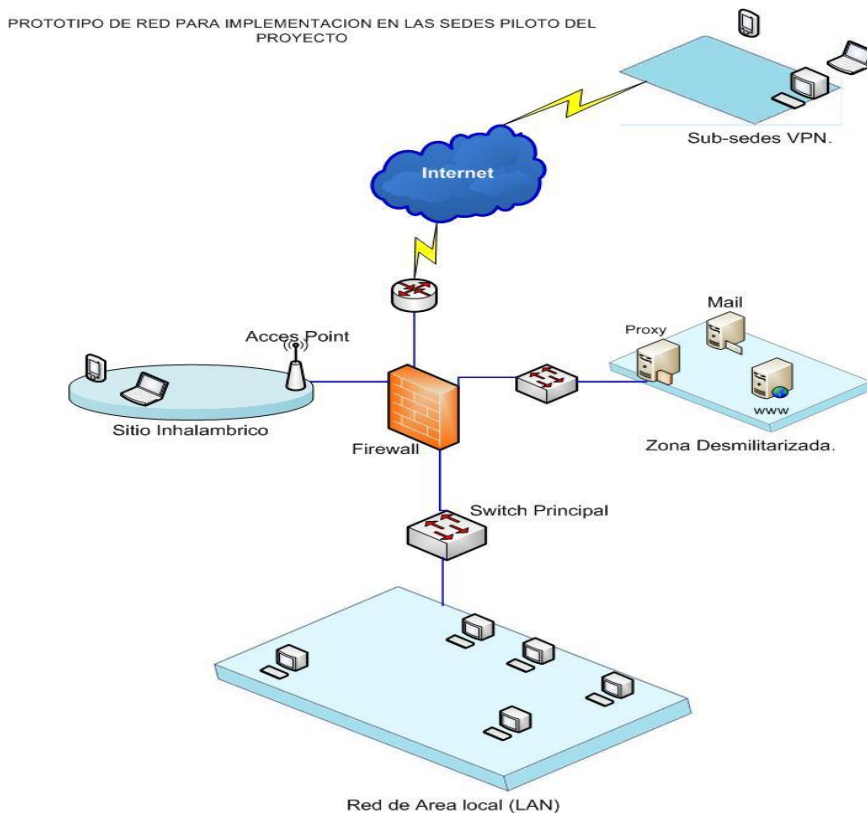


Modelo de monitorización del S.O.C

Aunque existen muchas formas de modelar la implementación de monitorización para un Centro de Operaciones de Seguridad, dependen de la distribución física y lógica de la red, el diseño de implementación para la captura de datos relevantes. Tomamos como base un esquema típico que representa la distribución de red mas común en nuestro medio donde se pueden observar las zonas o sitios de despliegue, Zona de red local LAN, Zona de red DMZ, Zona de Acceso inalámbrico y Zona remota o clientes VPN.

Grafica 1.1 Modelo típico de distribución de red por zonas.



Debemos considerar ahora los modelos de monitorización de las sondas implementadas a través de un sistema centralizado, que es la parte fundamental del S.O.C.

Es muy importante definir aquí los dos tipos a utilizar y sus diferentes modelos de monitorización de las sondas.

- **Modelo de SOC en sitio.**
- **Modelo de SOC remoto.**

El **modelo de SOC en sitio** hace referencia a aquellos ambientes donde el S.O.C. se instala directamente en las instalaciones físicas de la organización a la que se le implementa, y el **modelo de S.O.C remoto** es la gestión desde un sitio en un área física distante de la ubicación física de la empresa piloto. Para ambos modelos es preciso tener en cuenta que los sensores son considerados como el flujo de datos de seguridad, enviados de manera remota, por lo tanto los métodos de acceso

a las consolas de monitorización centralizadas de nuestro S.O.C. se pueden realizar de tres formas diferentes:

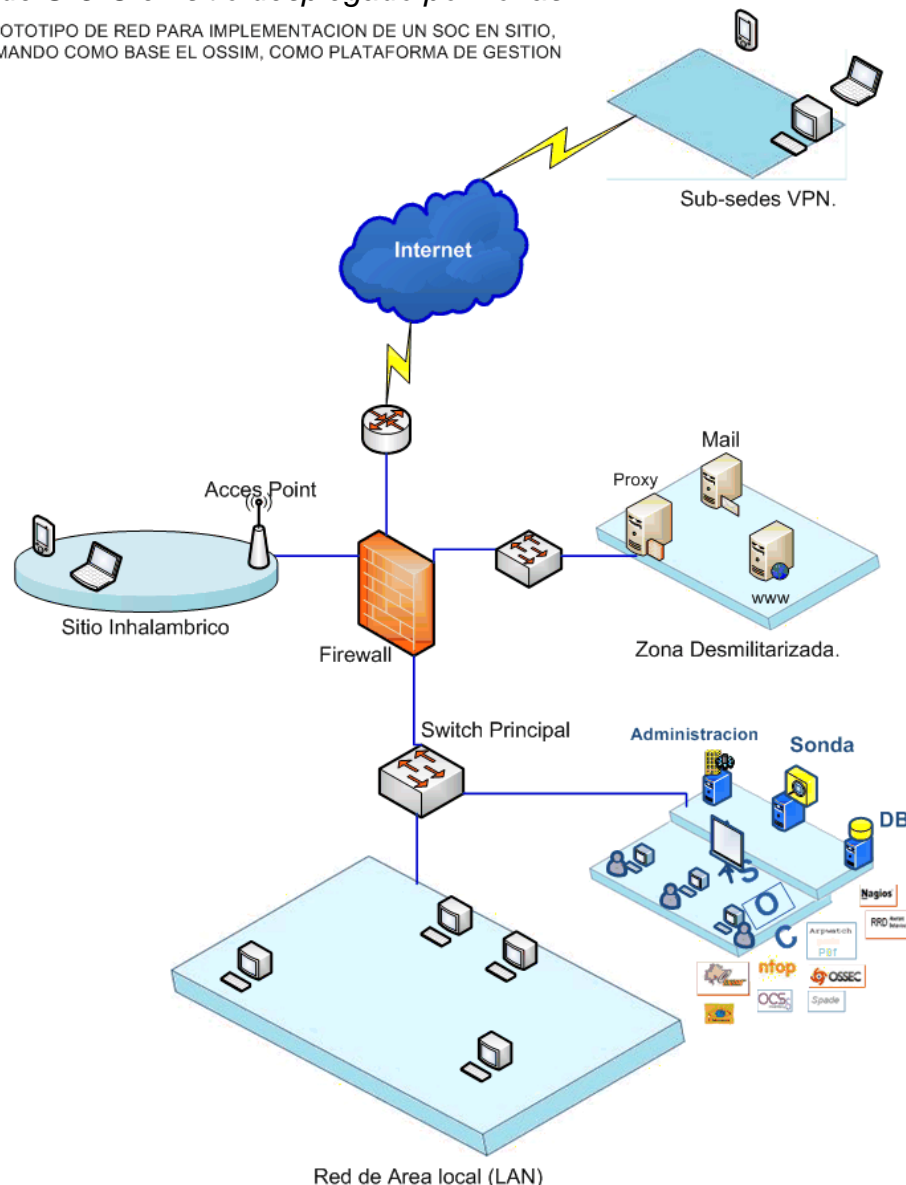
- **Acceso para la gestión del S.O.C en consola.**
- **Acceso remoto para la gestión del S.O.C en banda.**
- **Acceso remoto para la gestión del S.O.C fuera de banda.**

El acceso para la gestión del S.O.C en consola

Es el método más seguro pero complicado a la hora de hablar de centro de operaciones centralizado. Está ligado al modelo de S.O.C en sitio, ya que requeriría tener las sondas en el mismo equipo donde se gestiona el S.O.C, con un sistema OSSIM. Este tipo de acceso es mas comúnmente conocido como un “todo en uno” (Sondas y herramientas de administración en un mismo equipo).

Grafica 2.1 Modelo de S.O.C en sitio desplegado por zonas.

PROTOTIPO DE RED PARA IMPLEMENTACION DE UN SOC EN SITIO,
TOMANDO COMO BASE EL OSSIM, COMO PLATAFORMA DE GESTION

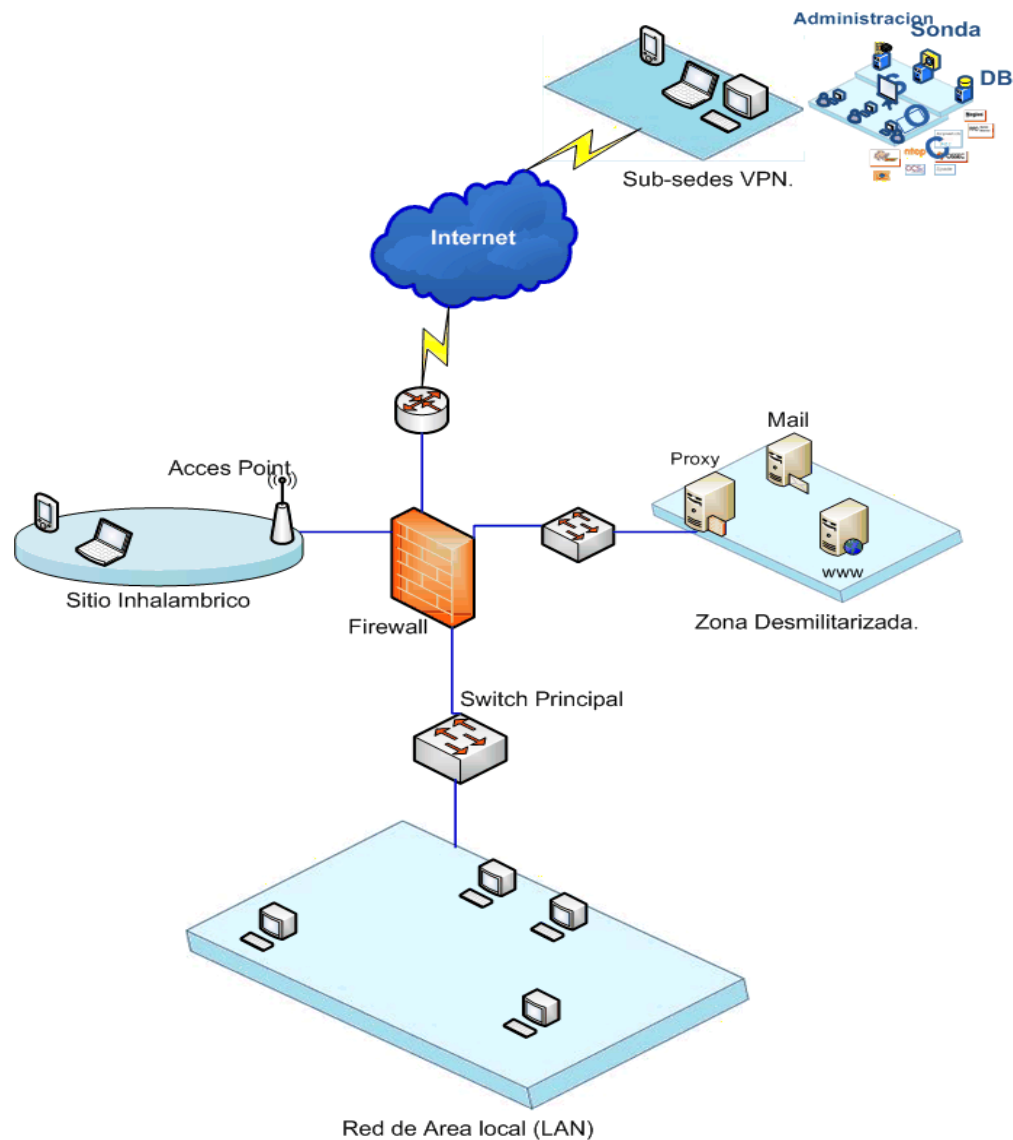


Prototipo de red para implementación de un SOC en sitio, con OSSIM como plataforma de gestión.

El acceso remoto para la gestión del S.O.C, en banda

Se utilizó en uno de los modelos de monitorización de los ambientes pilotos. Se trata de utilizar el mismo esquema de conectividad de la empresa piloto, para comunicación con el centro de operaciones centralizado. Este modelo es favorable ya que no incrementa costos y ajustes a los esquemas existentes en la implementación, pero tiene la desventaja de fallar con el sistema, si la red es sometida a una denegación del servicio provocada o accidental: Se requeriría de reparaciones algo tardías que podrían ser aprovechadas por un atacante desde un punto accesible para él, pero inaccesible para el S.O.C. Por eso que debe estar acompañado de planes de contingencia como conexiones a través de modem u otro tipo de conexión efectiva, que impidan la continuidad de los procesos de gestión, en casos de emergencias.

Grafica 3.1 Modelo de S.O.C remoto desplegado por zonas y Ossim como plataforma base.

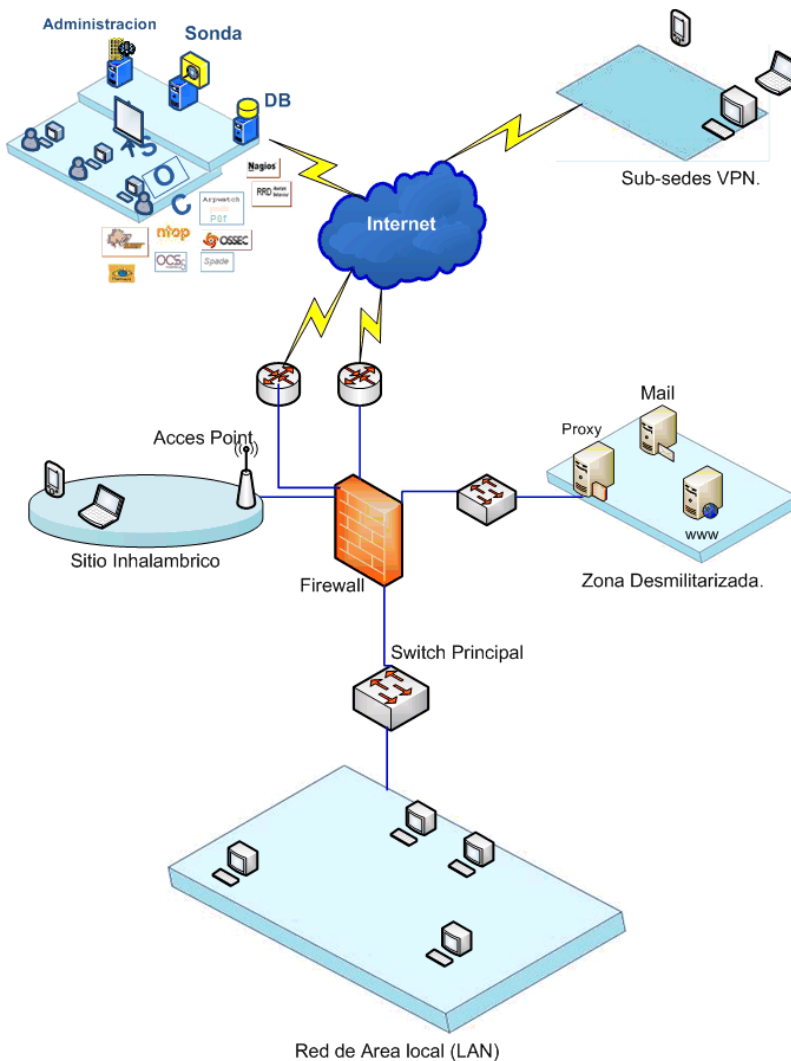


PROTOTIPO DE RED PARA IMPLEMENTACION DE UN SOC REMOTO EN BANDA, TOMANDO COMO BASE EL OSSIM, COMO PLATAFORMA DE GESTION

El modelo de acceso remoto para la gestión fuera de banda

Hace referencia al modelo de implementación de un S.O.C, con conectividad independiente. Es el método que brinda más garantías de continuidad de la gestión para el modelo de S.O.C remoto, pero el que quizás mayores costos pueda involucrar, pues requiere de conexiones dedicadas distintas a las existentes por la empresa piloto, que permitan una comunicación directa con el centro de gestión remota de la seguridad.

Grafica 4.1 Modelo de acceso remoto fuera de banda, Ossim como plataforma base



PROTOTIPO DE RED PARA IMPLEMENTACION DE UN SOC REMOTO,
TOMANDO COMO BASE EL OSSIM, COMO PLATAFORMA DE GESTION