Confianza

Seguridad, fiabilidad y privacidad de la información con los servicios a través de la nube de Cisco Meraki

Introducción

- 99,99% de fiabilidad con sus acuerdos de nivel de servicio
- Autenticación de dos factores
- Arquitectura redundante de alta disponibilidad
- Centros de datos auditados según SAS 70 de tipo II

Cisco Meraki opera el mayor servicio de red a través de la nube del sector. Sus servicios hacen funcionar más de 18.000 redes por todo el mundo. Además, Meraki cuenta con la mayor experiencia en la nube, ya que sus servicios de producción llevan cinco años funcionando ininterrumpidamente. Miles de profesionales de la informática, desde empresas a hospitales, bancos y comercios minoristas, confían en la plataforma de red a través de la nube de Meraki.

Este documento es el depósito central de información sobre seguridad, privacidad y fiabilidad con relación a los servicios alojados en la red de Meraki. Aquí encontrará información sobre:

- Nuestros centros de datos, procesos de seguridad y certificaciones.
- Cómo salvaguardar datos.
- Mejores prácticas para asegurar la red de su organización.
- Cómo siguen funcionando las redes Meraki cuando se desconectan de la nube.
- Información de conformidad con PCI, herramientas y mejores prácticas.
- Acuerdo de nivel de servicio de 99,99% de tiempo de actividad de Meraki.

Diseño de centros de datos Meraki

Los servicios Meraki están organizados en centros de datos de nivel 1 certificados según SAS70 tipo II. Estos centros de datos presentan las medidas de seguridad física y de software más modernas, así como diseños de alta fiabilidad. Todos los servicios Meraki se replican a lo largo de múltiples centros de datos independientes, de forma que, en caso de un fallo catastrófico del centro de datos, los servicios de cliente efectúan tolerancia a fallos rápidamente.

Seguimiento de disponibilidad

- Acuerdo de nivel de servicio de 99,99% de tiempo de actividad (menos de una hora al año de inactividad).
- Detección de fallos automatizada 24 horas: todos los servidores se comprueban cada cinco minutos desde múltiples ubicaciones.
- Procedimientos de escalado rápido a través de múltiples equipos de operaciones.
- Sistema independiente de alerta por interrupciones con triple redundancia

Redundancia

- Cinco centros de datos dispersos geográficamente.
- Datos de cliente (configuración de red y parámetros de uso) replicados en tres centros de datos independientes.
- Replicación en tiempo real de datos entre centros (cada 60 segundos).
- Archivado de copias de seguridad durante la noche.

Recuperación en caso de desastre

- Rápida tolerancia a fallos que conmuta en caliente en caso de fallo de hardware o desastre natural.
- La arquitectura fuera de banda mantiene la funcionalidad de la red del usuario final aunque la conectividad con los servicios a través de la nube de Meraki se vea interrumpida.
- Los procedimientos de tolerancia a fallos se realizan semanalmente.

Seguridad de los servicios a través de la nube

- Detección de intrusiones automatizada 24 horas.
- Protección mediante firewalls basados en puertos e IP.
- Acceso remoto restringido por dirección IP y verificado por clave pública (RSA).
- Sistemas sin acceso por contraseña.
- Alerta automática a administradores en caso de cambios de la configuración.

Arquitectura fuera de banda

- En la nube solo se almacenan la configuración de red y las estadísticas de uso.
- Los datos de usuarios finales no atraviesan el centro de datos.
- Todos los datos sensibles (p. ej., contraseñas) se almacenan en formato cifrado.

Seguridad física

- El acceso a las instalaciones se controla mediante lectores biométricos y un sistema de tarjetas codificadas de alta seguridad.
- Todas las entradas, salidas y armarios están sometidos a videovigilancia.
- Los guardias de seguridad vigilan 24 horas todo el tráfico entrante y saliente de los centros de datos, garantizando el seguimiento de los procesos de entrada.

Preparación ante desastres

- Los centros de datos cuentan con sofisticados sistemas de aspersores con bloqueos para evitar la descarga accidental de agua.
- Los generadores diésel ofrecen alimentación de respaldo en caso de corte de corriente.
- Los sistemas de alimentación ininterrumpida proporcionan alimentación y garantizan el correcto apagado en caso de corte total de la corriente.
- Cada centro de datos disfruta del servicio de, al menos, dos operadores de máximo nivel.
- El suelo elevado, los armarios y los sistemas de apoyo cuentan con tirantes antisísmicos.
- En caso de fallo catastrófico de un centro de datos, la tolerancia a fallos conmuta los servicios a otro centro de datos separado geográficamente.

Controles medioambientales

- Nuestros sistemas de calefacción, refrigeración y ventilación sobredimensionados ofrecen control de la humedad y refrigeración.
- Los sistemas de suelo se encargan de la distribución del aire.

Pruebas de penetración periódicas

- Todos los centros de datos Meraki se someten diariamente a pruebas de penetración realizadas por una empresa independiente.

Certificación de centros de datos

- Los centros de datos Meraki cuentan con la certificación SAS70 de tipo II.

Plano de control fuera de banda

El plano de control fuera de banda de Meraki separa los datos de gestión de la red de los datos de usuario. Los datos de gestión (p. ej., configuración, estadísticas, seguimiento, etc.) pasan de los dispositivos Meraki (routers y puntos de acceso inalámbricos) hasta la nube de Meraki a través de una conexión a Internet segura. Los datos de usuario (navegación web, aplicaciones internas, etc.) no atraviesan la nube, sino que van directamente a su destino a través de la LAN o WAN.

Ventajas de un plano de control fuera de banda:

Escalabilidad

- Rendimiento ilimitado: sin cuellos de botella de controladores centralizados.
- Agregue dispositivos o sitios sin túneles MPLS.

Fiabilidad

- El servicio redundante a través de la nube ofrece una alta disponibilidad.
- Funciones de red aunque el tráfico de gestión se vea interrumpido.

Seguridad

- El tráfico de usuario no pasa por los centros de datos Meraki.
- Conformidad total con HIPAA / PCI.

¿Qué sucede si mi red pierde la conectividad con Meraki Cloud Controller?

Gracias a la arquitectura fuera de banda de Meraki, la mayoría de usuarios finales no se verán afectados si los routers y puntos de acceso inalámbricos Meraki no pueden comunicarse con los servicios a través de la nube de Meraki (p. ej., debido a un fallo temporal de WAN):

- Los usuarios pueden acceder a la red local (impresoras, archivos compartidos, etc.).
- Si hay conectividad WAN, los usuarios pueden acceder a Internet.
- Las políticas de red (reglas de firewall, QoS, etc.) continúan vigentes.
- Los usuarios pueden autenticarse con 802.1X/RADIUS.
- Los usuarios inalámbricos pueden cambiar de punto de acceso.
- Los usuarios pueden iniciar y renovar asignaciones DHCP.
- Los túneles VPN establecidos siguen funcionando.
- Las herramientas de configuración local están disponibles (p. ej., configuración IP de dispositivos).

Mientras la nube de Meraki esté inaccesible, la gestión, el seguimiento y los servicios de host dejarán de estar disponibles temporalmente:

- Las herramientas de configuración y diagnóstico no estarán disponibles.
- Las estadísticas de uso quedarán almacenadas localmente hasta que se restablezca la conexión con la nube; en ese momento se subirán a la nube.
- Las páginas de inicio y sus funciones no estarán disponibles.

Herramientas de seguridad y mejores prácticas para administradores

Además de la arquitectura fuera de banda segura y los centros de datos reforzados de Meraki, la marca ofrece una serie de herramientas para que los administradores puedan maximizar la seguridad de sus implantaciones de red. El uso de estas herramientas proporciona una protección, visibilidad y control óptimos de la red Meraki. Desde esta página podrá aumentar de forma rápida y sencilla la seguridad de sus cuentas meraki.com y consultar las mejores prácticas recomendadas para controlar y auditar cuentas. Para más información, consulte el manual de Meraki Cloud Controller.

Habilitación de la autenticación de dos factores

La autenticación de dos factores agrega una capa de seguridad extra a la red de una organización al solicitar acceso al teléfono del administrador, además de su nombre de usuario y contraseña, para iniciar la sesión en los servicios a través de la nube de Meraki. La implementación de autenticación de dos factores de Meraki utiliza la tecnología SMS de forma segura, cómoda y económica: tras introducir el nombre de usuario y la contraseña, el administrador recibe un código de acceso de un solo uso por SMS, que deberá introducir para completar la autenticación. Aunque un hacker adivinara o descubriera la contraseña de un administrador, no podría acceder a la cuenta de la organización, ya que no tendría acceso al teléfono del administrador. Meraki incluye autenticación de dos factores para todos los usuarios de empresa sin coste adicional.

Endurezca sus políticas de contraseña

Puede configurar las políticas de seguridad de su organización de forma que las cuentas Meraki protejan aún mejor el acceso al panel de gestión Meraki. En Organization -> Configure (Organización -> Configurar), es posible:

- Forzar el cambio periódico de las contraseñas (p. ej., cada 90 días).
- Exigir una longitud y complejidad mínimas para las contraseñas.
- Bloquear a los usuarios tras una serie de intentos de inicio de sesión fallidos.
- No permitir usar la misma contraseña.
- Restringir el inicio de sesión por dirección IP.

Implante el principio de privilegios mínimos con la administración basada en roles

La administración basada en roles permite nombrar administradores para subconjuntos concretos de su organización y especificar si tendrán acceso de solo lectura a informes y herramientas de solución de problemas, si podrán administrar el acceso de visitantes gestionados a través de Meraki Lobby Ambassador o cambiar la configuración de la red. La administración basada en roles reduce la probabilidad de errores de configuración accidentales o maliciosos, y limita los errores a partes aisladas de la red.

Habilitación de alertas por correo electrónico de cambios en la configuración

El sistema Meraki permite enviar automáticamente alertas por correo electrónico con texto perfectamente legible si se realizan cambios en la configuración de red, lo que permite a toda la organización de TI estar al día de las nuevas políticas. Las alertas de cambios son especialmente importantes en las organizaciones de TI de gran tamaño o distribuidas.

Auditoría periódica de la configuración y los inicios de sesión

Meraki registra la hora, la IP y la ubicación aproximada (ciudad, provincia) de los administradores que inician una sesión. Además, Meraki ofrece un registro de cambios de configuración con función de búsqueda en el que podrá ver qué cambios se realizaron, quién los realizó y en qué parte de la organización tuvo lugar el cambio. Esta capacidad de auditar la información de configuración e inicio de sesión ofrece una gran visibilidad de la red.

Verificación de certificados SSL

Las cuentas Meraki solo están accesibles a través de https, lo que garantiza que toda la comunicación entre el navegador de un administrador y los servicios a través de la nube de Meraki esté cifrada. Al igual que sucede con los servicios web seguros, no inicie una sesión si su navegador muestra una advertencia de certificado, ya que podría tratarse de un ataque de suplantación de identidad.

Desconexión del servidor por inactividad

30 segundos antes de la desconexión, los usuarios reciben una notificación que les permitirá ampliar su sesión. Una vez transcurrido este plazo, se les pedirá que vuelvan a iniciar la sesión.

Conformidad con PCI

Meraki ofrece una completa solución para garantizar que los entornos inalámbricos cumplan la conformidad con PCI según los exigentes estándares de una auditoría PCI de nivel 1 (el nivel de auditoría más estricto). El potente conjunto de funciones de seguridad de Meraki cumple todos los estándares de seguridad de datos de PCI, ayudando a los clientes a crear y mantener una red segura, proteger los datos de los titulares de tarjetas, mantener un programa de gestión de las vulnerabilidades, implementar medidas de control de acceso estrictas y hacer un seguimiento de la seguridad de la red.

A diferencia de las LAN inalámbricas tradicionales, la infraestructura de seguridad inteligente de Meraki elimina las complejidades de gestión, las pruebas manuales y los problemas de mantenimiento que provocan las vulnerabilidades. Las características de seguridad intuitivas y económicas de Meraki resultan ideales para los administradores de red, mientras que sus potentes y eficaces herramientas de administración, protección de cuentas, auditoría y gestión de cambios son perfectas para los responsables de la seguridad informática.

Gracias a la gestión centralizada a través de la nube, Meraki permite implantar, vigilar y verificar de forma sencilla y económica las funciones WiFi conformes a PCI en redes distribuidas de cualquier tamaño.

Acuerdo de nivel de servicio Meraki

Durante el plazo de vigencia de la licencia de Meraki Cloud Controller (el "acuerdo"), la interfaz web de Meraki Cloud Controller estará operativa y disponible para el cliente al menos el 99,9% del tiempo de cualquier mes natural (el "acuerdo de nivel de servicio Meraki"). Si Meraki no cumple este acuerdo de nivel de servicio y el cliente cumple las obligaciones adquiridas en virtud de dicho acuerdo, el cliente tendrá derecho a recibir los créditos de servicio descritos a continuación. El acuerdo de nivel de servicio Meraki establece esta única y exclusiva compensación para el cliente en caso de que Meraki no cumpla dicho acuerdo de nivel de servicio Meraki.

Definiciones

Las siguientes definiciones son de aplicación en el Acuerdo de nivel de servicio Meraki.

Como "tiempo de inactividad" se entiende más de un cinco por ciento de índice de error para el usuario. El tiempo de inactividad se mide en función del índice de error en el servidor.

Como "servicios cubiertos por Meraki" se entiende el servicio de Meraki Cloud Controller para cualquier producto Meraki.

Como "porcentaje de tiempo de actividad mensual" se entiende el número total de minutos en un mes natural menos el número de minutos de inactividad sufridos durante dicho mes natural, dividido por el número total de minutos de dicho mes natural.

Como "Crédito de servicio" se entiende que Meraki agregará un número determinado de días de servicio al finalizar el plazo de vigencia de la licencia sin coste alguno para el cliente.

El cliente debe solicitar el crédito de servicio

Para recibir cualquiera de los créditos de servicio anteriormente descritos, el cliente deberá notificárselo a Meraki treinta días antes del momento en que el cliente tenga derecho a recibir el crédito de servicio. Si no cumpliera este requisito, el cliente perderá su derecho a recibir el crédito de servicio.

Crédito de servicio máximo

El número total máximo de créditos de servicio que Meraki otorgará al cliente por todo el tiempo de inactividad acaecido en un mes natural no excederá los 15 días de servicio, añadidos al término del servicio al cliente (o el valor de 15 días de servicio en forma de crédito monetario en la cuenta de un cliente con facturación mensual). Los créditos de servicio no pueden intercambiarse ni convertirse en cantidades monetarias.

Exclusiones del acuerdo de nivel de servicio Meraki

El acuerdo de nivel de servicio Meraki no se aplica a ningún servicio excluido expresamente de este acuerdo de nivel de servicio Meraki (según lo indicado en la documentación de tales servicios) ni a ningún problema de rendimiento: (i) causado por "fuerza mayor" o (ii) consecuencia de los equipos del cliente o de los equipos de terceros, o de ambos (fuera del control principal de Meraki).