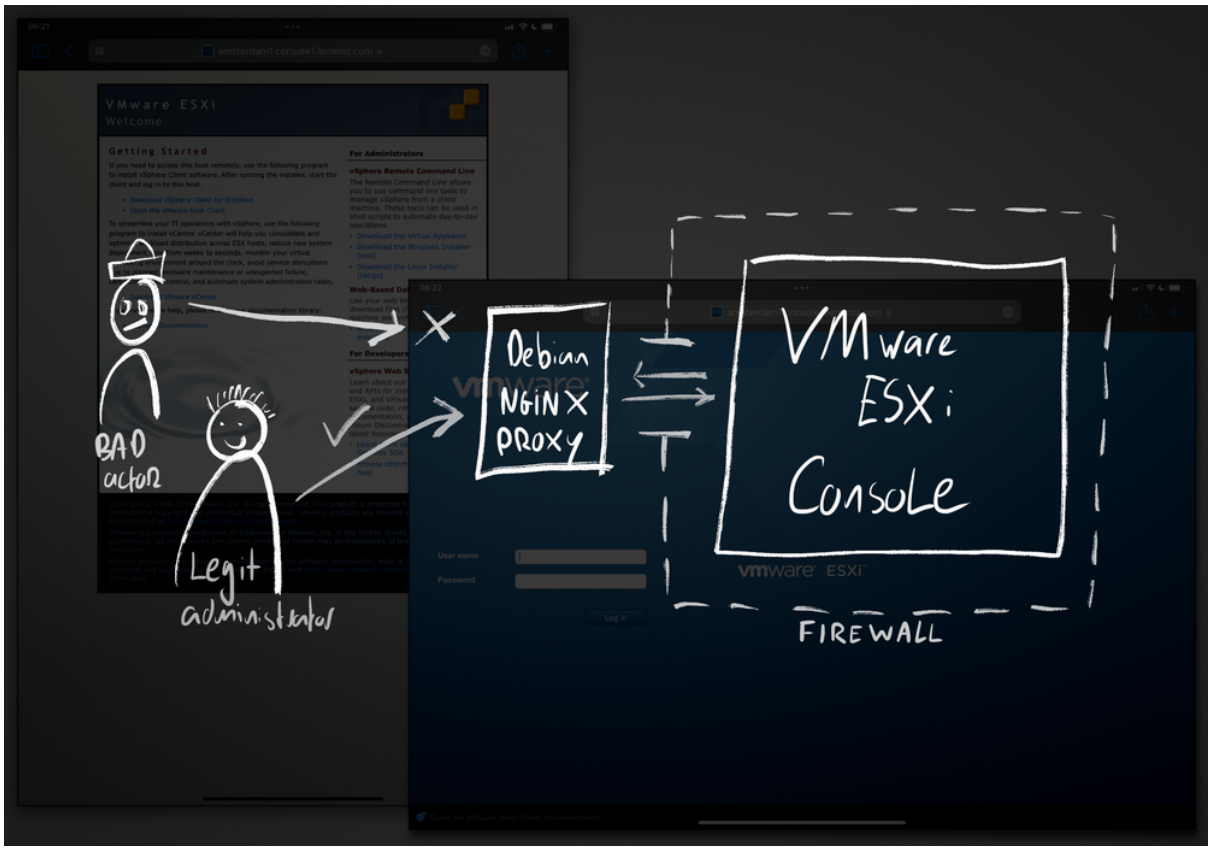
Protecting VMware ESXi

Improve security using a firewall and proxy server

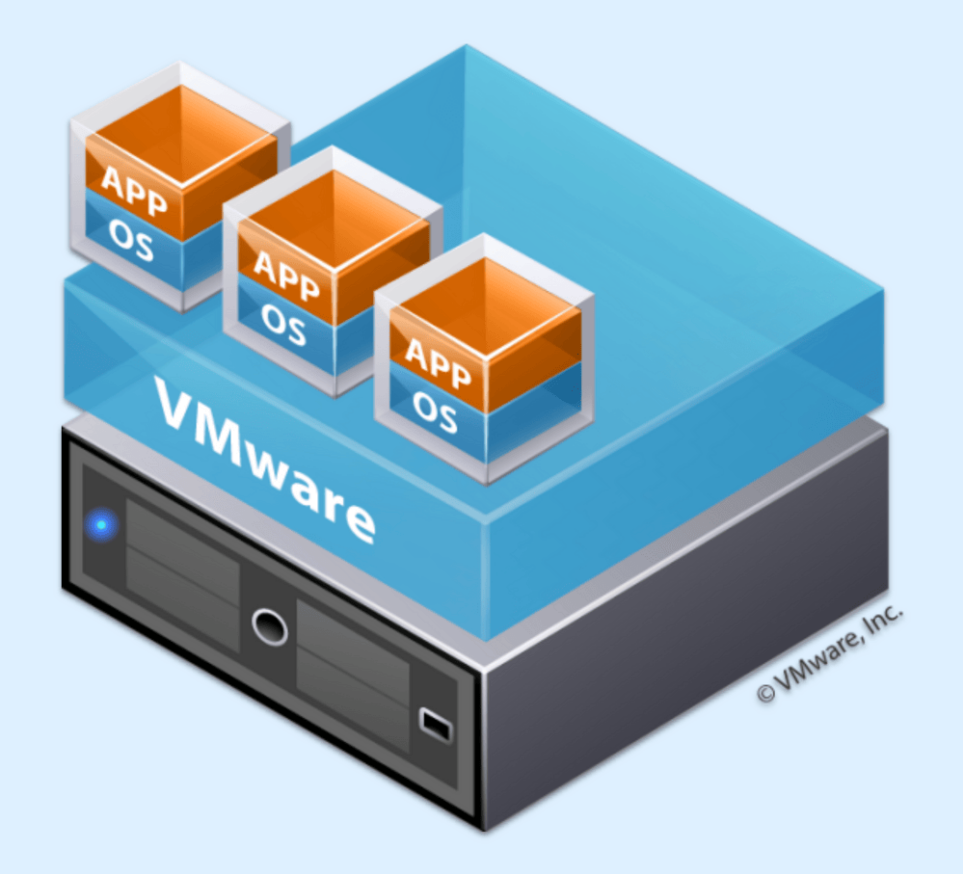
Willem L. Middelkoop

Aug. 31, 2021



In response to an incident on a server, I detected a possible security breach. The affected machine ran VMware ESXi, a bare metal hypervisor used to run virtual private servers. In standalone mode, a web based management console offers full control over the infrastructure, posing a risk.

Big and powerful server hardware offers a ton of computing capacity, often much more than one single application needs. Through virtualisation cloud operators can optimise hardware usage by dynamically loading multiple virtual machines onto a single physical machine.

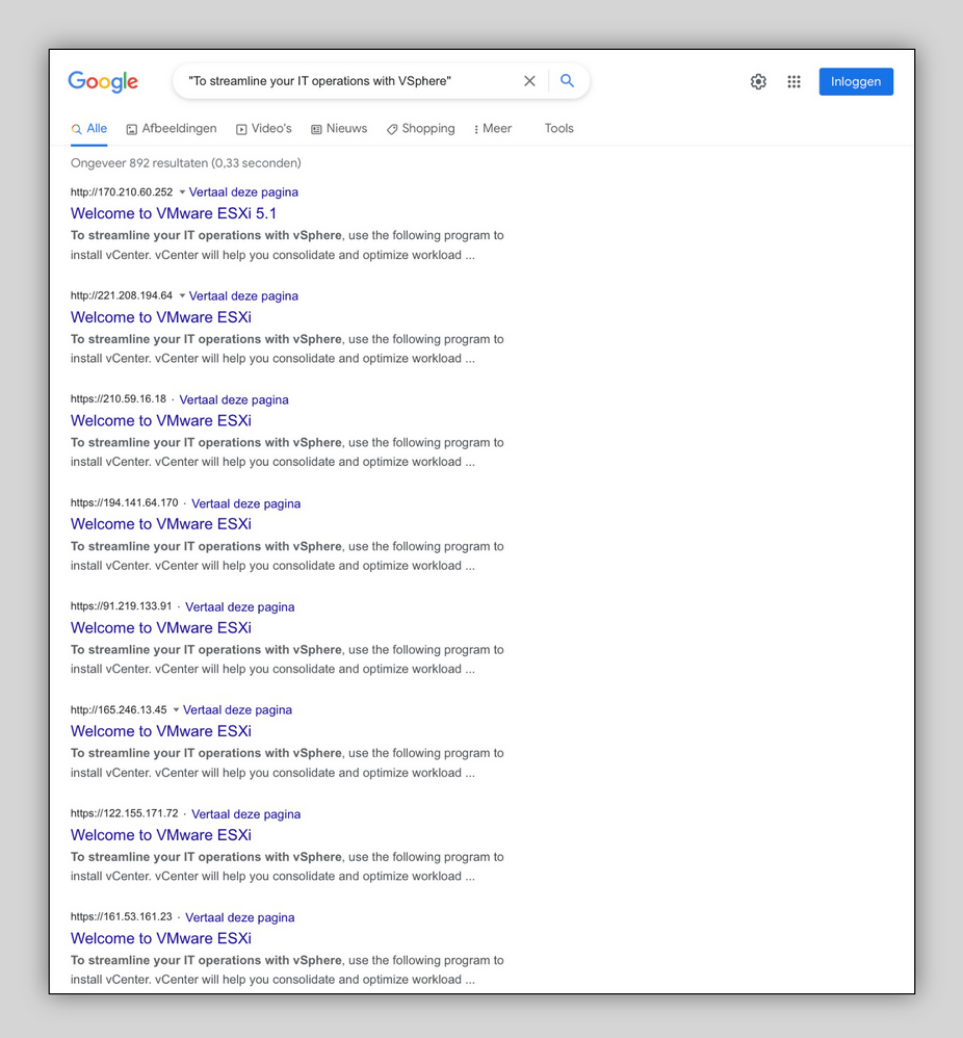


VMware ESXi is a bare metal hypervisor that divides one physical server into multiple virtual servers

Physical machines running VMware ESXi are managed as centralised VSphere network or as standalone machine. Administrators create, manage and configure virtual machines through a powerful web interface. Without a centralised VSphere network, administrators need this web interface - but exposing it on the public internet attracts unwanted attention from hackers.

VMware ESXi web interface - inviting you and others to manage this physical machine

Malicious actors actively search for exposed management consoles, hoping to find one with a weak password or with known security weaknesses. Unleash the curious explorer in yourself and simply utilise Google to find a whole bunch of exposed machines with a special query. See my blog post about special queries on Google if you need to brush up your searching skills.

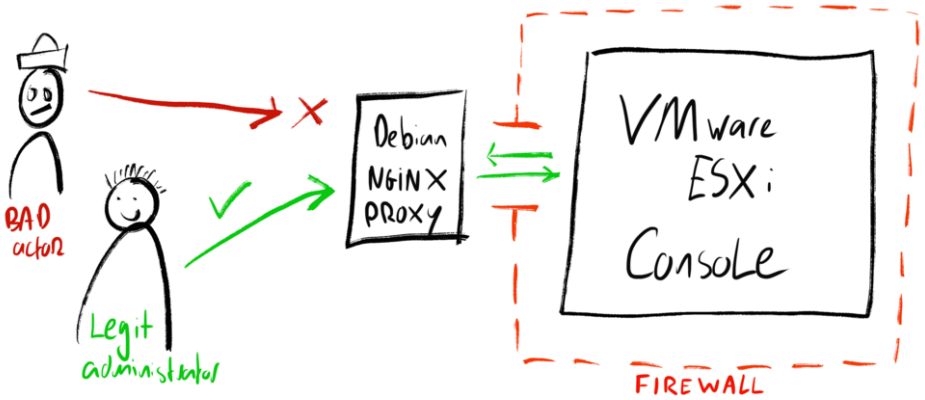


Finding exposed VMware ESXi web interfaces requires nothing but some Google skills

Leave the management console exposed and anybody can try to login. Hackers and their automated bots will certainly do so! Remote access for ESXi local user accounts will be temporarily locked after multiple failed login attempts - for everybody! This can be frustrating whenever you as legitimate administrator need access to the console.

Following my own easy cyber security tips the security of VMware ESXi can be improved by hiding the managent console altogether. You may be tempted to use a simple "cover it all" firewall for this, but do consider the need for the administrative console: it provides vital access to running virtual machines. You really want your administrators to be able to access the interface 24/7 from anywhere in case of emergency.

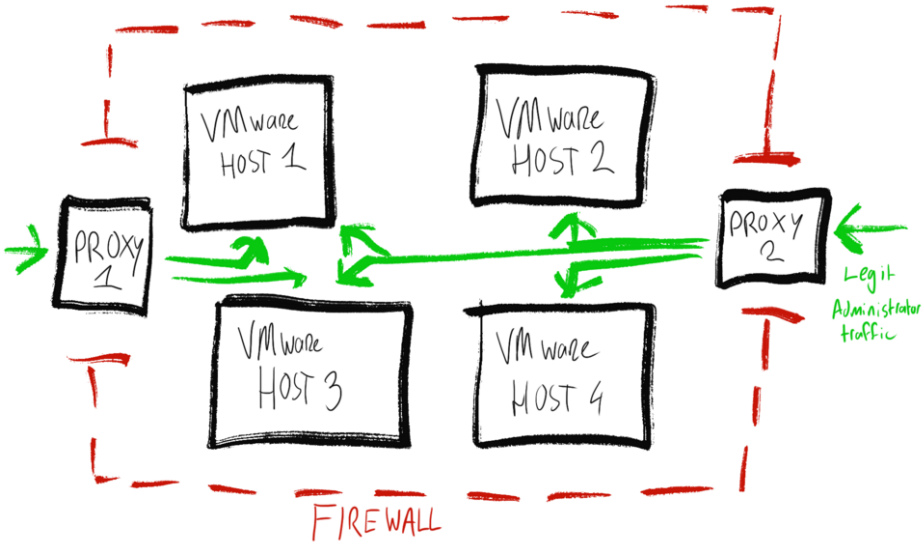
So instead of completely shutting down or hiding the management interface, I looked for a way to selectively allow access while maintaining a stealthy online profile. Because I want legit administrators to access the interface from anywhere in the world, I could not use a simple IP-address filter. Using a Debian GNU/Linux machine with nginx as a proxy server, I am able to pre-authenticate traffic to the management console.



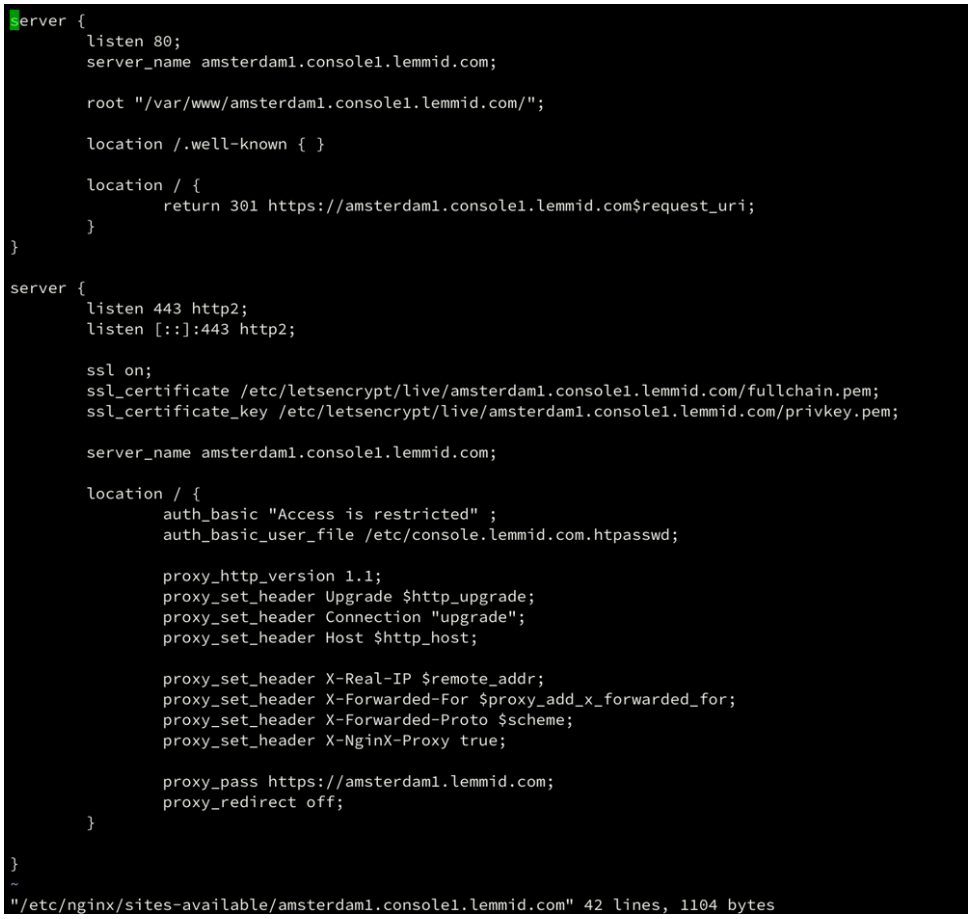
Pre-authenticate traffic to the administrative console through a small and simple Debian GNU/Linux server with nginx proxy

In this setup the Debian machine runs on a separate network, on different hardware, with a fixed IP-address. The VMware server only accepts traffic from this proxy server using its firewall. The proxy server filters traffic using HTTP-authentication over SSL/TLS. Anybody can connect to the proxy server, but only those with valid credentials can reach the VMWare administrative console. The proxy server appears to be a very tiny, standard webserver for anybody that scans it: providing a stealthy online signature.

Add another proxy server from another network on different hardware in the mix to prevent a single point of failure. Nginx can forward authenticated traffic to different administrative consoles based on different hostnames, enabling you to re-purpose a single proxy to secure multiple VMware machines. The proxy servers can be configured to use HTTP Basic authentication using standard and simple tools, check out the nginx documentation for tips on this.



Two proxy servers providing secure access to multiple VMware hosts



nginx configuration to authenticate and forward traffic to a VMware administrative console

Conclusion

By using nginx as a proxy to the administrative console you can add a layer of authentication *and* create a stealthy signature for anybody scanning your network. This improves the security of your VMware machines by making them harder to find and to access. Legit administrators can still access the administrative console using any computer without the need for a VPN or pre-authenticated IP-address. Bad actors, hackers and bots will have a hard time finding you. You're hiding in plain sight!