Red de Seguridad

Transcribed on July 26, 2025 at 11:38 AM by Minutes AI

Speaker 1 (00:08)

Bienvenidos a esta nueva sesión, en esta sesión vamos a ver de una forma práctica utilizando PFSense cómo aplicar algunas de las herramientas que hemos visto hasta ahora.

En concreto veremos cómo crear ACL o Listas de control de acceso o configurar un proxy transparente con Squid, pero también veremos cómo se puede gestionar todo el tráfico de nuestros usuarios utilizando tanto el proxy transparente como listas blancas o negras para emitir o bloquear el acceso a determinadas páginas web o direcciones IP.

Ahora os quiero hablar de algo bastante común que se utiliza mucho para lo que es el Hardening de una red de datos en la que hay clientes, usuarios y servicios, y es utilizar dos acciones, la primera es utilizar un proxy transparente para que todo el tráfico esté redirigido siempre por el mismo punto y que el usuario no tenga constancia de ese redireccionamiento y por otro lado utilizar lo que se llaman las Blacklist o las Wildlists, que son listas blancas o listas negras de access para permitir o no permitir acceso a diferentes páginas web o incluso a categorías de páginas web.

Esto es muy interesante, esta es una acción típica a la hora de hacer un hardening dentro de una empresa para evitar que los usuarios accedan a sitios peligrosos o sitios que pueden poner en riesgo tanto la máquina como la red de la empresa o de lo que sea, y de esa forma tendremos también un control de a qué se está accediendo desde nuestra red, pero con el mero hecho simplemente de protegernos.

Y para ello utilizaré Skid y skitguard, que ya lo he comentado en algunos otros vídeos y serán los dos elementos que utilizaré, porque Skit es un proxy que tiene la opción de proxy transparente y skidguard nos permite activar esa opción que os he dicho de las Blacklist y de las Whitelist.

El paso inicial es tenerlo instalado, yo ya lo tengo, pero si nos vamos aquí Assistant al Package Manager, si no lo tuviera instalado directamente aquí lo buscaría en la opción de Disponibles y doble clic Install y ya aparecerá directamente aquí en Servicios los tres, bueno yo utilizaré solo este y el scriptguard, estos son los dos que vamos a utilizar.

Bien, pues vamos a irnos al Script Proxy Server para ver la configuración genérica y bien, lo primero que tenemos que hacer es ir a la parte de General, pero también se recomienda ir a la parte del Local Caché.

Esta parte de Local Caché es crítica porque tiene cantidad de funcionalidades que permiten un rendimiento óptimo del sistema.

Por ejemplo, lo primero es eso, que una caché local lo que hace es almacenar el contenido de websol que ya se ha pedido previamente.

Entonces cuando el usuario lo pida de nuevo el contenido es que Skit ya lo puede servir directamente desde la caché en lugar de volver a cargarlo.

Y esto como podéis imaginar reduce mucho el tiempo de carga, etc.

También ahorra ancho de banda, porque al estar todo en caché, el contenido web, pues todo se reduce a conectar directamente con la caché y ver siempre el contenido, no hace falta tener que conectar hacia afuera, con el consiguiente gasto de ancho de banda.

También el usuario estará mucho más contento porque todo se cargará mucho más rápido y será mucho más.

Con lo cual tenemos que poner.

De momento no vamos a hacer nada porque ya por defecto con las opciones que trae son ya suficientes.

Podríamos entrar mucho en la configuración porque tiene muchísimo que se puede personalizar, pero directamente dejaremos las opciones y pincharemos en guardar para que al menos aplique las que trae por defecto y esto se va a actualizar.

Bien, volviendo a la configuración GenericAndesKit, pues vamos a dar un pequeño repaso de las opciones más importantes.

La primera es por supuesto habilitarlo.

Tenemos que hacer clic para que se active, activarlo.

Al ser un proxy, todo el tráfico va a ir redirigido a través de ese proxy que es kit, que será un servicio.

En ese momento podremos hacer todo tipo de operaciones con ese tráfico entrante, con lo cual lo primero será habilitarlo.

Después tenemos que ver qué interfaz vamos a utilizar.

Aquí tenemos que especificar la interfaz de red en la que Skit proxy va a escuchar las peticiones de los clientes.

Podemos decirle que todas la WAN, loopback, etc.

Después, otro punto clave es el puerto.

Por defecto el proxyskid trabaja en el puerto 3128, pero podemos cambiarlo y poner cualquier otro que fuera necesario.

Otra de las opciones críticas aquí, porque ya dijimos que queríamos configurar un proxy transparente, es justamente marcar la opción de proxy transparente que viene en skip.

Marcamos y bueno, igual marcamos la LAN, porque todo es.

El tráfico de LAN es el que queremos que sea transparente hacia Internet.

Y aquí ya nos hace un aviso si queremos también interceptar tráfico HTTPs tenemos que utilizar otra opción que está más abajo que es esta de aquí que es el SSL Band in the middle filtering para poder hacer esto es que será necesario tener un CA, tener un certificado instalado, yo ya lo tengo aquí, lo podéis ver abajo directamente lo asignamos, esto si acordáis están todos configurados aquí en la opción de certificates, pues ya por defecto Skype te va a crear uno, pero creamos también uno nosotros para los diferentes clientes si hiciera falta, pero bueno por defecto tenemos nosotros para los diferentes clientes hiciera falta, bueno por defecto tenemos ya un certificado que será utilizado con squid si hiciera falta, pero bueno por defecto tenemos ya un certificado que ha utilizado con con squid y bueno lo activamos porque si yo también quiero que el tráfico HTTPs, porque vamos prácticamente todo tráfico de Internet, no hay nadie que conecte ya sin seguridad no SSL, pues entonces queremos intentar ese tipo de tráfico, así que activamos la opción de SSL filtering y bueno aquí ya veremos que hay que jugar mucho con estas opciones, yo tengo la opción de Splice all, esto quiere decir, aquí podéis ver un poco la iuta que te explica cada uno de ellos, esto va asociado a skipguard, eso después lo veremos porque una utiliza las whitelist, las ACL que son las listas de acceso, después también una utiliza diferentes formas personalizadas de gestionar esas listas de acceso, eso lo veremos ahora más adelante, básicamente aquí ya ponemos el CA y yo creo que no hacemos así, esto es importante, marcar el login, esto es importante también para tener digamos ver en tiempo real cómo van los accesos de script, ahí veremos en tiempo real qué máquinas se están conectando y hacia dónde, en tiempo real es útil para un vistazo que estemos en urgencia, que lo queremos ver urgentemente qué está pasando, pero bueno ya sabéis que dos logs lo más normal es que se almacenen y después los veamos, pero en este caso podríamos ver los log en tiempo real, que eso es una opción que podéis ver aquí arriba que pone real time, si marcamos esta opción de abajo al pinchar en real time veríamos el tráfico aquí de máquinas que están en la misma red que están haciendo peticiones a páginas web o diferentes servicios dentro de nuestra LAN.

Pues bien esto era la parte de log y yo creo que ya esto un poco para personalizarlo, que esto siempre es bueno, no lo voy a hacer yo por temas de tiempo, pero lo normal es que en producción o en sistemas un poco más complejos sí que hace falta que pongáis la máxima información posible.

Es una pérdida de tiempo ver máquinas con direcciones IP sin un alias, que no sepamos lo que hacen o reglas que no sabemos lo que hacen, es una una locura y también puede ser un problema de seguridad.

También vemos que el Squid lleva también una opción de antivirus, que en este caso creo que es Clamat con Clamat directamente.

Si activamos esta opción tendríamos un antivirus que iría en tiempo real chequeando todo el tráfico de ficheros que ese usuario tuviera hacia Internet.

Es muy interesante, por supuesto esto tiene un coste computacional en la máquina y en el servidor, pero bueno, es una buena alternativa.

Bueno, ya sabemos lo que son las listas de acceso y aquí tenemos una gestión total sobre ellas.

Podemos poner cuáles son las subredes que están permitidas, cuáles son las IPs que no están restringidas, wildlist, también listas blancas, lo que pongamos aquí no va a pasar por el proxy, también direcciones que están baneadas, esta IP no puede trabajar aquí a través del proxy, etcétera.

Una forma muy digamos muy extensa de poder gestionar todo lo que son las listas de acceso.

También podemos autenticarnos, esto ya implica un poco más de gestión, pero podríamos hacer que todo usuario tuviera que autenticarse directamente contra el proxy para poder acceder a la navegación.

Esto nos daría un control absoluto y sería ideal para entornos con un directorio activo, con un LDAP, porque así tendríamos todo interrelacionado, veríamos las conexiones hacia fuera del usuario, etc.

Y aquí sería la sección en la que iríamos añadiendo los diferentes usuarios que tendrían que obtener autenticarse para poder trabajar con todo lo que es los servicios o la red o el proxy en este caso.

Pues bien, con esta configuración muy sencilla, cualquier usuario que esté dentro de la red va a pasar sí o sí por el proxy transparente y todo su tráfico tendría que ser interceptado.

Vamos a hacer una prueba y veremos si funciona, pero antes para hacerlo mucho más completo vamos a conectar skidguard y de esa forma vamos a activar lo que son las Blacklist.

Bien, ScriptGuard está también en los servicios porque ya lo hemos instalado y nos vamos a la opción de ScriptGuard proxy filter.

Vamos a dar un repaso muy rápido.

Aquí tenemos las configuraciones genéricas, en este caso veis lo que también os comentaba antes una conexión con un servicio LDAP o si fuera necesario también marcaríamos las opciones de login para tener también un gestor de log de todos los accesos y también, esto es importante, muy importante, hay que marcar esta opción porque esto lo que hace es habilitar la blacklist.

¿Qué es una blacklist?

Bueno, una blacklist es un listado de categorías y de diferentes accesos a Internet que no queremos que los usuarios puedan acceder.

Entonces lo normal es que aparezcan muchísimas direcciones y tú puedas decidir si quieres o no que esa dirección o esa categoría, porque también va por categorías, por ejemplo redes sociales, yo que sé, por ejemplo videojuegos y cosas así se podrían hacer en grupo, entonces si el proxy detecta que la categoría de esa página es de videojuegos pues te lo va a bloquear.

Lo primero, ¿Cómo importamos la blacklist?

Aquí tienes una opción que es blacklist, al pincharle aquí pondríamos una dirección web como la que os estoy mostrando en pantalla.

Pondríamos una dirección web como la que os estoy mostrando en pantalla, hay varios sitios o varias digamos publicaciones que tienen listados, yo he cogido este que se llama Standard, con pinchar aquí y darle a download te lo va a instalar, no lo voy a hacer porque ya lo tengo instalado y de esa forma se va a integrar con script y con scriptguard, ambos van a utilizar esa blacklist como forma de bloqueo a diferentes servicios y páginas web.

Aquí también tenemos una opción para listas de acceso que le añadiría mucho más control, por ejemplo aquí una vez hecho la parte de blacklist y haber cargado todo ese listado, podemos ir al Common ACL y aquí veríamos todas esas categorías que yo acabo de contar.

Como veis hay alcohol por ejemplo, automóviles, chatting, dating drugs, drogas por ejemplo y cada una categoría tiene una forma de activación, puede ser whitelist, quiere decir que vale, esta me vale, está permitido, directamente pasa a la lista blanca.

Tenemos otra que es denegación, esta no es imposible, la diferencia que hay entre hacer un allow o un whitelist es que allow es genérico, toda la categoría entera ya se permite, pero con whitelist es que podemos asociarle un fichero o un listado en el cual la categoría está OK, pero solamente a esta, ahí indicaríamos a cuáles están permitidas.

Bien, pues aquí al final tendríamos que ver la opción genérica que es la de aquí, este es el default, el default es acceso a todo el mundo, directamente le decimos que el acceso por defecto es a cualquiera de las categorías, pero yo por ejemplo aquí fijaos he activado una que es socialmed, o sea las redes sociales Deny, no quiero que nadie conecte a una red social, pero que sí pueda entrar en Shopping, en Amazon por ejemplo, entonces al yo poner aquí a lo pero especificar Deny directamente en una de ellas, esta va a sobreescribir a la principal, entonces si yo ahora voy por ejemplo voy a ir a esta misma máquina, si abro otra pestaña, intento ir a Facebook, veis, directamente ya me lo está bloqueando, me está interceptando el tráfico directamente y lo que hace es decirnos qué es lo que ha pasado, vale, pues fijaros, el proxy ha denegado el acceso y te dice por qué, digamos no el porqué, sino te dice cuál es el error que estás devolviendo Forbidden, prohibido y aquí sí que te dice el porqué, te explica un poco la razón o el motivo del bloqueo, pues mira pues que tú quieres esta IP, estás en un grupo de clientes, por defecto no tienes un cliente especial o un grupo especial que que te habilite a conexión a esta página web, pero esta es la clave, Facebook está dentro del grupo socialnet, con lo cual yo ponerle el Deny directamente me lo ha bloqueado.

Bien, pero si yo quisiera abrir otra página, por ejemplo una de noticias como puede ser el mundo, aquí directamente no tendría que pasar nada y me debería de abrir la página web y ya podría ver la información.

Y ahora por ejemplo si yo quisiera acceder a otra web, por ejemplo una que esté habilitada, que yo sé que la de noticias está habilitada, porque si me voy a la configuración, lo podemos ver aquí en alguna parte aparecerá News que debe estar en abierto, aquí está News, está Access, lo veis, está puesto que no está configurado, pero eso quiere decir que va a aplicar la regla general que es Allow, siempre que veáis un guión aquí es que va a aplicar la regla que está por defecto genérica, entonces si yo me voy aquí y abro una pestaña nueva, me voy al mundo, me debería de abrir la página web sin ningún problema.

Esto es algo fundamental en un hardening de redes de datos, porque ya fijaros el control que tenemos, esto nos permite gestionar perfectamente todo el tráfico, todos los usuarios.

Hay una cosa importante que tenemos que asignar, es que a la hora de que el usuario conecte desde su navegador tenemos que activarle el certificado que hemos creado antes para Skid, eso es sencillo, lo que hacemos es lo exportamos, eso se hace desde aquí, podemos ir a la configuración y coger el de script CA y directamente le decimos exportar CA, le diremos exportar aquí tampoco sería, sí perdón, sería exportar CA, cogeríamos notificado, que sería un formato si no me equivoco y con ese certificado iríamos a Firefox y aquí la configuración de seguridad y tal, pues no importaríamos, así de sencillo.

Y ya a partir de ese momento podríamos digamos gestionar, digamos inspeccionar el tráfico HTTPs y aquí vuelvo a hacer la misma especificación que ya he dicho antes o el comentario que antes he hecho en algunos otros vídeos.

Esto que veis aquí que utilizas Skit, es solamente una herramienta para que lo veáis.

Aquí lo que yo quiero que tengáis claro es todo el proceso que hemos visto para la configuración, porque este proceso se repite muchísimo, de hecho Skit también está integrado en multitud de máquinas que se dedican a la seguridad de red integrada, incluso en dispositivos hardware.

Entonces la configuración llámese Skit, llámese como sea, tenemos que tener claro lo que es un proxy transparente, también tenemos que saber cómo gestionar el tráfico HTTPs utilizando un Banned de Lidl, generando certificados, eso es un poco la parte que yo quiero que os quedéis, la parte de PFSense solamente educativa, para que veáis un poco esa implementación en vez de explicaroslo directamente con diapositivas o un poco en un entorno un poco más digamos feo, en un entorno en el que se viera de otra forma cómo configurarlo.

Esta es muy directa, es muy educativa y muy didáctica.

Bien, también quiero hacer aquí un pequeño comentario y es que Skid y SkidGuard se han discontinuado desde 2022, entonces hay alternativas, yo he utilizado Skid porque es una forma muy dinámica de hacerlo, pero hay alternativas para hacerlo, por ejemplo para utilizar el skip proxy puedes utilizar ha proxy que está como un paquete, de hecho si vemos aquí lo podemos ver en el Package manager y sería una alternativa directa al script proxy, si yo pongo aquí HAProxy debería de aparecer search, aquí está, ya con esto teníamos una forma de utilizar el script proxy con con esta alternativa.

Por supuesto en la versión comercial de pfsen, que es la pfsen Plus, sí que se incluye características avanzadas de filtrado de contenido y de seguridad a nivel de usuario para hacer pruebas, pues también Tenemos por ejemplo PFBlocker MG es un paquete de PFSense que también nos permite filtrar y bloquear IPs, diferentes opciones.

También tenemos por ejemplo DNSPL, que es digamos una forma de bloquear dominios directamente, o sea que alternativas hay, solo que son un poquito más complejas de instalar.

Pero bueno, Skid aún funciona, lo podemos utilizar así de base y para hacer pruebas y todo lo demás.

Bien, pues como podéis ver PFC nos ha servido muy bien para poder ver ciertas configuraciones o ciertas definiciones.

A partir de ahora sí que utilizaremos ya la línea de comandos y una configuración un poco más integrada.

Por ejemplo cuando veamos Snort y otros ids, otros ips, lo haremos desde el punto de vista de un servidor puro y duro, no desde PFSense, aunque PFSen también lo tiene, de hecho yo lo tengo instalado aquí, como podéis ver tengo Snor y tendría otros paquetes que se pueden integrar para todo lo que es la seguridad.

Pero bueno, de momento sólo quería explicaros pfsen como una herramienta base para poder practicar y tener nuestro propio laboratorio.

Yo de hecho es el que utilizo para mí, para diferentes opciones, para jugar con rutas, NAT, direccionamiento, gateway, todo tipo de cosas con PFSEN, Skid y SkidGuard.

En PFSEN ofrecen una mejora significativa en el almacenamiento temporal de datos web y el filtrado de contenido, lo que resulta en un aumento tanto en la eficiencia desde la red como en su seguridad.

Script agiliza el acceso a Internet al guardar en memoria local el contenido que se usa con frecuencia y eso hace que disminuya la carga de la conexión.

Por otro lado, SkipGuard permite establecer políticas de acceso personalizadas y bloquear sitios web no deseados o peligrosos, lo que fortalece la protección de la red y promueve un entorno de trabajo más seguro y y productivo.

En este caso Skid es un proxy y skillguard es un añadido al proxy para la gestión de listas.

Llegamos al final de la sesión, os esperamos en el siguiente vídeo.