VIPRINET VIRTUAL VPN HUB SETUP

General Information

The Viprinet Virtual VPN Hub is targeted for *VMWare ESXi*. For setup, two sets of files are provided: VMDK files for traditionalists and an OVA file for convenience. The Virtual VPN Hub image can be installed any number of times as it doesn't contain product identity/serial information by itself. However, before a Virtual VPN Hub can actually be used, it needs an identity: The Virtual VPN Hub's instance ID must be bound to a Viprinet product serial number.

As soon as a Virtual VPN Hub is launched for the first time, it will acquire a product serial number from a Viprinet VirtualCloud server which are redundant HTTPS servers located world-wide. Once this serial number is set, it may be used to assign a subscription license enabling the activation of VPN tunnels. Virtual Hubs have all software features included that are optional for physical hubs. These features as well as installation and serial number acquisition are free; however, any active VPN tunnel as well as any VPN Client will be charged. Subscription licenses for an individual number of concurrently enabled VPN tunnels can be created at the VLM portal (https://support.viprinet.com). These licenses will be automatically downloaded to the Virtual VPN Hub they have been assigned to.

Subscriptions for VPN tunnels and VPN Clients are limited not by number, but by operating life. This means, a Virtual Hub can have an unlimited number of tunnels and clients, but these tunnels and clients will be active for e.g. 30 days only, which is the minimum subscription interval. After this time, subscription needs to be renewed. Else, VPN tunnels and VPN Clients will disconnect. Also, subscription will not be halted if a VPN tunnel or VPN Client are not used all the time while subscription lasts.

Virtual VPN Hubs only work as long as they're able to access VirtualCloud servers. This means that the Virtual Hub must be able to access any IP of Viprinet cloud network servers (*.cloud.vipri.net) using the LAN interface on HTTPS port 443 at all times. In order to detect clones and license violations, the Virtual Hub contacts the VirtualCloud servers regularly to have its serial number verified. This verification process can take up to 30 minutes for the first time after a start-up. If a Virtual Hub cannot connect to any VirtualCloud server after start-up, it will not accept tunnels. If the disconnect lasts longer than 7 days, the Virtual Hub will shut down and no longer accept tunnels.

If the Virtual VPN Hub needs to be suspended for any reason, its serial number will have to be re-validated.

Copying a Virtual VPN Hub

A Virtual Hub may only ever have one specific product serial number. Running multiple identical Virtual Hubs with the same product serial number is a license violation and will result in a shutdown of all duplicate Virtual Hubs!

If you wish to ***copy*** an existing Virtual Hub, please make sure that the virtual host assigns a new Virtual Hub ID (SMBIOS UUID) for the copy! The Virtual Hub will then automatically detect that it has been copied, and acquire a new serial number without using the VPN tunnel licenses of the original Virtual Hub.

If you wish to ***move*** a Virtual VPN Hub from one virtual host to another, please make sure that the Virtual VPN Hub's instance ID (SMBIOS UUID) does **not** change! Only when the ID does not change, will the Virtual VPN Hub keep working seamlessly; otherwise, it will lose its serial number and licenses.

If a Virtual VPN Hub has no active subscriptions for VPN tunnels or VPN Clients and is powered off or suspended, its serial number may expire on next start-up of the Virtual Hub. In this case, the Virtual VPN Hub will automatically acquire a new serial number.

Setup Instructions

The current release can be downloaded from our update server at ftp://updates.vipri.net/.

VMWare

To install a Virtual VPN Hub on a VMWare host, you can either use:

- *viprinet_virtualhub.ova*

This OVA file will enable import of the appliance on your hypervisor.

Or you can use the following virtual drive in order to setup your own VM:

- *viprinet_virtualhub-flat.vmdk*
- *viprinet_virtualhub.vmdk*

Create a new VM on your ESXi host with the following attributes:

- Guest OS family: Linux
- Guest OS Version: Other 3.x or later Linux (64bit)
- Cores: 2 min.
- Memory: 1GB min.
- Disk image: *viprinet_virtualhub.vmdk*
- Default SATA controller, no need for the default SCSI one
- **2** network adapters from type VMXNET 3
  - First adapter will be the LAN port
  - Second adapter will be the WAN port

Important note: **Do not rename the files!** Otherwise you will have to change the filename inside of *viprinet_virtualhub.vmdk* manually!

For VMWare, you will not need *viprinet_virtualhub.img*. This file is used for installation on other virtual hosts.

Initial Setup

There are two ways to do the initial setup of the LAN interface. Once the LAN interface is configured, the final setup can be done using the Virtual VPN Hub's web interface.

Method 1

Use the Viprinet Setup Tool which you can download from the Viprinet website at www.viprinet.com/downloads.

Look for a ***01-05900-00-XXXXX*** serial. "XXXXX" means that no serial number has been assigned yet.

The setup tool must be run on a (virtual or physical) computer located in the same network segment (layer 2/3) as the Virtual Hub.

Method 2

Once the Virtual VPN Hub has been started, login with "setup/setup" on the tty1 to get into the Viprinet CLI.

You can setup the LAN interface with the following command:

```
user root
password viprinet
set LANSETTINGS.IPADDRESS <IP>
set LANSETTINGS.NETMASK <NETMASK>
set LANSETTINGS.DEFAULTGATEWAY <GW>
execute LANSETTINGS.APPLYSETTINGS
execute ROUTERLOGGINGSETTINGS.REBOOT
```

Update

After initial setup, please update the Virtual VPN Hub to the latest RuggedVPN firmware. For the, you may either use the online update (*Logging & Maintenance -> Router Firmware Update -> Install available updates now*) or you download the latest RuggedVPN firmware manually (updates.vipri.net/files/firmware/ruggedvpn/01-05900/) and install it via *Logging & Maintenance -> Router Firmware Update -> Manual Firmware Upload*.

AWS

You can find the latest Virtual VPN Hub version for AWS (Amazon Web Services) after login at AWS' marketplace (Community AMIs) under aws.amazon.com/marketplace/pp/B0747PX7H1?qid=1517403759065&sr=0-1&ref_=srh_res_product_title.

Other/Unsupported Platforms

Virtualbox

- Works
- Use *Intel PRO/1000 MT Desktop* for the NICs

KVM

- Reported to work

VMWare Player

- Reported to work

Hyper-V

- Not working yet
- *Linux Integration Services* are required, tbd

Miscellaneous

- On TTY2, you will find the Viprinet log
- *Open-vm-tools* (an open source version of the *VMware guest additions*) is shipped along

Setup

To install a Virtual VPN Hub on one of these virtual hosts, you will need the following file:

- viprinet_virtualhub.img

Technical Requirements	
Free Hard Disk Space	256 MB min.
CPU	2–4 Cores • Core i7 from 2.6 GHz • Xeon E3/E5 from 2.6 GHz • Xeon E7 from 2.3 GHz Support for VT-x, AES-NI
RAM	1–4 GB
VMware	ESXi 6.x

By adding CPU capacity and RAM space on the server used, the Viprinet Virtual VPN Hub can be adapted very easily to individual scenarios.

Higher CPU capacity is recommended for use cases that involve high throughput, as this creates more CPU load.

Higher RAM space is recommended for use cases with many single tunnels. Each tunnel means an increase of processing power and thus higher RAM usage.

Minor load: 1 CPU Core / 1 GB RAM

Medium load: 2 CPU Cores / 2 GB RAM

High load: 4 CPU Cores / 4 GB RAM