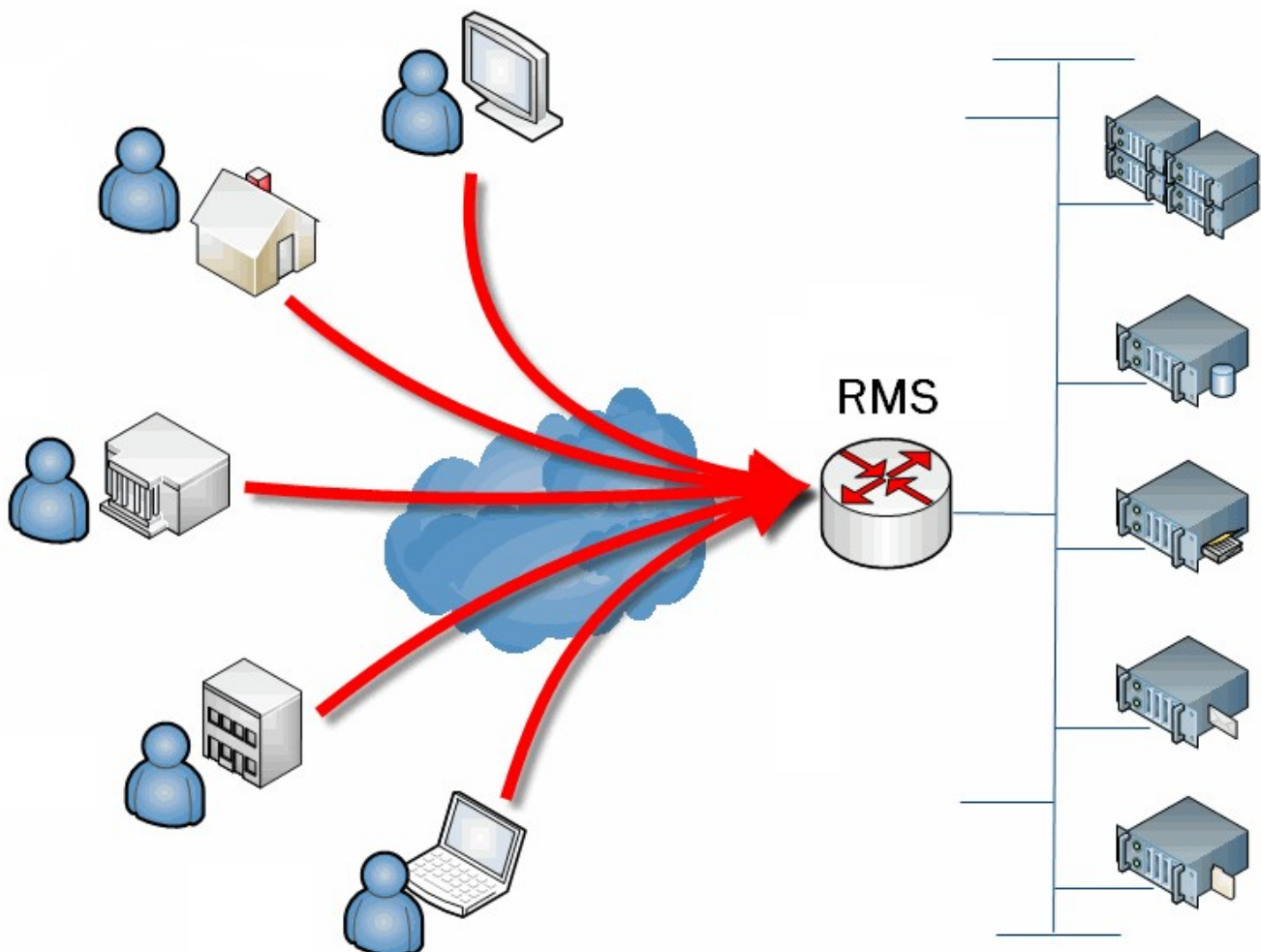


Felhasználói kézikönyv Az RMS VPN szerverként történő alkalmazásáról



Az RMS mint VPN szerver

Az RMS-M-2000-es sorozat VPN szerver funkciója biztosítja az RMS Ethernet portjára csatlakoztatott helyi hálózaton elérhető egyéb eszközök távoli elérését adatkapcsolati szinten, így – többek között – lehetőséget nyújt arra is, hogy elérjük az egyes eszközök telenet, SSH és webes felületét. Ezen felül – mivel a kapcsolat layer 2 szinten valósul meg, – a kliens igénybe veheti RMS hálózatában lévő DHCP szerver szolgáltatásait is.

A VPN kapcsolat megvalósítása

1. RMS oldali beállítások

A VPN szolgáltatás beállítása és engedélyezése:

1. Administrator Menu
6. Communication Settings
8. OpenVPN Server
 1. Protocol <TCP> - a kommunikációs protokoll beállítása
 2. Port <1194> - a port beállítása (alapértelmezés: 1194)
 6. Automatic IP Addressing <...> - az RMS automatikus IP cím osztás funkciója engedélyezhető arra az esetre, ha a kliensnek nem az RMS helyi hálózatában lévő DHCP szerver oszt IP címet

Amennyiben az automatikus IP cím osztás engedélyezésre került, a 7-9. menüpontokban megadhatóak a kiosztandó tartomány paraméterei:

7. Start IP Address <...> - a tartomány kezdő címe
8. End IP Address <...> - a tartomány utolsó címe
9. Netmask <...> - hálózati maszk
- E. Access <Enabled>

Mivel az autentikáció az RMS-ben regisztrált felhasználónév-jelszó párossal történik, a felhasználóhoz megfelelő jogosultságot szükséges rendelni:

1. Administrator Menu
4. Security Settings
 1. User Settings
 1. Users
 - 1...W. User {...}
 9. Access Rights
 5. VPN Access: <Enabled>

2. OpenVPN kliens alkalmazás telepítése

Amennyiben operációs rendszere nem rendelkezik OpenVPN kliens alkalmazással, töltsse le, majd telepítse a megfelelő programcsomagot például az openvpn.net honlapról.

Ha az első RMS VPN kapcsolatot építi fel, akkor az adott RMS SFTP felületéről mentse le számítógépére a CA tanúsítványt (/vpn/ca.cert). Ez a fájl minden RMS-hez érvényes.

A VPN kapcsolat létrehozásához szükséges paramétereket lehet közvetlenül, vagy konfigurációs fájlon keresztül átadni az OpenVPN kliensnek. Ez az adott szoftvertől függően történhet parancssorban, vagy grafikus felületen.

```
openvpn --client --dev tap --remote my_rms --proto tcp-client --port 1194 --ca ca.cert --auth-user-pass
```

```
openvpn --config rms.ovpn
```

Az OpenVPN kliens alap beállításait az alább megtekinthető konfigurációs fájl mintában mutatjuk be. A paraméterezéssel kapcsolatos további, részletes leírás az [OpenVPN kézikönyvekben](#) olvasható.

```
#####  
# Kliens oldali OpenVPN konfigurációs fájl minta RMS-ek eléréséhez. #  
#####  
  
# A kliens szerepkör meghatározása  
client  
  
# A TUN/TAP interfész definiálása  
# Mivel az RMS VPN elérése layer 2 szinten történik, TAP beállítása szükséges  
dev tap  
  
# A protokoll meghatározása  
# Használja az RMS-ben megadott beállítást  
proto tcp  
;proto udp  
  
# Az RMS hosztnevének /IP címének, illetve portjának megadása  
remote my_rms 1194  
  
# Az RMS-ek eléréshez szükséges CA tanúsítvány megadása  
# Ha a fájl nem a helyi könyvtárban található, szükséges az elérési út definiálása is  
ca ca.cert  
  
# Az autentikáció módjának megadása  
# Az RMS-ben regisztrált és megfelelő jogosultsággal rendelkező felhasználók  
# a jelszavuk megadásával autentikálhatnak  
auth-user-pass  
  
#####  
# Opcionális paraméterek #  
#####  
  
# Névvoldás beállítása  
# A rendszer folyamatosan próbálkozik az OpenVPN szerver hosztnevének oldásával  
# Állandó internet kapcsolattal nem rendelkező számítógépek esetén javasolt  
resolv-retry infinite  
  
# A bind funkció tiltása  
# A legtöbb kliens nem igényel egyedi port hozzárendelést  
nobind  
  
# Bizonyos beállítások megtartása a VPN kapcsolat újraindulása során  
persist-key  
persist-tun  
  
# HTTP proxy szerver beállítások  
;http-proxy-retry  
;http-proxy [proxy server] [proxy port #]  
  
# Duplikált csomagok tiltása  
# Vezeték nélküli hálózatok gyakran állítanak elő duplikált csomagokat  
# A flag beállításával letilthatóak az erre vonatkozó figyelmeztetések  
;mute-replay-warnings  
  
# A log fájlok „bőbeszédűségének” beállítása  
verb 3  
  
# Ugyanabba a kategóriába tartozó, ismétlődő üzenetek számának maximalizálása  
;mute 20
```