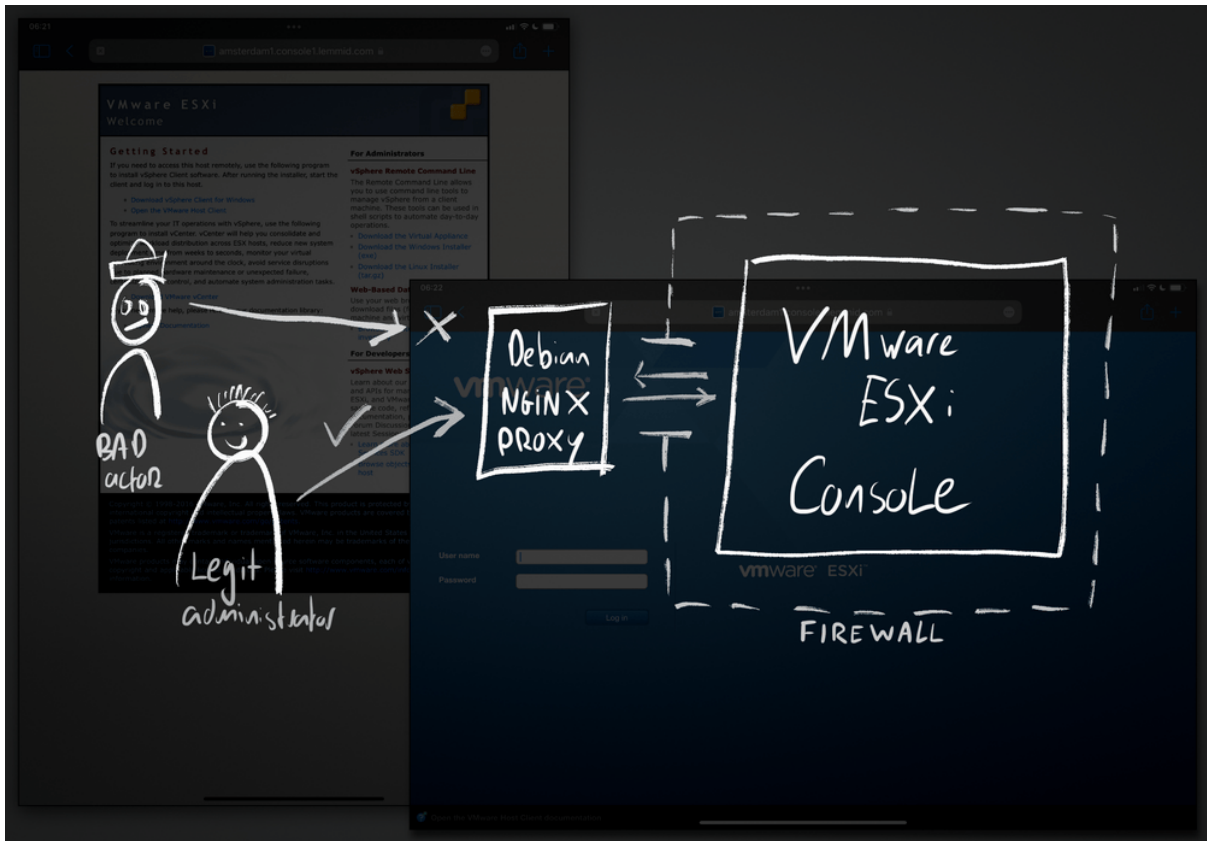


VMware ESXi schützen

Sicherheit mit Firewall und Proxyserver verbessern

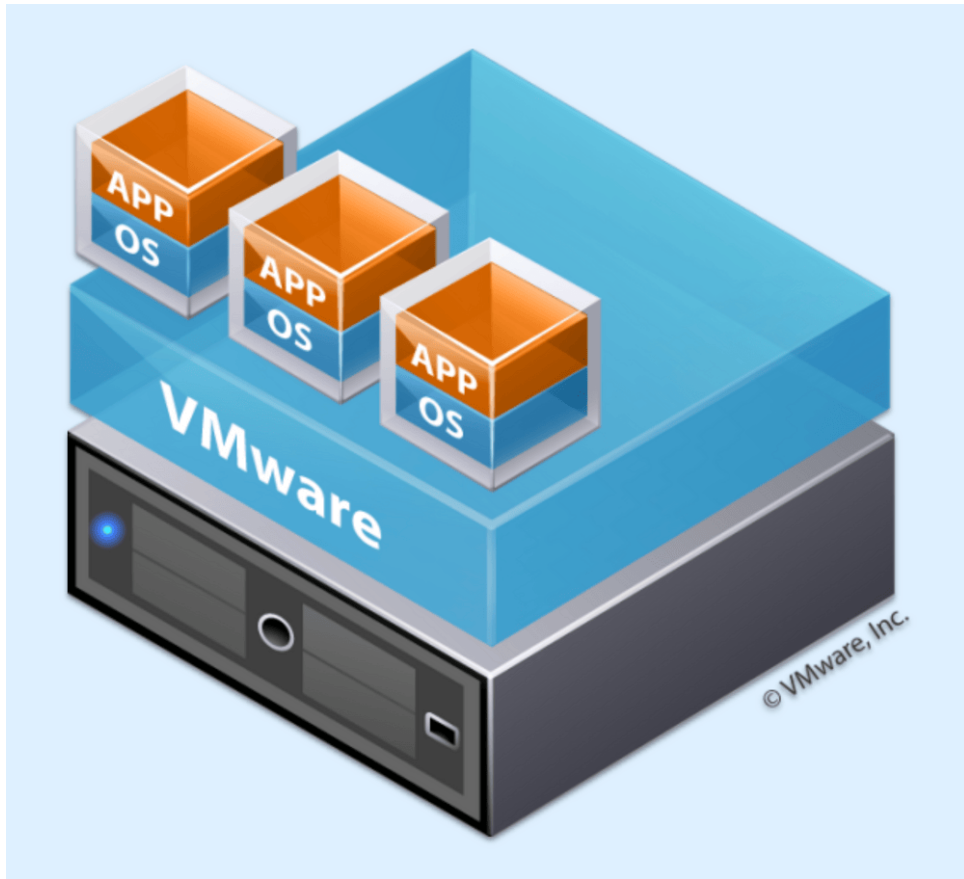
Willem L. Middelkoop

31 Aug. 2021



Als Reaktion auf einen Vorfall auf einem Server habe ich einen möglichen Sicherheitsverstoß festgestellt. Die betroffene Maschine lief mit VMware ESXi, einem Bare-Metal-Hypervisor, der zum Betrieb virtueller privater Server verwendet wird. Im Standalone-Modus bietet eine webbasierte Managementkonsole volle Kontrolle über die Infrastruktur, was ein Risiko darstellt.

Große und leistungsstarke Serverhardware bietet eine Menge Rechenkapazität, oft viel mehr, als eine einzelne Anwendung benötigt. Durch Virtualisierung können Cloud-Betreiber die Hardwareauslastung optimieren, indem sie dynamisch mehrere virtuelle Maschinen auf eine einzige physische Maschine laden.



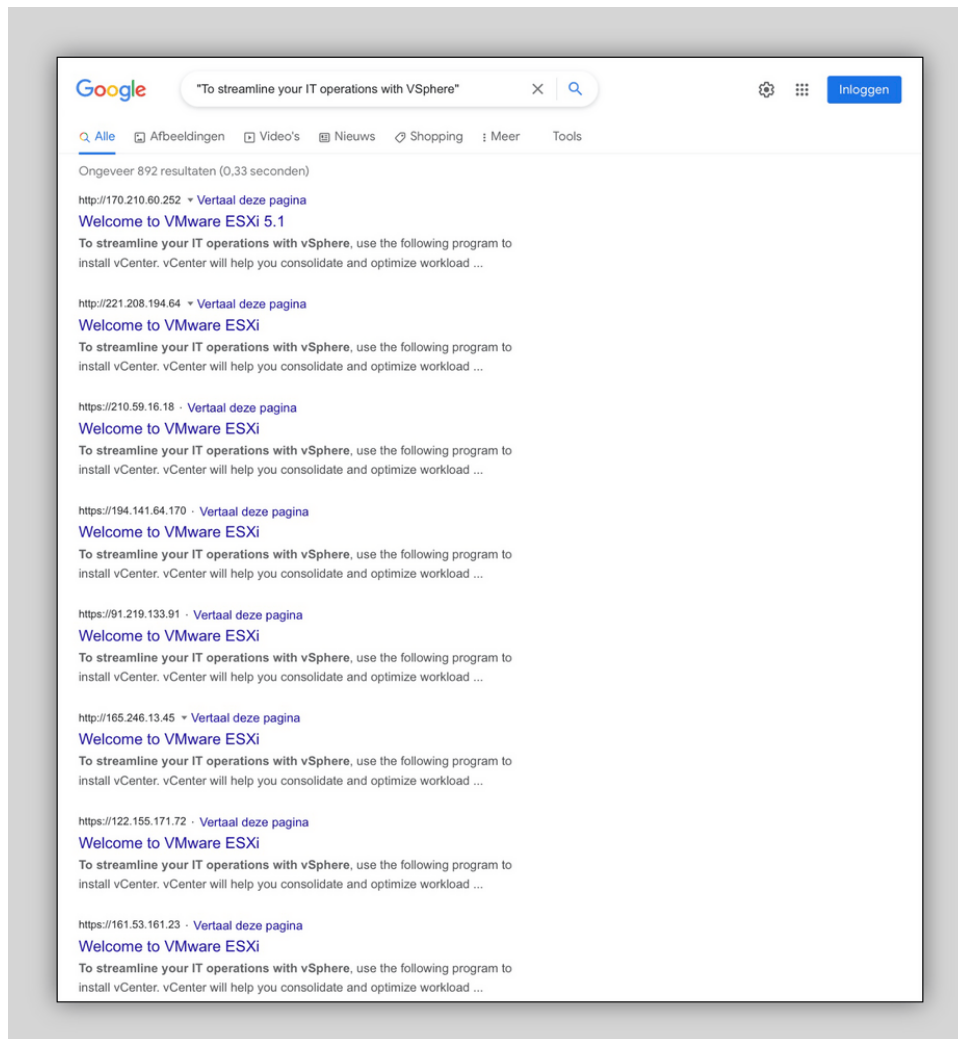
VMware ESXi ist ein Bare-Metal-Hypervisor, der einen physischen Server in mehrere virtuelle Server unterteilt

Physische Maschinen, auf denen VMware ESXi läuft, werden als zentralisiertes vSphere-Netzwerk oder als eigenständige Maschine verwaltet. Administratoren erstellen, verwalten und konfigurieren virtuelle Maschinen über eine leistungsstarke Weboberfläche. Ohne ein zentralisiertes vSphere-Netzwerk benötigen Administratoren diese Weboberfläche - aber die Bereitstellung im öffentlichen Internet zieht unerwünschte Aufmerksamkeit von Hackern auf sich.



VMware ESXi Webinterface - lädt Sie und andere zur Verwaltung dieses physischen Rechners ein

Böswillige Akteure suchen aktiv nach exponierten Verwaltungskonsolen, in der Hoffnung, eine mit einem schwachen Passwort oder mit bekannten Sicherheitslücken zu finden. Entfesseln Sie den neugierigen Entdecker in sich und nutzen Sie einfach Google, um eine_ganze_Reihe_von_exponierten_Maschinen_mit_einer_speziellen_Abfrage zu finden. Sehen Sie sich meinen Blogbeitrag über_spezielle_Abfragen_auf_Google an, wenn Sie Ihre Suchfähigkeiten auffrischen müssen.

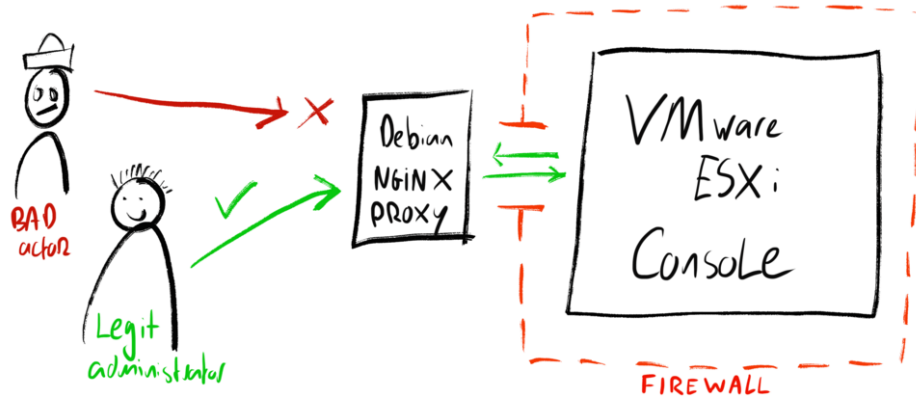


Das Finden von exponierten VMware ESXi Webinterfaces erfordert nichts weiter als ein paar Google-Kenntnisse

Lassen Sie die Verwaltungskonsole exponiert und jeder kann versuchen, sich anzumelden. Hacker und ihre automatisierten Bots werden dies mit Sicherheit tun! Der Fernzugriff für lokale ESXi-Benutzerkonten wird nach mehreren fehlgeschlagenen Anmeldeversuchen vorübergehend gesperrt - für alle! Dies kann frustrierend sein, wenn Sie als legitimer Administrator Zugriff auf die Konsole benötigen.

Indem Sie meinen [einfachen Cyber-Sicherheits-Tipps](#) folgen, kann die Sicherheit von VMware ESXi verbessert werden, indem die Verwaltungskonsole vollständig versteckt wird. Sie könnten versucht sein, dafür eine einfache "Alles abdecken"-Firewall zu verwenden, aber bedenken Sie den Bedarf an der Verwaltungskonsole: Sie bietet wichtigen Zugriff auf laufende virtuelle Maschinen. Sie möchten wirklich, dass Ihre Administratoren im Notfall rund um die Uhr von überall auf der Welt auf die Oberfläche zugreifen können.

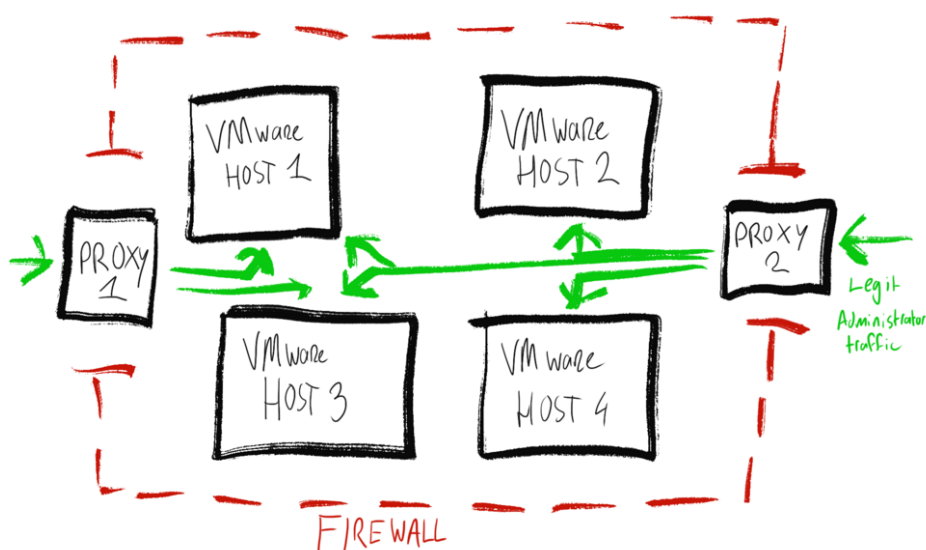
Anstatt die Verwaltungsoberfläche komplett zu schließen oder zu verstecken, habe ich nach einer Möglichkeit gesucht, den Zugriff selektiv zu erlauben und gleichzeitig ein unauffälliges Online-Profil zu wahren. Da ich möchte, dass legitime Administratoren von überall auf der Welt auf die Oberfläche zugreifen können, konnte ich keinen einfachen IP-Adressfilter verwenden. Mit einem Debian GNU/Linux-Rechner mit nginx als Proxy-Server kann ich den Datenverkehr zur Verwaltungskonsole vorab authentifizieren.



Vorabauthentifizierung des Datenverkehrs zur Administrationskonsole über einen kleinen und einfachen Debian GNU/Linux Server mit nginx Proxy

In diesem Setup läuft der Debian-Rechner in einem separaten Netzwerk, auf anderer Hardware, mit einer festen IP-Adresse. Der VMware-Server akzeptiert nur Datenverkehr von diesem Proxy-Server über seine Firewall. Der Proxy-Server filtert den Datenverkehr mithilfe der HTTP-Authentifizierung über SSL/TLS. Jeder kann sich mit dem Proxy-Server verbinden, aber nur diejenigen mit gültigen Anmeldeinformationen können die VMWare-Verwaltungskonsole erreichen. Der Proxy-Server erscheint jedem, der ihn scannt, als ein sehr kleiner, standardmäßiger Webserver: Er bietet eine unauffällige Online-Signatur.

Fügen Sie einen weiteren Proxy-Server aus einem anderen Netzwerk auf anderer Hardware hinzu, um einen Single Point of Failure zu vermeiden. Nginx kann authentifizierten Datenverkehr basierend auf verschiedenen Hostnamen an verschiedene Verwaltungskonsolen weiterleiten, sodass Sie einen einzelnen Proxy wiederverwenden können, um mehrere VMware-Maschinen zu sichern. Die Proxy-Server können so konfiguriert werden, dass sie die HTTP-Basisauthentifizierung mit Standard- und einfachen Tools verwenden. Sehen Sie sich die [nginx_Dokumentation_für_Tipps_dazu](#) an.



Zwei Proxyserver, die sicheren Zugriff auf mehrere VMware-Hosts bieten

```

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

```

nginx-Konfiguration zur Authentifizierung und Weiterleitung des Datenverkehrs an eine VMware-Administrationskonsole

Fazit

Durch die Verwendung von nginx als Proxy zur Verwaltungskonsole können Sie eine Authentifizierungsebene hinzufügen *und* eine unauffällige Signatur für jeden erstellen, der Ihr Netzwerk scannt. Dies verbessert die Sicherheit Ihrer VMware-Maschinen, indem es sie schwerer auffindbar und zugänglich macht. Legitime Administratoren können weiterhin mit jedem Computer auf die Verwaltungskonsole zugreifen, ohne dass ein VPN oder eine vorab authentifizierte IP-Adresse erforderlich ist. Böswillige Akteure, Hacker und Bots werden es schwer haben, Sie zu finden. Sie verstecken sich in aller Öffentlichkeit!