

Konfigurieren eines On-Demand-Supports für den technischen SSH-Tunnel für virtuelle Umbrella-Appliances

Inhalt

[Einleitung](#)

[Technischer On-Demand-Support SSH-Tunnel](#)

[Voraussetzungen](#)

[Aktivieren des Tunnels](#)

[Aktivieren des Tunnels auf virtuellen Appliances, die auf VMware und Hyper-V gehostet werden](#)

[Aktivieren des Tunnels auf virtuellen Appliances, die auf anderen Plattformen gehostet werden](#)

[Einholen Ihrer Anmeldeinformationen für den Support](#)

[Tunnel deaktivieren/reaktivieren](#)

[Tunnelstatus](#)

[Verbunden](#)

[Deaktiviert](#)

[Verbindung](#)

[Zeitüberschreitung](#)

[Tunnelpersistenz](#)

Einleitung

In diesem Dokument wird die Konfiguration eines On-Demand-SSH-Tunnels für den technischen Support für Umbrella Virtual Appliances beschrieben.

Technischer On-Demand-Support SSH-Tunnel

Ein Support-Techniker kann Remote-Zugriff auf Ihre virtuelle Appliance (VA) anfordern, um einen Support-Fall weiter zu diagnostizieren und möglicherweise Einstellungen zu überprüfen oder zu aktualisieren, um die VA-Verfügbarkeit zu verbessern. Damit ein Umbrella Support-Techniker vor Ort auf eine Umbrella VA zugreifen kann, müssen diese Richtlinien befolgt werden.



Anmerkung: Diese Informationen gelten nur für VA mit Version 2.1.0 oder höher.

Voraussetzungen

- Alle Anforderungen für die Konfiguration einer VA auf VMWare oder Hyper-V aus der Setup-Dokumentation müssen erfüllt sein.
- Jede Firewall muss konfiguriert werden, um ausgehende Verbindungen zu `s.tunnels.ironport.com` zuzulassen.
- Die VA versucht, eine Verbindung auf den TCP-Ports 22, 25, 53, 80, 443 oder 4766 nacheinander herzustellen.

So testen Sie die Verbindung:

Telnet `s.tunnels.ironport.com` 25

63.251.108.107 wird versucht...

Verbunden mit `s.tunnels.ironport.com`.

Das Escapezeichen ist '^'].

SSH-2.0-OpenSSH_6.2 CiscoTunnels1

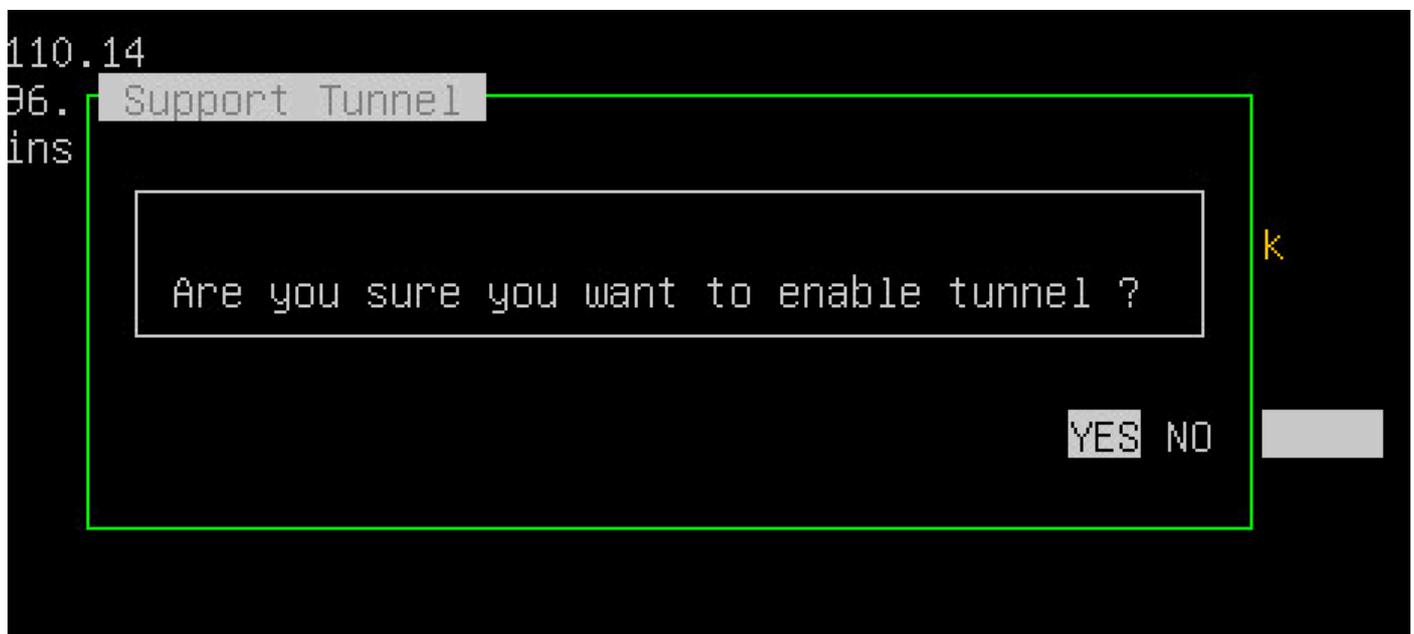
Aktivieren des Tunnels

Der SSH-Tunnel stellt eine Verbindung mit s.tunnels.ironport.com her. Die Dauer der Verbindung ist konfigurierbar, standardmäßig 72 Stunden.

Aktivieren des Tunnels auf virtuellen Appliances, die auf VMware und Hyper-V gehostet werden

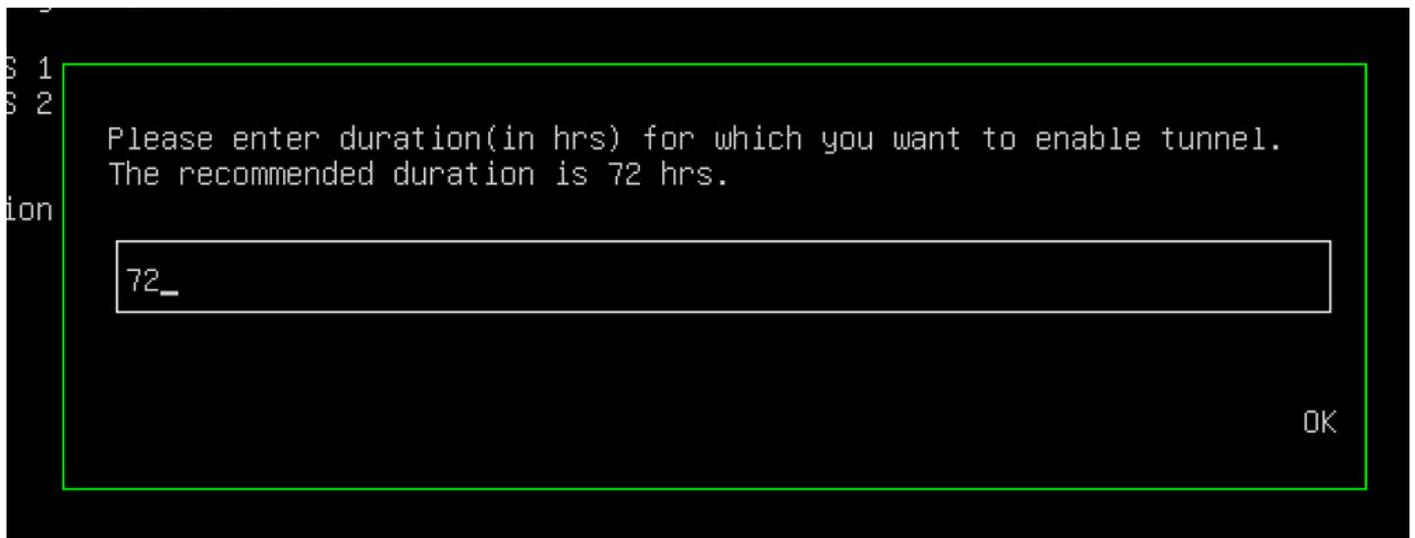
Tunnel können über die VA-Konsole mit dem Tastaturbefehl "STRG+T" aktiviert werden.

Wählen Sie Ja aus, wenn Sie dazu aufgefordert werden:



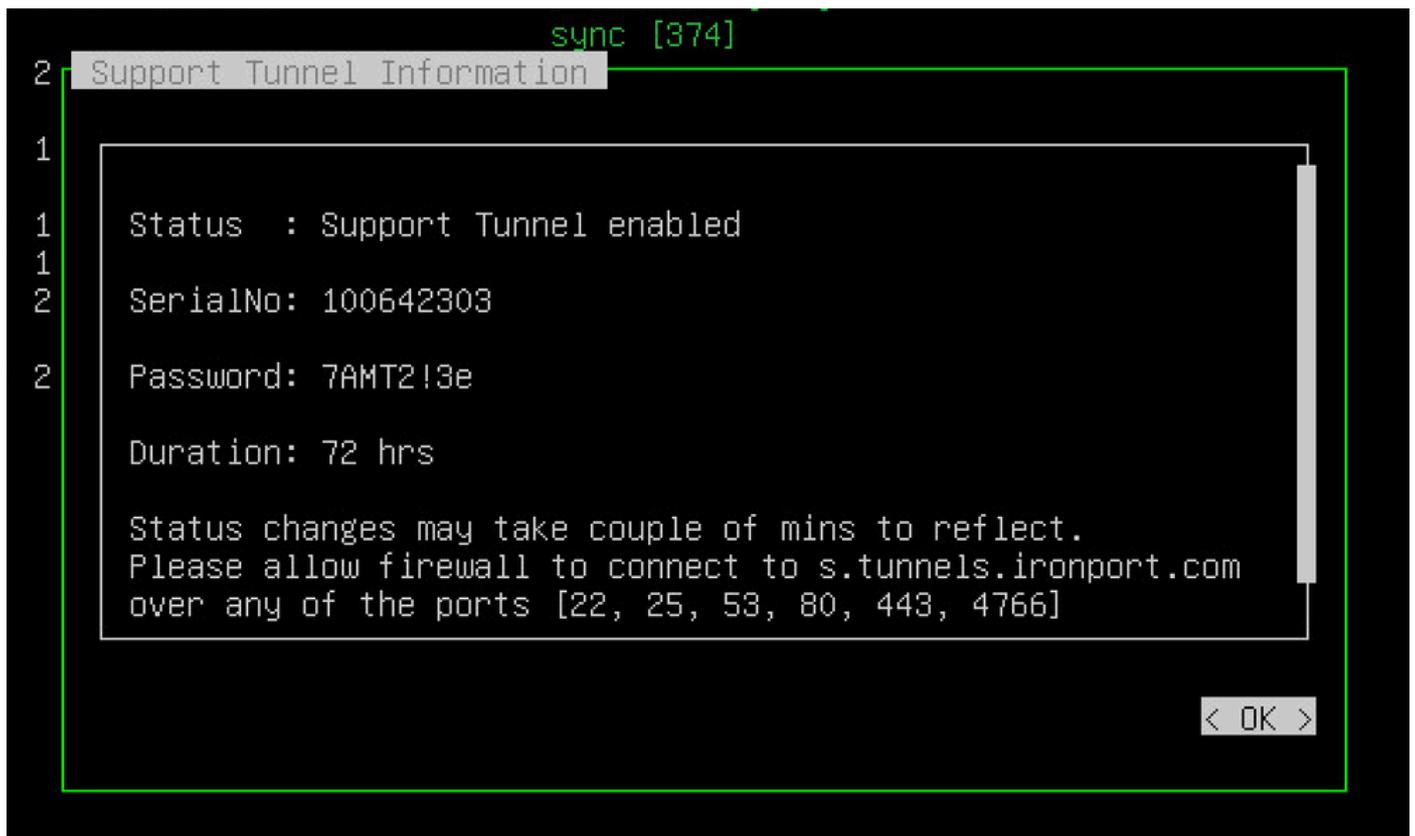
115013855903

Zunächst werden Sie aufgefordert, die Dauer der Tunnelsitzung festzulegen:



115013856003

Wählen Sie OK, um ein Fenster mit der Seriennummer und dem Kennwort für den Supporttunnel anzuzeigen. Diese Informationen müssen an den Supporttechniker übermittelt werden. Nachdem Sie OK ausgewählt haben, versucht die VA, eine Verbindung zum Support-Tunnel-Server herzustellen:



115013853243

Klicken Sie auf OK, um das Fenster zu schließen. Überprüfen Sie, ob auf der VA-Konsole "Remote Support Tunnel: Verbunden".

Connectivity

```
This DNS Server: DNS ok
Local DNS Servers: All DNS ok
Umbrella DNS Servers: All DNS ok
AD Connectors: Active
Remote Support Tunnel: Connected
Umbrella Cloud: SSL ok
Updates: SSL GET ok
```

360000820923

Aktivieren des Tunnels auf virtuellen Appliances, die auf anderen Plattformen gehostet werden

Stellen Sie über SSH eine Verbindung zur VA her, und verwenden Sie den folgenden Konfigurationsbefehl:

- Um den Support-Tunnel zu aktivieren, geben Sie `config tunnel enable <Dauer in Stunden>` ein.
- Um den Support-Tunnel zu deaktivieren, geben Sie `config tunnel disable` ein.
- Um den Status des Support-Tunnels zu überprüfen, geben Sie `config tunnel status` ein.
- Um diese Optionen anzuzeigen, geben Sie `config tunnel help` ein.

Einholen Ihrer Anmeldeinformationen für den Support

Die Seriennummer und das Kennwort, die in der VA-Konsole oder bei Verwendung des Befehls `config tunnel status` angezeigt werden, müssen dem Supporttechniker mitgeteilt werden.



Anmerkung: Das Kennwort, das Sie abrufen und für den Support freigeben, kann nicht direkt für den Zugriff auf die VA verwendet werden. Aus Sicherheitsgründen wird das echte Passwort kryptographisch aus dem Passwort abgeleitet, das Sie sehen. Um die Seriennummer und das Kennwort von der VA-Konsole abzurufen, erstellen Sie einen Screenshot, nachdem Sie den Tunnel mit Strg+T aktiviert haben. Stellen Sie sicher, dass der Screenshot für Menschen lesbar ist.

Tunnel deaktivieren/reaktivieren

Der Tunnel bleibt standardmäßig für 72 Stunden eingerichtet, Sie können die Tunneldauer jedoch mit der Option Re-enable verlängern.

Auf VMware und Hyper-V kann der Tunnel jederzeit mit dem Tastaturbefehl STRG+T deaktiviert oder erneut aktiviert werden:

1

Support Tunnel

14

1

Status : Support Tunnel enabled

SerialNo: 100933673

Password: 6zGQ%c3K

S ok
ok

ted

DISABLE RE-ENABLE OK



Anmerkung: Es kann bis zu einer Minute dauern, bis der Tunnelstatus von "Verbunden" in "Deaktiviert" geändert wird, sowohl in der Benutzeroberfläche als auch im Back-End, da der Tunnel ordnungsgemäß entfernt wird, anstatt beendet zu werden.

Auf anderen Plattformen können Sie den folgenden Befehl verwenden:

- `config tunnel reenable <Dauer in Stunden>`

Wenn Sie versuchen, den Tunnel unmittelbar nach der Deaktivierung wieder zu aktivieren, kann dies zu einer ungeraden Bedingung und Fehlermeldung führen, da der Tunnel zu diesem Zeitpunkt nicht vollständig deaktiviert ist.

Durch die erneute Aktivierung des Tunnels wird das Kennwort für die vorhandene Tunnelsitzung der VA nicht geändert. Durch Auswahl der Option Re-enable werden standardmäßig 72 Stunden Tunneldauer ab der aktuellen Zeit hinzugefügt.

Tunnelstatus

Verbunden

Der Status ändert sich von Deaktiviert zu Verbunden, sobald Sie den Tunnel aktivieren. Wenn die Verbindung erfolgreich hergestellt wurde, wird der Status ungefähr eine Minute lang im Verbindungsmodus belassen, während die VA versucht, den Tunnel mit dem Server herzustellen.

Deaktiviert

Wenn Sie den Tunnel nicht explizit aktiviert haben, wird der Status Disabled (Deaktiviert) angezeigt. Beachten Sie, dass es nach der expliziten Deaktivierung des Tunnels ungefähr eine Minute dauert, bis der Tunnelstatus von Verbunden zu Deaktiviert wechselt.

Verbindung

Im Verbindungszustand versucht die VA, den Tunnel (Ports 22, 25, 53, 80, 443 und 4766 werden nacheinander versucht) mit einer Verzögerung von 5 Minuten zwischen jedem Versuch einzurichten. Die VA bleibt in diesem Zustand, bis eine Verbindung hergestellt ist oder 30 Minuten ohne erfolgreiche Verbindung verstrichen sind.

Die Verbindung kann aufgrund von Netzwerkproblemen (z. B. blockierte Ports) fehlschlagen.

Zeitüberschreitung

Wenn die VA keine Verbindung mit dem Remote-Server herstellen kann, wird der Status auf "Time out" (Zeitüberschreitung) gesetzt. Die Zeitüberschreitung tritt etwa 30 Minuten nach dem Versuch der VA auf, einen Tunnel mit dem Remote-Server einzurichten.

Tunnelpersistenz

Sobald ein Support-Tunnel aktiviert ist, entspricht die VA dem eingegebenen Wert für die Dauer, selbst wenn die VA neu gestartet oder aktualisiert wird. Sie müssen keine weiteren Aktionen durchführen. Wenn die VA neu startet oder aktualisiert wird und die Zeit immer noch die angegebene Zeit beträgt, versucht die VA automatisch, erneut eine Verbindung zum SSH-Tunnelserver herzustellen.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.