

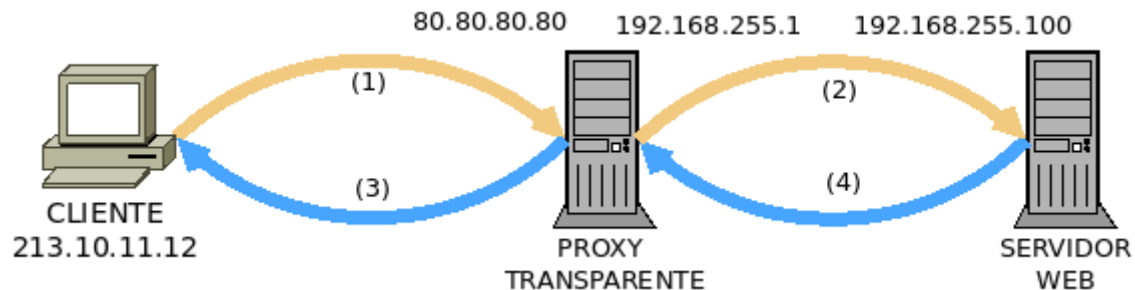
Índice:

Ejercicio 3 informes	2
a) Squid modo transparente	2
b) Modo inverso	3
c) Servidor ICAP	4

Ejercicio 3 informes

a) Squid modo transparente

Solución:



El modo transparente es una configuración en la que el servidor proxy opera de manera transparente (de manera que los clientes no son conscientes de que están usando un proxy) sin requerir la configuración de un cliente en este modo los clientes no necesitan realizar ajustes para usar el proxy, este intercepta y redirige el tráfico automáticamente.

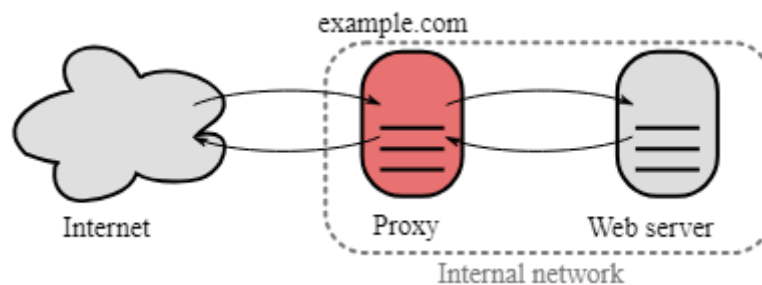
Este generalmente se coloca entre la red interna e internet actúa como intermediario gestionando las solicitudes y respuestas de los clientes de la red interna y los servidores externos.

Este modo puede ser útil para implementar políticas de seguridad, monitorear el tráfico, filtrar el contenido o acelerar el acceso a sitios web mediante caché.

Es importante configurar correctamente el Squid transparente correctamente para evitar problemas con aplicaciones o servicios.

b) Modo inverso

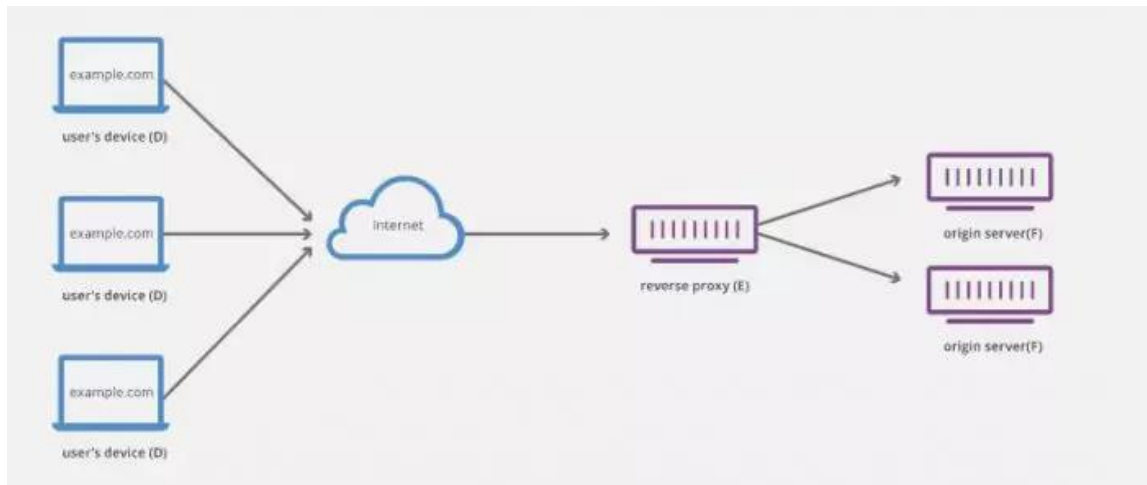
Solución:



El modo inverso es la configuración en el que el proxy actúa como intermediario entre los clientes externos y los servidores internos redirigiendo las solicitudes desde los clientes hacia los servidores y enviando la respuesta de vuelta a los clientes. Este en lugar de proteger a los clientes internos de la red y ocultar su identidad como en el proxy tradicional este se utiliza para mejorar el rendimiento la seguridad y la administración de servicios web.

Este puede almacenar caché para mejorar la velocidad de carga al proporcionar contenido almacenado en el caché directamente a los clientes.

Este también permite distribuir el tráfico entre varios servidores para lograr un equilibrio de carga, esto permite que ningún servidor se sobrecargue mejorando la eficiencia y disponibilidad.

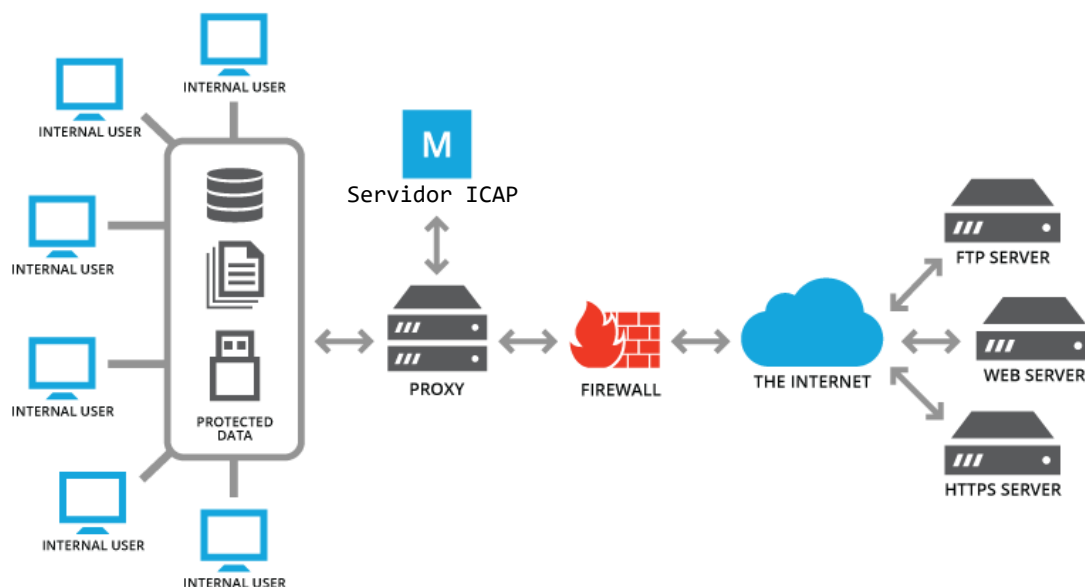


Al actuar como intermediario agrega una capa adicional de seguridad ocultando la topología de red interna y actuar como nexo permitiendo filtrar y validar el tráfico antes de que llegue a los servidores.

Al conjuntar varios servicios en un solo punto de entrada el modo inverso simplifica la administración y las tareas como la configuración de SSL/TSL, gestión de certificados e implementación de políticas de seguridad

c) Servidor ICAP

Solución:



ICAP permite la adaptación de contenido en tiempo real al pasar por un servidor proxy. Este puede realizar modificaciones en el contenido de una solicitud o respuesta HTTP antes de que llegue al cliente o al servidor de origen.

Un servidor ICAP puede ser utilizado para aplicar políticas de seguridad, filtrar contenido, realizar escaneo antivirus, aplicar optimizaciones de contenido, entre otras funciones.

Cuando un servidor proxy intercepta una solicitud o respuesta HTTP, puede enviar esa solicitud a un servidor ICAP para su procesamiento adicional.

Funcionamiento:

1. **Cliente realiza una solicitud HTTP:** Cuando un cliente realiza una solicitud a través de un servidor proxy, el proxy intercepta la solicitud.
2. **Solicitud enviada al servidor ICAP:** El servidor proxy puede enviar la solicitud al servidor ICAP para realizar alguna acción, como escanear el contenido en busca de malware o aplicar políticas de filtrado de contenido.
3. **Procesamiento en el servidor ICAP:** El servidor ICAP procesa la solicitud según las políticas configuradas y devuelve una respuesta modificada o sin cambios al servidor proxy.
4. **Respuesta al cliente:** El servidor proxy, después de recibir la respuesta del servidor ICAP, puede enviar la respuesta modificada o sin cambios al cliente.

ICAP permite una mayor flexibilidad y personalización en el manejo del contenido web que pasa a través de un servidor proxy. Se utiliza comúnmente en entornos corporativos para aplicar políticas de seguridad y filtrar contenido no deseado. Algunos servidores proxy, como Squid, son capaces de trabajar con servidores ICAP para proporcionar funciones avanzadas de adaptación de contenido..