VIPRINET VIRTUAL VPN HUB SETUP

Allgemeine Information

Der Viprinet Virtual VPN Hub wurde auf die Verwendung von *VMWare ESXi* ausgelegt. Zur Installation auf diesem Virtual Host gibt es zwei Dateisätze: traditionale VMDK-Dateien und eine OVA-Datei, die den Installationsprozess etwas erleichtert. Das Virtual Hub-Image kann unbegrenzte Male installiert werden, da es selbst keine Produkt-ID bzw. Seriennummer trägt. Dennoch benötigt der Virtual Hub für vollen Funktionsumfang durchaus eine Identität: Die Instanz-ID eines Virtual VPN Hub muss an eine Viprinet Produkt-Seriennummer gebunden werden.

Sobald ein Virtual VPN Hub das erste Mal gestartet wird, zieht er sich eine Produkt-Seriennummer von einem Viprinet VirtualCloud-Server – redundante, überall weltweit verteilte HTTPS-Server. Sobald diese Seriennummer gesetzt wurde, kann sie dazu genutzt werden, eine Abonnement-Lizenz zur Aktivierung von VPN-Tunnels zu erstellen. Der Virtual VPN Hub umfasst bereits alle Software Features, die für physikalische Hubs optional sind. Diese Features, ebenso wie die Installation und das Zuweisen der Seriennummer sind kostenlos; die Nutzung jedes aktiven VPN-Tunnels und VPN-Clients sind hingegen kostenpflichtig. Abonnement-Lizenzen für eine individuelle Anzahl an gleichzeitig aktiven VPN-Tunneln können im VLM-Portal (https://support.viprinet.com) erstellt werden. Diese Lizenzen werden dann automatisch auf den Virtual Hub hochgeladen, dem sie zugewiesen wurden.

Abonnements für VPN-Tunnel und VPN-Clients werden nicht nach Anzahl, sondern nach Nutzungsdauer begrenzt. Das bedeutet, dass für einen Virtual Hub eine unbegrenzte Anzahl an Tunnels und Clients angelegt werden kann, dass diese aber jeweils nur für z.B. 30 Tage (Mindestdauer des Abonnements) aktiviert bleiben. Nach Ablauf dieser Zeit muss das Abonnement erneuert werden oder die VPN-Tunnels und VPN-Clients werden getrennt. Nicht genutzte Abonnement-Zeit kann zudem nicht gutgeschrieben werden: Wenn VPN-Tunnels oder VPN-Clients während der Dauer des Abonnements nicht genutzt werden, wird das Abonnement nicht automatisch verlängert.

Virtual VPN Hubs funktionieren nur, solange sie in der Lage sind, sich mit VirtualCloud-Servern zu verbinden. Das bedeutet, dass ein Virtual Hub jederzeit in der Lage sein muss, über das LAN-Interface auf HTTPS-Port 443 jegliche IP-Adresse der Viprinet Cloud-Netzwerkserver (*.cloud.vipri.net) zu erreichen. Um Klone und Lizenzverletzungen zu erkennen, kontaktiert ein Virtual Hub zur Verifizierung seiner Seriennummer regelmäßig die VirtualCloud-Server. Dieser Verifizierungsprozess kann das erste Mal nach einem Systemstart bis zu 30 Minuten dauern. Wenn ein Virtual Hub sich nach einem Systemstart mit keinem VirtualCloud-Server verbinden kann, baut er keine Tunnel auf. Wenn ein Virtual Hub länger als 7 Tage keinen VirtualCloud-Server erreichen kann, fährt er runter und baut ab dann keine Tunnel mehr auf.

Wenn der Virtual VPN Hub angehalten wird, muss er danach seine Seriennummer erneut bestätigen lassen.

Kopieren eines Virtual VPN Hub

Ein Virtual Hub kann immer nur eine spezifische Produkt-Seriennummer haben. Mehrere identische Virtual Hubs mit derselben Produkt-Seriennummer (sogenannte Klone) zu betreiben, stellt eine Lizenzverletzung dar und hat zur Folge, dass alle duplizierten Virtual Hubs herunterfahren!

Wenn Sie einen existierenden Virtual VPN Hub ***kopieren*** möchten, stellen Sie bitte sicher, dass der Virtual Host der Kopie eine neue Instanz-ID (SMBIOS UUID) zuweist! Der Virtual VPN Hub erkennt dann automatisch, dass er kopiert wurde und fordert eine neue Seriennummer an, ohne die Lizenzen des originalen Virtual Hubs zu nutzen.

Wenn Sie einen Virtual VPN Hub von einem Virtual Host zu einem anderen ***umziehen*** möchten, stellen Sie bitte sicher, dass sich die Instanz-ID des Virtual VPN Hubs (SMBIOS UUID) **nicht** ändert! Nur in diesem Fall arbeitet der Virtual Hub problemlos weiter, während er ansonsten seine Seriennummer und Lizenzen verliert.

Wenn einem Virtual VPN Hub keine aktiven Abonnements für VPN-Tunnels oder VPN-Clients zugewiesen sind und er abgeschaltet bzw. angehalten wurde, kann seine Seriennummer beim nächsten Hochfahren verfallen. In diesem Fall zieht sich der Virtual VPN Hub automatisch eine neue Seriennummer.

Installationshinweise

Das aktuelle Release steht auf unserem Update-Server unter ftp://updates.vipri.net/ zum Download bereit.

VMWare

Um einen Virtual VPN Hub auf einem VMWare-Host initial zu installieren, können Sie entweder folgende Datei nutzen:

- *viprinet_virtualhub.ova*

Diese Datei ermöglicht den Import der Appliance auf Ihrem Hypervisor.

Oder Sie nutzen die folgende virtuelle Festplatte, um selbst eine VM anzulegen:

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

Erstellen Sie eine neue VM auf Ihrem ESXi-Host mit folgenden Eigenschaften:

- Guest OS family: Linux
- Guest OS Version: Other 3.x oder später Linux (64bit)
- Cores: 2 mind.
- Speicher: 1GB mind.
- Disk-Image: *viprinet_virtualhub.vmdk*
- Standard SATA-Controller, Standard SCSI-Controller nicht nötig
- **2** Netzwerk-Adapter vom Typ VMXNET 3
  - Der erste Adapter wird der LAN-Port
  - Der zweite Adapter wird der WAN-Port

Wichtiger Hinweis: **Benennen Sie die Dateien nicht um!** Andernfalls müssen Sie die Dateinamen innerhalb *viprinet_virtualhub.vmdk* manuell ändern!

Für VMWare benötigen Sie *viprinet_virtualhub.img* nicht. Diese Datei dient zur Installation des Virtual VPN Hub auf anderen Hypervisoren, bzw. wenn Sie selbst eine virtuelle Festplatte erstellen möchten.

Erstes Setup

Es gibt zwei Arten, um das erstmalige Setup des LAN-Interface durchzuführen. Sobald das LAN-Interface konfiguriert wurde, kann das weiterführende Setup über das Web-Interface des Virtual VPN Hub erfolgen.

Methode 1

Nutzen Sie das Viprinet Setup-Tool, das Sie von der Viprinet-Website unter www.viprinet.com/downloads herunterladen können.

Suchen Sie nach einer ***01-05900-00-XXXXX*** Seriennummer. Das „XXXXX" bedeutet, dass noch keine Seriennummer zugewiesen wurde.

Das Setup-Tool muss auf einem (virtuellen oder physikalischen) Rechner ausgeführt werden, welches sich im gleichen Netzwerksegment (Layer 2/3) mit dem Virtual Hub befindet.

Methode 2

Sobald der Virtual VPN Hub gestartet wurde, loggen Sie sich mit „setup/setup" auf TTY1 ein, um in die Viprinet-CLI zu kommen.

Setzen Sie das LAN-Interface mit folgendem Befehl auf:

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

Update

Bitte updaten Sie den Virtual VPN Hub nach dem erstmaligen Setup auf die aktuellste RuggedVPN-Firmware. Dafür können Sie entweder das Online-Update nutzen (*Logging & Maintenance -> Router Firmware Update -> Install available updates now*) oder Sie laden manuell die aktuellste RuggedVPN-Firmware (updates.vipri.net/files/firmware/ruggedvpn/01-05900/) herunter und installieren diese unter *Logging & Maintenance -> Router Firmware Update -> Manual Firmware Upload*.

AWS

Die aktuellste Version des Virtual VPN Hub für AWS (Amazon Web Services) finden Sie nach Ihrer Anmeldung bei AWS im Marketplace (Community AMIs) unter aws.amazon.com/marketplace/pp/B0747PX7H1?qid=1517403759065&sr=0-1&ref_=srh_res_product_title.

Andere/Nicht unterstützte Plattformen

Virtualbox

- Funktioniert
- Nutzen Sie *Intel PRO/1000 MT Desktop* für die NICs

KVM

- Funktioniert vermutlich

VMWare Player

- Funktioniert vermutlich

Hyper-V

- Funktioniert noch nicht
- *Linux Integration Services* werden benötigt, tbd

Diverse

- Sie finden das Viprinet-Log auf TTY2
- *Open-VM-Tools* (eine Open-Source-Version der *VMWare Guest Additions*) wird mitgeliefert

Setup

Um einen Virtual VPN Hub auf einem dieser Virtual Hosts zu installieren, benötigen Sie folgende Datei:

- viprinet_virtualhub.img

Technische Spezifikationen	
Freier Platz auf Festplatte	mind. 256 MB
CPU	2–4 Cores • Core i7 ab 2,6 GHz • Xeon E3/E5 ab 2,6 GHz • Xeon E7 ab 2,3 GHz Unterstützung für VT-x, AES-NI
RAM	1–4 GB
VMware	ESXi 6.x

Durch Hinzufügen von CPU-Kapazität und RAM-Speicherplatz auf dem eingesetzten Server kann der Virtual VPN Hub sehr einfach auf individuelle Szenarien angepasst werden.

Höhere CPU-Kapazität wird für Anwendungsfälle empfohlen, bei denen viel Durchsatz benötigt wird, weil dadurch mehr CPU-Last anfällt.

Höherer RAM-Speicherplatz eignet sich für Einsätze, die viele einzelne Tunnel erfordern. Jeder Tunnel bedeutet einen Zuwachs an Rechenleistung und damit einen höheren RAM-Verbrauch.

Geringe Last: 1 CPU Core / 1 GB RAM

Mittlere Last: 2 CPU Cores / 2 GB RAM

Hohe Last: 4 CPU Cores / 4 GB RAM