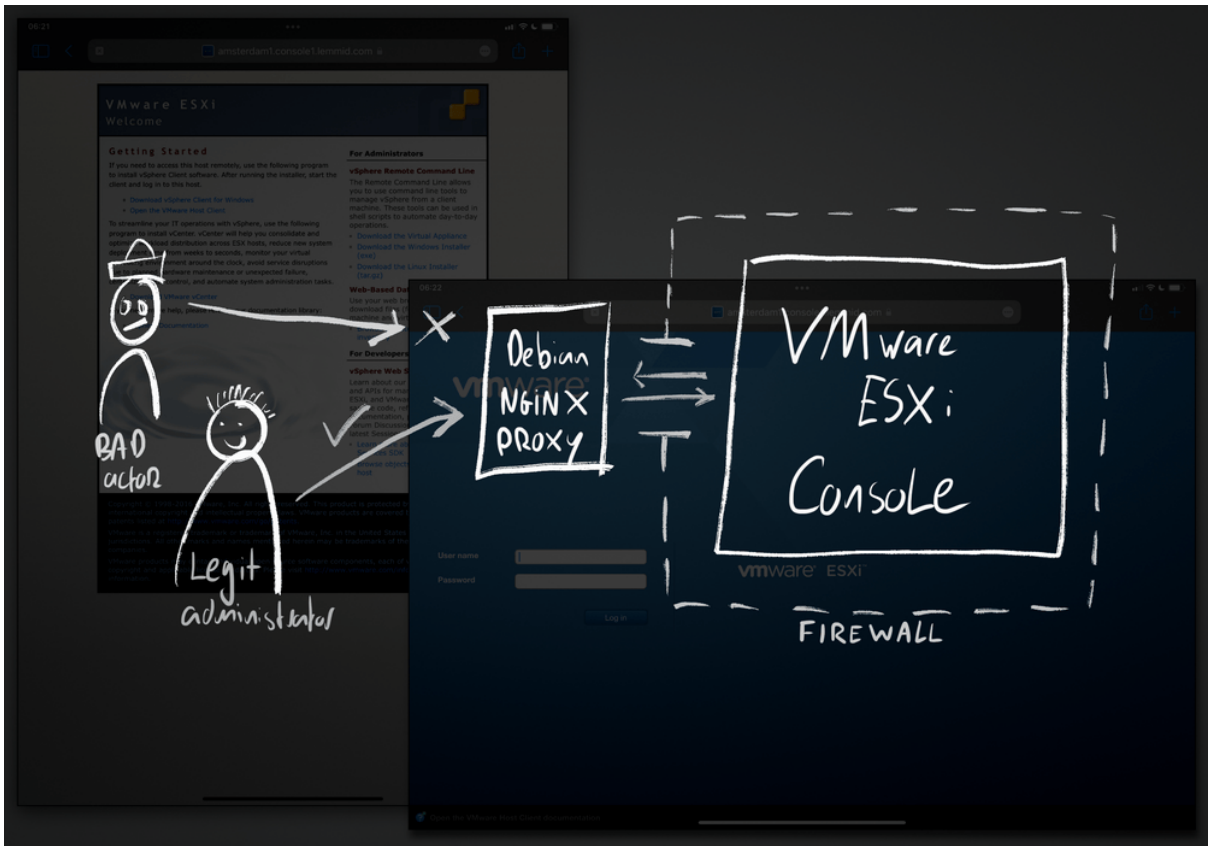
Proteger VMware ESXi

Mejora la seguridad usando un firewall y un servidor proxy

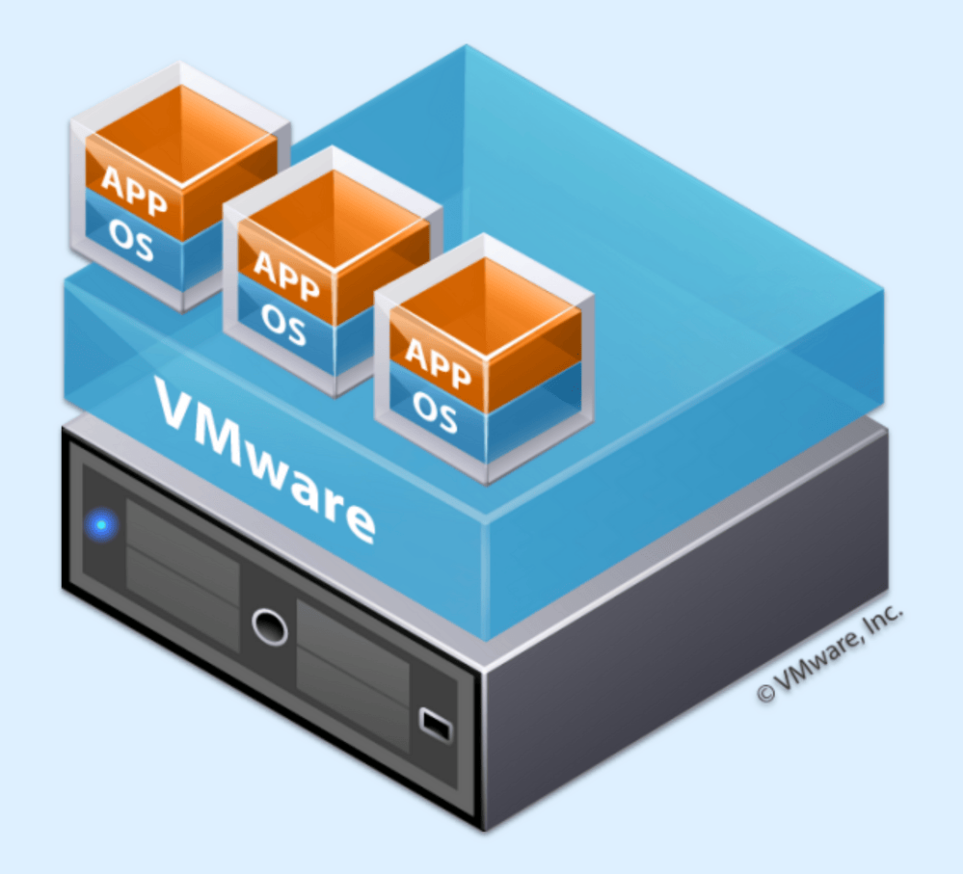
Willem L. Middelkoop

Aug. 31, 2021



En respuesta a un incidente en un servidor, detecté una posible brecha de seguridad. La máquina afectada ejecutaba VMware ESXi, un hipervisor bare metal utilizado para ejecutar servidores privados virtuales. En modo independiente, una consola de administración basada en web ofrece control total sobre la infraestructura, lo que representa un riesgo.

El hardware de servidor grande y potente ofrece una tonelada de capacidad de cómputo, a menudo mucho más de lo que una sola aplicación necesita. A través de la virtualización, los operadores de la nube pueden optimizar el uso del hardware cargando dinámicamente múltiples máquinas virtuales en una sola máquina física.

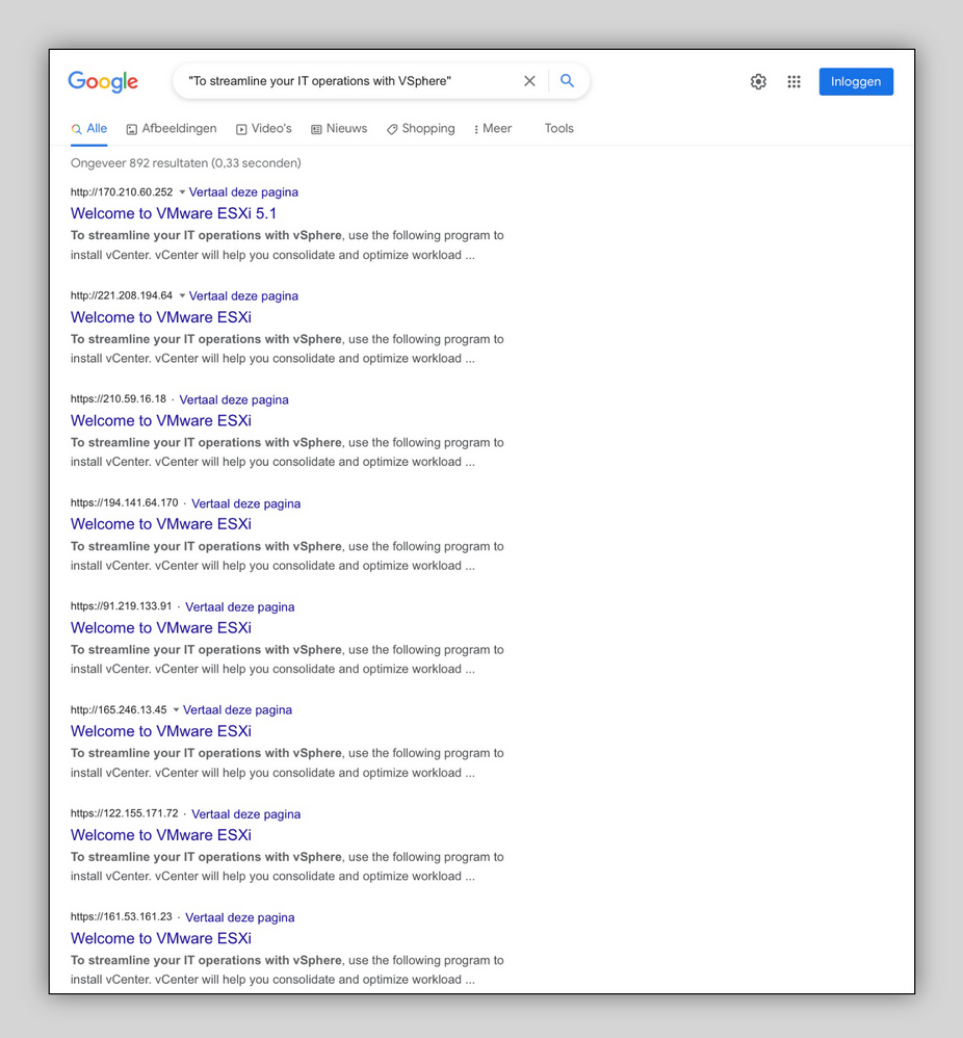


VMware ESXi es un hipervisor de tipo bare metal que divide un servidor físico en múltiples servidores virtuales

Las máquinas físicas que ejecutan VMware ESXi se administran como una red VSphere centralizada o como una máquina independiente. Los administradores crean, administran y configuran máquinas virtuales a través de una potente interfaz web. Sin una red VSphere centralizada, los administradores necesitan esta interfaz web, pero exponerla en la internet pública atrae la atención no deseada de los hackers.

Interfaz web de VMware ESXi: invitándote a ti y a otros a administrar esta máquina física

Los actores maliciosos buscan activamente consolas de administración expuestas, con la esperanza de encontrar una con una contraseña débil o con debilidades_de_seguridad conocidas. Libera al explorador curioso que llevas dentro y simplemente utiliza Google para encontrar un montón de máquinas expuestas con una consulta especial. Consulta mi publicación de blog sobre consultas especiales en Google si necesitas repasar tus habilidades de búsqueda.

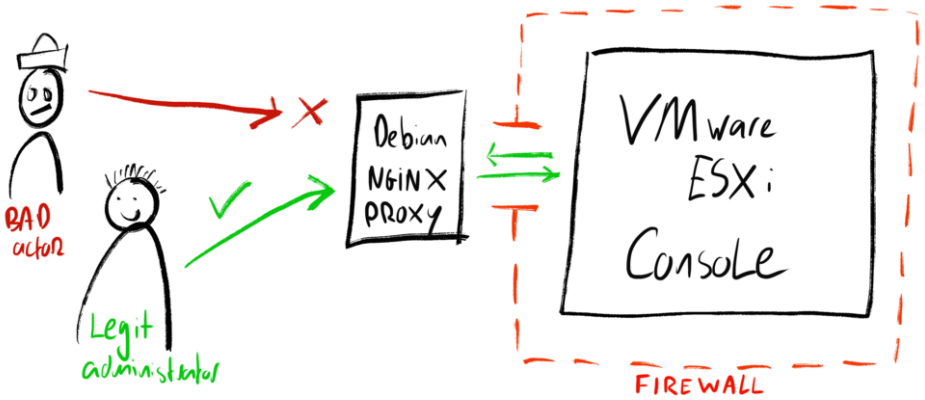


Encontrar interfaces web de VMware ESXi expuestas no requiere nada más que algunas habilidades de Google

Deja la consola de administración expuesta y cualquiera puede intentar iniciar sesión. ¡Los hackers y sus bots automatizados ciertamente lo harán! El acceso remoto para las cuentas de usuario locales de ESXi se bloqueará temporalmente después de varios intentos fallidos de inicio de sesión, ¡para todos! Esto puede ser frustrante cuando tú, como administrador legítimo, necesitas acceder a la consola.

Siguiendo mis propios consejos fáciles de ciberseguridad la seguridad de VMware ESXi se puede mejorar ocultando por completo la consola de administración. Puedes sentirte tentado a usar un simple firewall que "lo cubra todo" para esto, pero considera la necesidad de la consola administrativa: proporciona acceso vital a las máquinas virtuales en ejecución. Realmente quieres que tus administradores puedan acceder a la interfaz 24/7 desde cualquier lugar en caso de emergencia.

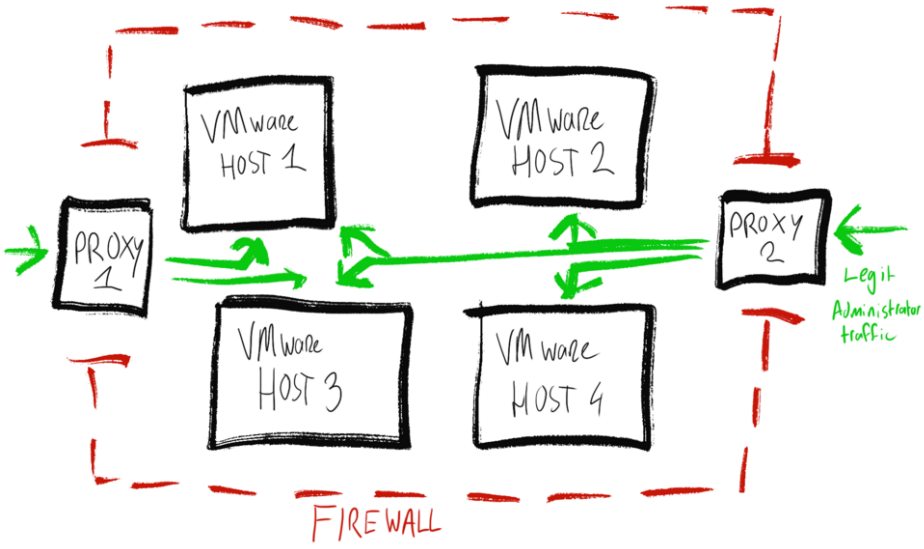
Así que, en lugar de cerrar o ocultar completamente la interfaz de administración, busqué una forma de permitir el acceso de forma selectiva mientras mantenía un perfil en línea sigiloso. Debido a que quiero que los administradores legítimos accedan a la interfaz desde cualquier parte del mundo, no pude usar un simple filtro de dirección IP. Usando una máquina Debian GNU/Linux con nginx como servidor proxy, puedo pre-autenticar el tráfico a la consola de administración.



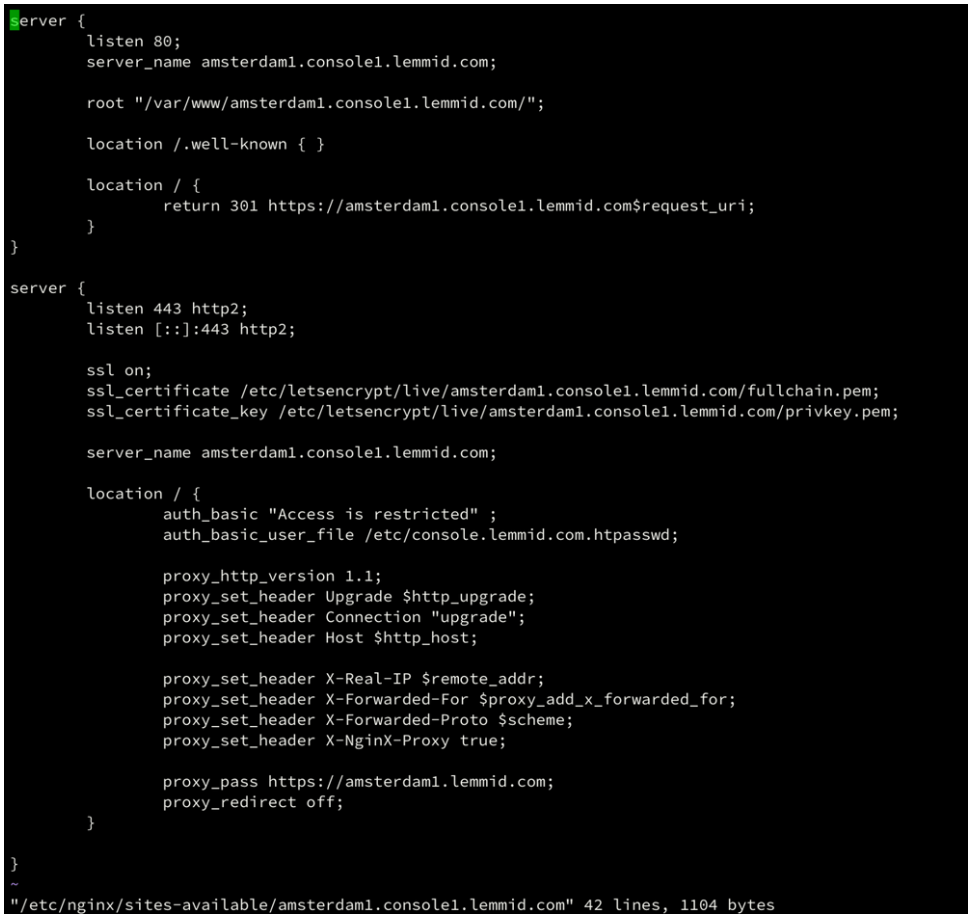
Preautentica el tráfico a la consola administrativa a través de un pequeño y simple servidor Debian GNU/Linux con proxy nginx

En esta configuración, la máquina Debian se ejecuta en una red separada, en un hardware diferente, con una dirección IP fija. El servidor VMware solo acepta tráfico de este servidor proxy utilizando su firewall. El servidor proxy filtra el tráfico mediante autenticación HTTP sobre SSL/TLS. Cualquiera puede conectarse al servidor proxy, pero solo aquellos con credenciales válidas pueden acceder a la consola administrativa de VMWare. El servidor proxy parece ser un servidor web estándar muy pequeño para cualquiera que lo escanee: proporcionando una firma en línea sigilosa.

Agrega otro servidor proxy de otra red en un hardware diferente a la combinación para evitar un único punto de falla. Nginx puede reenviar el tráfico autenticado a diferentes consolas administrativas basadas en diferentes nombres de host, lo que te permite reutilizar un solo proxy para asegurar múltiples máquinas VMware. Los servidores proxy se pueden configurar para usar la autenticación HTTP básica utilizando herramientas estándar y simples, consulta la documentación de nginx para obtener consejos sobre esto.



Dos servidores proxy que proporcionan acceso seguro a múltiples hosts VMware



```
server {
        listen 80;
        server_name amsterdam1.console1.lemmid.com;

        root "/var/www/amsterdam1.console1.lemmid.com/";

        location /.well-known { }

        location / {
                return 301 https://amsterdam1.console1.lemmid.com$request_uri;
        }
}

server {
        listen 443 http2;
        listen [::]:443 http2;

        ssl on;
        ssl_certificate /etc/letsencrypt/live/amsterdam1.console1.lemmid.com/fullchain.pem;
        ssl_certificate_key /etc/letsencrypt/live/amsterdam1.console1.lemmid.com/privkey.pem;

        server_name amsterdam1.console1.lemmid.com;

        location / {
                auth_basic "Access is restricted" ;
                auth_basic_user_file /etc/console.lemmid.com.htpasswd;

                proxy_http_version 1.1;
                proxy_set_header Upgrade $http_upgrade;
                proxy_set_header Connection "upgrade";
                proxy_set_header Host $http_host;

                proxy_set_header X-Real-IP $remote_addr;
                proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
                proxy_set_header X-Forwarded-Proto $scheme;
                proxy_set_header X-NginX-Proxy true;

                proxy_pass https://amsterdam1.lemmid.com;
                proxy_redirect off;
        }

}
~
"/etc/nginx/sites-available/amsterdam1.console1.lemmid.com" 42 lines, 1104 bytes
```

Configuración de nginx para autenticar y reenviar el tráfico a una consola administrativa de VMware

Conclusión

Al usar nginx como proxy para la consola administrativa, puedes agregar una capa de autenticación *y* crear una firma sigilosa para cualquiera que escanee tu red. Esto mejora la seguridad de tus máquinas VMware al hacerlas más difíciles de encontrar y acceder. Los administradores legítimos aún pueden acceder a la consola administrativa usando cualquier computadora sin la necesidad de una VPN o una dirección IP pre-autenticada. Los malos actores, los hackers y los bots tendrán dificultades para encontrarte. ¡Te estás escondiendo a plena vista!