Sophos RED (Remote Ethernet Device)

Sophos Remote Ethernet Device (RED) es un dispositivo de red pequeño, diseñado para ser lo más fácil de implementar posible. Su objetivo principal es proporcionar un túnel seguro desde su ubicación de despliegue a un firewall de Sophos UTM.

No hay una interfaz de usuario en el dispositivo RED. Está diseñado para ser completamente configurado y gestionado desde un Sophos UTM. Los dispositivos RED se pueden enviar a un sitio remoto, conectarse a cualquier conexión DHCP a Internet y ser configurados completamente por un administrador remoto sin conocimiento previo del sitio y sin necesidad de guiar al personal local a través de los pasos de configuración técnica.ciertos

Esta guía detalla cómo configurar Sophos RED en cada uno de sus modos operativos, y describe los pasos comunes de solución de problemas para resolver problemas de conexión.

Descripción técnica RED

Cuando se configura un RED en un firewall Sophos UTM, las opciones de configuración elegidas por el administrador se cargan en los servidores de aprovisionamiento de Sophos. La configuración es un poco más que los siguientes elementos:

- Dirección del firewall al que hará túnel
- Modo de enlace ascendente WAN (DHCP, IP estático)
- Modo de funcionamiento del túnel (estándar)
- Si se elige el modo de enlace ascendente estático, la configuración de la dirección RED WAN (dirección, máscara de red, puerta de enlace predeterminada y servidor DNS)
- Opcionalmente, configuraciones de conexión de banda ancha móvil para RED v2 y hardware anterior
- Código de desbloqueo

El código de desbloqueo no se almacena en el dispositivo RED, pero se usa para evitar que un RED que esté en uso sea redirigido accidental o maliciosamente. Se debe suministrar el código de desbloqueo correcto para que los servidores de aprovisionamiento acepten una nueva configuración para un RED. Inicialmente, el código de desbloqueo está en blanco, hasta que se haya conectado un RED a un UTM una vez. La primera vez que se configura un dispositivo RED en un UTM, el código de desbloqueo debe dejarse en blanco. Cada vez que se conecta un RED a un nuevo UTM, se debe ingresar el código de desbloqueo anterior en el nuevo UTM para mover el RED. Una vez que la configuración se envía al servidor de aprovisionamiento, se emite un nuevo código de desbloqueo y se muestra en WebAdmin del UTM.

Los servidores de aprovisionamiento almacenan la configuración proporcionada por el administrador en un conjunto de servidores centralmente accesible. Los dispositivos RED se pueden configurar centralmente debido a este mecanismo. Cuando un dispositivo RED no tiene configuración, o la configuración que tiene no es exitosa, buscará las instrucciones actualizadas en los servidores de aprovisionamiento. Una búsqueda DNS de red.astaro.com devolverá el servidor de aprovisionamiento más cercano, con el que se conectará de forma segura, y buscará nuevas

instrucciones de los servidores de aprovisionamiento. Siempre que un RED tenga una configuración de trabajo, no volverá a verificar con los servidores de aprovisionamiento.

Descripción general de los modos operativos RED

RED puede operar en varios modos. Esta sección ayudará a comprender cómo funciona cada uno de estos modos, y le ayudará a decidir qué modos son los más adecuados para cada circunstancia.

La pestaña del asistente de implementación en UTM WebAdmin puede ayudar a configurar nuevos dispositivos con gran rapidez. Hace gran parte del trabajo necesario para habilitar completamente un túnel RED para que esté activo y pueda permitir el tráfico. En los ejemplos siguientes, no usaremos el asistente, sino que recorreremos todos los pasos manualmente. Estos escenarios harán referencia a dos dispositivos de Sophos diferentes. Uno es el dispositivo RED, que se encuentra en la ubicación remota. El otro es el dispositivo UTM con el cual el dispositivo RED establecerá un túnel. Ambos tendrán una conexión a internet, como se muestra en la figura 1.

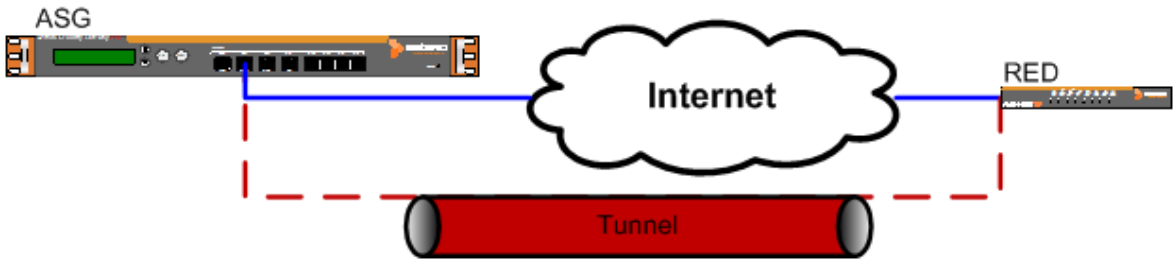


Figura 1: diseño general RED

Standard/Unified Mode

Este es el modo más comúnmente utilizado. En este modo, esperamos que la red remota sea totalmente administrada por el UTM, a través del RED. El UTM puede ofrecer DHCP para la LAN remota, y el RED puede ser el único dispositivo que conecta la LAN a Internet. No hay una ruta paralela alrededor del RED a Internet.

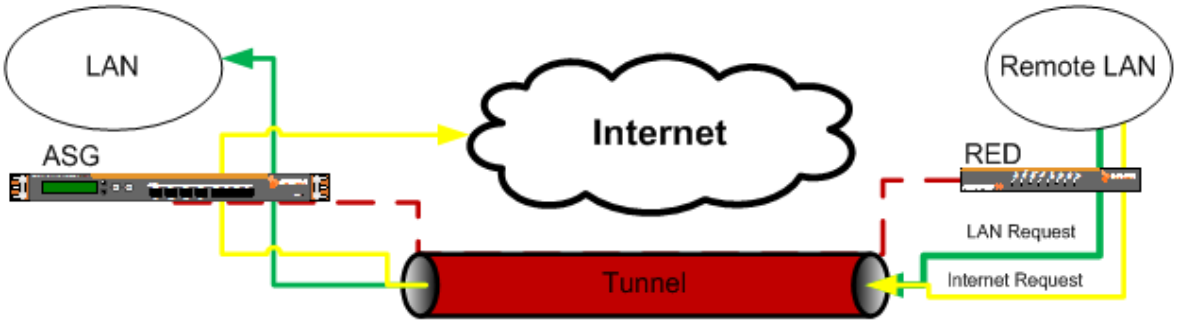


Figure 2: RED Usado en Modo Standard/Unified

La Figura 2 Muestra el flujo de datos en este modo operativo. Todo el tráfico de la LAN remota pasará por el túnel RED, ya sea que se dirija a la LAN local o a Internet. Esto permite que el UTM permita o rechace solicitudes exactamente de la misma manera que lo hace para el tráfico procedente de la LAN local. El tráfico entre las LAN locales y remotas puede bloquearse o permitirse solo mediante el uso de reglas de firewall en el UTM. El tráfico web se puede filtrar utilizando el módulo de seguridad web y las aplicaciones como Skype o BitTorrent se pueden controlar para usuarios de LAN remotos, al igual que para los usuarios de LAN. Esto proporciona el más alto nivel de seguridad y capacidad de administración para redes remotas. Su mayor inconveniente es el aumento de los requisitos de ancho de banda que puede colocar en el enlace de Internet de UTM. Dado que todo el tráfico de Internet desde la LAN remota también utiliza ancho de banda de Internet en el UTM, el ancho de banda de Internet en el UTM debe ser lo suficientemente grande como para atender las solicitudes de sus propios usuarios locales y todos los usuarios remotos de RED. El dispositivo RED 10 es capaz de canalizar datos a hasta 30 Mbps.

En caso de que el RED pierda contacto con el ASG y el túnel falle, el RED se cerrara. Los usuarios de LAN remota perderán el acceso a Internet, así como a las LAN UTM hasta que el túnel pueda volver a conectarse.

Standard/Split Mode

El modo estándar / Split es físicamente similar al estándar / unificado. Esperamos que la red remota pueda ser administrada por el UTM, y UTM puede proporcionar DHCP a la LAN remota. Además, el RED es probablemente el único dispositivo entre la LAN e Internet; sin embargo, solo el tráfico de las redes seleccionadas se envía a través del túnel. El resto del tráfico se envía directamente a la conexión de internet local. El RED ocultará el tráfico saliente proveniente de su dirección IP pública. Esto minimiza el uso del ancho de banda sobre el túnel y aligera los requisitos de ancho de banda en el UTM, pero también reduce sustancialmente la capacidad de administración de la red remota. El tráfico hacia o desde Internet no se puede filtrar ni proteger de las amenazas. La seguridad solo se puede aplicar entre las LAN remotas y locales.

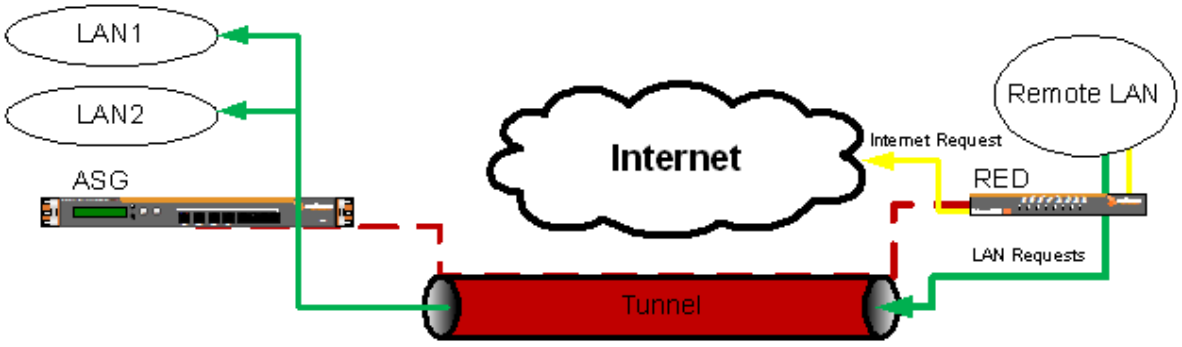


Figure 3: RED Used in Standard/Split Mode

En caso de que el RED pierda contacto con el UTM, y el túnel falle, el RED fallará. Los usuarios de LAN remota perderán el acceso a Internet, así como a las LAN UTM hasta que el túnel pueda volver a conectarse.

Transparent/Split

En esta opción, no se espera que el UTM administre la red remota. Se conectará entre la LAN remota y la puerta de enlace de la LAN remota, y esperará recibir una dirección en la LAN remota a través de DHCP. De forma similar a la opción Estándar / División, solo el tráfico destinado a ciertas redes se enviará por el túnel. En este caso, el RED no actúa como puerta de enlace, pero como está en línea con la puerta de enlace, puede redirigir paquetes de forma transparente por el túnel.

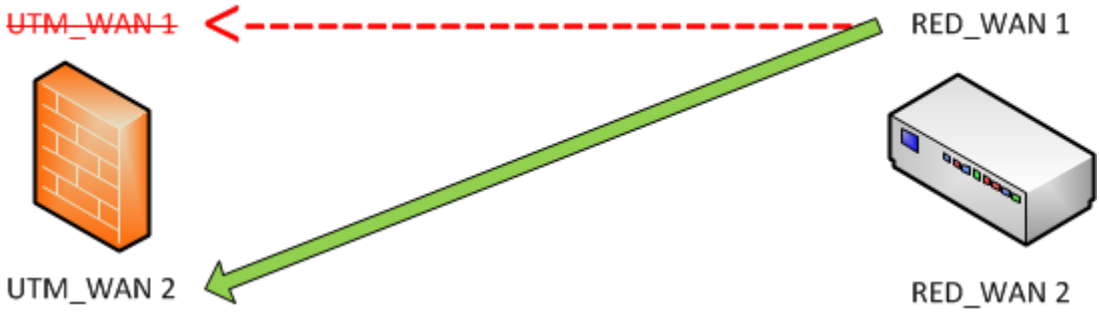
Esta opción no requiere reconfiguración de la red remota, pero no permite ninguna administración de la LAN remota. Solo puede proporcionar seguridad entre la LAN remota y cualquier subred local a la que se pueda acceder a través del túnel. Además, en caso de que el túnel se apague, la conexión a Internet también se desactivará para cualquier dispositivo detrás del RED.

Deployment Scenarios

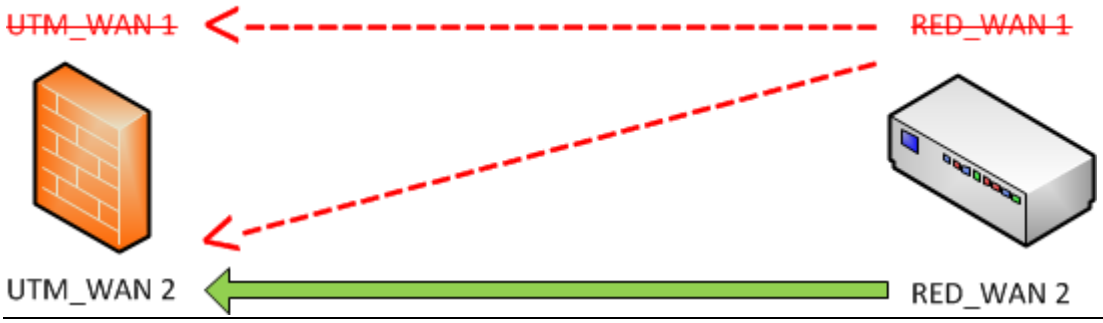
- **UTM hostname = Failover**
- **RED uplink = Failover**

Sophos RED eestablece una connection entre RED_WAN1 and UTM_WAN1.

Si UTM_WAN1 esta caído: RED_WAN1 se conectara al UTM_WAN2

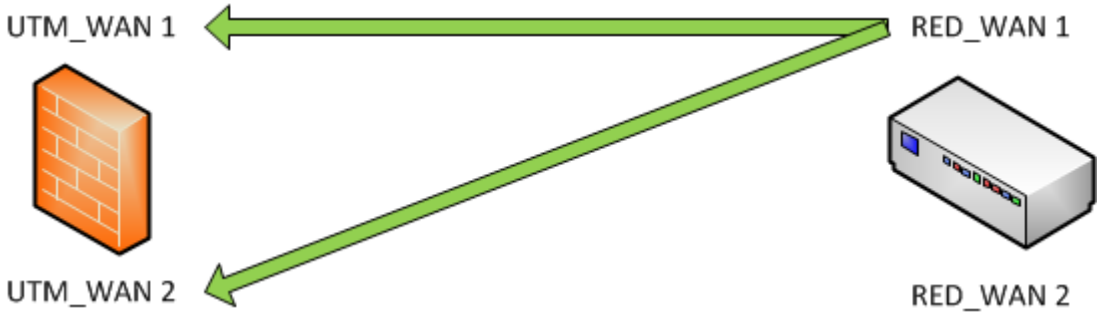


SI UTM_WAN1 y RED_WAN1 están caídos: RED_WAN2 se conectará a UTM_WAN2

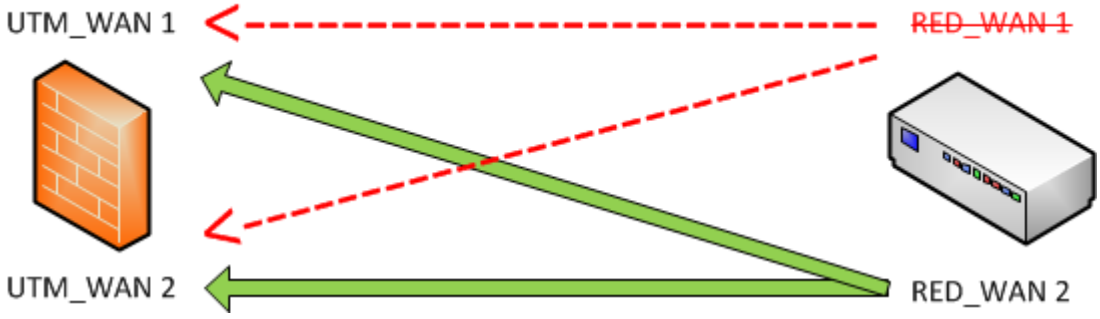


- **UTM hostname = Balancing**
- **RED uplink = Failover**

Sophos RED establece una coeccion entre RED_WAN1 y UTM_WAN1/UTM_WAN2

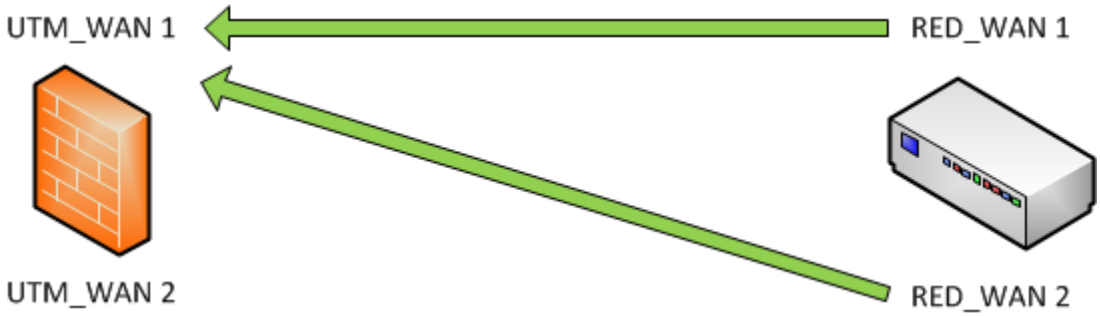


SI RED_WAN1 esta caído: RED_WAN2 se conectara a UTM_WAN1/UTM_WAN2

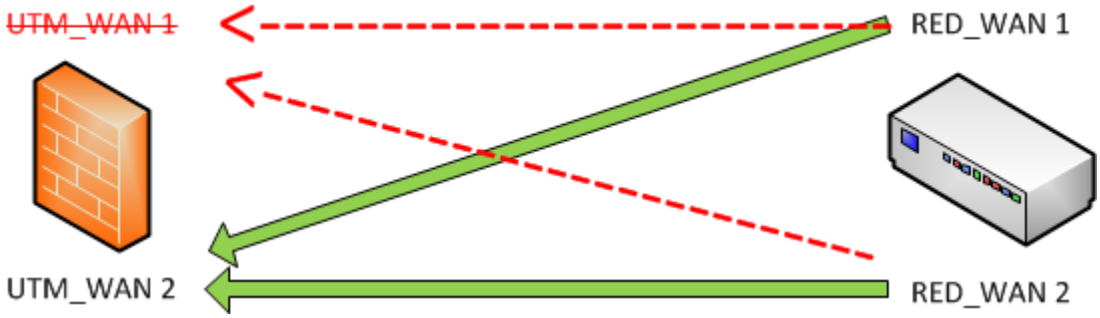


- **UTM hostname = Failover**
- **RED uplink = Balancing**

Sophos RED establece una conexión entre RED_WAN1/RED_WAN2 y UTM_WAN1

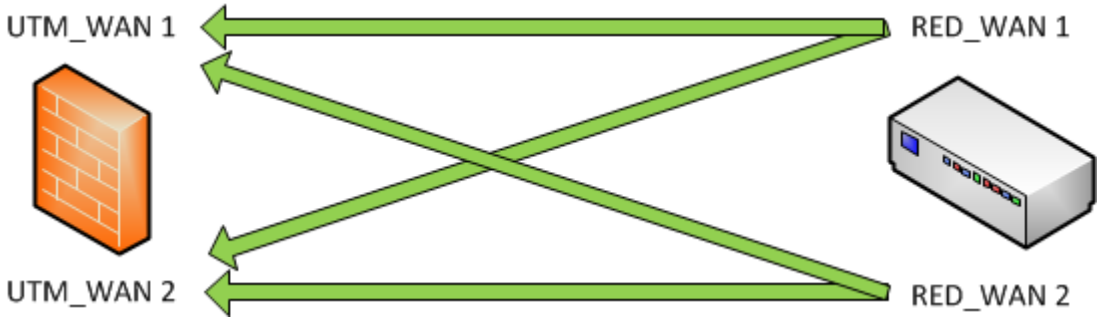


Si UTM_WAN1 este caído: RED_WAN1 / RED_WAN2 se conectan a UTM_WAN2



- **UTM hostname = Balancing**
- **RED uplink = Balancing**

Sophos RED establece una conexión entre RED_WAN1 / RED_WAN2 y UTM_WAN1/UTM_WAN2



Nota: Si cualquier interfaz se cae, la interface será checada hasta que este trabajando nuevamente. La conexión será restaurada a la interfase original si está disponible nuevamente

OPCIONES AVANZADAS

Manual / Split Setup

Esta no es una opción que se pueda elegir al configurar el RED, pero se implementa principalmente a través de la configuración física. Este modo no difiere del modo transparente / dividido, pero permite que el túnel se apague sin desactivar también el acceso local a Internet. En este escenario, el RED se configura en modo Estándar / Unificado, pero no se coloca delante de la LAN remota. Está conectado como una puerta de enlace alternativa en la LAN remota, y las rutas se deben agregar en la puerta de enlace predeterminada existente para acceder a redes remotas detrás de la RED.

El puerto WAN está conectado al mismo conmutador LAN al que están conectados los clientes LAN, y una vez que el RED recibe su configuración de modo, conecta un puerto LAN al mismo conmutador LAN.

La configuración es marginalmente más compleja físicamente que otros modos, pero es lógicamente más simple y permite la falla de hardware de túnel o RED, sin interrumpir el tráfico normal de Internet.

Bridged RED Setup

Cuando se trata de una gran cantidad de dispositivos RED, puede ser más sencillo tratar todas las redes remotas RED como una sola LAN. El UTM admite la creación de una única interfaz de puente, puenteando cualquier cantidad de NIC. Si aún no ha configurado una interfaz de puente, puede conectar más de una conexión RED juntas, para tratar eficazmente todas las conexiones remotas de RED como una única LAN. El acceso de RED a RED todavía puede controlarse mediante reglas de firewall, por lo que la seguridad no necesita disminuir en esta configuración.

Para configurar la creación de puentes, siga las instrucciones de Agregar RED a UTM para al menos dos dispositivos RED. Luego, en UTM WebAdmin, vaya a Interfaces y enrutamiento> Bridging. Asegúrese de que Bridging esté habilitado, luego seleccione Bridge NIC seleccionados (modo mixto). En NIC miembros, seleccione todas las interfaces RED agregadas, y en Convertir interfaz, seleccione << Sin conversión >>. Haga clic en Crear puente para completar. Luego, siga los pasos de configuración RED restantes, pero seleccione la interfaz de hardware br0, en lugar de la interfaz reds #. Solo necesitará seguir las instrucciones básicas de configuración de Sophos RED una vez, sin importar cuántos se agreguen al UTM. Se pueden agregar RED adicionales al puente en Interfaces y enrutamiento> Puenteo. Seleccione la nueva interfaz RED y haga clic en guardar para aplicar los cambios. Todas las reglas configuradas para un RED, se aplicarán inmediatamente al dispositivo RED recién agregado.