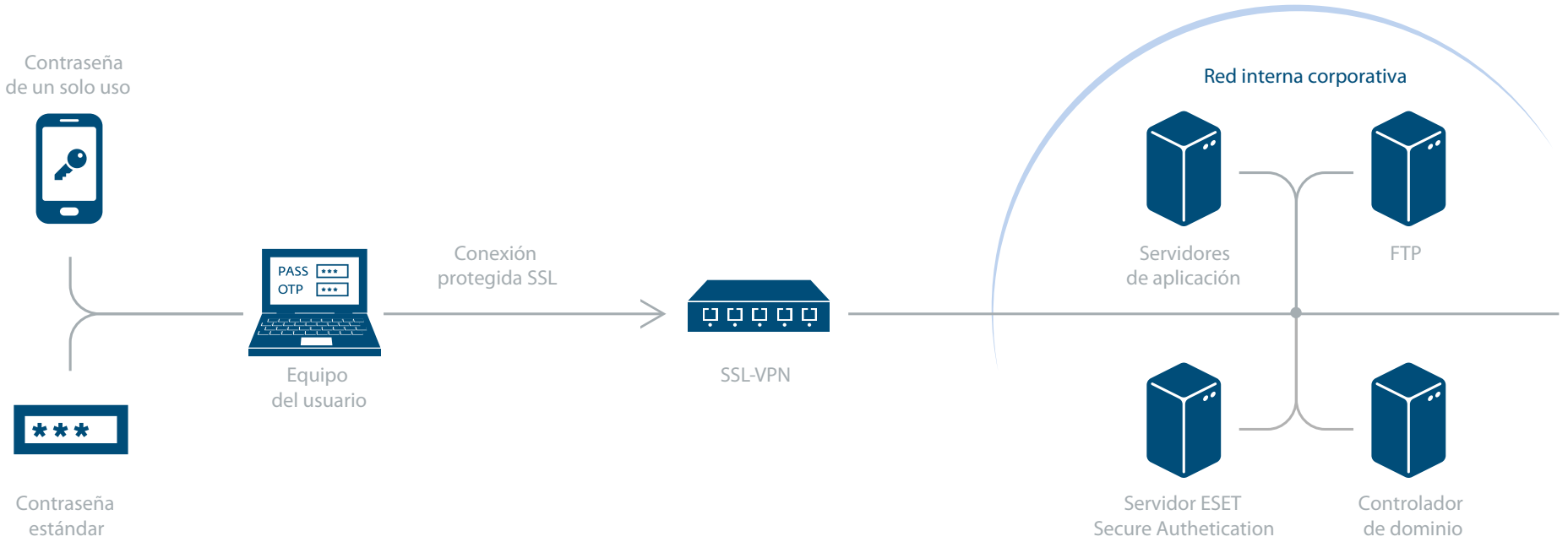
¿Cómo funciona la autenticación en dos fases con ESET Secure Authentication?

La autenticación en dos fases requiere el uso de un servicio de autenticación provisto por terceros. El servicio de autenticación está conformado por dos partes:

- Un Servidor RADIUS de ESET Secure Authentication que se ejecuta en la red de Windows, donde un administrador puede usar Usuarios y equipos de Active Directory (ADUC) para configurar la 2FA de los usuarios.
- Una aplicación móvil (para todos los sistemas operativos móviles) que se ejecuta en el teléfono móvil del usuario, utilizada para generar una OTP en cada intento de autenticación. Alternativamente, las OTP se pueden enviar por SMS bajo demanda.

Cuando el usuario ya está habilitado para usar 2FA, deberá ingresar una OTP válida junto con su contraseña estática para obtener acceso. Recibe los códigos de 6 dígitos de la aplicación que se está ejecutando en el teléfono móvil; estos códigos también se generan sin que el teléfono esté conectado a la red. La contraseña estática se reenvía mediante la VPN al back-end (controlador de dominio) para verificar que sea correcta. La OTP se reenvía y se comprueba con el servidor ESET Secure Authentication que se ejecuta en la red. El usuario se autentica solo cuando ambas son correctas.

SSL VPN con ESET Secure Authentication



Especificaciones técnicas

Información general

La autenticación RADIUS con ESET Secure Authentication funciona de la siguiente manera:

1. . Un usuario remoto inicia una conexión VPN
2. La VPN recopila el ID del usuario, la contraseña estática y la OTP, y envía dichas credenciales al servidor RADIUS de ESET Secure Authentication
3. El servidor presenta las credenciales en el Servicio de autenticación principal de ESET Secure Authentication
4. El Servicio de autenticación autentica la contraseña estática con AD, y la OTP con los datos secretos almacenados en la cuenta AD del usuario
5. A continuación, el dispositivo VPN le otorga al usuario autenticado el acceso a la red corporativa

Autenticación VPN con ESET Secure Authentication

El propósito principal de la autenticación VPN es proteger todos los tipos de conexiones. Para llevar a cabo dicha autenticación, se verifica con un servicio externo mediante el protocolo RADIUS: esto le permite al Servidor RADIUS de ESET Secure Authentication funcionar como un servicio back-end para la VPN.

Los usuarios primero son autenticados por el Servidor ESET Secure Authentication, que se puede vincular a Active Directory en el back-end. En efecto, el Servidor ESET Secure Authentication se despliega entre la VPN y Active Directory.

Esto significa que ESET Secure Authentication recibe todas las solicitudes de autenticación desde la VPN. La OTP con las solicitudes de autenticación son verificadas por el Servidor RADIUS de ESET Secure Authentication. El Servidor retransmite la contraseña estática al back-end (Servidor RADIUS o Active Directory) para su verificación si se solicita. Tras la verificación con éxito, se envía un mensaje ACCESS-ACCEPT de RADIUS a la VPN para la respuesta de autenticación.

Requisitos previos para proteger la VPN con ESET Secure Authentication

Requisitos previos de la VPN

Una VPN configurada y en funcionamiento es un requisito previo esencial para proteger la VPN con ESET Secure Authentication. Es importante que esté funcionando correctamente antes de que empiece a implementar ESET Secure Authentication.

Active Directory

Active Directory ya debe estar configurado: se usará como back-end para la autenticación correspondiente a las contraseñas estáticas de los usuarios. Las cuentas de usuarios también deben estar creadas en Active Directory.

Servidor ESET Secure Authentication

ESET Secure Authentication debe estar instalado en el Dominio de Active Directory. ESET Secure Authentication incluye un Servidor RADIUS autosostenible, por lo que tiene todo lo que necesita para incorporar la autenticación en dos fases a su VPN.

Guías de integración

La Base de conocimientos de ESET tiene guías disponibles para:

Barracuda SSL

Cisco ASA ipsec

Cisco ASA SSL

Citrix Access Gateway

Citrix Netscaler SSL

F5 Firepass SSL

Check Point Software

Fortinet Fortigate SSL

Juniper SSL

Microsoft RRAS

Microsoft RRAS with NPS

OpenVPN Access Server

Palo Alto SSL

Sonicwall SSL

Acerca de ESET

ESET es proveedor global de soluciones de seguridad para la empresa y el hogar. Su sede global está ubicada en Bratislava (Eslovaquia) y cuenta con oficinas en la región de Europa, Medio Oriente y África; la región de Asia Pacífico, América Latina y EE.UU. Más de 100 millones de expertos en TI y de usuarios domésticos en todo el mundo confían en los productos de ESET. Los centros globales de investigación de la empresa suministran innovación en seguridad a clientes de 180 países.

www.eset-la.com